Host-based Intrusion Detection and Prevention System (HIDPS)

Kopelo Letou
Dept. of CS & IT, Assam Don Bosco University, Assam.

Dhruwajita Devi
Dept. of CS & IT, Assam Don Bosco University, Assam.

Y. Jayanta Singh
Dept. of CS & IT, Assam Don Bosco University, Assam.

ABSTRACT
This paper is deliberated to provide a model for Host-based Intrusion Detection and Prevention (HIDPS). HIDPS is increasingly becoming important to protect the host computer systems and its own network activities. HIDPS with intelligence is integrated into the computer systems to detect the intruder attacks activities, malicious Behaviour, application anomalies and protect the Information Systems from intruders and report the events to the HIDPS System Administrator. HIDPS is composed of software to monitor and analyze events occurring in the computer systems and information systems and to identify and stop potentially harmful incidents to the Systems. In this context, computer security is an essential property. HIDPS is one of the promising research areas of computer security as most of the security violations in systems occur due to malicious code and intruder activities being able to penetrate to the system barriers. Malicious code and intruder activities affect the computer systems by compromising integrity, confidentiality and availability of resources. It also changes the system Behaviour and extracts the system's vital informations. This paper reviewed and compared the related various research papers on HIDPS to provide a suitable norm on HIDPS at two levels of intrusion detection and prevention i.e., user level and kernel level along with two phases of intrusion detection engines- Misuse and Anomaly detections for the best-fit system to any unique host computer systems.

General Terms
Host-based Intrusion Detection and Prevention System.

Keywords
Misuse detection, Anomaly detection, Support Vector Machine (SVM) algorithm, C4.5 Algorithm.

1. INTRODUCTION
Using computer Systems in all over the world has made computer security an international priority with Intrusion Detection and Prevention System (IDPS). It is not feasible to build a secure system without vulnerabilities, so intrusion detection and prevention system becomes a vital and essential area of research in the near future. James P Alderson [1] gave the first concept of intrusion detection. First, he defined threat as the deliberate unauthorized access, manipulating the system and rendering the system both unreliable and unusable. He defined attack as 'to carry out the threats'. Audit trials are used to test whether the system observations is normal or abnormal. Dorothy Denning [2] in 1987 first introduced an Intrusion-Detection System Model. The Intrusion-Detection System Model was to detect penetrations and intrusions either from the insiders or from the outsiders. An Intrusion Detection System (IDS) [3] is a software that automates the intrusion detection process. Intrusion Detection and Prevention System [4] identifies possible incidents, log information about them, attempt to stop them and produce report for security administrators. The main aim of Intrusion Detection and Prevention System is to protect the availability, confidentiality and integrity of critical information systems and computer systems by identifying malicious activities, intrusions and attacks from insiders and outsiders and to stop all possible incidents - abuse of computer resources and systems.

Table 1. Performance comparison of testing of attacks Normal, Probe, DoS, U2R and R2L classifications [5].

Classifiers	SVM	ANN	MARS	Ensemble of ANN, SVM and MARS
Accuracy (%)	98.85	97.09	92.75	99.82

Abbreviations:- SVM: Support vector machine. ANN: Artificial Neural Network training algorithm, MARS: Multivariate Adaptive Regression Splines. In Table 1 shows that SVM is better in detection malicious activities than ANN. In previous studies done by Sushil Kumar Chaturvedi et al [6, 7, 8, 9] it was found that C4.5 is better in detection malicious activities and false alarm than SVM in KDD '99 in both training and testing dataset. This paper categorized the types of IDPS, types of HIDPS, levels of HIDPS and described the best possible algorithms for Misuse detection technique (supervised algorithm) and Anomaly detection technique (unsupervised algorithm) respectively. Intrusions detection training data and test data have two phases to pass through; first is misuse detection engine and then anomaly detection engine.

2. INTRUSION DETECTION AND PREVENTION SYSTEMS
Classification [3,10,11] of Intrusion Detection and Prevention Systems is shown below in Fig 1. IDPS systems can be categorized into i) types of intruders, ii) types of intrusions, iii) detection techniques and iv) types of intrusion detection and prevention. Intruder is an attempt to gain unauthorized access to the computer systems. External intruders are unauthorized users of the computer system and internal intruders have permission to access the system but not all portions of it. Intrusion is the activity that attempt to compromise the integrity, confidentiality and availability of a resource. Types of intrusions are:

1. Attempted break-ins are detected by a typical Behaviour profile or violations of security constraints.
2. Masquerade attacks are also detected by a typical Behaviour profile or violations of security constraints.
3. Penetrations of the security control system are detected by monitoring for specific patterns of activity.
4. Leakage is detected by typical use of system resources.

