A study of Methodologies used in Intrusion Detection and Prevention Systems (IDPS)

David Mudzingwa
Department of ECIT
North Carolina A&T State University
Greensboro, NC 27411
Email: dmudzing@ncat.edu

Rajeev Agrawal
Department of ECIT
North Carolina A&T State University
Greensboro, NC 27411
Email: ragrawal@ncat.edu

Abstract— **Intrusion detection and prevention systems (IDPS) are security systems that are used to detect and prevent security threats to computer systems and computer networks. These systems are configured to detect and respond to security threats automatically there by reducing the risk to monitored computers and networks. Intrusion detection and prevention systems use different methodologies such as signature based, anomaly based, stateful protocol analysis, and a hybrid system that combines some or all of the other systems to detect and respond to security threats. The growth of systems that use a combination of methods creates some confusion when trying to choose a methodology and system to deploy. This paper seeks to offer a clear explanation of each methodology and then offer a way to compare these methodologies.**

Keywords— **Intrusion Detection and Prevention Systems (IDPS), Anomaly Based Detection, Signature Based Detection, Stateful Protocol Analysis Based Detection, Hybrid Based Detection.**

I. INTRODUCTION

Intrusion detection and prevention systems (IDPS) have become a valuable tool in keeping information systems secure. IDPS are security tools that are used to monitor, analyse, and respond to possible security violations against computer and network systems. These violations can be a result of break in attempts by unauthorized external intruders trying to compromise the system or internal privileged users miss-using their authority. As the intrusion detection and prevention field continue to evolve and produce new systems, the underlying methodologies are not evolving at the same pace and are slowly being merged together. This creates confusion when trying to understand the detection methodologies that are utilized by newer systems. Past and current work in this area mainly focuses on explaining or improving one or two methodologies. Some works offer an evaluation of one methodology against a proposed a new methodology.

This paper bridges this gap by offering an explanation of the four major underlying IDPS detection methodologies and a way to compare them. The four main detection methodologies used by IDPS are signature based, anomaly based, stateful protocol analysis based, and hybrid based. The remaining part of this paper is organized as follows: Section ll gives an overview of related works. Section lll offers a detailed description of the four main methodologies, while Section lV offers a detailed way to compare and evaluate IDPS methodologies. Section V concludes the paper and suggests future work.

II. RELATED WORK

Intrusion detection and prevention systems are a combination of intrusion detection systems and intrusion prevention systems. Intrusion prevention came out of research on the short comings of intrusion detection. Intrusion detection evolved out of a report that proposed a threat model [1]. This report laid down the foundation for intrusion detection systems by presenting a model for identifying abnormal behaviour in computer systems. This model broke down threats into three groups, external penetrations, internal penetrations, and misfeasance. The report used these three groups of threats to develop an anomaly based user behaviour monitoring system. In 1987 “a model for a real-time intrusion-detection expert system that aims to detect a wide range of security violations ranging from attempted break-ins by outsiders to system penetrations and abuses by insiders” was produced [2]. This model was based on the idea that security breaches to any systems can be identified and monitored by analyzing the system’s audit logs. The model was comprised of profiles, metrics, statistical models, and rules for analyzing the logs. This model provide the “a framework for a general-purpose intrusion-detection system expert system” that is still in use today [3]. The two main methodologies used in intrusion detection and prevention systems are combined to form a collaborative intelligent intrusion detection system (CIIDS)[4]. This work looked and addressed current challenges to collaborative intrusion detection systems and the algorithms they employ for alert correlation. It also suggested ways to reduce false positives while improving the detection accuracy. In [5] a structured approach to intrusion detection systems by defining and classifying the components of an IDS system is offered. This classification offered a clear understanding of all the parts that make up intrusion detection systems and the challenges the systems faces. James and Jay offered survey of where the current research is on the techniques and methodologies used in intrusion detection [6]. Their focus was to summarize the research done in intrusion detection to this point and in so doing offer a starting point for future research to start from. A technical overview of intrusion detection systems starting with

