JOURNAL OF CRITICAL REVIEWS

ISSN-2394-5125 VOL 5, ISSUE 03, 2018

INPUT DATA PROCESSING TECHNIQUES IN INTRUSIONDETECTION SYSTEMS – SHORT REVIEW

Dr. Sunil Mishra (Cse)[1] , Dr. Surya Kant (Cse)[2] , Dr. Deepak Dambla (Cse)[3]

[1] *,[2,3,4]Accurate Institute Of Management & Technology, Greater Noida

***Corresponding Author:** Dr. Sunil Mishra
*Accurate Institute Of Management & Technology, Greater Noida

Abstract—
In This Paper Intrusion Detection Systems (Idss) Are Classified According To The Techniques Applied To Processing Input Data. This Process Is Complex Because Idss Are Highly Coupled In Actual Implemented Systems. Eleven Input Data Processing Techniques Associated With Intrusion Detection Systems Are Identified. They Are Then Grouped Into More Abstract Categories. Some Approaches Are Artificially Intelligent Such As Neural Networks, Expert Systems, And Agents. Others Are Computationally Based Such As Bayesian Networks, And Fuzzy Logic. Finally, Some Are Based On Biological Concepts Such As Immune Systems And Genetics. Characteristics Of And Systems Employing Each Technique Are Also Mentioned.

I. Introduction

wHen Traditionally Classifying Intrusion DetectionSystems (Idss) As Misuse, Anomaly Or Hybrid, The Systems Are Grouped According To The Technique They UtilizeTo Detect Intrusions. For Example, Misuse-Based Idss Match Already Stored Attack Signatures Against The Audit DataGathered While The Monitored System Is Or Was Running. In Anomaly Based Idss, Detection Utilize Models Of NormalBehavior Where Any Deviation From Such Behavior Is Identified As An Intrusion. Another Type Of TraditionalClassification Is Categorizing An Ids According To Its Setup AsNetwork-Based, Host-Based Or Hybrid. Network BasedSystems Monitor Network Activities Whereas A Host BasedSystem Monitor The Activities Of A Single System For IntrusionTraces [1]. In General, Idss May Apply Many Techniques ToDetect Intrusions And Improve Detection Such As NeuralNetworks, Expert Systems, Agents, Bayesian Networks, FuzzyLogic, Immune Systems And Genetics. Little Attention HasBeen Given To Classifying The Processing Techniques AppliedOn The Input Data Provided To The Ids. In This Paper WeClassify Input Data Processing Techniques Utilized With IdssThat May Use And May Not Use The Same Processing TechniqueTo Detect Intrusions. In Section 2, Abstract Classification OfThe Different Input Data Processing Techniques Utilized With Idss Will Be Presented.

Eleven Input Data Processing Techniques Associated With Idss Are Identified. Then They Are Grouped Into More Abstract Categories. In Section 3, A General Description As Well As Some Advantages And Disadvantages Of Each Technique And Examples Of System Employing These Techniques Will Be Presented.

II. Classification Of Input Data Processing Techniques In Idss

In This Paper, We Are Concerned With The Techniques Used To Process Input Data That Is Considered When Designing And Implementing Idss. Classifying Such Techniques Are Not Easy Because In The Actual Implemented System, CombinationOf Techniques May Be Used. However, Identifying Them Individually Helps Better Understand The Merits And Limitations Of Each, And How To Improve A Techniques Performance By Using Another. Eleven Techniques Are Identified [Shown At The Lower Level Of Diagram 1] That Are Widely And Currently Used For Processing Input Data Of Idss. They Are Then Grouped Into More Abstract Categories That Are Identified At The Upper Levels Of Diagram 1. This Is Important Because The Characteristics Of Each Technique Are Highly Affected By The Category(Ies) That It Belongs To. In The Lower Level Of Fig. 1, Techniques Such As Agents And Data Mining Belong To The Intelligent Data Analysis Category. This Is Indicated By The Dotted Relation Between Data Analysis And Ai Categories. The Techniques: Expert Systems And Fuzzy Logic Are Intelligent Model-Based-Rule-Based Systems Shown By The Dotted Relation Between Rule Based And Ai Categories In Fig. 1. Next Is An Explanation Of Each Item In Fig. 1, AlongWith Some Identified Characteristics.

