AN INTELLIGENT CRYPTO-LOCKER RANSOMWARE DETECTION TECHNIQUE USING SUPPORT VECTOR MACHINE CLASSIFICATION AND GREY WOLF OPTIMIZATION ALGORITHMS

By

ABDULLAHI MOHAMMED MAIGIDA * SHAFI'I MUHAMMAD ABDULHAMID **
MORUFU OLALERE *** IDRIS ISMAILA ****

*-**-***-**** *Department of Cyber Security Science, Federal University of Technology Minna, Nigeria.*

Date Received: -/-/- *Date Revised: -/-/-* *Date Accepted: -/-/-*

ABSTRACT

Ransomware is advanced malicious software which comes in the forms of different forms, with the intention to attack and take control of basic infrastructures and computer systems. The majority of these threats are meant to extort money from their victims by asking for a ransom in exchange for decryption keys. Most of the techniques deployed to detect this could not completely prevent ransomware attacks because of its obfuscation techniques. In this research work, an intelligent crypto-locker ransomware detection technique using Support Vector Machine (SVM) and Grey Wolf Optimization (GWO) algorithm is proposed to overcome the malware obfuscation technique because of its ability to learn, train and fit dataset based on the observed features. The proposed technique has shown remarkable prospects in detecting crypto-locker ransomware attacks with high true positive and low false positive rate.

Keywords: Support Vector Machine, Greywolf Optimization, Ransomware, Crypto-locker, Malware.

INTRODUCTION

Ransomware is a special kind of malicious software that capitalized on system vulnerability to lock a computer system and encrypt data using various encryption scheme to prevent access to the infected system until ransom is paid for the decryption key (Richardson & North, 2017). Malware developer considered the massive usage of information technology system in the management and running of the world affairs to make the end users suffer in a very massive scale. The hackers direct the malware code to attack the information system using the internet via the browser exploit kits, attached email and other available vulnerabilities in order to take control of the entire systems (Bhardwaj, Avasthi, Sastry, & Subrahmanyam, 2016). Figure 1 explains the stages of ransomware attack.

Crypto-locker ransomware is the most advance types of ransomware attack that perform dual functions of encrypting system files and locking the system screen with a ransom note, requesting for payment in exchange for decryption key (Savage, Coogan, & Lau, 2015). There are five distinct phases of a ransomware attack, regardless of whether it's a mass distribution or a targeted attack (Brewer, 2016). The Exploitation and Infection phase, this is where the malware use phishing and pharming of email and exploit kit to execute files on the computer system. Delivery and Execution phase, is where the crypto-locker executables are delivered to the target system. Back-up spoliation is the phase where the malware remove the back-up files and folders to avoid system restore. File Encryption and the final phase which is the User Notification and clean-up, this is where ransom note are displayed and back-up files removed from the system.

Support Vector Machine (SVM) is a type of classification algorithm that is designed to adapt to a range of various classification problems with ability to implicitly perform a non-linear feature space transform (Boswell, 2002). In recent times, application of SVMs in classification problems has increased because of its capability to segregate datasets using the best hyperplane. SVMs have been applied in multidimensional data classification,

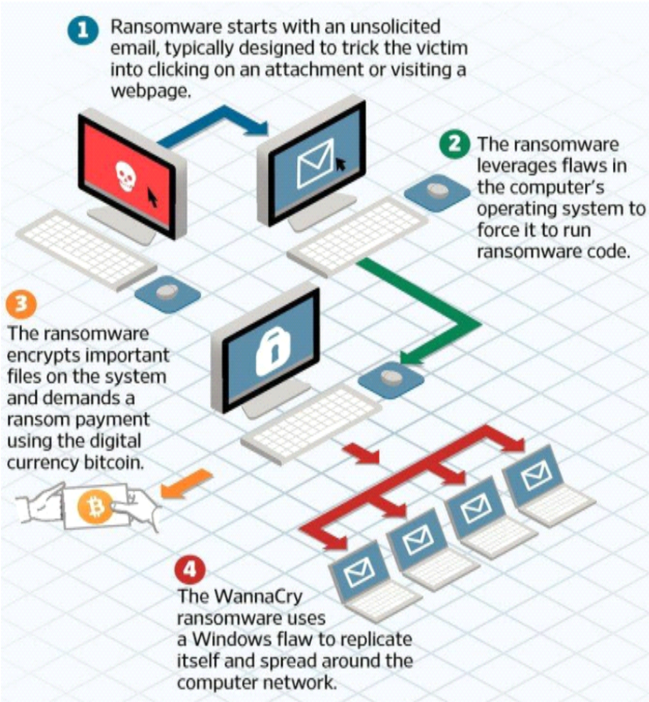

Figure 1. Stages of Ransomware attack (The Business Times, 2017)

classification of microarrays, wind speed prediction, voltage stability monitoring, classification of power quality events, and contingency ranking (Boswell, 2002).

