ICSITech
International Conference on Science in Information Technology

IEEE
Advancing Technology for Humanity

# PROCEEDING

# 2015 International Conference on Science in Information Technology (ICSITech)

## Big Data Spectrum for Future Information Economy

Yogyakarta, October 27th - 28th, 2015

IEEE Catalog Number: CFP15B09-USB
ISBN : 978-1-4799-8385-8

# 2015 International Conference on Science in Information Technology (ICSITech)



## COPYRIGHT AND REPRINT PERMISSION



IEEE Catalog Number : CFP15B09-USB
ISBN : 978-1-4799-8385-8

Additional copies of this publication are available from

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571 USA

+1 845 758 0400
+1 845 758 2633 (FAX)
email: curran@proceedings.com

Editor : Andri Pranolo, Yana Hendriana, Adhi Prahara, Dewi Pramudi Ismi
Publisher : IEEE
Secretariat : Informatics Engineering, Faculty of Industrial Technology, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

# PROCEEDING

2015 International Conference on Science in Information Technology (ICSITech)

**“Big Data Spectrum for Future Information Economy”**

27 - 28 October 2015
Yogyakarta, Indonesia

# Organizers and Sponsors

## Organized by

Universitas Ahmad Dahlan, Indonesia
Universitas Pendidikan Indonesia, Indonesia
Universitas Mulawarman, Indonesia
UPN "Veteran" Yogyakarta, Indonesia
Universiti Teknologi Malaysia, Malaysia

## Sponsored by

IEEE Indonesia Section

## Funded by

Ministry of Research, Technology, and Higher Education (RISTEKDIKTI), Republic of Indonesia

## Supported by

Universitas Sriwijaya, Indonesia
Universiti Malaysia Pahang, Malaysia
PT. Qwords International Company

# Committee

## Steering Committee

- Dwi Hendratmo Widyantoro (Institut Teknologi Bandung, Indonesia)
- Kuncoro Wastuwibowo (IEEE Indonesia Section)
- Siti Mariyam Shamsuddin (Universiti Teknologi Malaysia)
- Tole Sutikno (Universitas Ahmad Dahlan, Indonesia)
- Tutut Herawan (Universitas Ahmad Dahlan, Indonesia)

## Organizing Committee

### General Chair

- Rusydi Umar (Universitas Ahmad Dahlan, Indonesia)

### General Co-Chair

- Anton Yudhana (Universitas Ahmad Dahlan, Indonesia)

### Secretary

- Sarina Sulaiman (Universiti Teknologi Malaysia)
- Dewi Octaviani (Universiti Teknologi Malaysia)
- Dewi Pramudi Ismi (Universitas Ahmad Dahlan, Indonesia)

### Treasury

- Yana Hendriana (IEEE Member, Universitas Ahmad Dahlan, Indonesia)
- Hidayatullah Himawan (UPN Veteran, Yogyakarta, Indonesia)

### Marketing and Public Relation

**Chair**

- Andri Pranolo (IEEE Member, Universitas Ahmad Dahlan, Indonesia)

**Co-Chair**

- Ummi Rabaah Hashim (Universiti Teknikal Malaysia Melaka)

**Members**

- Azhari SN (Universitas Gadjah Mada, Indonesia)
- Chatchada Kaewpruksapimon (Suan Dusit Rajabhat University, Thailand)
- Danial Hooshyar (University of Malaya, Malaysia)
- Houssen Ahmadi (Universiti Teknologi Malaysia)
- Intan Ermahani A Jalil (Universiti Teknikal Malaysia Melaka)
- Julian Supardi (University of Sriwijaya, Indonesia)
- Mahmoud Ali Ahmed (Khartoum University, Sudan)
- Rasim (Universitas Pendidikan Indonesia, Bandung, Indonesia)
- Rofilde Hasudungan (University of Mulawarman, Samarinda, Indonesia)
- Rosdiyana Binti Samad (Universiti Malaysia Pahang)
- Ridwan Suhud (Lembaga Ilmu Pengetahuan Indonesia)
- Wahyudin (Universitas Pendidikan Indonesia, Bandung, Indonesia)

- Yudi Wibisono (Universitas Pendidikan Indonesia, Bandung, Indonesia)

**Publication**

- Deris Stiawan (Faculty of Computer Science, Sriwijaya University, Indonesia)
- Imam Riadi (Universitas Ahmad Dahlan, Indonesia)
- Kartika Firdausy (Universitas Ahmad Dahlan, Indonesia)
- Nur Ahmadi (Institut Teknologi Bandung, Indonesia)
- Shafaatunnur Hasan (Universiti Teknologi Malaysia)
- Siti Nurmaini (Faculty of Computer Science, Sriwijaya University, Indonesia)
- Yuliah Qotimah (Institut Teknologi Bandung, Indonesia)