978-1-4673-1375-9/12/$31.00 ©2012 IEEE

the fundamentals of how these systems are structured to the techniques they use to detect and identify potential security threats [7]. The paper also explains how an intrusion detection system responds to violations of the security policies they are monitoring. Intrusion detection and prevention systems suffer from scalable and efficiency problems, these two problems are addressed by high performance deep packet pre-filtering and memory efficient technique [8]. This technique allows the Intrusion detection and prevention systems to have high accuracy rates and high performance numbers by utilizing a deep packet pre-filter and changing how it handles and processes memory and captured data. Anomaly detection methodologies are plagued with high rates of false positives and a new detection system for anomaly based methodology that strikes a balance between generalizations is proposed [9]. The proposed system balances the generalizations in anomaly detection methodologies and in doing so it achieves both a high accuracy rate and a low false positive rate. Combining the two most used methodologies in intrusion detection and prevention systems into a system that uses both anomaly and signature based detection methodologies produces a better detection system [10]. This combination of methodologies produces a better system by pre-processing the data with the anomaly detection engine and then passing the results to the signature based engine. This results in a very high accuracy rate and very low false positives. In a proposal for a new signature based intrusion detection and prevention system [11], the authors started by presenting the basic organization and implementations of intrusion detection and prevention systems.

III. IDPS Methodologies

There are many different methodologies used by IDPS to detect changes on the systems they monitor. These changes can be external attacks or misuse by internal personnel. Among the many methodologies, four stand out and are widely used. These are the signature based, anomaly based, Stateful protocol analysis based, and hybrid based. Most current IDPS systems use the hybrid methodology which the combination of other methodologies to offer better detection and prevention capabilities. All the methodologies use the same general model and the differences among them is mainly on how they process information they gather from the monitored environment to determine if a violation of the set policy has occurred. Fig. 1 shows a broad architecture of which these systems are based on. This architecture was developed by the Intrusion Detection Working Group and has four functional blocks, the Event blocks which are the event boxes that gathers events to from the monitored system and will be analyzed by other blocks, then the Database blocks which are the database boxes which stores the events from the Event blocks, then the Analysis blocks that processes the events and sends an alert, and final the Response blocks whose purpose is to respond to an intrusion and stop it [12].

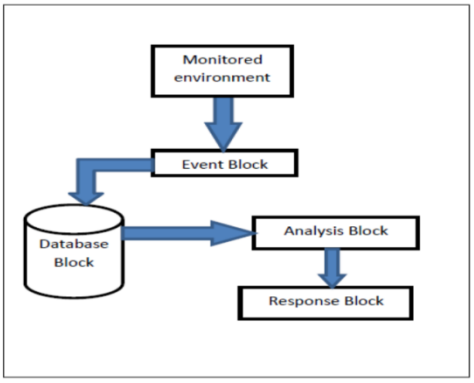

Fig. 1 General architecture for IDPS systems.

A. Anomaly Based Methodology

Anomaly based methodology works by comparing observed activity against a baseline profile. The baseline profile is the learned normal behaviour of the monitored system and is developed during the learning period were the IDPS learns the environment and develops a normal profile of the monitored system. This environment can be networks, users, systems and so on.

The profile can be fixed or dynamic. A fixed profile does not change once established while a dynamic profile changes as the systems been monitored evolves [13]. A dynamic profile adds extra over head to the system as the IDPS continues to update the profile which also opens it to evasion. An attacker can evade the IDPS that uses a dynamic profile by spreading the attack over a long time period. In doing so, her attack becomes part of the profile as the IDPS incorporates her changes into the profile as normal system changes. Using a predefined threshold any deviations that fall outside the threshold are reported as violations. A fixed profile is very effective at detecting new attacks since any change from normal behaviour is classified as an anomaly.

Anomaly based methodologies can detect zero-day attacks to environment without any updates to the system. Anomaly intrusion detection methodology uses three general techniques for detecting anomalies and these are the statistical anomaly detection, Knowledge/data-mining, and machine learning based [13].