Grey Wolf Optimizer (GWO) is one of the Meta-heuristic optimization techniques whose designed concepts was inspired by the social hierarchy and hunting behaviour of a grey wolves. Grey wolves have been considered as the apex predator with a high social dominant hierarchy because of their natural hunting patterns which comprises of tracking, encircling and attacking of prey (Mirjalili, Mirjalili, & Lewis, 2014).

This research work hereby proposed an intelligent crypto-locker ransomware attack detection using GWO algorithm for feature selection so as to improve the performance of SVM classifier for better results.

The sections of the manuscript are structured as follows: Section II presents a detailed analysis of previous related literature. Section III details the proposed SVM-GWO detection framework whereas Section IV throw light on the dataset and experimental setup; Section V put up a comprehensive results and discussion before concluding part of the paper in Section VI.

1. Related Works

In recent times, studies have been carried out on the detection of ransomware attack. (Brewer, 2016; Boswell, 2002; Mirjalili et al., 2014; Weckstén, Frick, Sjöström, & Järpe, 2016) mostly proposed a signature-based approach which relies on the malware information stored in the repository for detection. The drawback of this technique is the inability to detect ransomware whose signature are yet to be stored in the malware repository. (Savage et al., 2015; Continella et al., 2016; Patyal, Sampalli, Ye, & Rahman, 2017; Kolodenker, Koch, Stringhini, & Egele, 2017; Al-rimy & Maarof, 2018; Cabaj, Gregorczyk, & Mazurczyk, 2015; Yang, Yang, Qian, Lo, Qian, & Tao, 2015; Moore, 2016; Kiraz, Genç, & Öztürk, 2017; Sgandurra, Muñoz-González, Mohsen, & Lupu, 2016; Shaukat & Ribeiro, 2018; Ferrante, Malek, Martinelli, Mercaldo, & Milosevic, 2017; Scaife, Carter, Traynor, & Butler, 2016) focused on improving the signature-based approach by designing a behavioural-based system with different detection mechanisms and classifier to perform live monitoring of window and android event logs in real-time to detect ransomware attack. The limitation of this system is the inability to stand the malware sophisticated packing techniques (obfuscation) and created system noise which resulted in misclassification of the crypto-locker and benign applications with high false positive and error rate.

After intensive exploration of the research on ransomware detection approaches, users still find themselves vulnerable to crypto-locker ransomware attacks (Ahmadian & Shahriari, 2016; Hong, Liu, Ren, & Chen, 2017; Kharraz, Arshad, Mulliner, Robertson, & Kirda, 2016; Kharraz & Kirda, 2017). This indicators call for further improvement in the current detection techniques or build another with a unique characteristics that will match crypto-locker ransomware method of attack.

To overcome the noticeable drawback of the existing techniques, we proposed an intelligent crypto-locker ransomware detection technique with GWO algorithm for feature selection of the extracted features from crypto-locker and benign application datasets, to enhance the performance of SVM classifier for better accuracy with low false positive rate.

The key contributions in this research manuscript include:

- To propose an intelligent crypto-locker ransomware feature selection algorithm with GWO.
- To developed a crypto-locker ransomware classification technique using SVM and GWO algorithms.
- To evaluate the developed intelligent crypto-locker ransomware detection technique using standard parameters utilize in relevant literatures.

2. Proposed SVM-GWO Detection Framework

The proposed framework of SVM-GWO crypto-locker ransomware detection consists of features selection, extraction and classification as shown in Figure 2.

2.1 Mathematical Model of SVM

Given a training dataset sample l such that {xi, yi}, i = 1, . . . , l, such that each sample with d inputs (xi ϵ Rd), with a class label with one or two values (yi ϵ {-1, 1}).

2.1.1 Linearly Classifier

This follows all the hyperplanes in Rd which was parameterized with a vector (w), constant (b), and expressed