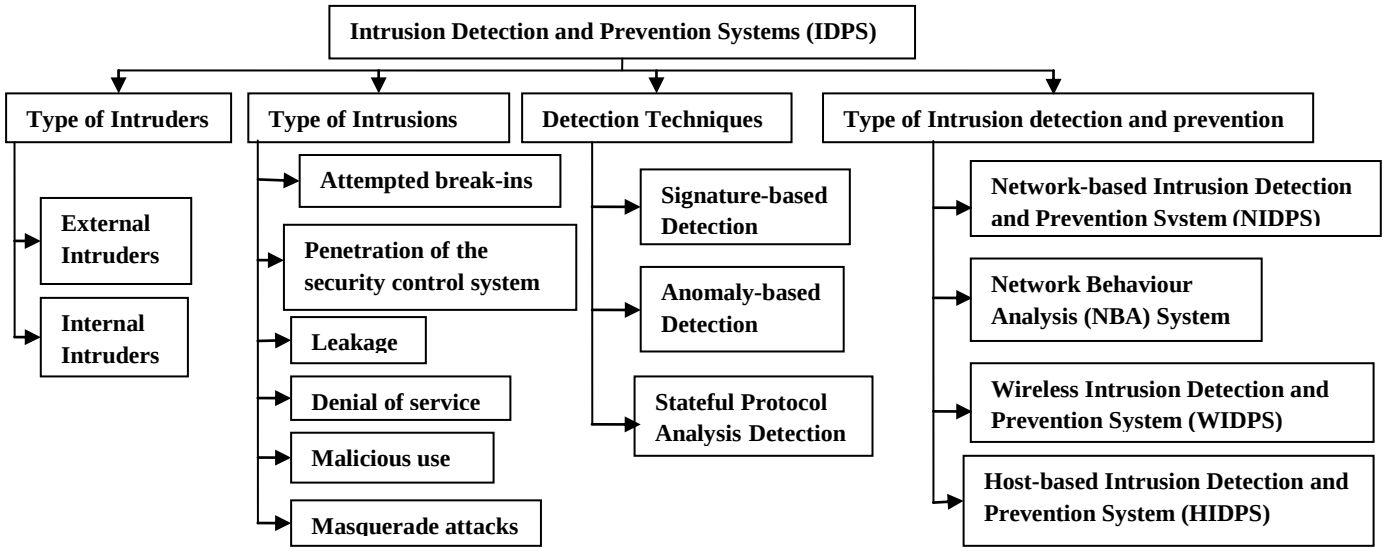

Fig 1: Classification of intrusion detection and prevention systems

5. Denial of service is detected by typical use of system resources.
6. Malicious use is detected by typical Behaviour profiles, violations of security constraints or use of special privileges.

2.1 Types of IDPS

An Intrusion Detection and Prevention System (IDPS) is an automated system design to detect and prevent malicious attacks on computer systems through the Internet. Intrusion Detection and Prevention Systems can be classified into four different types:-

1. Network-based Intrusion Detection and Prevention System (NIDPS): monitors the entire network for suspicious traffic by analyzing protocol activity.
2. Wireless Intrusion Detection and Prevention Systems (WIDPS): monitors a wireless network for suspicious traffic by analyzing wireless networking protocols.
3. Network Behaviour Analysis (NBA): examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations.
4. Host-based Intrusion Detection and Prevention System (HIDPS): an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.

In Table 2, we have shown the comparison the types IDPS technology, types of malicious detected, technology strengths and technology limitations.

2.2 Sub-systems of HIDPS

Host-based Intrusion Detection and Prevention System is used to check and maintain securely host's system and its network activities if a system has been attacked or not. If there is any such attack to the host's system or abnormality of the host's system then the HIDPS will alert and warn to the system administrator. Host-based Intrusion Detection and Prevention Systems [12] can be divided into four sub-systems:- Files system monitoring, Log file analysis, Connection analysis and Kernel-based intrusion detection and prevention as shown in Fig 2.