The statistical anomaly techniques are used to build the two required profiles, one during the learning phase which is then used as the baseline profile and the current profile which is compared to the baseline profile and any differences that found a marked as anomalies depending on the threshold settings of the monitored environment [14]. The threshold must be tuned according to the requirements and behaviour of the environment being monitored for the systems to be effective.

The knowledge/data-mining technique is used to automate the way the technique monitor searches for anomalies and this process places a very high overheard on the system. The technique produces the most false positives and false negatives due to the high overhead that result from the complicated task of identifying and correctly categorizing observed events on the system [15]. The machine learning technique works by analyzing the system calls and it is the widely used technique [16].

The general architecture of an anomaly based IDPS system is shown in figure 2. The monitored environment is monitored by the detector that examines the observed events against the baseline profile. If the observed events match the baseline, no action is taken, but if it does not match the baseline profile and it is within the acceptable threshold range then the profile is updated. If the observed events do not match the baseline profile and falls outside the threshold range they are marked as an anomaly and alert is issued.

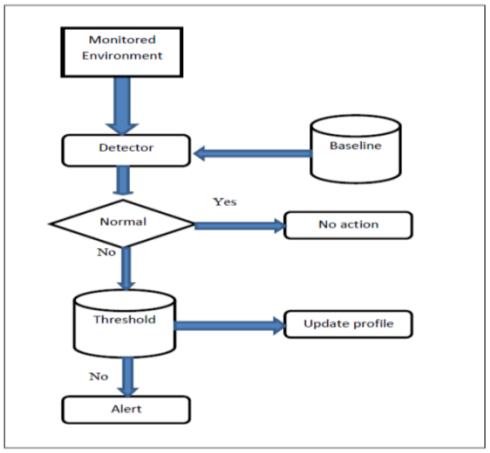

Fig. 2 Anomaly based methodology architecture

B. Signature Based Methodology

Signature based methodology works by comparing observed signatures to the signatures on file. This file can be database or a list of known attack signatures. Any signature observed on the monitored environment that matches the signatures on file is flagged as a violation of the security policy or as an attack. The signature based IDPS has little overhead since it does not inspect every activity or network traffic on the monitored environment. Instead it only searches for known signatures in the database or file. Unlike the anomaly based methodology, the signature based methodology system is easy to deploy since it does not need to learn the environment [16]. This methodology works by simply searching, inspecting, and comparing the contents of captured network packets for known threats signatures. It also compares behaviour signatures against allowed behaviour signatures. Signature based methodology also analyzes the systems calls for known threats payload [17]. Signature based methodology is very effective against know attacks/violations but it cannot detect new attacks until it is updated with new signatures. Signature based IDPS are easy to evade since they are based on known attacks and are depended on new signatures to be applied before they can detect new attacks [18]. Signature based detection systems can be easily bypassed by attackers who modify known attacks and target systems that have not been updated with new signatures that detect the modification. Signature based methodology requires significant resources to keep up with the potential infinite number of modifications to known threats. Signature based methodology is simpler to modify and improve since its performance is mainly based on the signatures or rules deployed [19].

The general architecture of a signature based methodology is shown in fig. 3. This architecture uses the detector to find and compare activity signatures found in the monitored environment to the known signatures in the signature database. If a match is found, an alert is issued and there is no match the detector does nothing.