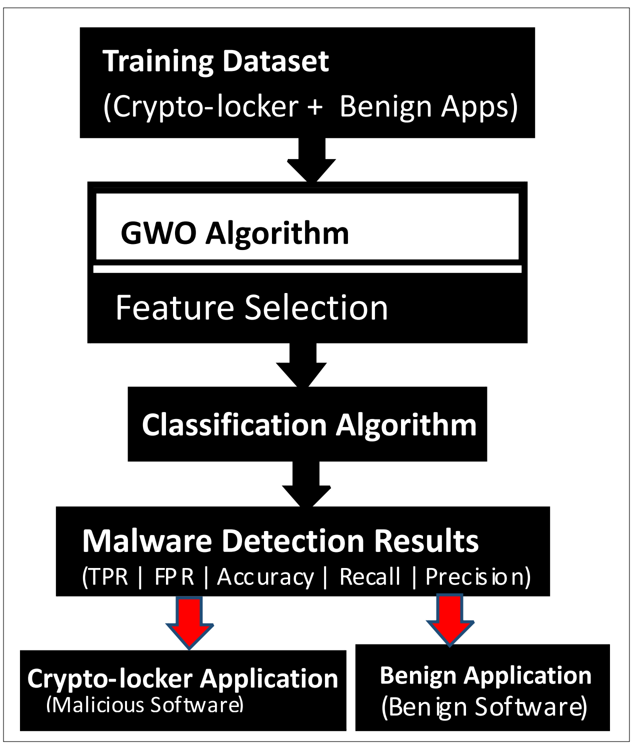

Figure 2. Proposed SVM-GWO detection framework

as:

$$w \,.\, x + b = 0 \quad (1)$$

(We can recall that vector w is orthogonal to the hyperplane.) Given such hyperplane (w, b) which separates the data and gives the function as:

1) Perception Classifier

$$f(x) = \text{sign}\,(w \,.\, x + b) \quad (2)$$

This equation perfectly classified the training data and possibly other unknown dataset. Meanwhile, a given hyperplane which was denoted by (w,b) is similarly expressed by all pairs {λw, λb} for λ ϵ R+. This means that we

can now define the canonical hyperplane to be that which separates the data from the hyperplane by a "distance" of at least 1 which satisfy:

$$x_i \,.\, w + b \geq +1 \text{ when } y_i = +1 \quad (3)$$

$$x_i \,.\, w + b \leq -1 \text{ when } y_i = -1 \quad (4)$$

to make it more compressed, we say:

$$y_i(x_i \,.\, w_i + b) \geq 1 \qquad I_i \quad (5)$$

All such kind of hyperplanes have a "functional distance" ≥ 1 (which exactly means, the Function's value is ≥ 1). It shouldn't be muddled with the "geometric" or "Euclidean distance" (known as the margin). For any given hyperplane *(w, b)*, all pairs *{λw, λb}* define the same hyperplane, but with a different functional distance to a given data point. For us to find the geometric distance from the hyperplane to a data point, we have to regularize the magnitude of w which will define the distance as:

$$d((w,b),x_i) = \frac{y_i(x_i.w+b)}{\|w\|} \geq \frac{1}{\|w\|} \quad (6)$$

$$d((w,b),x_i) = \frac{y_i(x_i.w+b)}{\|w\|} \geq \frac{1}{\|w\|}$$

Relating to the equation, we can see that this is accomplished by minimizing $||\, w \,||$ which is subject to the distance constrains. The entire problem is ultimately transformed into:

minimize: $W(\alpha) = -\sum l_i = 1\ \alpha_i + \frac{1}{2} \sum l_i = 1 \sum l_{j=1}\ y_i y_j\ \alpha_i \alpha_j (x_i \,.\, x_j)$

Subject to: $\sum l_i = 1\ y_i \alpha_i = 0$

$0 \leq \alpha_i \leq C\,(l_i)$

Where α is the vector of l non-negative Lagrange multiplers to be determine, and C is a constant. The matrix can define:

$(H)ij = yiyj(xixj)$, which will present more compact notation:

Minimize: $W(\alpha) = -\alpha T1 + 1/2\, \alpha T H\alpha$ (7)

Subject to: $\alpha Ty = 0$ (8)

$0 \leq \alpha \leq C1$ (9)

from the derivation of these equations, hyperplane becomes

$$w = \sum \alpha i\, yixi \quad (10)$$

Meaning that vector w is a linear combination of the training examples shown as:

$$\alpha i\,(yi\,(w\,.\,xi + b) - 1) = 0 \quad (Ii)$$

That is to say, that the functional distance of an example is higher than 1 when $yi(xi\ .\ wi + b) > 1$, then $\alpha i = 0$. Which means that only the nearest data points contribute to w. the training example $\alpha i > 0$ are referred to as support vector. This is the only one required to define optimal hyperplane.

If we have optimal α (where we construct w), we have to find to fully specified the hyperplane. To implement this, let take any "positive" and "negative" support vector, x+ and x-, for which we know

$(w\,.\,x+ + b) = +1$

$(w\,.\,x- + b) = -1$

To solve these equations gives us

$B = -1/2(w\,.\,x+ + w\,.\,x-)$ (11)

Based on the analysis presented above, any app in the dataset that tend to possess some characteristic of a violator is made a Support Vector (SV). Blocking points will be identify and pruned using the ideas presented in the equation. The algorithm stops when all points are classified within an error bound plane, for instance, $yi\ f(xi) > 1 - \varepsilon\ V$. The outline of the algorithm is presented in Figure 3.