**Technical Program Committee**

- Andri Pranolo (IEEE Member, Universitas Ahmad Dahlan, Indonesia)
- Anton Yudhana (Universitas Ahmad Dahlan, Indonesia)
- Adhi Prahara (Universitas Ahmad Dahlan, Indonesia)
- Arda Yunianta (University of Mulawarman, Indonesia)
- Dewi Octaviani (Universiti Teknologi Malaysia)
- Haviluddin (University of Mulawarman, Indonesia)
- Herlina Jayadianti (UPN Veteran Yogyakarta, Indonesia)
- Lili Ayu Wulandhari (Bina Nusantara University, Indonesia)
- Shafaatunnur Hasan (Universiti Teknologi Malaysia)

**Sponsor**

- Ali Tarmuji (IEEE Member, Universitas Ahmad Dahlan, Indonesia)
- Eddy Prasetyo Nugroho (Universitas Pendidikan Indonesia, Bandung, Indonesia)
- Imam Azhari (Universitas Ahmad Dahlan, Indonesia)
- Tawar (Universitas Ahmad Dahlan, Indonesia)
- Wawan Setiawan (Universitas Pendidikan Indonesia, Bandung, Indonesia)

# Reviewers

- Abderrafiaa Koukam (Université de Technologie de Belfort-Montbéliard (UTBM), France)
- Agus Harjoko (Universitas Gadjah Mada, Indonesia)
- Amer Ali Sallam (Limkokwing University of Creative Technology, Sama'a, Yamen)
- Anca Ralescu (University of Cincinnati Ohio, USA)
- Arda Yunianta (University of Mulawarman, Indonesia)
- Azuraliza Abu Bakar (Universiti Kebangsaan Malaysia)
- Deris Stiawan (Faculty of Computer Science, Sriwijaya University, Indonesia)
- Didi Rosiyadi (Research Center for Informatics LIPI, Indonesia)
- Edi Kurniawan (Research Center for Informatics LIPI, Indonesia)
- Esa Prakasa (Research Center for Informatics LIPI, Indonesia)
- Hamzah Bin Ahmad (Universiti Malaysia Pahang)
- Hanung Adi Nugroho (Universitas Gadjah Mada, Indonesia)
- Herlina Jayadianti (Universitas Pembangunan Nasional Veteran Yogyakarta, Indonesia)
- Ito Wasito (Universitas Indonesia)
- Iwan Tri Riyadi Yanto (Universitas Ahmad Dahlan, Indonesia)
- Kamarul Hawari Bin Ghazali (Universiti Malaysia Pahang)
- Lala Septem Riza (Universidad de Granada, Spain)
- Lian Duan (New Jersey Institute of Technology, USA)
- Khabib Mustofa (Universitas Gadjah Mada, Indonesia)
- Masayu Leylia Khodra (Institut Teknologi Bandung, Indonesia)
- Mohd Shahizan Bin Othman (Universiti Teknologi Malaysia)
- Moslem Yousefi (Universiti Tenaga Nasional (UNITEN), Malaysia)
- Munir (Universitas Pendidikan Indonesia, Bandung, Indonesia)
- Mustafa Kaiiali (Mevlana University, Turkey)
- Nataniel Dengen (University of Mulawarman, Indonesia)
- Noel Lopes (Polytechnic of Guarda, Portugal)
- Omar Al Jadaan (Medical and Health Sciences University, United Arab Emirates)
- Omid Motlagh (Commonwealth Scientific and Industrial Research Organization, Australia)
- Ouri Wolfson (University of Illinois, USA)
- Paulus Insap Santosa (Universitas Gadjah Mada, Indonesia)
- Per Johan Runeson (Systems Lund University, Sweden)
- Rafah Mohamed Almuttairi (University of Babylon, Iraq)
- Rafał Dreżewski (AGH University of Science and Technology, Poland)
- Reza Firsandaya Malik (Sriwijaya University, Indonesia)
- Reza Pulungan (Universitas Gadjah Mada, Indonesia)
- Rinaldi Munir (Institut Teknologi Bandung, Indonesia)
- Riyanarto Sarno (Institut Teknologi Sepuluh Nopember (ITS), Indonesia)
- Rodina binti Ahmad (University of Malaya, Malaysia)
- Ronny Mardiyanto (Institut Teknologi Sepuluh Nopember (ITS), Indonesia)
- Romi Satria Wahono (Universitas Dian Nuswantoro, Indonesia)
- Sarina Sulaiman (Universiti Teknologi Malaysia)