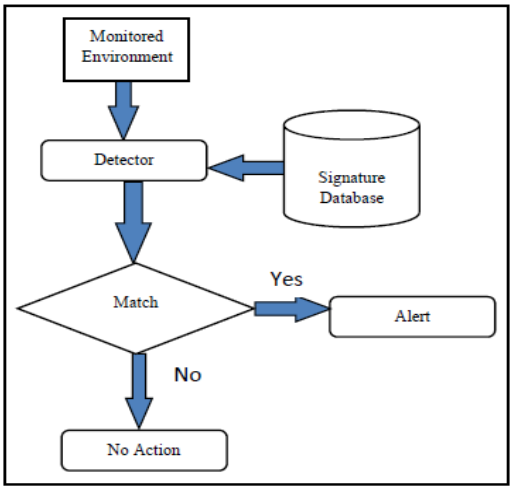

Fig. 3 Signature based methodology architecture

C. Stateful Protocol Analysis Based Methodology

The Stateful protocol analysis methodology works by comparing established profiles of how protocols should behave against the observed behaviour. The established protocol profiles are designed and established by vendors. Unlike the signature based methodology which only compares observed behaviour against a list, Stateful protocol analysis has a deep understanding of how the protocols and applications should interact/work. This deep understanding/analysis places a very high overhead on the systems [13]. Stateful protocol analysis blends and compliments other IDPS methodologies well which has led to rise of Hybrid methodologies [19]. Stateful protocol analysis's deep understanding of how protocol should behave is used as a base for developing IDPS that understand web traffic behaviour and are effective at protecting websites [19]. Although the Stateful protocol analysis has a deep understanding of the monitored protocols, it can be easily evaded by attacks that follow and stay within the acceptable behaviour of protocols. Stateful protocol analysis methodologies and techniques have slowly been adapted and integrated into other methodologies over the past decade. This has led to the decline of IDPS that utilize just Stateful protocol analysis methodology. The majority of the research on IDPS methodologies mainly concentrates on anomaly, signature, and hybrid methodologies which further reduce the viability of Stateful protocol analysis as a standalone IDPS methodology.

The general architecture of Stateful protocol analysis is shown in fig.4. This architecture is identical to that of the signature based methodology with one exception, instead of the signature database the Stateful protocol analysis has database of acceptable protocol behaviour.

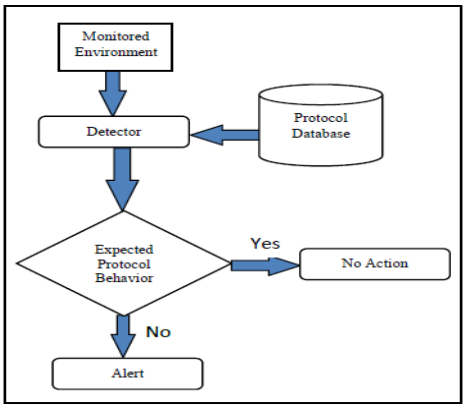

Fig.4 Stateful protocol analysis based methodology architecture

D. *Hybrid Based Methodology*

The hybrid based methodology works by combining two or more of the other methodologies. The result is a better methodology that takes advantage of the strengths of the combined methodologies. Prelude is one of the first hybrid IDS that offered a framework based on the Intrusion Detection Message Exchange Format (IDMEF) an IETF standard that allows different sensors to communicate[20]. In [21] Snort is modified by adding an anomaly based engine to its signature based engine to create a better detection and then the new hybrid systems is tested against the regular Snort using same test data. The hybrid system detected more intrusions than the regular one. A hybrid intrusion detection system of cluster-based wireless sensors networks was proposed that worked by breaking the detection into two, first it used anomaly based model to filter the data and then it used signature based model to detect intrusion attempts. Another model for a hybrid methodology was proposed based on how the human immune system works [22]. The proposed system is "based on the framework of the human immune system, that uses a hybrid architecture which applies both anomaly and misuse detection approaches" [22]. A general over view of a hybrid based methodology is shown in Fig. 5 three other methodologies are combined. The monitored environment is analyzed by first methodology and passed to the next and then the last one. This produces a better system.