A. Mathematical Model of GWO algorithm

1) Encircling prey

Considering the analysis carried out, the grey wolves encircle prey during the hunting period which has been mathematically model in the following equations as

Algorithm :1 Simple SVM

```
candidateSV = { closest pair from opposite classes }
while there are violating points do
        Find a violator
        candidateSV = ∪ candidateSV
                  S
        violator
        if any αp < 0 due to addition of c to S then
                  candidateSV = candidateSV \ p
                  repeat till all such points are pruned
        end if
end while
```

Figure 3. Pseudocode for SVM Classifier

$$\vec{D} = |\vec{C}.X_p(t) - \vec{X}(t)| \quad 7$$

$$\vec{D} = |\vec{C}.X_p(t) - \vec{X}(t)|$$

$$\vec{X}(t+1) = \vec{X}_p(t) - \vec{A}.\vec{D} \quad 8$$

$$\vec{X}(t+1) = \vec{X}_p(t) - \vec{A}.\vec{D}$$

Where t refers to the current iteration, $\vec{A}$ and $\vec{C}$ are coefficient vectors, $\vec{X}_p$ while defines the position vector of the prey, and $\vec{X}$ specifies the position vector of a grey wolf. The vectors A and $\vec{C}$ are formulated as follows

$$\vec{A} = 2\vec{a}.\vec{r} - \vec{a}$$

$$\vec{C} = 2.\vec{r}_2$$

At this point, components of $\vec{a}$ linearly decreased from 2 to 0 over the course of the iterations while r1 and r2 are random vectors in [0, 1] coordinates.

1) Hunting:

The hunting style of a Grey-wolf is usually conducted by the alpha, but the beta and delta may also participate in hunting sometimes. More so, in an abstract search space we have no idea about the location of the prey. To mathematically simulate the hunting behavior of grey wolves, we assume that the alpha, beta, and delta have better information of the targeted location of a prey. Therefore, we save the first three best solutions gotten already and oblige the other search agents (including the omegas) to update their positions according to the position of the best search agent whose formula is presented below.

$$\vec{D}_{\alpha} = |\vec{C}_1.\vec{X}_{\alpha}-\vec{X}|,\ \vec{D}_{\beta}=|\vec{C}.\vec{X}_{\beta}-\vec{X}|,\ \vec{D}_{\delta}=|\vec{C}_3.\vec{X}_{\delta}-\vec{X}| \quad 11$$

$$\vec{X}_1=\vec{X}_{\alpha}-\vec{A}_1.(\vec{D}_{\alpha}),\ \vec{X}_2=\vec{X}_{\beta}-\vec{A}_2.(\vec{D}_{\beta}),\ \vec{X}_3=\vec{X}_{\delta}-\vec{A}_3.(\vec{D}_{\delta}) \quad 12$$

$$\frac{\vec{X}_1+\vec{X}_2+\vec{X}_3}{3}$$

$$\frac{\vec{X}_1+\vec{X}_2+\vec{X}_3}{3}$$

1) Attacking prey (exploitation):

Finally, the grey wolves' conclude the hunting exercise by attacking the prey after the movement has stopped. In order to mathematically model the grey wolf approaching the prey, we decrease the value of $\vec{a}$. while, the variation range of $\vec{A}$ is also decreased by $\vec{a}$; meaning that, $\vec{A}$ is a random value in the interval [-2a, 2a] where a is decreased from 2 to 0 over the course of iterations, the random values of $\vec{A}$ are in [-1,1], and next position of a search agent can be in any position between its present position and the position of the prey which will finally leads to the attack on the prey as shown in Figure 4.

2. Dataset and Experimental Setup

The crypto-locker ransomware and benign applications datasets was gotten from (Sgandurra et al., 2016) research work, titled "Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection". The dataset contains 582 samples (38.19%) of crypto-locker ransomware and 942 (61.81%) of benign applications making a total of 1524 samples from 11 different families. GWO is employed to evaluates the following categories of features found in crypto-locker and benign application datasets. Crypto-locker extracted features includes: (i) Windows API calls (ii) Registry Key Operations (iii) File System Operations (iv) the set of file operations performed per File Extension, (v) Directory Operations (vi) Dropped Files and (vii) Strings contain in the binary.

The benign application features includes: (i) generic utilities for Windows (ii) drivers (iii) popular browsers (iv) file utilities (v) multimedia tools (vi) developers tools (vii) games (viii) network utilities (ix) paint tools (x) databases (xi) emulator and virtual machines monitors and office tools.

```
Algorithm 2: Simple GWO

Initialize the grey wolf population Xi (i = 1, 2, ..., n)
Initialize a, A, and C
Calculate the fitness of each search agent
Xα=the best search agent
Xβ=the second best search agent
Xδ=the third best search agent
while (t < Max number of iterations)
        for each search agent
                Update the position of the current
                search agent by equation (7)
        end for
        Update a, A, and C
        Calculate the fitness of all search agents
        Update Xα, Xβ, and Xδ
        t=t+1
end while
return Xα
```

Figure 4. Pseudocode of the GWO

GWO does the feature selection using the Mutual Information (MI) criterion which allows the algorithm to select the most discriminating features extracted from crypto-locker and benign application datasets to improve SVM classification problem with better performance.