# Program Schedule

## Day 1: Tuesday, October 27th, 2015

07.00 – 08.00 **Registration** – Room: Ballroom (4th Floor)

08.00 – 08.45 **Opening Ceremony** – Room: Ballroom (4th Floor)
Qur'an Recitation

**Welcome Messages:**
1. ICSITech 2015 Chairman : Rusydi Umar, Ph.D
2. Rector of UAD : Dr. Kasiyarno, M.Hum.
3. IEEE Indonesia Section : Satriyo Dharmanto

08.45 – 09.00 **Coffee Break I** – Room: Ballroom (4th Floor)

09.00 – 10.40 **Keynote Speech Session 1** – Room: Ballroom (4th Floor)

**Data Science vs Big Data @ UTM Big Data Centre**,
by Prof. Siti Mariyam Shamsuddin
(UTM Big Data Centre, Universiti Teknologi Malaysia, Malaysia)

**Comparison of Data Mining Techniques for Money Laundering Detection System**,
by Assist Prof. Rafał Dreżewski
(AGH University of Science and Technology, Poland)

10:40 – 12:00 **Parallel Class Session I-A : Informatics Track** – Room : Frangipani (3rd Floor)

10:40 – 11:00 (1570182343) Recognition of Malaysian Sign Language Using Skeleton Data with Neural Network
*Sutarman (University Technology of Yogyakarta, Indonesia; Universiti Malaysia Pahang, Malaysia), Mazlina Abdul Majid (Universiti Malaysia Pahang, Malaysia), Jasni Mohamad Zain (Universiti Malaysia Pahang, Malaysia), Arief Hermawan (University Technology of Yogyakarta, Indonesia)*

11:00 – 11:20 (1570148107) Active Contour Bilateral Filtering for Breast Lesions Segmentation on Ultrasound Images
*Anan Nugroho (Universitas Gadjah Mada, Indonesia), Hanung Adi Nugroho (Universitas Gadjah Mada, Indonesia), Lina Choridah (Sardjito Hospital, Universitas Gadjah Mada, Indonesia)*

11:20 – 11:40 (1570148091) Automatic Image Segmentation using Sobel Operator and *k*-Means Clustering: A Case Study in Volume Measurement System for Food Products
*Joko Siswantoro (Universitas Surabaya, Indonesia; Universiti Kebangsaan Malaysia, Malaysia), Anton Satria Prabuwono (King Abdulaziz University, Saudi Arabia; Universiti Kebangsaan Malaysia, Malaysia), Azizi Abdullah (Universiti*

# Intrusion Prevention in Heterogeneous System based on Behavior Approaches

Deris Stiawan[1], Ahmad Fali Oklilas[1], Ahmad Heryanto[1], Tri Wanda Septian[1], Rahmat Budiarto[2],
[1] Computer Engineering Department, Faculty of Computer Science, Sriwijaya University, Palembang, Indonesia
[2] Smart Networked Computing Research Group, College of Comp. Sc. & IT, Albaha University, Albaha, Saudi Arabia
{deris, fali, hery, triwandaseptian}@ilkom.unsri.ac.id, rahmat@bu.edu.sa

***Abstract*— This paper proposes the learning phase for enhancing the learning phase of intrusion prevention systems in heterogeneous environment. We represent accuracy and precision as means to identify and recognize suspicious threats through new model examination alarms and assessment that match with an event database. The aims of this work are: firstly to present a comprehensive analysis mapping problem in terms of intrusion prevention, and secondly to provide a promising model for examining new emerging suspicious threats. Throughout this paper, the proposed a model are implemented to evaluating system security in order to help security officers to be more aware of their network status.**

***Keywords*— intrusion prevention; accuracy; precision alarm; hybrid architecture***

## I. INTRODUCTION

Analysis and predictions of current attacks by [1-4] show there has been an explosion of security threats in recent years, such as Trojan, worms, spyware, password theft and denial-of-service (DoS) attacks, which continue to grow, multiply and evolve towards a future in which cyber warfare is common. Authors in [5] describe the heterogeneity of the security event sources such as network and diverse host types, and the Intrusion Detection Systems (IDSs) which are heterogeneous in their type, how they operate, and in their diverse alert output formats.