ISSN-2394-5125 VOL 5, ISSUE 03, 2018

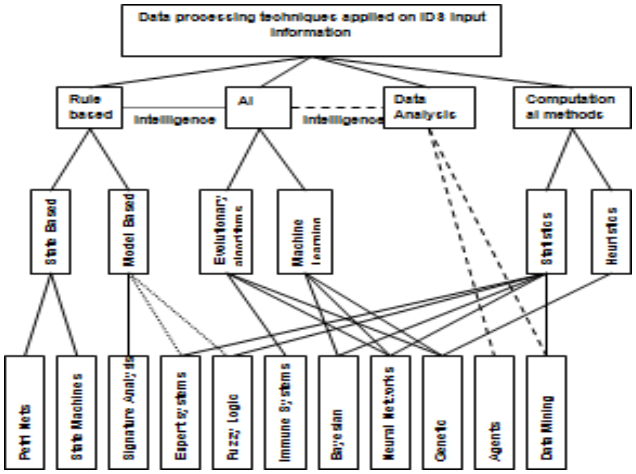

Fig.1. Data Processing Techniques Applied On Input Data Processed By Intrusion Detection Systems

A. Rule Based

If A Rule-Based Ids Is To Use Input Data Or Audit Data, Such Information Will Be In A Codified Rules Format Of Known Intrusions. The Input Data Will Represent Identified Intrusive Behavior And Categorizing Intrusion Attempts By Sequences Of User Activities That Lead To Compromised System States. The Ids Will Take As Input The Predefined Rules As Well As TheCurrent Audit Data And Check If A Rule Is Fired. In General, Using Rule Bases Are Affected By System Hardware Or SoftwareChanges And Require Updates By System Experts As The System Is Enhanced Or Maintained. Such Input Data Technique Is VeryUseful In An Environment Where Physical Protection Of The Computer System Is Not Always Possible (E.G., A Battlefield Situation) But Require Strong Protection [Http://Www.Sei.Cmu.Edu/Str/Descriptions/Rbid.Html].

In General, Rule Based Systems Can Be:

I) State-Based: In The Audit Trails, Intrusion Attempts Are Defined As Sequences Of System States Leading From An Initial State To A Final Compromised State Represented In A State Transition Diagram. The Two Inputs To The Ids Will Include The Audit Trail And The State Transition Diagrams Of Known Penetrations ThatWill Be Compared Against Each Other Using An Analysis Tool. One Advantage Of Using State Based Representation Of Data Is That It Is Independent Of TheAudit Trail Record And Is Capable Of Detecting Cooperative Attacks And Attacks That Span Across Multiple User Sessions. However, Some Attacks Cannot Be Detected Because They Cannot Be ModeledWith State Transitions [Http://Www.Sei.Cmu.Edu/Str/Descriptions/Rbid.Html]

II) Model-Based: Intrusion Attempts In Input Data Can Be Modeled As Sequences Of User Behavior. This Approach Allows The Processing Of More Data, Provide More Intuitive Explanations Of Intrusion Attempts And Predict Intruder's Next Action. More General Representation Of Penetrations Can Be Generated Since Intrusions Are Modeled At A Higher Level Of Abstraction. However, If An Attack Pattern Does Not Occur In The Appropriate Behavior Model It Cannot Be Detected[Http://Www.Sei.Cmu.Edu/Str/Descriptions/Rbid.Html]

B. Artificial Intelligence

Ai Improves Algorithms By Employing Problem Solving Techniques Used By Human Beings Such As Learning, Training And Reasoning. One Of The Challenges Of Using Ai TechniquesIs That It Requires A Large Amount Of Audit Data In Order To Compute The Profile Rule Or Pattern Sets. From The Audit Trails, Information About The System Is Extracted And Patterns Describing The System Are Generated. In General, Ai Can Be Employed In Two Ways: (1) Evolutionary Methods (Biologically Driven) Are Mechanisms Inspired By Biological Evolution, Such As Reproduction, Mutation And Recombination. (2) Machine Learning Is Concerned With The Design And Development Of Algorithms And Techniques That Allow The Learning Of Computers. The Major Focus Of Machine Learning Research Is To Extract Information From Data Automatically [2].