The experiment on the classification of Crypto-locker datasets was implemented using SVM classification scheme together with GWO optimization algorithm on standard simulation platforms. The GWO algorithm (java source code) was uploaded on the simulation platform to perform feature selection of the dataset and output fed into SVM classifier for classification of the dataset into crypto-locker and benign applications.

3. Results and Discussion

Table 1. shows the family of the crypto-locker ransomware with their identifiable codes as contain in Sgandurra dataset.

The Table 2. gives full details of the descriptive features of the Sgandurra ransomware dataset with their respective codes and attributes types to aid the classification experiment.

The performance evaluation of Support Vector Machine after feature extraction and selection with Grey-Wolf Optimization algorithm using different percentage split on 10-folds cross validation.

The Table 3 summarized the results obtained in Table 3 to calculate the average, minimum, maximum, variance and standard deviation for the performance metrics of the test carried out.

The performance evaluation of the SVM and GWO accuracy is used to show level of perfection with regards to the correctly classified crypto-locker ransomware as against the benign app. The highest level of accuracy is considered to be 100. The experimental test result obtained after using different percentage split values of the crypto-locker dataset with constant 10-folds cross validation is shown in Figure 5.

$$Accuracy\ (\mathrm{A}) = \frac{TP + TN}{TP + FP + FN + TN} \times 100\% \qquad 13$$

S/N	Family Name	ID Nos.
	Goodware Application	0
1	Critroni	1
2	CryptLocker	2
3	Crypto-Wall	3
4	KOLLAH	4
5	Kovter	5
6	Locker	6
7	MATSNU	7
8	PGCODER	8
9	Reveton	8
10	TeslaCrypt	10
11	Trojan-Ransom	11

Table 1. Families of Sgandurra Crypto-locker Ransomware Dataset

ID	Description	Attribute	No. of Attributes
API	API invocations	Nominal	8
DROP	Extension of the drop files	Nominal	5
REG	Registry key operations	Nominal	20
FILES	File operations	Nominal	20
FILES_EXT	Extension of the files involved in file operations	Nominal	20
DIR	File directory operations	Nominal	10
STR	Embedded string	Nominal	5
	Total number of attributes		88

Table 2. Sgandurra Dataset Id Terms with Descriptive Features

Parameters	Average	Min	Max	Variance	STD
Accuracy	99.167	98.361	99.672	0.157095	0.396352
Precision	0.983	0.967	0.993	0.000062	0.007875
Recall	0.992	0.984	0.997	0.000015	0.003919
F-measure	0.987	0.975	0.995	0.000035	0.005936
RMSE	0.01534	0.0029	0.0573	0.000276	0.016618

Table 3. SVM With GWO Classification Result

$$Accuracy\ (\mathrm{A}) = \frac{TP + TN}{TP + FP + FN + TN} \times 100\%$$

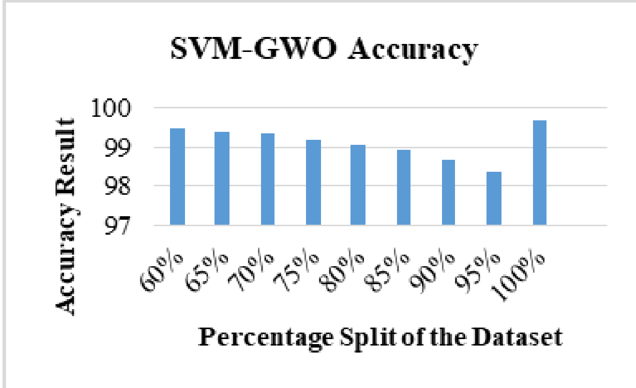

Figure 5. Performance evaluation of SVM accuracy at percentage split of the datasets

The RMSE is one of the parameters used to indicate the levels of the classifier perfection during and after the experiment. The lower the values of RMSE the better the classifier predictions. This means that value zero gives the perfect result while a higher value indicate a poor performance of the classifier. The result below shows the gradual decline of error as the percentage split of the dataset increases. Figure 6 shows various results of other performance metric from the SVM classifier as against each percentage split of the crypto-locker datasets.

