INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

# DESIGN A NOVEL SELF ADAPTING SIEM TECHNIQUE USING ARTIFICIAL NEURAL NETWORK

**[1]Ramesh Kumar Sharma, [2]S. K. Abdul Rahim, [3]Satyendra Nath Mandal, [4]Arun Prasad Burnwal**

*[1,2]Department. of Computer Science and Engineering, Bengal College of Engineering and Technology Durgapur (W.B), India-713212*
*[1]sharmarameshdhn@gmail.com*
*[3]Department. of Information Technology, Kalyani Government Engineering College, Kalyani, Nadia (W.B), India-741235, satyen_kgec@rediffmail.com*
*[4]Department of Mathematics, GGSESTC, Bokaro, Jharkhand, India-827013, apburnwal@yahoo.com*

**Abstract: -** Security Information and Event Management (SIEM) is the combined form of Security Information Management (SIM) and Security Event Management (SEM), where SIM collects accounting and audits logs at large volume and SEM analysis those logs, picks out the important behaviours and flagging them for review via alerts. It is focused on the need of SIEM for the purpose of security of the data in a present era of IT. In this paper, a novel self-adaptive technique is proposed based artificial neural network.

**Keywords**: Security Information Management, Security Event Management, Artificial Neural Network, Event Correlation.

## 1. Introduction

Security Information and Event Management (SIEM) [1] is considered to be a promising paradigm to reconcile traditional IDS/IPS processes along with latest recent advances Security Device based on Artificial Intelligence techniques to automatic and self-adaptive systems. It is challenges arise when dealing with the adaptation to newly encountered and multi-step attacks. In this thesis, the SIEM correlation with self-adaptation capabilities to optimize and significantly reduce the intervention of operators. The enhanced log correlation engine automatically learns and produces correlation rules based on the context for different types of multi-step attacks using Genetic Programming. A number of artificial neural networks are trained to classify events according to the corresponding context established for the attack. SIEM basically is a collection of two technologies:

1. Security Information Management (SIM)
2. Security Event Management (SEM)

SIEM is the combined form of SIM and SEM, where SIM collects accounting and audits logs at large volume and SEM analysis those logs, picks out the important behaviours and flagging them for review via alerts. The SIEM system is a complex collection of technologies designed to provide vision and clarity on the Govt.

organization, Corporate IT system as a whole, benefitting security analysts and IT Administrators. Security professional and Analyst use the SIEM system to monitor, identity, document, and sometimes respond to security affronts.

Rest of this paper is organized as follows: Section 2 addresses the preliminaries of the proposed method. The details of proposed method describes in section 3. Finally, Section 4 concludes the paper and future work highlights.

## 2. Preliminaries

Artificial Neural Network (ANN) is part of soft computing [2], [3] as well as artificial intelligence [4], [5]. It a mathematical modelling [6] based on human neuron. Apart from ANN, several constituent elements are available in soft computing such as fuzzy logic, genetic algorithm etc. Fuzzy logic [7], [8], [9], [10] is a multi-value logic which works between true and false. It deals with linguistic data such as very low, low, medium, short, very short etc. Sometimes it is also known as intelligent system because it deals with inference engine which consist rule base system defined by human knowledge [11], [12], [13]. Its extension is known as vague set which deals with two data sets true membership function and false membership function. It is also known as interval based membership function [14], [15]. These components of soft computing used in various application areas [16], [17], [18], [19], [20], [21], [22] and day by day its influence rapidly.

## 3. Proposed Method

In this section, a novel self-adapting SIEM technique is illustrates based on ANN. It divided by four phases. Details illustrations of these phases are given below:

### *3.1. ANN Processing*

The purpose of processing event is extracted into two fault:

(i) Constructing a training set which supervised the evaluation event.
(ii) Pre-processing assists users in in fessing specific correlation information for the context representation.

Let R is a setup registers such $R_1$, $R_2$, $R_3$,…..$R_n$, where $R_i$ contains a sequence of K events.
Event= A combination of Positive events.
A combination of Negative events.

Correspondingly, we have two different types of register (i) Positive and (ii) Negative Register containing Positive context and negative context respectively. So, user need two different trainings. A positive training set, Pt and Negative training set Nt. Attribute of events may be name type Address from, address to, plug-in etc.

### *3.2. Initialization of the Population:*

A tree building method, which implements a complete procedure to initialize a population of individuals. In this process, nodes are inserted into the tree according to a certain probability which determines how much the tree spreads itself.

Advanced attributes intrinsically depend on the length and width of the generated trees, and also on the information of the Relevant attributes.
In order to revisit the generated tree by performing the following two phases:

(1) A new method is added aimed at counting the total number of leaves which match up with plugin ID and plugins ID values for each tree branch.
(2) A new method is included which uniformly distributes the attributes timeout, reliability and the total number of occurrences stored in the positive training set along the tree branches.