2.2.1Files system monitoring

HIDPS utilizes files system monitoring regularly and compares files that contain information on a machine with previously gathered files, about the size, editing of the file and user's file. In this way if an attacker gains access to host's computer and tries to edit files, then this edit changes can be detected and prevented.

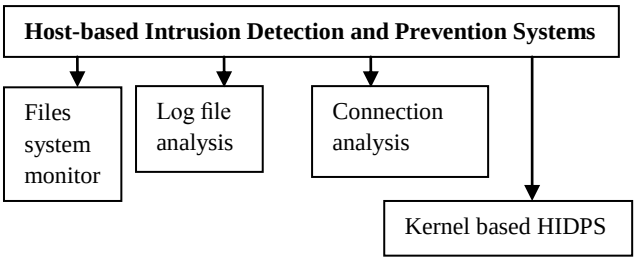

Fig 2. Sub-systems of Host-based Intrusion Detection and Prevention System

2.2.2 Log file analysis

The activities of the computer is maintained in a file. The log file is checked to determine if there is abnormal data and activities are then logged. The events are logged in a log file like change in login and password information; if these events were changed and detected, then the HIDPS can alert to the system administrators about any danger and harm to the system.

2.2.3 Connection analysis

Connection Analysis determines the network TCP/IP packets activity. Connection analysis in HIDPS implementations detect and prevent the incoming network intrusion activities and disorder sequence of TCP packets to the host's computer system.

2.2.4 Kernel-based HIDPS

A kernel based HIDPS is an extra feature to enhance security of a kernel to have the kernel itself detect and prevent malicious activities and abnormal Behaviours.

2.3 Levels of HIDPS

There are two levels of intrusion detection systems:

Table 2. Comparison of IDPS Technology Types [3, 13, 14, 15, 16, 17].

Types of IDPS Technology	Types of Malicious activities Detected	Technology Strengths	Technology limitations
Network-based Intrusion Detection and Prevention System (NIDPS).	Network, transport, and application of TCP/IP layer activity .	• Able to analyze the traffic of entire network by analyzing application protocols activities and take appropriate actions. • Identify intrusions by monitoring network traffic. • Need to place only on underlying network. • Can monitor multiple systems and networks at a time. • Can prevent network attacks before it reaches to the targeted systems. • Platform-independent and relatively easy to deploy.	• Cannot monitor wireless protocols. • High false positive and false negative rates. • Cannot detect attacks within encrypted traffic. • No full analysis support under high loads. • It helps only for detecting external intrusions. • Difficult to detect network intrusions in virtual network, HTTP over SSL. • Can overwhelmed by very high traffic volumes, may not be able to process all packet • Can't detect encrypted date & can miss attack. • Switches that provide monitoring or scanning port can at least partially mitigate. • Cannot determine with certainty whether an attack was successful.
Wireless Intrusion Detection & Prevention System (WIDPS).	Wireless protocol activity; unauthorized wireless local area networks in use.	• Only WIDPS can analysis the traffic of Wireless network by analyzing wireless protocol activities and take appropriate actions.	• Cannot monitor application layer, transport layer and network layer protocol activities. • Cannot avoid evasion techniques. • Cannot compensate for insecure wireless protocols. • Insecure WLAN and devices, DoS attacks.
Network Behaviour Analysis (NBA) System.	Network, transport, & application TCP/IP layer Distributed denial of service.	• Better detecting reconnaissance scanning. • DoS attacks, and at reconstructing major malware infections. • Can examines traffic to identify threats that generate unusual traffic flow, such as DDOS attack, malware and Policy Violation.	• Delay in detection attacks, caused by transferring flow data to NBA in batches, but not in real time.
Host-based Intrusion Detection and Prevention System (HIDPS).	Host application & operating system (OS) activity; Its own network, TCP/IP layer activity.	• Can analyze activity that transferred in end-to-end encrypted communications. • Identify intrusions within that host by monitoring host's file system, file access, system calls or network events. • No extra hardware required. • Can prevent system level attacks. • Can monitors events local to a host and detect attacks that a NIDPS cannot. • The hosts load can be distributed over the network. • Interacts between users & servers/applications allow to trace misuse to a known individual.	• More challenging in detection accuracy due to a lack of context knowledge. • Delays in alert generation and centralized reporting. • Consume host resources, affect host system efficiency. • Can Conflict with existing security controls. • Need to install on each machine (VMs,hypervisor or host machine). • It can monitor attacks only on host where it isdeployed. • An OS-specific need to installed, configured & maintained on each host to be protected.