Meanwhile, Intrusion Prevention Systems (IPSs) is a new approach for defending computer network, combining the features of a firewall with that of active intrusion detection systems properly. The IPSs allow for the leveraging of proactive techniques in order to prevent the attacks from entering the network, which is accomplished by examining various data records and detection demeanors using a pattern recognition sensor. When an attack is identified, the IPS blocks and logs the offending data. The primary intrusion prevention method uses signatures to identify activities in network/host traffic, as well as performing detection analysis on inbound – outbound packets, so as to provide an active response aimed at blocking malicious violations before harming the network resources.

In this paper we present a model to increase accuracy and precision regarding suspicious violations that originate from a heterogeneous network. The objective is to reduce the number of false alarms by using event list handling combined with an event list database of signatures, logging system and rules. The main contribution is the enhancement of a learning phase, which aims to provide more accurate early prevention and mitigation of threats.

The rest of the paper is organized as follows. Related works on mapping of the problem in the IPS field research area is described in Section 2. Section 3 presents the details of our hybrid architecture model. Section 4 discusses the improved accuracy and precision mechanism to help identify and recognize potential threats. Finally, Section 5 provides our conclusion and identified potential future work to be carried out in this area.

## II. RELATED WORKS

Most of the existing model related to network intrusion only work in term of detection. So far they simple notify the security officer by producing alerts after threats have been identified or otherwise provide only limited administrative notifications via trigger reports which then request the receiver take action manually. Furthermore, various models and frameworks have been published in regards to providing intrusion detection that deals with mitigating external threats. However, there is a lack of attention given to detecting and preventing attacks from insider threats. In this section, we present a mapping technique to determine each stage in a fully inclusive IPS architecture as illustrated in Fig. 1.

### *A. Intrusion Prevention System (IPS)*

IPS is still a relatively new approach to defend network systems, which prevents attacks from entering the network by examining various data records and leveraging prevention demeanor through the use of a pattern recognition sensor. IPSs are able to identify attacks, act as an intrusion prevention block, log identified data and automatically retrieve the response as being of a malicious nature. On the other hand, IDSs prove the capability to detect hostile traffic, allowing them to send alerts, but they did nothing to actually stop the attacks from happening [6]. As IDS is passive, it is rarely able to detect all forms of malicious programs and activities at any given point in time, whilst also being incompatible for integrating with control restrictions designed to stop malicious forms of traffic. IPS is designed and developed for more

active protection to improve upon the IDS and other traditional security solutions [7, 8]. The comparison of IDS and IPS has been discussed in [9].

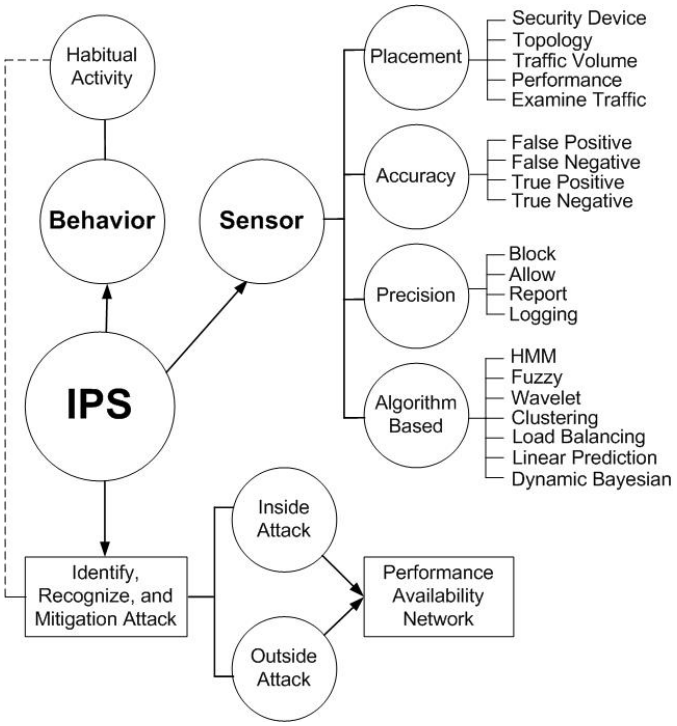


Fig. 1. The learning IPS mapping problems

### B. Sensor

In most instances, the source of a large number of alarms is caused by the nature of some categories of attack which operated by sending a large number of malicious packets. As seen in earlier proposals [10, 11], alarm that informs the malicious is a critical aspect in IPS. This is further explored in [12], which presented a distribution sensor with three main modules. The sensor produces alerts, so as to identify suspicious threats which then trigger alerts if offending data is found using a signature technique to recognize algorithm-based packets. A technique that utilized wavelets was presented previously [5], and followed by [6] that suggested to use a technique for leveraging a Hidden Markov Model (HMM) as a sensor model. Authors in [7] proposed an incremental-learning algorithm. A Pattern-matching algorithm is used in [8], and an artificial immune algorithm is experimented in [9]. Authors in [13] described a circumstance issues, gaps and challenging in IPS.