(3) An heuristic to aggregate events is also added based on the source and destination IP addresses and ports information contained within events. Basically, a tuple of events can be aggregated in a N : M topology manner, where N is the number of different sources and M represents destinations. Thus, we generate different rules according to the following types of interaction: (i) unidirectional (aggregating events to/from a given computer), (ii) bidirectional (putting together events exchanged between a given pair of computers), and (iii) Multi-directional (aggregating in terms of a different attribute as there is no correlation between IP addresses). This heuristic facilitates population building and systematically categorizes correlations between events according to the way events are aggregated.

### *3.3 Evaluation of the Individuals*

The process of evaluating individuals is supervised by the training sets as follows. First, each individual is evaluated using both types of registers, i.e., positive and negative, previously generated. Basically, trees are visited by applying pre-order traversal which recursively visits each node on the left and right subtrees from the root. In particular, nodes are evaluated in the following terms:

(1) Leaf nodes are evaluated according to the events in each register. In this regard, event characteristics are compared with the relevant attributes of the rule being evaluated. Additionally, we seek for potential correspondences between each rule and the number occurrence of events in chronological order.
(2) Nodes are evaluated by applying AND and OR functions to the values produced in the evaluation of their children.
(3) Once individuals have been iterated, they will be classified into:
    (i) A positive individual returns true as a positive register matches up; or
    (ii) A negative individual occurs when a negative register evaluated over the individual returns false.

Thus, we make the population evolve for a series of generations in which a fitness function is evaluated on every individual (Algorithm 1–line 10). The fitness function is used for measuring and ranking every individual based on its quality to represent a candidate solution. Since our objective is to maximize the number of positive classifications over positive registers as well as to maximize the number of negative classifications over negative registers, we have defined the fitness function by following way:

Fitness= 1- (P+N)*P/(Tp+Tn)*Tp

| Positive Events(EP) | Negative Events(NE) |
|---|---|
| PE1 | NE1 |
| PE2 | NE2 |
| PE3 | NE3 |
| …… | |
| PEk | NEn |

No. of PEk may be same or different to no. of NEn

For the +ve

| r1 | r2 | r3 |
|---|---|---|
| $PE_1$ | $PE_1$ | $PE_1$ |
| $PE_2$ | $PE_2$ | $PE_2$ |
| ……. | ……. | …… |
| $PE_{r1}$ | $PE_{r2}$ | $PE_{R3}$ |

For the -ve

| R1 | R2 | R3 |
|---|---|---|
| $NE_1$ | $NE_1$ | $NE_1$ |
| $NE_2$ | $NE_2$ | $NE_2$ |
| ……. | ……. | …… |
| $NE_{r1}$ | $NE_{r2}$ | $NE_{R3}$ |

**A1 = r1 Ụ R1**
**A2 = r2 Ụ R2**

**Ak = rn Ụ Rn**
**Event -> Training set->individual**

### *3.4 Algorithm*

**Algorithm1: Proposed algorithm for GENIAL**

Step 1: E is the Collection of Events
Step 2: N E = Collection of Negative Events
Step 3: P E = Collection of Positive events
Step 4: R = { $r_1, r_2, r_3, ..., r_n$ ,R1,R2,R3,.....Rn} Containing Positive or Negative Events
Step5: Individuals
Step6:{Initialization of the population events either negative & positive events
Step7:if Negative then individual of relevant attributes
Step8: {Initialization of the Advanced attributes}
Step9: else repeat statement
Step 10: directive = null; $best_{individual}$ = null; $best_{fitness}$ = 1
Step 11: for all Generations do
Step12: for all i in Individuals do
Step13: fitness = eval(i, R) as in Eq. 2
Step14: if fitness is better than $best_{fitness}$ then
Step15: $best_{fitness}$ = fitness
Step16: $best_{individual}$ = i
Step17: end if
Step18: end for
Step19: Individuals←{Breed(Individuals) # $best_{individual}$ }
Step20: end for
Step 21: directive
=ToOssimSintax($best_{individual}$)
Step22: return directive

## 4. Conclusion and Future Work

In this paper, a novel self-adaptive SIEM technique is illustrates based on soft computing technique. ANN is used as a soft computing technique. It produce optimal solution because in this situation traditional approach is fails to achieve this goal. It handle security issues that arise in critical infrastructure. Future work will conduct experimental and analytical approach for solving same issue. Because it is more effectiveness than earlier approach.

## REFERENCES

[1] Di Sarno, Cesario, et al. "A novel security information and event management system for enhancing cyber security in a hydroelectric dam." International Journal of Critical Infrastructure Protection 13 (2016): 39-51.
[2] S. K. Das, A. Kumar, B. Das, and A. Burnwal, "On soft computing techniques in various areas," *Computer Science & Information Technology (CS & IT)*, 2013, vol. 3, pp. 59-68, DOI : 10.5121/csit.2013.3206.
[3] S. K. Das, S. Tripathi, and A. Burnwal, "Some relevance fields of soft computing methodology," *International Journal of Research in Computer Applications and Robotics*, 2014, vol. 2, pp. 1-6.
[4] A. Burnwal, A. Kumar, and S. K. Das, "Survey on application of artificial intelligence techniques," *International Journal of Engineering Research & Management*, 2014, vol. 1, no. 5, pp. 215–219.