Application level intrusion detection system and Operating system level intrusion detection system [18].Fig 3 shows the levels of HIDPS along with its sub-systems and its detection techniques.

Level-I (User Space)	**HIDPS Sub-types**	**Detection Techniques:-**
Application-Level Intrusion Detection And Prevention	File System Monitors. Log File Analyzers Connection Analyzers	Misuse-Based Approaches Anomaly-Based Approaches Specification-based approaches

Level-II (Kernel Space) Kernel–Level Intrusion Detection and Prevention	**HIDPS Sub-type** Kernel based	**Detection Techniques:-** Misuse-Based Approaches Anomaly-Based Approaches Specification-based approaches

Fig 3. HIDPS with its two levels of Detection, Sub-types, and Detection Techniques.

Table 3 Advantages and disadvantages of intrusion detection techniques [10, 13, 14, 15, 17, 22, 23].

Signature-based (knowledge-based)	Anomaly-based (Behaviour-based)	Stateful analysis
Advantages :- • Simplest and effective method to detect known attacks. • Detail contextual analysis and identifies attacks by matching captured signatures with predefine in knowledge base. • High detection accuracy for known attacks. • Low computational cost. • Very low false alarm rate. • Can track security problems on the systems, initiating incident handling procedures. **Disadvantages :-** • Cannot detect Novel attacks, unknown attacks, evasion attacks, & variants of known attacks. • Little understanding to states & protocols. • Hard to keep signatures/patterns up to date. • Time consuming to maintain the knowledge. • High false alarm rate for unknown attacks etc • Detect only the attacks for which they are trained. • Need updates with signatures attacks.	**Advantages :-** • Ability to detect novel attacks or unknown attacks. • Can detect new & unforeseen vulnerabilities. • Less dependent on OS & Facilitate detections of privilege abuse. • Uses statistical test on collected Behaviour to identify intrusion. • Can lower the false alarm rate for unknown attacks. • No need for priori knowledge of security flaws. • Can turn to define signatures for misuse detectors. **Disadvantages :-** • Weak profiles accuracy due to observed events being constantly changed. • Unavailable during rebuilding of Behaviour profiles. • More time is required to identify attacks. • Detection accuracy is based on amount of collected Behaviour/features. • Well-known attacks may not be detected, if they fit established of user. • Easy to defeat i.e., changing the profile slowly with time. • High false alarm rates due to the fixed user profile distribution • High false negative rate due to broadly trained detection algorithm. • Less effective in dynamic Environment. • Need large "training sets" to characterize normal patterns.	**Advantages :-** • Know and trace the protocol states. • Distinguish unexpected sequences of commands. **Disadvantages :-** • Resource consuming to protocol state tracing and examination. • Unable to inspect attacks looking like benign protocol Behaviours. • Might incompatible to dedicated OSs/APs.

2.3.1 Application Level Intrusion Detection and Prevention System

Host-based IDPS utilize the audit data, Incoming traffic, logs produced by the Applications to detect malicious activities, to prevent intruder's activities and to trace the attacks. It takes decision either to deny or permit the applications to execute and process base on the event logs, data and normal Behaviour kept in the Knowledge based database and Knowledge Behaviour database.

2.3.2 Operating System Level Intrusion Detection and Prevention System

Host-based IDPS utilizes the audit data, incoming traffic, logs generated by the operating system to detect attacks, to prevent attacks and to trace the attacks. It is used to take the decision either to permit or deny the system calls based on the events, logs, data and normal Behaviour kept in the Knowledge based database and Knowledge Behaviour base database.

2.4 Intrusion Detection Techniques

The three techniques of intrusion detections are Misuse-based, Anomaly-based, and Stateful protocol analysis. Their comparison of advantages and disadvantages is shown in Table 3. The proposed Host-based Intrusion Detection and Prevention System Model used Misuse-based and Anomaly-based techniques.