C. Data Analysis

With Data Analysis, Data Is Transformed In Order To Extract Useful Information And Reach Conclusions. It Is Usually Used To Approve Or Disapprove An Existing Model, Or To Extract Parameters Necessary To Adapt A Theoretical Model To An Experimental One. Intelligent Data Analysis Indicates That The Application Is Performing Some Analysis Associated With UserInteraction And Then Provides Some Insights That Are Not Obvious. One Of The Problems Faced When Applying Such An Approach Is That Most Application Logs (Input Information) DoNot Conform To A Specific Standard. Analysis Of Logs Should Be Performed To Find Commonalities And Different Types Of Logs Should Be Grouped. Another Problem Is The Existence Of Noise, Missing Values And Inconsistent Data In The Actual Log

ISSN-2394-5125 VOL 5, ISSUE 03, 2018

Information. Attackers May Take Advantage Of The Fact That Logs May Not Record All Information And Therefore Exploit This Point. Finally, Real World Data Sets Tend To Be Too Large And Multidimensional Which Requires Data Cleaning And Data Reduction [3].

D. Computational Methods

Computational Intelligence Research Aims To Use Learning, Adaptive, Or Evolutionary Algorithms To Create Programs. These Algorithms Allow The Systems To Operate In Real Time And Detect System Faults Quickly. However, There Are Costs Associated With Creating Audit Trails And Maintaining Input User Profiles As Well As Some Risks. For Example, Because User Profiles Are Updated Periodically, It Is Possible To AcceptA New User Behavior Pattern Where An Attack Can Be Safely Mounted. This Is Why It Is Difficult Sometimes To Define User Profiles Especially If They Have Inconsistent Work Habits. In General, There Are Two Types Of Idss That Utilize A Computational Method: (1) Statistics-Based Ids AreEmployed To Identify Audit Data That May Potentially Indicate Intrusive Behavior. These Systems Analyze Input Audit Trail Data By Comparing Them To Normal Behavior To Find Security Violations. (2) Heuristics-Based Ids Which Can Be A Function That Estimates The Cost Of The Cheapest Path From One Node To Another [Http://Www.Sei.Cmu.Edu/Str/Descriptions/Sbid.Html].

III.Capabilities And Examples Of ProcessingTechniques Of Input Data Used By Idss

Because Some Ids Data Processing Techniques Are Closely Interacting And Similar, Classifying Them Is Complex. However, We Believe That The Identified Eleven Categories Capture Most Of The Well Known Types. For Example, From Fig. 1, Although Expert Systems And Fuzzy Logic Belong To The Categories Ai And Rule Based They Have Distinguishing Characteristics And Usages. The Output Of The Expert SystemIs Specific; The Data That Is Used To Build The System Is Complete, And The Set Of Rules Are Well Defined. As For Fuzzy

Logic, It Is Usually Used In Systems Where The Output Is Not Well Defined And Is Continuous Between 0 And1.

A. Bayesian Networks

Bayesian Networks Are Used When We Want To Describe The Conditional Probability Of A Set Of Possible Causes For A GivenObserved Event That Are Computed From The Probability Of Each Cause And The Conditional Probability Of The Outcome OfEach Cause. They Are Suitable For Extracting Complex Patterns From Sizable Amounts Of Input Information That Can Also Contain Significant Levels Of Noise. Several Systems Have Been Developed Using Bayesian Network Concepts. In The Following System, Scott'S [4] Ids Is Based On Stochastic Models Of User And Intruder Behavior Combined Using Bayes' Theorem Which Mitigates The Complexity Of Network Transactions That Have Complicated Distributions. Intrusion Probabilities Can Be Calculated And Dynamic Graphics Are Used To Allow Investigators To Use The Evidence To Navigate Around The System.

B. Neural Networks

Training Neural Networks Enable Them To Modify A State Of ASystem By Discriminating Between Classes Of Inputs. They Also Learn About The Relationship Between Input And Output Vectors And Generalize Them To Extract New Input And Output Relationships. They Are Suitable When Identification And Classification Of Network Activities Are Based On Incomplete And Limited Input Data Sources. They Are Able To Process Data From A Number Of Sources, Accept Nonlinear Signals As Input And Need A Large Sample Size Of Input Information. Finally, Neural Networks Are Not Suitable When The Information Is Imprecise Or Vague And It Is Unable To Combine Numeric Data With Linguistic Or Logical Data. In The Following System, Bivens Et Al. [5] Employed The Time- Window Method For Detection And Were Able To Recognize Long Multi-Packet Attacks. They Were Able To Identify Aggregate Trends In The Network Traffic In The Preprocessing Step By Looking Only At Three Packet Characteristics. Once The System Is Trained And By Using The Input Data, The Neural Network Was Able To Perform Real-Time Detection.