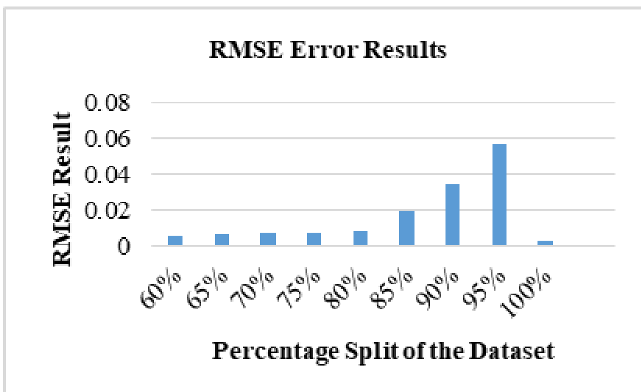

Figure 6. RMSE results against percentage split of the datasets

Precision (P) indicates the number of instances which are positively classified and are relevant. A high precision shows high relevant in detecting positives.

$$P = \frac{TP}{TP + FP} \times \frac{100}{1}$$

$$P = \frac{TP}{TP + FP} \times \frac{100}{1}$$

Recall (R) shows how well a system can detect positives

$$R = \frac{TP}{TP + FN} \times \frac{100}{1} \quad 15$$

$$R = \frac{TP}{TP + FN} \times \frac{100}{1}$$

F-Measure = 2 x Precision * Recall /Precision + Recall (16)

TPR and FPR True Positive Rate and False Positive Rate was calculate based on the true overall number of benign and ransomware processes after about 10 fold of cross-validation using different percentage split

$$TPR = \frac{TP}{TP + FP} \times \frac{100}{1}$$

$$TPR = \frac{TP}{TP + FP} \times \frac{100}{1}$$

$$FPR = \frac{FP}{TP + FP} x \frac{100}{1}$$

The Table 4 shows results of each performance metric obtained at different levels of the percentage split of the crypto-locker dataset using a fixed 10-folds cross validation. The results obtained show the highest level of accuracy and perfection over other detection techniques proposed. This is an indication of superiority of a machine learned behavioral detection techniques against crypto-locker ransomware attacks.

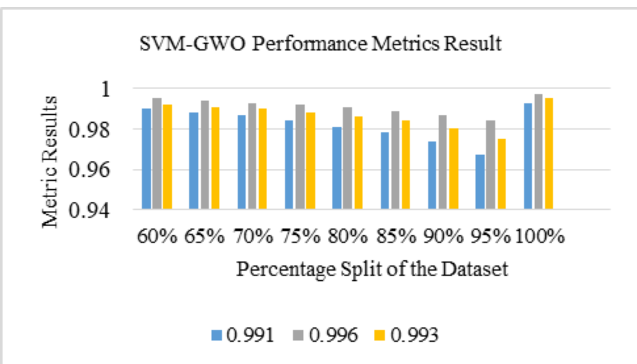

Figure 7. Performance Metrics of other Parameters

Performance Result Comparison

Table 5 and Figure 8 shows the comparative analysis and comparison of the accuracy result of our proposed system (SVM with GWO) against other related works.

Conclusion and Recommendation

Ransomware has become a significant problem to a growing number of individuals, communities, organizations and companies. The actors are beginning to consume each other; which is a sign of adverse rivalry among ransomware mobs. The geography statistics show that attackers will shift to the previously unreached countries, where users are not as well prepared for fighting ransomware, and where competition among criminals is not so high, if this eventually happens, the consequence will be devastating.

Several detecting techniques have been proposed ranging from a static-based approach which depends heavily on the store signature in malware repository, but could not detect unknown ransomware whose signature are yet to be store in the malware repository. The behavioural-based approach which monitor the system logs and actions on the stored files in real time could not stand the malware obfuscation techniques which result into generated system noise from the detection mechanism.

Therefore, the proposed intelligent crypto-locker ransomware detection technique using SVM classification and GWO algorithm is a machine learned behavioral-based approach that has the ability to learn, train and fit crypto-locker applications, extract some behavioral trait to improve the classification and prediction result.

The experiment was performed on a standard simulation platform where GWO optimized and select the extracted features to improve SVM classifier for better result. The test was carried out using 10-folds cross validation with

Parameters	55%	60%	65%	70%	75%	80%	85%	90%	95%	100%
Accuracy	99.563	99.495	99.405	99.342	99.180	99.065	98.901	98.684	98.361	99.672
Precision	0.991	0.990	0.988	0.987	0.984	0.981	0.978	0.974	0.967	0.993
Recall	0.996	0.995	0.994	0.993	0.992	0.991	0.989	0.987	0.984	0.997
F - measure	0.993	0.992	0.991	0.990	0.988	0.986	0.984	0.980	0.975	0.995
SE	0.0049	0.0054	0.0063	0.0069	0.0074	0.0083	0.0199	0.0341	0.0573	0.0029

Table 4. SVM Classification On Sgandurra Crypto-locker Datasets Using Different Percentage Split On 10-folds Cross Validation