### C. Attack

Authors in [11] presented a case study of the technical counter measures and processes used to deter, detect and mitigate malicious insider threats using non-classified anonymous interview techniques and the analysis of anonymous qualitative field data. A malicious insider action model analysis included reconnaissance, access, entrenchment, extraction infiltration, and communication is proposed in [12]. According to works in [9, 13], we may conclude that attacks from insiders have more a lethal effect on overall security network.

### D. Behaviour

Behavior-based approach is similar to pattern prevention approach, but differs in its attempts to define specific patterns. Behaviour rule based intrusion detection methods which analyze the correlation of communication behavior by rules are introduced in [14, 15]. The authors used auxiliary variables approach in each case in order to figure out various correlations between event and communication behavior present in various software and attack scenarios.

## III. The Proposed IPS Hybrid Architecture

To detect suspicious threats, there are two approaches that can be taken [1, 2, 6]. (i) Host-based approach which currently becomes popular technologies. The approach checks suspicious activities from a host computer or on an operating system level. The monitoring location uses the agent component. (ii) Network-based approach which sniffs and identifies all inbound-outbound packets that crosses the network. Combining Network-based with other security components provides an active comprehensive network security solution.

The proposed architecture of intrusion prevention system as seen in Fig. 2 describes the relationship among the components, as follows:

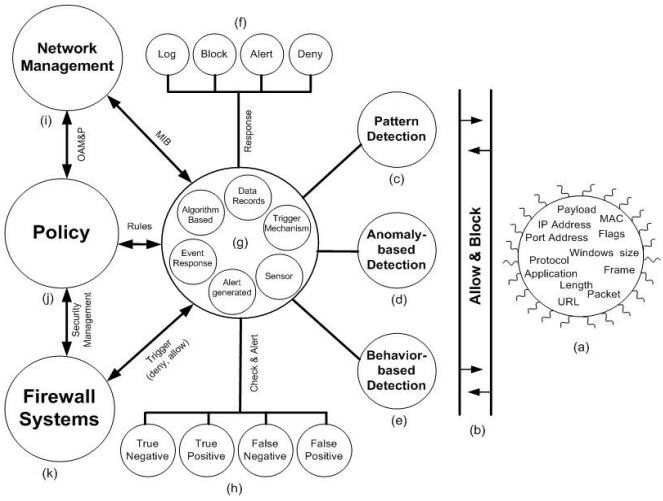


Fig. 2. The Architecture of the hybrid intrusion prevention

a. Attack: payload, port address, MAC address, flags, windows size, frame, length, packet, URL, application and protocol.
b. Allow and Block from stage event response.
c. Sensor mechanism, as shown in Fig. 2 (c), (d) and (e), enables the IPS to recognize and identify suspicious data which will trigger an alert if offending data is found. Pattern-based detection: to identify a specific pattern, represented as either a textual or binary string. Pattern detection provides the following mechanisms [16]:

(i) Pattern Detection (regex). A regex is a pattern-matching language that enables the ability to define a flexible custom search string and pattern.
(ii) Deobfuscation techniques [17]. These techniques focus on obfuscating the concrete syntax of the program. The idea is to prevent an attacker from understanding the inner workings of a program by obfuscating the program. An example of this is changing variable names or renaming different variables in different scopes to the same identifier.