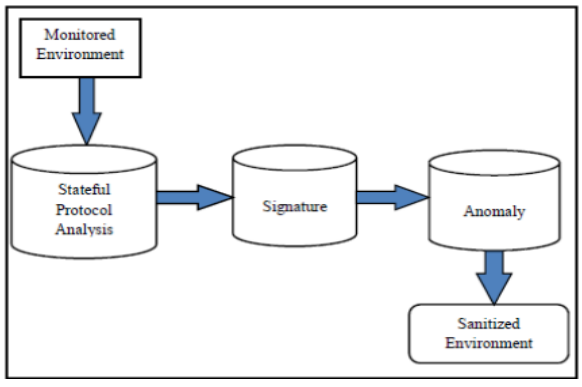

Fig. 5- Hybrid based methodology architecture

IV. Evaluations of Methodologies

This section offers a description of ways for evaluating intrusion detection and prevention system (IDPS) methodologies and the systems that are based on these methodologies. Table 1 can be used to evaluate any intrusion detection and prevention system (IDPS) whether it uses one of the three main methodologies or a combination of the two or more of the other methodologies.

TABLE 1.
Parameters for evaluating IDPS methodologies.

	Anomaly	**Signature**	**Stateful Protocol Analysis**	**Hybrid**
Resistance to Evasion	Medium	Low	Low	High
High accuracy rate	Medium	Medium	Medium	High
Market Share	Medium	High	Medium	Medium
Scalability	Medium	High	High	Medium
Maturity Level	High	High	High	Medium
Overhead on Monitored System	Medium	Low	Low	Medium
Maintenance	Low	Medium	Medium	Medium
Performance	Medium	High	High	Medium
Easy to Configure	No	Yes	Yes	No
Easy to Use	Medium	Low	Low	Low
Protection against New Attacks	High	Low	Medium	High
False Positives	High	Low	Low	Low
False Negatives	High	Medium	Medium	Low

A. *Resistance to evasion*

The intrusion detection and prevention system (IDPS) should be able to detect evasion attempts and stop them. These attempts are more common with the signature and stateful protocol analysis based intrusion detection and prevention system (IDPS) due their dependence on signatures. Anomaly based intrusion detection and prevention system (IDPS) have better resistance to evasion, but the hybrid based system offers the best resistance to evasion attempts due to the combination of other methodologies.

B. *High Accuracy Rate*

An IDPS should have a high accuracy rate when detecting and analyzing possible threats. The signature based methodology has a high accuracy rate on known threats but its overall rate is lower that the anomaly based methodology

which can detect previously known threats. The hybrid based methodology offers the best accuracy rates.

C. Market Share

Market share is the measure of the methodology's dominance in the deployed systems. The signature based methodology far outweighs the other three methodologies, followed by Stateful protocol analysis. The anomaly and hybrid based methodology are the bottom but their adaption is growing much faster and will soon surpass the first two methodologies.

D. Scalability

Scalability is the ability of an IDPS to scale and grow with environment once deployed. The signature and Stateful protocol analysis based methodologies are easy to scale since they are based on signatures that can be easily scaled. A hybrid based methodology can be easily scale depending on the underlying methodologies. The anomaly based methodology is the least scalable methodology due the time it requires to learn and build its baseline profiles.

E. Resistance to evasion

The intrusion detection and prevention system (IDPS) should be able to detect evasion attempts and stop them. These attempts are more common with the signature and stateful protocol analysis based intrusion detection and prevention system (IDPS) due their dependence on signatures. Anomaly based intrusion detection and prevention system (IDPS) have better resistance to evasion, but the hybrid based system offers the best resistance to evasion attempts due to the combination of other methodologies.

F. High Accuracy Rate

An IDPS should have a high accuracy rate when detecting and analyzing possible threats. The signature based methodology has a high accuracy rate on known threats but its overall rate is lower that the anomaly based methodology which can detect previously known threats. The hybrid based methodology offers the best accuracy rates.

G. Market Share

Market share is the measure of the methodology's dominance in the deployed systems. The signature based methodology far outweighs the other three methodologies, followed by Stateful protocol analysis. The anomaly and hybrid based methodology are the bottom but their adaption is growing much faster and will soon surpass the first two methodologies.

H. Scalability

Scalability is the ability of an IDPS to scale and grow with environment once deployed. The signature and Stateful protocol analysis based methodologies are easy to scale since they are based on signatures that can be easily scaled. A hybrid based methodology can be easily scale depending on the underlying methodologies. The anomaly based methodology is the least scalable methodology due the time it requires to learn and build its baseline profiles.