Author	System/Classifier	Accuracy
Cabaj and Gregorczyk (2016)	SDN-based system.	97.23%
Sgandurra and González (2016)	Elderan Classifier	96.34%
Ahmadian and Shahriari (2016)	2entFOX and Bayesian Classifier	93.33%
Kharraz and Arshad (2016)	UNVEIL System	96.33%
Continella and Guagnelli (2016)	SheildFS System	97.70%
Shaukat and Ribeiro, (2018)	GTB Algorithm Classifier	98.25%
SVM + GWO, (2018)	SVM + GWO	99.18%

Table 5. Accuracy Result Comparison

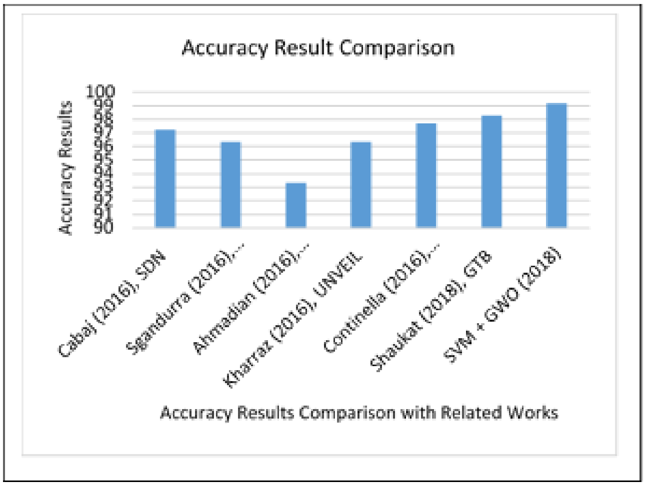

Figure 8. Performance Metrics of other Parameters

percentage split of the dataset and obtained 99.18% accuracy on the average. The result comparison from SVM with GWO algorithm has outperformed other related detection techniques in term of accuracy.

References

[1]. **Richardson, R., & North, M. (2017).** Ransomware: Evolution, mitigation and prevention. *International Management Review,* 13(1), 10-21.

[2]. **Bhardwaj, A., Avasthi, V., Sastry, H., & Subrahmanyam, G. V. B. (2016).** Ransomware digital extortion: a rising new age threat. *Indian Journal of Science and Technology*, 9(14), 1-5.

[3]. **The Business Times. (2017).** How Ransomware Works. New York City, Retrieved from https://www.businesstimes.com.sg/infographics/how-ransomware-works

[4]. **Savage, K., Coogan, P., & Lau, H. (2015).** The Evolution of Ransomware, Secur. Response, p. 57.

[5]. **Brewer, R. (2016).** Ransomware attacks: detection, prevention and cure. *Network Security*, 2016(9), 5-9.

[6]. **Boswell, D. (2002).** Introduction to Support Vector Machines, Svm, pp. 1–15.

[7]. **Mirjalili, S., Mirjalili, S. M., & Lewis, A. (2014).** Grey wolf optimizer. *Advances in engineering software*, 69, 46-61.

[8]. **Weckstén, M., Frick, J., Sjöström, A., & Järpe, E. (2016).** A novel method for recovery from Crypto Ransomware infections. *In Computer and Communications (ICCC), 2016 2nd IEEE International Conference on* (pp. 1354-1358). IEEE.

[9]. **Continella, A., Guagnelli, A., Zingaro, G., De Pasquale, G., Barenghi, A., Zanero, S., & Maggi, F. (2016).** ShieldFS: a self-healing, ransomware-aware filesystem. *In Proceedings of the 32nd Annual Conference on Computer Security Applications* (pp. 336-347). ACM.

[10]. **Patyal, M., Sampalli, S., Ye, Q., & Rahman, M. (2017).** Multi-layered defense architecture against ransomware. *International Journal of Business and Cyber Security,* 1(2). 52–64.

[11]. **Kolodenker, E., Koch, W., Stringhini, G., & Egele, M. (2017).** PayBreak: defense against cryptographic ransomware. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (pp. 599-611). ACM.

[12]. **Al-rimy, B. A. S., & Maarof, M. A. (2018).** Recent Trends in Information and Communication Technology, 5.

[13]. **Cabaj, K., Gregorczyk, M., & Mazurczyk, W. (2015).** Software-Defined Networking-based Crypto Ransomware Detection Using HTTP Traffic Characteristics, *In Computers & Electrical Engineering.*

[14]. **Yang, T., Yang, Y., Qian, K., Lo, D. C. T., Qian, Y., & Tao, L. (2015).** Automated detection and analysis for android ransomware. In High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conferen on Embedded Software and Systems (ICESS), 2015 IEEE 17th International Conference on (pp. 1338-1343). IEEE.

[15]. **Moore, C. (2016).** Detecting ransomware with honeypot techniques. In Cybersecurity and Cyberforensics Conference (CCC), 2016 (pp. 77-81). IEEE.