d. Anomaly-based detection is also sometimes used as profile-based detection. To do this it is necessary to build profiles that obviously define what activity is considered normal activity. After defining what (show in mark (a)) is considered normal, then anything that deviates from this normal profile generates trigger alerts.
e. Behavior-based detection is similar to pattern detection, but instead of trying to define specific patterns, the behavior defines classes of activity that are known to be suspicious [5, 10].
f. Incident response. In this case security must respond to the traffic by performing some type of predefined actions such as deny, alert, block or log.
g. Core hybrid architecture which consists of:
   - Algorithm: meaning the components to classify, predict, calculate, segment, technique, mechanism, and formulate.
   - Data records: a collection of data for archive logs, may be centralized or distributed mechanism.
   - Trigger mechanism: with alert generation and event response.
   - Sensor: the sensor comes with produce alert. The placement sensors affect and ensure accuracy of the sensor.
   - Alert generated.
   - Incident response, namely deny, alert, block and log.
h. Alert Generate: the situation trigger of alarms (valid or invalid but feasible) from sensor, such as (i) true positive, (ii) true negative, (iii) false positive, (iv) false negative.
i. Network Management: network management is one of the most important, yet confusing, topics in networking today. It includes operations, administration, maintenance and provisioning (OAM&P) functions required to provide, monitor, interpret and control the network and the services it carries [18].
j. Policy. The policy should contain a list of criteria required for entry and items that deny entry. The guard matches the captured information with an item on the policy list, assesses the state of the system and then takes the action associated with the policy object that matched [18]. The policy may be explicit and contain standard operating parameters, as in a corporate policies, procedures or guidelines. However it is more commonly implicit, as in the configuration of devices governed by a policy.
k. Firewall. This is a mechanism (hardware, software and policy) to restrict access from the outside to inside the network. They work by examining the data of the network layer (Layer 3: IP Address) and transport layer (Layer 4: Port number, multiplexing). The limitation of firewalls include: (i) a firewall cannot prevent attack coming from inside by trust users, (ii) the access control policy of a firewall is static. It cannot adapt itself to changes in attacks from the outside, (iii) the filtering rules of the firewall are usually very simple, which means that the firewall cannot prevent attacks coming from Layer 7 or from viruses and (iv) the firewall cannot prevent the monitoring of packet data.

## IV. Accuracy And Precision Sensor Analysis

In this section, we present a strategy to increase the accuracy of precision sensors when trying to identify and recognize security violations, such as suspicious traffic or malicious threats. We assume in this approach that appropriate alarms, risk ratings and event responses will in turn lead to increased accuracy. We identified there are some instances [1, 3, 14] conducted to propose composite and associate between accuracy and precision. Unfortunately, elementary correlation is not described accurately and clearly.

### *A. Alarm Accuracy*

From our observation, accuracy affects the correctness of deciding whether an attack exists in real-traffic, thus notifying the logging system of an attack based on the list in the database. Therefore, accuracy performance can be used to measure the percentage of successful detections, with failures being seen as the number of false alarms, the goal of which should be to reduce the number of false positive alerts [19, 20].

Having reviewed the proposal literature of [16], who present that as a consequence of high variability, user profiles are very inaccurate in terms of establishing a detection system, thus raising a large amount of false alarms. In intrusion prevention, positive data is considered to be attack data, while negative data is considered to be a normal data. Furthermore, evaluation accuracy and speed were proposed as being relevant factors by [16], who suggested these should be measured in terms of FP and FN with timeline activity approaches.

The main problem with properly leveraging sensors relate to their accuracy and timeliness in regards to identifying threats. This means that sensitivity is very important, as how effective a particular filter is in blocking known and unknown threats. As such results should be measured in terms of FP and FN.

As show in Fig. 3, there are four alerts: (i) True negative (TN), which is normal user traffic which does not generate an alarm. (ii) True positive (TP), which generates an alarm after detecting attack traffic. TN as well as TP both corresponds to a correct operation of the intrusion prevention system, which is events that are successfully labeled as normal and attack. (iii) False negative (FN), which will be silent, meaning no alarm is generated during legitimate attack traffic. With false negatives attack events are incorrectly perceived as being normal events, and (iv) False positive (FP) produces an alert if it falsely identifies normal traffic activity as being malicious in

nature. Reducing false positive alerts should be a main focus when building the detection system.

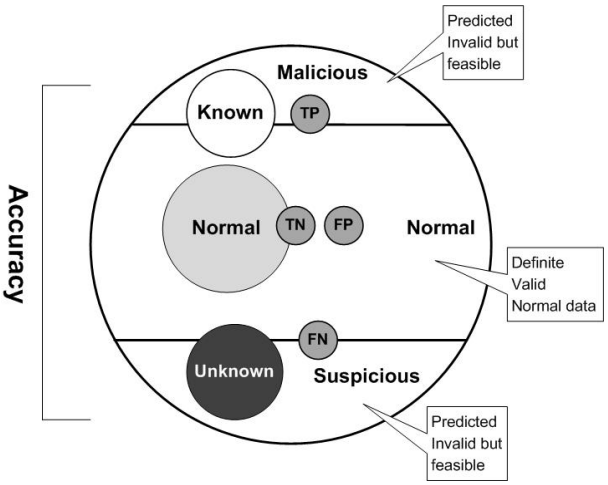


Fig. 3. Alarm Accuracy

Based on both a confusion matrix [21] and traditional approach, a numerical measurement can be applied to quantify the performance of IPSs as shown in (1) to (4).