2.4.1 Misuse Detection

Misuse Detection known as Signature Detection [19, 20] or Knowledge-based Detection is used to detect known attack patterns and intruders who exploit known software and system vulnerabilities. Misuse detection techniques use one or hybrid of three different approaches: static, dynamic, or hybrid. Static approach utilizes the structural and syntax features of the applications/programs and static observations and information to detect the intrusions activities and its code. Static analysis attempts to determine intrusion activities of the program and its code before the application is executed. Dynamic analysis utilizes the structural and syntax features of the applications/programs and runtime observations and information to detect the intrusions activities and its code. Dynamic analysis attempts to determine the abnormal Behaviours and activities of the application during or after application execution. Hybrid approach is the integration of the static approach and dynamic approach. This hybrid analysis uses the observations and information for detection of malicious code and attacks activities. Detection [13] have knowledge base database contain specific known attacks patterns for exploiting the systems created by intruders. This techniques search for known attacks patterns represented by signatures saved in the knowledge base database and if attack is found, then it sends a signal alarm to the system Administrator [21].

2.4.2 Behaviour-based Detection

Behaviour-based Detection also known as Statistical Anomaly Detection [19, 20] is used to detect the intrusions, malicious activities and penetration attacks from established user

profile/base-line which is the normal and expected Behaviour of the system or the user's activities. Anomaly Detection techniques used one or hybrid of three different approaches: static, dynamic, or hybrid. Static approach utilizes the structural and syntax features of the applications/programs, and static observations and information to detect the intrusions activities and its code. Static analysis attempts to determine intrusion activities of the program and its code before the application is executed. Dynamic analysis utilizes the structural and syntax features of the applications/programs and runtime observations and information to detect the intrusions activities and its code. Dynamic analysis attempts to determine the abnormal Behaviours and activities of the application during or after application execution. Hybrid approach is the integration of the static approach and dynamic approach. This hybrid analysis used the observations and information for detection of malicious code and attacks activities. The new gathered data measure with the created user profile. When the Behaviour of the data is above threshold and or deviated from the normal or expected Behaviour then the alarm signal is issued. Behaviour-based Detection [13] have knowledge base database, which contain profiles of the monitored activities. Many types of profiles are kept in the anomaly database detection. User's profile contains typical sessions. Some other profiles are resource profiles, which are used for monitoring the system, applications, ports and others, executable profile monitoring the files, printers and others. The inputs to the Anomaly Detection Method are from the audit records generated from the operating system.

3. Proposed Host-based Intrusion Detection and Prevention System Model

HIDPS monitors various types of host events and activities to detect any malicious code and intrusion activities in the host systems such as Desktop, Mail Servers, DNS Servers, web servers, database servers, etc. When malicious code and unexpected Behaviours such as buffer overflow, accessing file systems are detected then it is prevented from execution by HIDPS. HIDPS detects intrusion for host system by collecting information such as file systems used, network events, system calls, etc. It detect and prevent the intrusions when found change the host kernel, file systems and Behaviour of the programs. The proposed Host-based Intrusion Detection and Prevention System Model is shown in Fig 4. HIDPS components [13] are Data Pre-processing, Feature extraction, Selection of Features, Misuse Detection Engine, Anomaly Detection Engine, Knowledge-based Database, Behaviour-based Database, Counter Measure, Launch Action, and System Administrator.

Components of HIDPS : -

1. Data Pre-Processing – datas are filtered and segmentation of data is done.
2. Features Extraction – decomposition of packets.
3. Selection of Features – features vector are selected as input to the machine learning algorithms.
4. Misuse Detection Engine – The algorithm processing the input of the data to search and match for the previous known attacks i.e., signature, events and alerts.
5. Anomaly Detection Engine - The algorithm processing the input of the data to search and match with user's defined profile for a normal Behaviour, events and alerts of the systems.
6. Knowledge-based Database – The types of previous known attacks and misuse attacks, events and alerts are kept and maintained in the database, which is required by the Misuse Detection Engine.
7. Behaviour-based Database – The types of Normal Behaviour / data, events and alerts are kept and maintained in the database which is needed by the Anomaly Detection Engine.
8. Counter Measure – Reaction to the detected attacks by blocking and preventing the detected attacks.
9. Launch Action – Displays Warning, Generates Report of events produced by the system and Tracing the Attacks/Intruders activities.
10. System Administrator – (S)He will takes the appropriate action based on the Display Warning , Report Generated and Tracing the Attacks/Intruders activities.