[16]. **Kiraz, M. S., Genç, Z. A., & Öztürk, E. (2017).** Detecting

Large Integer Arithmetic for Defense Against Crypto Ransomware. Cryptology ePrint Archive, Report 2017/558.(2017). http://eprint. iacr. org/2017/558.

[17]. Sgandurra, D., Muñoz-González, L., Mohsen, R., & Lupu, E. C. (2016). Automated dynamic analysis of ransomware: Benefits, limitations and use for detection. arXiv preprint arXiv:1609.03020.

[18]. Shaukat, S. K., & Ribeiro, V. J. (2018). RansomWall: A layered defense system against cryptographic ransomware attacks using machine learning. In Communication Systems & Networks (COMSNETS), 2018 10th International Conference on (pp. 356-363). IEEE.

[19]. Ferrante, A., Malek, M., Martinelli, F., Mercaldo, F., & Milosevic, J. (2017). Extinguishing Ransomware-a Hybrid Approach to Android Ransomware Detection. In International Symposium on Foundations and Practice of Security (pp. 242-258). Springer, Cham.

[19]. Scaife, N., Carter, H., Traynor, P., & Butler, K. R. (2016). Cryptolock (and drop it): stopping ransomware attacks on user data. In Distributed Computing Systems (ICDCS), 2016 IEEE 36th International Conference on (pp. 303-312). IEEE.

[20]. Ahmadian, M. M., & Shahriari, H. R. (2016). 2entFOX: A framework for high survivable ransomwares detection. In Information Security and Cryptology (ISCISC), 2016 13th International Iranian Society of Cryptology Conference on (pp. 79-84). IEEE.

[21]. Hong, S., Liu, C., Ren, B., & Chen, J. (2017). Poster: Sdguard: An Android Application Implementing Privacy Protection and Ransomware Detection. In Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services (pp. 149-149). ACM.

[22]. Kharraz, A., Arshad, S., Mulliner, C., Robertson, W. K., & Kirda, E. (2016). UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware. In USENIX Security Symposium (pp. 757-772).

[23]. Kharraz, A., & Kirda, E. (2017). Redemption: real-time protection against ransomware at end-hosts. In International Symposium on Research in Attacks, Intrusions, and Defenses (pp. 98-119). Springer, Cham.

ABOUT THE AUTHORS

Abdullahi Mohammed Maigida is a staff of Ibrahim Badamasi Babangida University, Lapai, Nigeria. He obtained his first degree in 2004 from the Departmentof Electrical and Computer Engineering, Federal University of Technology Minna, Nigeria. He also received his MSc from the Department of Cyber Security Science in Federal University of Technology Minna, Nigeria. He is a certified member of Nigerian Society of Engineer (NSE), The Council for the Regulation of Engineering in Nigeria (COREN), Cyber Security Experts Association of Nigeria (CSEAN). His current research interests are on Malware Attack Detection.

Shafi'i Muhammad Abdulhamid received his PhD in Computer Science from University of Technology Malaysia (UTM), MSc in Computer Science from Bayero University Kano (BUK), Nigeria and a Bachelor of Technology in Mathematics with Computer Science from the Federal University of Technology (FUT) Minna, Nigeria. His current research interests are in Cyber Security, Cloud Computing, Soft Computing, Internet of Things Security, Malware Detection and Big Data. He has published many academic papers in reputable International journals, conference proceedings and book chapters. He has been appointed as an Editorial board member for Big Data and Cloud Innovation (BDCI) and Journal of Computer Science and Information Technology (JCSIT). He has also been appointed as a reviewer of several ISI and Scopus indexed International journals. He has also served as Program Committee (PC) member in many National and International Conferences.

Morufu Olalere is currently working as a lecturer in the Department of Cyber Security Science, Federal University of Technology Minna, Niger, Nigeria. He graduated in 2005 from the Department of Industrial Mathematics and Computer Science of the Federal University of Technology Akure, Nigeria with Bachelor of Technology in Industrial Mathematics. He bagged MSc in Computer science from the University of Ilorin, Kwara State, Nigeria in 2011. He completed his PhD in Security in computing in 2016 from the Faculty of Computer Science and Information Technology of the University Putra Malaysia, Selangor, Malaysia. He has a number of professional certifications including OCH, CWSA and CWSP. He is a member of the following professional bodies; The Computer Professionals Registration Council of Nigeria (CPN),The Nigeria Computer Society (NCS), The Institute of Electrical and Electronics Engineers (IEEE) Computer Society, and The Association for Information Systems (AIS). His current research interests include: Access control, Biometrics, Information Security,and Network Security.

Ismaila Idris is with the Department of Cyber Security Science. He obtains his Bachelor degree with Federal University of Technology, Minna. MSc with University of Ilorin and PhD degree with University of Teknologi Malaysia (UTM). His research interest are Information Security, Data Mining, Machine Learning, Evolutionary Algorithm.