C. Data Mining

Data Mining Refers To A Set Of Techniques That Extracts Previously Unknown But Potentially Useful Data From Large Stores System Logs. One Of The Fundamental Data Mining Techniques Used In Intrusion Detection Is Associated With Decision Trees [6] That Detect Anomalies In Large Databases. Another Technique Uses Segmentation Where Patterns Of Unknown Attacks Are Extracted From A Simple Audit And Then Matched With Previously Warehoused Unknown Attacks [7]. Another Data Mining Technique Is Associated With Finding Association Rules By Extracting Previously Unknown Knowledge On New Attacks And Building Normal Behavior Patterns [8]. Data Mining Techniques Allows Finding Regularities And Irregularities In Large Input Data Sets.

However, They Are Memory Intensive And Require Double Storage: One For The Normal Ids Data And Another For The DataMining. The System Of Lee, Solto And Mok'S [7] Was Able To Detect Anomalies Using Predefined Rules; However, It Needed A Supervisor To Update The System With The Appropriate Rules Of Certain Attacks. The Rule

ISSN-2394-5125 VOL 5, ISSUE 03, 2018

Generation Methodology Developed, First Defines An Association Rule ThatIdentifies The Relation Between Rules And Specifies The Confidence For The Rule.

D. Agents

Agents Are Self Contained Processes That Can Perceive Their Environment Through Sensors And Act On The Environment Through Effectors. Agents Trace Intruders And Collect Input Information That Is Related Only To The Intrusion Along The Intrusion Route And Then Decide If An Intrusion Has Occurred From Target Systems Across The Network. One Of The Major Disadvantages Associated With Agents Is That It Needs A HighlySecure Agent Execution Environment While Collecting AndProcessing Input Information. It Is Difficult Also ToPropagate Agent Execution Environments Onto Large Numbers Of Third-Party Servers. Several Systems Have Been Developed Utilizing Agents. Spafford And Zamboni [9] Introduced Autonomous Agents For Intrusion Detection (Aafid) Using Autonomous Agents For Performing Intrusion Detection. TheirPrototype Provides A Useful Framework For The Research And Testing Of Intrusion Detection Algorithms And Mechanisms. Gowadia, Farkas And Valtorta [10] Implemented A Probabilistic Agent-Based Intrusion Detection (Paid) System That Has Cooperative Agent Architecture. In Their Model Agents Are Allowed To Share Their Beliefs And Perform Updates. Agent Graphs Are Used To Represent Intrusion Scenarios. Each Agent Is Associated With A Set Of Input, Output, And Local Variables.

E. Immune Based

Immune Based Ids Are Developed Based On Human Immune System Concepts And Can Perform Tasks Similar To Innate And Adaptive Immunity. In General, Audit Data Representing The Appropriate Behavior Of Services Are Collected And Then A Profile Of Normal Behavior Is Generated. One Challenge Faced Is To Differentiate Between Self And Non-Self Data WhichWhen Trying To Control Causes Scaling Problems And The Existence Of Holes In Detector Sets.

There Have Been Several Attempts To Implement Immunity- Based Systems. Some Have Experimented With Innate Immunity Which Is The First Line Of Defense In The Immune System And Is Able To Detect Known Attacks. For Example, Twycorss And Aickelin [11] Implemented Libtissue That Uses A Client/Server Architecture Acting As An Interface For A Problem Using Immune Based Techniques. Pagnoni And Visconti [12] Implemented A Native Artificial Immune System(Nais) That Protects Computer Networks. Their System Was Able To Discriminate Between Normal And Abnormal Processes, Detect And Protect Against New And Unknown Attacks And Accordingly Deny Access Of Foreign Processes To

The Server. For Adaptive Immunity Two Approaches Have Been Studied: Negative Selection And Danger Theory Concepts.Kim And Bentley [13] Implemented A Dynamic Clonal Selection Algorithm That Employs Negative Selection By Comparing Immature Detectors To A Given Antigen Set. Immature Detectors That Bind To An Antigen Are Deleted And The Remaining Detectors Are Added To The Accepted Population. If A Memory Detector Matches An Antigen An Alarm Is Raised. A Recent Approach To Implement Adaptive Immunity Uses The Danger Theory Concept [14]. Danger Theory Suggests That An Immune Response Reacts To Danger Signals Resulting From Damage Happening To The Cell And Not Only For Being Foreign Or Non-Self To The Body.