$$TrueNegativeRate\ (TNR) = \frac{TN}{TN+FP} \quad (1)$$

$$TruePositiveRate\ (TPR) = \frac{TP}{TP+FN} \quad (2)$$

$$FalsePositiveRate\ (FPR) = \frac{FP}{TN+FP} \quad (3)$$

$$FalseNegativeRate\ (FNR) = \frac{FN}{TP+FN} \quad (4)$$

$$Accuracy = \frac{TN+TP}{TN+TP+FN+FP} \quad (5)$$

$$Precision = \frac{TP}{TP+FP} \quad (6)$$

Where *FP* = Number of clean responses detected as threat / Total number of clean response, *Sensitivity* = Number of unknown activity responses detected / Total number of unknown activity responses

The most popular performance metrics are detection rate (*DR*) combined with false alarm rate (*FAR*). In some instances involve precision and recall, or sensitivity and specificity.

### B. Precission

Authors in [22] presented an attack prevention framework that is targeted at detecting, as well as reacting against distributed and coordinated attack scenarios using a broker that is connected to a distributed sensor alert for gathering and correlating information held by multiple sources.

In such instances, we use a spread database to store the events, such as: (i) a global database to update rules identifications, (ii) a signature database, from Snort rules, with the signatures have to be updated in the database for future verification process, (iii) regex: regular expression that can be used in selectors to define ranges of values instead of defining each possible value separately, and (iv) an archive database, which is an event database, logging system, operating system events, application logs, file system information and report log.

Additionally from our survey, in order to identify, recognize and mitigate external threats from habitual activity it is necessary to combine our approach with a signature database. In Fig. 4, we associate and combine events and list databases from signatures, logging system and rules. We designed a sensor module to interface with outbound and inbound traffic by considering each category of activity behavior. Thus, this approach is combined well with other information collected from our databases (archive event, signature, regex and global). Furthermore, the module uses two ways to composite, these being OR-based composite, as well as AND-based composite.

When a new type of events are detected and the sensor suspects an attack, an analyst can check the event's habitual activity components, then store the results in the archive event database if it is not already present in the list. The database module then assigns a rate marking and lists it within the defined risk rating.

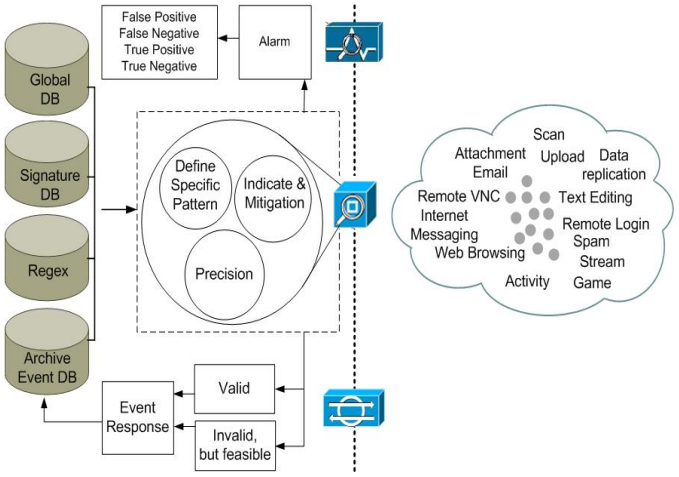


Fig. 4. Combining event and list database

## V. Conclusion And Future Works

In this paper, an approach has been proposed for increasing detection and actively preventing attacks in heterogeneous network, this is done through establishing an accurate alarm and precision event list database. This approach can be to use to raise the amount of TN alarms and decrease FP. The results indicate that this approach can be combined with other defense systems such as firewalls and network monitoring. In the future, we will experiment with behavior-based attack algorithms across a real-traffic network.

## ACKNOWLEDGMENT

This research is supported by a grant from Sriwijaya University, under contract number: 216/UN9.3.1/LT/2015.

## REFERENCES

[1] A. Patel, M. Taghavi, K. Bakhtiyari, and J. Celestino Júnior, "An Intrusion Detection And Prevention System In Cloud Computing: A Systematic Review," Journal of Network and Computer Applications, vol. 36, pp. 25-41, 2013.

[2] P. Louvieris, N. Clewley, and X. Liu, "Effects-based feature identification for network intrusion detection," Neurocomputing, vol. 2013, pp. 265-273, 2013.

[3] S. S. C. Silva, R. M. P. Silva, R. C. G. Pinto, and R. M. Salles, "Botnets: A survey," Computer Networks, vol. 57, pp. 378–403, 2013.