3.1 Algorithm for Misuse detection

C4.5 Decision Tree (DT) algorithm is a supervised learning algorithm approach, which uses divide and conquer strategy. Attributes in DT are nodes and each leaf node represents a classification. C4.5 is an algorithm used to generate decision trees and used for classification. Decision tree is built in C4.5 from a collection of training data and testing data as ID3. C4.5 [9],[24] Algorithm:

Input: an attribute-valued dataset D (after apply Dimensionality reduction method PCA)
Output: a decision tree
1: Tree = {}
2: if D is "pure" OR other stopping criteria met then
3: terminate
4: end if
5: for all attribute a € D do
6: Compute information-theoretic criteria if we split on a
7: end for
8: a_{best} = Best attribute according to above computed criteria
9: Tree = Create a decision node that tests abest in the root
10: D_v = Induced sub-datasets from D based on abest
11: for all Dv do
12: $Tree_v = C4.5(D_v)$
13: Attach $Tree_v$ to the corresponding branch of Tree
14: end for
15: return Tree.

3.2 Algorithm for Anomaly detection.

Support vector machine (SVM) is used for unsupervised learning. SVM algorithm is used for Anomaly detection. SVM handles binary class classification problems. SVM – Classifier is used to test whether the data is normal or attack data. SVM polynomial kernel functions performs well in most of the datasets.