F. Genetic Algorithms

Genetic Algorithms Are A Family Of Problem-Solving Techniques Based On Evolution And Natural Selection. Potential Solutions To The Problem To Be Solved Are Encoded As Sequences Of Bits, Characters, Or Numbers. The Unit Of Encoding Is Called A Gene, And The Encoded Sequence Is Called A Chromosome. The Genetic Algorithm Begins With Chromosomes Population And An Evaluation Function That Measures The Fitness Of Each Chromosome. Finally, The Algorithm Uses Reproduction And Mutation To Create New Solutions. In The System Of Shon And Moon [15] The Enhanced Support Vector Machine (Enhanced Svm) Provides Unsupervised Learning And Low False Alarm Capabilities. Profile Of Normal Packets Is Created Without Preexisting Knowledge. After Filtering The Packets They Use A Genetic Algorithm For Extracting Optimized Information From Raw Internet Packets. The Flow Of Packets That Is Based On Temporal Relationships During Data Preprocessing Is Used In The Svm Learning.

G. Fuzzy Logic

Fuzzy Logic Is A System Of Logic That Mimics Human DecisionMaking And Deals With The Concept Of Partial Truth And In Which The Rules Can Be Expressed Imprecisely. Several Systems Have Been Developed Using Fuzzy Logic. Abrahama Et Al. [16] Modeled Distributed Soft Computing-Based Ids (D-Scids) As A Combination Of Different Classifiers To Model Lightweight And Heavy Weight Idss. Their Empirical Results Show That A Soft Computing Approach Could Play A Major Role For Intrusion Detection Where The Fuzzy Classifier Gave 100% Accuracy For All Attack Types Using All Used Attributes. Abadeh, Habibi And Lucas [17] Describe A Fuzzy Genetics-Based Learning Algorithm And Discuss Its Usage To Detect Intrusion In A Computer Network. They Suggested A New Fitness Function That Is Capable Of Producing More Effective Fuzzy Rules That Also Increased The Detection Rate As Well As False Alarms. Finally, They Suggested Combining Two Different Fitness Function Methods In A Single Classifier, To Use

ISSN-2394-5125 VOL 5, ISSUE 03, 2018

The Advantages Of Both Fitness Functions Concurrently

H. Expert Systems

Expert Systems-Based Idss Build Statistical Profiles Of Entities Such As Users, Workstations And Application Programs And Use Statically Unusual Behavior To Detect Intruders. They Work On A Previously Defined Set Of Rules That Represent A Sequence Of Actions Describing An Attack. With Expert Systems, All Security Related Events That Are Incorporated In An Audit Trail Are Translated In Terms Of If- Then-Else Rules. The Expert System Can Also Hold And Maintain Significant Levels Of Information. However, The Acquisition Of Rules From The Input Data Is A Tedious And Is An Error-Prone Process. The System Of Ilgun, Kemmerer And Porras [18], Is An Approach To Detect Intrusions In Real Time Based On State Transition Analysis. The Model Is Represented As A Series Of State Changes That Lead From An Initial Secure State To A Target Compromised State. The Authors Developed Ustat Which Is A Unix Specific Prototype Of A State Transition Analysis Tool (Stat) Which Is A Rule Based Expert System That Is Fed With The Diagrams. In General, Stat Extracts And Compares The State Transition Information Recorded Within The Target System Audit Trails To A Rule Based Representation Of Known Attacks That Is Specific To The System.

I. Signature Analysis Or Pattern Matching

In This Approach The Semantic Description Of An Attack Is Transformed Into The Appropriate Audit Trail Format Representing An Attack Signature. An Attack Scenario Can Be Described, For Example, As A Sequence Of Audit Events That A Given Attack Generates. Detection Is Accomplished By Using Text String Matching Mechanisms. Human Expertise Is Required To Identify And Extract Non Conflicting Elements Or Patterns From Input Data. The System Of Kumar'S [19] Is Based On The Complexity Of Matching. Based On The Desired Accuracy Of Detection, He Developed A Classification To Represent Intrusion Signatures And Used Different Encodings Of The Same Security Vulnerability. His Pattern Specification Incorporated Several Abstract Requirements To Represent The Full Range And Generality Of Intrusion Scenarios That Are: Context Representation, Follows Semantics, Specification Of Actions And Representation Of Invariants.