[4] A. Akhunzada, M. Sookhak, N. B. Anuar, A. Gani, E. Ahmed, M. Shiraz, *et al.*, "Man-At-The-End attacks: Analysis, taxonomy, human aspects, motivation and future directions," Journal of Network and Computer Applications, vol. 48, pp. 44-57, 2// 2015.

[5] R. Zuech, T. Khoshgoftaar, and R. Wald, "Intrusion detection and big heterogeneous data: a survey," Journal of Big Data, vol. 2, pp. 1-41, 2015/02/27 2015.

[6] Y. Weinsberg, S. Tzur-David, D. Dolev, and T. Anker, "High performance string matching algorithm for a network intrusion prevention system (NIPS)," in High Performance Switching and Routing, Workshop on 2006, pp. 147-153.

[7] A. Patel, Q. Qassim, and C. Wills, "A survey of intrusion detection and prevention systems," Information Management & Computer Security, vol. 18, pp. 277 - 290, 2010.

[8] D. Stiawan, M. Y. Idris, and A. H. Abdullah, "Penetration testing and network auditing: Linux " Journal of Information Processing Systems, vol. 11, pp. 104-115, 2015.

[9] D. Stiawan, A. L. A. Yaseen, M. Y. Idris, K. A. B. U. Bakar, and A. H. Abdullah, "Intrusion prevention system : a survey," Journal of Theoretical and Applied Information Technology, vol. 40, pp. 44-54, 2012.

[10] R. Perdisci, G. Giacinto, and F. Roli, "Alarm clustering for intrusion detection systems in computer networks," Engineering Application of Arificial Inteligence, vol. 19, pp. 429-438, 2006.

[11] A. D. Todd, R. A. Raines, R. O. Baldwin, B. E. Mullins, and S. K. Rogers, "Alert verification evasion through server response forging," Alert Verification Evaluation Through Server Response Forging, LNCS, vol. 4637/2007, pp. 256-275, 2007.

[12] H. T. Elshoush and I. M. Osman, "Alert correlation in collaborative intelligent intrusion detection systems—A survey," Applied Soft Computing, vol. 11, pp. 4349-4365, 2011.

[13] D. Stiawan, A. H. Abdullah, and M. Y. Idris, "The trends of intrusion prevention system network," in International Conference on Education Technology and Computer (ICETC), Shanghai, China, 2010, pp. 217-221.

[14] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, "Future directions for behavioral information security research," Computers & Security, vol. 32, pp. 90-101, 2013.

[15] C. Nithiyanandam, D. Tamilselvan, S. Balaji, and V. Sivaguru, "Advanced framework of defense system for prevetion of insider's malicious behaviors," in Recent Trends In Information Technology (ICRTIT), 2012 International Conference on, 2012, pp. 434-438.

[16] K. Haslum, M. E. G. Moe, and S. J. Knapskog, "Real-time intrusion prevention and security analysis of networks using HMMs," in Local Computer Networks, 2008. LCN 2008. 33rd IEEE Conference on, 2008, pp. 927-934.

[17] S. K. Udupa, S. K. Debray, and M. Madou, "Deobfuscation: reverse engineering obfuscated code," in Reverse Engineering, 12th Working Conference on, 2005, p. 10 pp.

[18] J. Lianxing, Z. Wei, Z. Chenggong, and D. Yi, "Research on an integrated network management system," in Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007. Eighth ACIS International Conference on, 2007, pp. 311-316.

[19] H. W. Njogu, L. Jiawei, J. N. Kiere, and D. Hanyurwimfura, "A comprehensive vulnerability based alert management approach for large networks," Future Generation Computer Systems, vol. 29, pp. 27-45, 2013.

[20] R. Shittu, A. Healing, R. Ghanea-Hercock, R. Bloomfield, and M. Rajarajan, "Intrusion alert prioritisation and attack detection using post-correlation analysis," Computers & Security, vol. 50, pp. 1-15, 5// 2015.

[21] Wu Shelly Xiaonan and B. Wolfgang, "The use of computational intelligence in intrusion detection systems : A review," Applied Soft Computing, vol. 10, pp. 1-35, 2010.

[22] J. Garcia-Alfaro, M. A. Jaeger, G. Mühl, I. Barrera, and J. Borrell, "Distributed exchange of alerts for the detection of coordinated attacks open," Communication Networks and Services Research Conference, pp. 96-103, 2008.

ISBN 978-1-4799-8385-8

## Partners and Sponsor