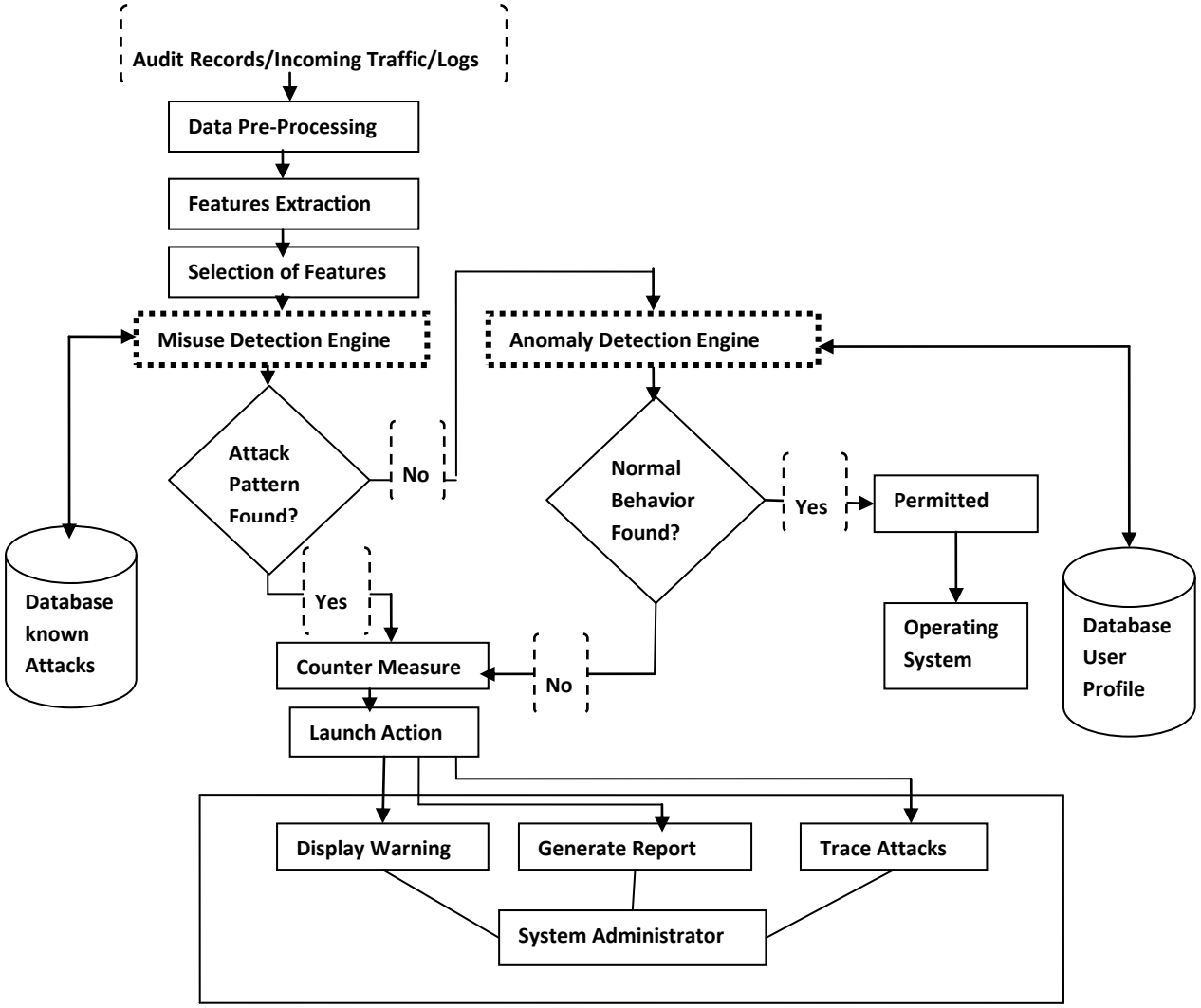

Fig 4: Proposed Host-based Intrusion Detection and Prevention System Model

The SVM algorithm [25] is as shown in Fig.5.

Support vector machine

Problem def:

For a classification problem, we try to estimate a function $f: \Re^n \rightarrow \{\pm\}$ using training data. So, let us denote two classes – A and B. The class A with x∈ A, y=1 and the class B with x∈B, y= -1 $(x_i, y_j) \in \Re^n \times \{\pm\}$. If the training data are linearly separable then there exists a pair (w,b)$\in \Re^n \times R$ such that $y(w^t x+b) \geq 1$, for all x∈ A∪B.

1. SVM belongs to the type of maximal margin classifier, in which the classification problem can be represented as an optimization problem

$$\underset{w,b}{Minimize}\ \phi(w) = \frac{1}{2}\|w\|^2 \qquad s.t.\ y(w^t x+b) \geq 1$$

2. The dual of the optimization problem: find multipliers λ_i which maximize

$$W(\Lambda)=\sum_{i=1}^{l} \lambda_i - \frac{1}{2}\|w\|^2 = \sum_{i=1}^{l} \lambda_i - \frac{1}{2}\sum_{i=1}^{l}\sum_{j=1}^{l} \lambda_i \lambda_j\ y_i\ y_j X_i^t X_j\ ,$$

and by the Karush-Kuhn-Tuker (KKT) complementary conditions

$$\lambda_i [\ y_i\ (w^t\ X_i + b) - 1] = 0, \qquad i=1,\ldots..,l$$

Fig. 5: SVM algorithm

4. FINDINGS

The proposed model will securely protect the host computer systems and its own network activities from intrusions, attacks of DoS, probe, R2L and U2R by detection and prevention. The audit trials data and logs generated by the applications and operating system is used to detect the type of intrusions and block the intruder's activities and to trace the origin of the attacks. HIDPS uses both the technology of Intrusion Detection System and Intrusion Prevention System. HIDPS uses C4.5 algorithm which is considered as the best and most suitable algorithm for signature detection technique. Support vector machine algorithm is considered as the best and most suitable algorithm for anomaly detection technique. HIDPS integrates the Application level Intrusion Detection and Prevention, and Kernel level Intrusion Detection and Prevention for detecting and preventing intrusive activities, malicious Behaviours, and to trace the origin of the attacks. HIDPS used two gates of intrusion detection engines to check and decide if the programs/applications and its code that reside within the systems and that come from external source is malicious or benign.

5. CONCLUSIONS

Firstly, we have surveyed the latest up-to-date technology trend on HIDPS and then selected the best intrusions detection techniques and algorithms for building the proposed model

expecting high promising security, performance and accuracy. The field of HIDPS is intensive; recent research areas offer a hundred percent security on computer systems and Information Systems that can detect and prevent all types of intrusions and malicious activities in real time, creating no false alarms and without any human intervention. This HIDPS chooses the best algorithm individual for Misuse detection is C4.5 Decision tree algorithm and Anomaly detection techniques is Support vector machine algorithm respectively, and intrusions detection test data have to pass through two phases i.e., first misuse detection engine and then anomaly detection engine. Any malicious activities and abnormal Behaviours of internal or external intrusions and attacks can be detected and prevented from the computer systems by HIDPS.

6. ACKNOWLEDGMENTS

We are thankful to Mr. Jahid Ahmed, research Scholar of Department of Computer Science & IT of Assam Don Bosco University for sharing us his valuable knowledge in this research on Host-based Intrusion Detection and Prevention System (HIDPS).

7. REFERENCES

[1] James P. Anderson. 1980. Computer Security Threat Monitoring and Surveillance. Technical report Co, Fort Washington.

