ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

Feature Selection and Classification Techniques for the Detection of web-based Attacks

K.G. Maheswari

Assistant Professor (Senior), Department of MCA, Institute of Road and Transport Technology, Anna University, Erode, Tamil Nadu, India

ABSTRACT: In recent years, web security has become the major concern due to popularity of internet and usage of online web applications. Web data mining plays a significant role in prediction, analysis and decision making. Most of the existing systems fail to detect the web attacks at real time since it has to handle huge volume of data and this huge volume of data requires effective feature selection and classification techniques. In order to overcome the issues of existing systems, in this paper a novel intelligent feature selection and classification techniques are proposed to identify the most relevant features to identify the web attacks. Thereby, the proposed system optimizes the number of selected features and reduces the large amount of data to be preprocessed to provide accurate classification for both normal and anomaly requests in real time. The performance of the proposed system is analyzed and compared with various classification algorithms. Results justify that proposed algorithm provides better efficiency in detection of web attacks.

KEYWORDS: Pre processing, feature section, classification, web attacks, efficient detection.

I. INTRODUCTION

The rapid development in Information Technology has needed of security in multiple levels. The latest technology developments are integrated with all technology like grid, web and cloud computing. An IDS (Intrusion Detection System) is an effective approach to detect and prevent the intruder in network, application and in the system level. Due to increasing number of data, being transmitted day by day from one network to another network by using different types of applications and browsers. It is very difficult to detect intrusion in web and cloud environment. But providing security is necessary aspects for user communication and also it is big challenges to developers. Because attacker can access the sensitive information through the unauthorized access of applications, networks and database etc. There are many possibilities of attacks through applications, networks, operating systems and database. But in application level most of the attackers use the serious repercussions and vulnerabilitieswhich have been exploited. The input manipulation attacks are most serious one, from various types of application level vulnerabilities which are dynamically inject by attacker. Because of the low level API Application Programe Interface (API) between browser, web server and database server, the input can easily manipulated by the attacker. Detection of such type of dynamic attack is more important. In this paper, the dynamic analysis of input manipulation attacks in web environment is carried out. In web application, the users input query is dynamically constructed and executed by the web server. Before query construction and execution, it is manipulated by the attackers dynamically. Such a type of attack is called Cross Site Scripting (XSS) attack. Like that, before execution and construction of Structure Query Language (SQL) query to database server, it is manipulated by the attacker. Such a type of attack is called SQL injection attack. So these two attacks SQL Injection and XSS attacks are consider as input manipulation attacks in web environment. The Hybrid detection technique has been proposed to detect the SQL injection attack. It is occur due to dynamic manipulation in SQL Query.XSS attacks occur due to manipulation in the scripting language. Mostly MIT DARPA'99 dataset is used to detect the intrusion which is based on network attacks. To detect the input manipulation attacks in web environment, in

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

this paper HTTP CSIC2010 dataset is used.HTTP CSIC 2010 dataset consists of 30 features to detect the intrusion in web application. In this paper, two feature selection algorithms are used to select the optimal features from the HTTP CSIC 2010 dataset. First one is IGR (Information Gain Ratio) based feature selection algorithm. It is used to select 18 features form the dataset. Second one is the proposed intelligent hybrid relevant feature algorithm which is used to select 8 features from the 30 features. This type of optimal feature selection helps to reduce the classification time of normal and abnormal attributes classification and also improve the performance.