I. Maturity Level

Maturity level looks at how long a methodology has been around and how stable it is. The signature based methodology is the most mature, followed by the Stateful protocol analysis and anomaly based methodologies. The hybrid methodology is at the bottom of this list, but it is growing at a much faster than the others.

J. Overhead on Monitored System

The intrusion detection and prevention system (IDPS) should not place a lot of overhead on the monitored systems; it should work without affecting the performance of monitored systems. Signature and Stateful protocol analysis places the least overhead on the monitored systems. The hybrid based methodology can place a high overhead burden on the monitored system depending on the combined methodologies. The anomaly based methodology places the most overhead on the monitored system.

K. Maintenance

The anomaly based methodology requires the least amount of maintenance since it does not require updates to detect new threats. The other three methodologies require constant signature updates in order to keep up with new threats. This constant updating of signatures adds to the resources required to maintain the methodology.

L. Performance

The intrusion detection and prevention system should be able to perform at peak performance under all condition on the monitored system without becoming a bottle neck or reducing its efficiency. The signature and Stateful protocol analysis based methodologies offers better performance than anomaly and hybrid based methodologies since they only check for well-defined signatures which do not require as much resources.

M. Easy to Configure

The intrusion detection and prevention system (IDPS) should be easy to install and integrate with other security tools already in the environment. The signature and the Stateful protocol analysis methodologies are easier to install and configure. They do not require as much time to tune since they use signatures that can be updated automatically in some cases. The anomaly and the hybrid depending on the combined methodologies require more time to configure, learn, and tune the environment.

N. Easy to Use

The intrusion detection and prevention system should be easy to use and understand. This means it produces less false positives and false negatives which makes it easier to analyze and understand the alerts. The signature and the Stateful protocol analysis methodologies are easier to use since they produce fewer alerts. The hybrid based methodology can be easier than the anomaly depending on its underlying methodologies. The anomaly requires more resources to manage the high volumes of alerts it produces.

O. Protection against New Attacks

The intrusion detection and prevention system should be able to detect new threats. The anomaly based methodology does detect new attacks without any updates unlike the signature and Stateful protocol analysis that require their signatures to be updated before they can detect previously unknown threats. The hybrid based methodology can detect new threats if one of the underlying methodologies is anomaly based.

P. False Positives

False positives happen as a result of a methodology misclassifying a non-threat event as a threat. The anomaly based methodology is plagued by false positives. The signature and Stateful protocol analysis based methodologies produces the least number of false positives. The hybrid based methodology's level of false positives is low if anomaly based is not part of its underlying methodologies.

Q. False Negatives

False negatives are a result on a methodology classifying threats as non-threats. The anomaly based methodology produces the most false negatives when compared with signature and the Stateful protocol analysis based methodologies. The hybrid based methodology produces less false negatives if it does not use anomaly based methodology as one of its underlying methodologies.

The above criterion encompasses all possible parameters to evaluate IDPS system. We believe that using these, we can compare IDPS systems in a more effective manner.

V. CONCLUSION

This paper presented the four main methodologies that are used in intrusion detection and prevention systems. These methodologies are anomaly based, signature based, stateful protocol analysis, and hybrid based. Although the anomaly based methodology has the edge on the other two on detecting new threats without any updates or input for the users, most current IDPS on the market utilizes a combination of the four main methodologies. The paper also offered ways to easily compare and evaluate IDPS methodologies that are used by IDPS products on the market. Our future research includes experiments using some commercial and open source tools using our evaluation criteria.

VI. REFERENCES

[1] Animesh Patcha, Jung-Min Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends, Computer Networks," The International Journal of Computer and Telecommunications Networking, Vol.51, No.12, August, 2007, pp.3448-3470.

[2] Rebecca Bace, "An introduction to intrusion detection and assessment for system and network security management." ICSA Intrusion Detection Systems Consortium Technical Report, 1999.