[2] Dorothy E. Denning. 1987. An Intrusion-Detection Model. IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, VOL. SE-13, NO. 2.

[3] Karen Scarfone and Peter Mell. 2012. Guide to Intrusion Detection and Prevention Systems. National Institute of Standards and Technology, U.S.

[4] Mauritian Computer Emergency Response Team. 2011. Guideline on Intrusion Detection and Prevention Systems. National Computer Board, Issue No. 10.

[5] Srinivas Mukkamala, Andrew H. Sung, and Ajith Abraham. 2005. Intrusion detection using an ensemble of intelligent paradigms. Journal of Network and Computer Applications, Vol. 28, Issue 2, pp. 167–182.

[6] Mohammadreza Ektefa, Sara Memar, Fatimah Sidi and Lilly Suriani Affendey. 2010. Intrusion Detection Using Data Mining Techniques. Proceedings Of IEEE International Conference on Information Retrieval & Knowledge Management, Exploring Invisible World, CAMP

[7] Upendra. 2013. An Efficient Feature Reduction Comparison of Machine Learning Algorithms for Intrusion Detection System. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Vol. 2, Issue 1.

[8] Reza Entezari-Maleki, Arash Rezaei, and Behrouz Minaei-Bidgoli. Comparison of Classification Methods Based on the Type of Attributes and Sample Size.

[9] Sushil Kumar Chaturvedi, Vineet Richariya and Nirupama Tiwari. 2012. Anomaly Detection in Network using Data mining Techniques. International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Vol. 2, Issue 5.

[10] Tarek S. Sobh. 2005. Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art. Computer Standards & Interfaces.

[11] Joseph S. Sherif and Tommy G. Dearmond. 2002. Intrusion Detection: Systems and Models . California Institute of Technology, JPL, Pasadena, CA 91 I09.

[12] Pieter de Boer & Martin Pels. 2005. Host-based Intrusion Detection Systems.

[13] Palika Jajoo and Dayama Meeta. 2011. Intrusion Detection And Prevention System. International conference on Advanced Computing, Communication and Networks'.

[14] Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Hiren Patel,Avi Patel, Muttukrishnan Rajarajan. 2012. Review A survey of intrusion detection techniques in Cloud . Journal of Network and Computer Applications, Vol. 36, pp. 42–576.

[15] Hung-Jen Liao, Chun-Hung Richard Lin ,Ying-Chih Lin, Kuang-Yuan Tung. 2013. Intrusion detection system: A comprehensive review. Journals of network and computer Applications, Vol. 36, pp. 16-24.

[16] Bilal Maqbool Beigh and Prof.M.A.Peer. 2012.Intrusion Detection and Prevention System: Classification and Quick Review. ARPN Journal of Science and Technology, Vol. 2, No. 7, ISSN 2225-7217.

[17] Ant Allan. 2002. Intrusion Detection Systems (IDSs): Perspective. Technology Overview, DPRO-95367.

[18] Giovanni Vigna and Christopher Kruegel. 2005. Host-Based Intrusion Detection, JWBS001C.

[19] Andreas Fuchsberger.2005.Intrusion Detection Systems and Intrusion Prevention Systems. Information Security Technical Report, Vol. 10, pp. 134-139.

[20] Herve Debar. 2000. An Introduction to Intrusion-Detection Systems. IBM Research and ZurichResearch Laboratory, Switzerland.

[21] Muriel Baudrion. 2004. Fighting system intrusions: from detection to prevention. Global Information Assurance Certification Paper, Amsterdam.

[22] Srilatha Chebrolua, Ajith Abrahama, Johnson P. Thomas. 2005. Feature deduction and ensemble design of intrusion detection systems. Computers & Security, Vol. 24, pp. 295-307.

[23] M. Govindarajan, RM. Chandrasekaran. 2011. Intrusion detection using neural based hybrid classification methods. Computer Networks.

[24] Sushil Kumar Chaturvedi and Vineet Richariya. 2012. Attack Detection over Network based on C45 and RF Algorithms. International Journal of Computer Applications Vol. 57, No.9.

[25] Wun-Hwa Chen, Sheng-Hsun Hsu , Hwang-Pin Shen. 2005. Application of SVM and ANN for intrusion detection. Computers & Operations Research, Vol.32, pp.2617–2634.