J. State Machines

State Machines Model Behavior As A Collection Of States, Transitions And Actions. An Attack Is Described With A Set Of Goals And Transitions That Must Be Achieved By An Intruder To Compromise A System. Several Systems Have Been DevelopedUsing This Technique. Sekar Et Al. [20] Employ State-Machine Specifications Of Network Protocols That Are Augmented With Information About Statistics That Need To Be Maintained To Detect Anomalies. The Protocol Specifications Simplified The Manual Feature Selection Process Used In Other Anomaly Detection Approaches. The Specification Language Made It Easy To Apply Their Approach To Other Layers Such As Http And Arp Protocols. Peng, Leckie And Ramamohanarao [20]

Proposed A Framework For Distributed Detection Systems. They Improved The Efficiency Of Their System By Using A Heuristic To Initialize The Broadcast Threshold And Hierarchical System Architecture. They Have Presented A Scheme To Detect The Abnormal Packets Caused By The Reflector Attack By Analyzing The Inherent Features Of The Reflector Attack.

K. Petri Nets

The Colored Petri Nets Are Used To Specify Control Flow In Asynchronous Concurrent Systems. It Graphically Depicts The Structure Of A Distributed System As A Directed Bipartite GraphWith Annotations. It Has Place Nodes, Transition Nodes And Directed Arcs Connecting Places With Transitions. In The System Of Srinivasan And Vaidehi [22] A General Model Based On Timed Colored Petri Net Is Presented That Is Capable Of Handling Patterns Generated To Model The Attack Behavior As Sequence Of Events. This Model Also Allows Flagging An Attack, When The Behavior Of One Or More Processes Matches The Attack Behavior. Their Use Of A Graphical Representation Of A Timed Colored Petri Net Gives A Straightforward View Of Relations Between Attacks.

IV. Conclusion

Choosing An Ids To Be Deployed In An Environment Would Seem To Be Simple, However, With The Different Components, Types And Classifications Such A Decision Is Quite Complex. There Have Been Many Attempts To Classify Idss As A Mean To Facilitate Choosing Better Solutions. In This Paper We Classified Idss According To The Data Processing Techniques Applied To Input Information. Careful Design Of An Ids May Allow Correct Implementation Of An Ids. However, The Actual Merits And Limitations Of Each Approach, Which Is AlsoDiscussed In This Paper, Indicate That Obtaining Complete Security And Different Desirable System Characteristics Can Not Be Achieved By Employing Only One Type Of An Implementation Approach. The Data Processing Techniques Were Grouped Into General (Abstract) Categories And Were Then Further Expanded Into Eleven More Specialized Techniques.

We Discussed And Summarized The Characteristics Of Each Technique Followed By Examples Of Developed Systems

UsingEach Technique. Fig. 1, For Example, Helps Us Understand ThatWe Can Use The State Machine Technique To Build An Ids, And That We Can Add Intelligence To It And Use The Expert System Technique With Added Merits And Costs. The Merits Are The Ability To Perform And Provide Intelligent Actions And Answers. Unrealistic Actions Or Answers Can Be Refuted Or Ignored. It Also Borrows From Statistics The Ability To Detect Intrusions Without Prior Information About The Security FlawsOf A System. Some Of The Incurred Costs Are The Conflicting Requirement Of Maintaining High Volume Of Data Which Affects Throughput And Selecting The Appropriate Thresholds That Lower False Positive And Negatives. To Conclude, Selecting The Appropriate Technique Should Be Carried Out Carefully. Each Organization Should State Prior To Development The Requirements Of Its Agency And The Acceptable Costs. Accordingly, The Selected System Should BeAble To Incorporate Most Of The Requirements, As Complete Security Can Not Be Achieved.