[5] A. Kumar, A. Kumar and A. P. Burnwal, "Correlation of artificial intelligence techniques with soft computing in various areas", *International Journal of Indestructible Mathematics & Computing*, 2017, vol. 1, no. 1, pp. 27-34.
[6] A. Burnwal, A. Kumar, and S. K. Das, "Assessment of mathematical modeling in different areas," *International Journal of Advanced Technology & Engineering Research*, 2013, vol. 3, no. 3, pp. 23–26.
[7] A. Burnwal, A. Kumar, and S. K. Das, "Assessment of fuzzy set theory in different paradigm," *International Journal of Advanced Technology & Engineering Research*, 2013, vol. 3, no. 3, pp. 16–22.
[8] B. K. Mishra, B. Yadav, S. Jha, and A. Burnwal, "Fuzzy set theory approach to model super abrasive grinding process using weighted compensatory operator," *International Journal of Research in Computer Applications and Robotics*, 2015, Vol. 3, no. 5, pp. 62-68.
[9] S. Murmu, S. Jha, A. Burnwal, and V. Kumar, "A proposed fuzzy logic based system for predicting surface roughness when turning hard faced components," *International Journal of Computer Applications*, 2015, vol. 125, no. 4.
[10] A. Burnwal, S. Mukherjee, and D. Singh, "An additive model of fuzzy geometric programming," *Mathematics Education India*, 2000, vol. 34, no. 1, pp. 25-29.
[11] S. K. Das, B. Das, and A. Burnwal, "Intelligent energy competency routing scheme for wireless sensor networks", *International Journal of Research in Computer Applications and Robotics*, 2014, vol. 2, no. 3, pp. 79–84.
[12] A. Kumar, A. Kumar and A. P. Burnwal, "Application of intelligent game theory approach in cognitive radio ad hoc networks", *International Journal of Indestructible Mathematics & Computing*, 2017, vol. 1, no. 1, pp. 35-40.
[13] S. K. Das, S. Tripathi, and A. Burnwal, "Intelligent energy competency multipath routing in wanet," *in Information Systems Design and Intelligent Applications*, Springer, 2015, pp. 535-543, DOI: 10.1007/978-81-322-2250-7_53.
[14] S. K. Das and S. Tripathi, "Energy efficient routing protocol for manet based on vague set measurement technique," *Procedia Computer Science*, 2015, vol. 58, pp. 348-355, doi:10.1016/j.procs.2015.08.030.
[15] S. K. Das and S. Tripathi, "Energy Efficient Routing Protocol for MANET Using Vague Set," *in Proceedings of Fifth International Conference on Soft Computing for Problem Solving*, Springer, 2016, pp. 235-245, DOI: 10.1007/978-981-10-0448-3_19.
[16] S. K. Das, A. Kumar, B. Das, and A. Burnwal, "Ethics of reducing power consumption in wireless sensor networks using soft computing techniques," *International Journal of Advanced Computer Research*, 2013, vol. 3, no. 1, pp. 301-304.
[17] S. K. Das, S. Tripathi, and A. Burnwal, "Fuzzy based energy efficient multicast routing for ad-hoc network," *in Computer, Communication, Control and Information Technology (C3IT), 2015 Third International Conference on, IEEE*, 2015, pp. 1-5, DOI: 10.1109/C3IT.2015.7060126.
[18] S. K. Das, S. Tripathi, and A. Burnwal, "Design of fuzzy based intelligent energy efficient routing protocol for WANET," *in Computer, Communication, Control and Information Technology (C3IT), 2015 Third International Conference on, IEEE*, 2015, pp. 1-4, DOI: 10.1109/C3IT.2015.7060201.
[19] N. Kumari and A. P. Burnwal, "Interactive fuzzy programming model in multi-objective inventory control", *International Journal of Indestructible Mathematics & Computing*, 2017, vol. 1, no. 1, pp. 38-26.
[20] S. K. Das, A. K. Yadav and S. Tripathi, "IE2M: Design of intellectual energy efficient multicast routing protocol for ad-hoc network," *Peer-to-Peer Networking and Applications*, 2016, pp. 1-18, DOI 10.1007/s12083-016-0532-6.
[21] S. K. Das and S. Tripathi, "Intelligent energy-aware efficient routing for MANET," *Wireless Networks*, 2016, pp. 1-21, DOI 10.1007/s11276-016-1388-7.
[22] S. K. Das, A. Kumar, B. Das, and A. Burnwal, "Ethics of E-Commerce in Information and Communications Technologies," *International Journal of Advanced Computer Research*, 2013, vol. 3, no. 1, pp. 122-124, doi=10.1.1.300.9397.