[3] James P. Anderson, "Computer security threat monitoring and surveillance," James P. Anderson Co., Fort Washington, Pennsylvania, technical Report, April 1980.

[4] Tarek S. Sobh, "Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art," Computer Standards & Interfaces 28 , 2006, pp. 670– 694.

[5] Fredrik.Valeur, Giovanni Vigna, Christopher Kruegel, Richard A. Kemmerer, "A comprehensive approach to intrusion detection alert correlation," IEEE Transactions on Dependable and Secure Computing, Vol. 1, NO. 3, 2004.

[6] Shelly X. Wu, Wolfgang Banzhaf, "The use of computational intelligence in intrusion detection systems: A review," Applied Soft Computing Journal 10, 2010, pp. 1-35.

[7] Xuan D. Hoang, Jiankun Hu, Peter Bertok, "A program-based anomaly intrusion detection scheme using multiple detection engines and fuzzy inference," Journal of Net- work and Computer Applications 32, 2009, pp. 1219–1228.

[8] Elshoush H. Tagelsir, Izzeldin M. Osman, "Alert correlation in collaborative intelligent intrusion detection systems—A survey." Applied Soft Computing 11, 2011, pp. 4349-4365.

[9] Shanbhag, Shashank, Tilman Wolf. "Accurate anomaly detection through parallelism." IEEE Network 23.1, 2009, pp. 22-28.

[10] James Cannady, Jay Harrell, "A comparative analysis of current Intrusion detection technologies," Houston 1996, Proc. 4th Technology for Information Security Conference.

[11] Bejtlich, Richard, "The Tao of Network Security Monitoring: Beyond Intrusion Detection," Addison-Wesley, 2004.

[12] Terry Brugger, "KDD cup'99 dataset (network intrusion) considered harmful," http://www.kdnuggets.com/news/2007/n18/4i.html, 2007.

[13] Karen Scarfone and Peter Mell, "Guide to Intrusion Detection and PreventionSystems(IDPS)," http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf, 2007.

[14] Pedro Garcı´a-Teodoroa, Jesus E. Dı´az-Verdejoa, Gabriel .Macia-Ferna´ndeza, Enrique Va´zquezb, "Anomaly-based network intrusion detection: Techniques, systems and challenge," Computers Security 28.1-2, 2009, pp. 18-28.

[15] Chih-Fong Tsai, YuFeng Hsu, Chia-Ying Lin, W.Y.Lin, "Intrusion detection by machine learning: A review," Expert Systems with Applications, Vol 36, No.10. December 2009, pp.11994-12000.

[16] Dorothy, Denning. "An intrusion-detection model," IEEE Transactions on Software Engineering, Vol. SE-13, No.2. February, 1987.

[17] Alfonso Valdes, Keith Skinner, "Probabilistic alert correlation," 4th International Symposium on Recent Advances in Intrusion Detection (RAID2001), 2001, pp.54–68.

[18] Indraneel Mukhopadhyay, Mohuya Chakraborty and Satyajit Chakrabarti, "A Comparative Study of Related Technologies of Intrusion Detection & Prevention Systems," Journal of Information Security, Vol. 2 No. 1, pp. 28-38.

[19] Justin Lee, Stuart Moskovics, Lucas Silacci, "A Survey of Intrusion Detection Analysis Methods," CSE 221, University of California, San Diego, Spring 1999.

[20] Ning Weng, Luke Vespa, Benfano Soewito, "Deep packet pre-filtering and finite state encoding for adaptive intrusion detection system," Computer Networks, Vol. 55, 2011, pp. 1648–1661.

[21] Ali M. Aydın, Halim A. Zaim, Gokhan K. Ceylan, "A hybrid intrusion detection system design for computer network security," Computers and Electrical Engineering, Vol. 35, 2009, pp. 517–526.

[22] Kenneth L. Ingham, Anil Somayaji, "A Methodology for Designing Accurate Anomaly Detection Systems," 4th international IFIPACM Latin American conference on Networking LANC 07, 2007, pp.139.