V. References

1. H. Debar, M. Dacier, A. Wespi, ―Towards A Taxonomy Of Intrusion-Detection Systems,‖ Computer Networks, Vol. 31, Pp. 805-822, 1999.
2. S. Peddabachigari, A. Abraham, C. Grosan And J. Thomas, ―Modeling Intrusion Detection System Using Hybrid Intelligent Systems,‖ Journal OfNetwork And Computer Applications, Vol. [Mat02], No. 1, Pp. 114-132, 2007.
3. Andre‘ Muscat, ―A Log Analysis Based Intrusion Detection System For The Creation Of A Specification Based Intrusion Prevention System‖, Csaw 2003 Proceedings, 2003.
4. S. L. Scott, ―A Bayesian Paradigm For Designing Intrusion Detection Systems,‖ Computational Statistics Data Analysis, Vol. 45, No. 1, Pp. 69-83, 2004.
5. Bivens, M. Embrechts, C. Palagiri, R. Smith, And
6. B. K. Szymanski, ―Network Based Intrusion Detection Using Neural Networks,‖ Intelligent Engineering Systems Through Artificial Neural Networks, Vol. 12, 2002.
7. W. Fan, M. Miller, S. Stolfo, W. Lee, And P. Chan,
8. ―Using Artificial Anomalies To Detect Unknown And Known Network Intrusions‖, In Proceedings Of The First Ieee International Conference On Data Mining, San Jose, Ca, 2001.
9. W. Lee, S. J. Stolfo, And K. W. Mok, ―Adaptive Intrusion Detection: A Data Mining Approach,‖ Artificial Intelligence Review, Vol. 14, No. 6, Pp. 533–567, 2000.
10. T. Bass, ―Intrusion Detection Systems Multi-Sensor Data Fusion: Creating Cyberspace Situational Awareness,‖ Communication Of The Acm, Vol. 43, No. 1, Pp. 99-105, 2000.
11. H. Spafford And D. Zamboni, ―Intrusion Detection Using Autonomous Agents,‖ In ComputerNetwork, Vol. 34, No. 4, Pp. 547-570, 2000.
12. Gowadia, C. Farkas, And M. Valtorta, ―Paid: A Probabilistic Agent-Based Intrusion Detection System,‖ Computers & Security, 2005.
13. J. Twycross, And U. Aickelin, ―Libtissue - Implementing Innate Immunity,‖ Proceedings Of The Ieee Congress On Evolutionary Computation (Cec 2006), Vancouver, Canada, 2006.
14. Pagnoni, And A. Visconti, ―An Innate Immune System For The Protection Of Computer Networks,‖ Acm International Conference Proceeding Series, Vol. 92 Archive Proceedings Of The 4th InternationalSymposium On Information And Communication Technologies, 2005.
15. J. Kim, And P. J. Bentley, ―A Model Of Gene Library Evolution In The Dynamic Clonal Selection Algorithm,‖ Proceedings Of The First International Conference On Artificial Immune Systems (Icaris) Canterbury, Pp.175-182, 2002.
16. P. Matzinger, ―The Danger Model: A Renewed Sense Of Self,‖ Science, Vol. 296, Pp. [Mat02]1- [Mat02]5, 2002.
17. T. Shon And J. Moon, ―A Hybrid Machine Learning Approach To Network Anomaly Detection,‖ Information Sciences: An International Journal, Vol. 177, No. 18, Pp. 3799-3821, 2007.
18. Abrahama, R. Jainb, J. Thomasc, And S. Y. Hana,
19. ―D-Scids: Distributed Soft Computing Intrusion Detection System,‖ Journal Of Network And Computer Applications, Vol. 30, Pp. 81–98, 2007.
20. S. Abadeh, J. Habibi And C. Lucas, ―Intrusion Detection Using A Fuzzy Genetic Based Learning Algorithm,‖ Journal Of Network And Computer Applications, Vol. 30, No. 1, Pp. 414-428, 2007.
21. Ilgun, R. A. Kemmerer, And P. A. Porras, ―State Transition Analysis: A Rule- Based IntrusionDetection Approach,‖ Ieee Transactions OnSoftware Engineering, Pp. 181-199, 1995
22. S. Kumar.
23. ―Classification And Detection Of Computer Intrusions,‖ *Ph.D. Dissertation*, PurdueUniversity, 1995.
24. R. Sekar, A. Gupta, J. Frullo, T. Hanbhag, A. Tiwari, H. Yang, And S. Zhou, ―Specification- Based Anomaly Detection: A New Approach For Detecting,‖ *International Journal Of Network Security*, Vol. 1, No.2, Pp. 84–102, 2005.
25. T. Peng, C. Leckie And K. Rama Mohana Rao,

ISSN-2394-5125 VOL 5, ISSUE 03, 2018

26. ―Information Sharing For Distributed Intrusion Detection Systems,‖ *Journal Of Network And Computer Applications*, Vol. [Mat02], No. 3, Pp. 877-899, 2007.
27. N. Srinivasan And V. Vaidehi. ―Timed Coloured Petri Net Model For Misuse Intrusion Detection.‖ *First International Conference On Industrial And Information Systems*, 8-11 Aug. 2006.