II. RELATED WORKS

Various mechanisms have been proposed in the literature for various web attacks. Generally, threat is an event with the potential to cause harm to an web application through disclosure, hide the information, denial of service. To provide web application security, measure the risk assessment to identify the key of issues of vulnerabilities. Based on the assessment, necessary component hardware (or) software, used to secure dynamic web application environment. Firewalls, IDS, digital signature to IPS are some of the example used to secure the web application environment. But unfortunately, the installed security method does not prevent the application layer attacks and also the application layer protocol vulnerabilities are the access point for the attackers, and those attacks are very hard to defend. Several techniques and tools are available to analyze the web applications attacks.These types of vulnerabilities in web environment are discussed and analysed by various researchers (Scholte,et al. [1], Frajt, K, et al.[2], Kirit, I & Patel [3] for the security of applications Open Web Application Security Project (OWASP) published in every three year Top ten risks which affect the web application security. Among all the threats to web applications, the most prevalent are the injection attack, cross site scripting attack. In this paper, web input manipulation attacks such as SQL Injection attacks, cross site scripting attacks, cloud malware injection attacks and co resident attacks are discussed. In the recent years and based on the research, IDS has most powerful technology that protects the client, server and also network from malicious actions. Compare to other technique IDS has proved to be effective technique used for intrusion detection. Cao[4]proposed learning based Intrusion Detection System (IDS) to detect SQLIAs using a machine learning technique. This machine learning technique builds models during at the runtime, if the query is different from the model, it is consider as attack. This tool successfully detects attacks but it will generate many false positives and false negatives. Another approach in this category is SQL-IDS, it is used to writing specifications for the web application that express the structure of SQL statement. So SQL statements violations execution automatically monitor with respect to specifications. Kumar, P&Pateriya, RK [5] proposed an enhanced intrusion detection system and the proposed IDS is language independent i.e. it will support any web application which use any type of language java, php, dot net etc. In addition the proposed IDS detects all type of attacks also including web application attacks like SQL injection attacks, command injection attacks, cross site scripting attacks. But in the existing IDS these types of attacks are not detected. Our proposed IDS based on the web application parameter, it will detect the web attacks. He et al.[6] proposed and implemented web Intrusion Protection System (web IPS) based on P2P and reverse proxy architecture. The P2P based web IPS has multi web firewall nodes and nodes with same program cooperate with each other under P2P architecture. Different nodes work as net flow allocator and some work as detector and they can convert to each other according to the requirements dynamically. The WAF program has the characteristics of session keeping and load balancing and it can detect messages by using expert library and many plug-in components. The technology of reverse proxy is used for response the web request. Experiments show that the system can effectively prevent attacks form application layer. It is proved more efficient and stable than single node. There are many works in the literature that deal with detection of SQL injection attack in web environment (Artzi, S, et al. [8],Livshits, B,et al. [7],Manmadhan, S&Manesh [9], Kruegel, C, et al. [11] Among them , Yeole, AS &Meshram, BB [10] have analysis seven different technique for detection of SQL Injection in client side and server side both in static analysis and dynamic analysis and they suggest server side input validation technique is most important because most of the attacker by pass the client side validation .

Fonseca, J et al. [12] presented a field study on two of the most widely spread and critical web application vulnerabilities, SQL injection and XSS. They analysis the source code of web applications written in different

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

languages. Results show that small subset of software fault types, affecting a restricted collection of statements and it will affect the outcomes of this study can be used to train software developers and code inspectors in the detection of such faults, and are also the establishment for the research of realistic vulnerability and attack injectors that can be used to assess security mechanisms, like intrusion detection systems, vulnerability scanners, and static code analysers.
Pack, DJ et al. [13] proposed the novel intrusion detection system to analysis HTTP protocol activities and network activities are analysised in packet level and session level and verification module detect the both malicious and unauthorized HTTP tunnelling activities. Maheswari KG et al. [14] proposed IDS intrusion Detection System for detection attacks in web applications. Maheswari KG et al. [15] discuss the intelligent classification algorithm using minkowski distance. Maheswari KG et al. [16] discussed VM's co- residency recognition plan to improve the security in cloud environment.Nalinipriya et al [17] discuss the security scheme policies of VM allocation policies. For that work , they used network analyser tool and cloud sim tool.

III. PROPOSED SYSTEMS ARCHITECTURE

The proposed system architecture of this work consists of five major modules namely pre processing Module and feature selection, Intrusion Detection module, Trust Based module and prevention module as shown in Figure 1.The overall process of this proposed system maintain by the decision Manager. The decision manager makes the decisions about the classification of web based attacks and prevention activities are carried out with the help of knowledge base.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

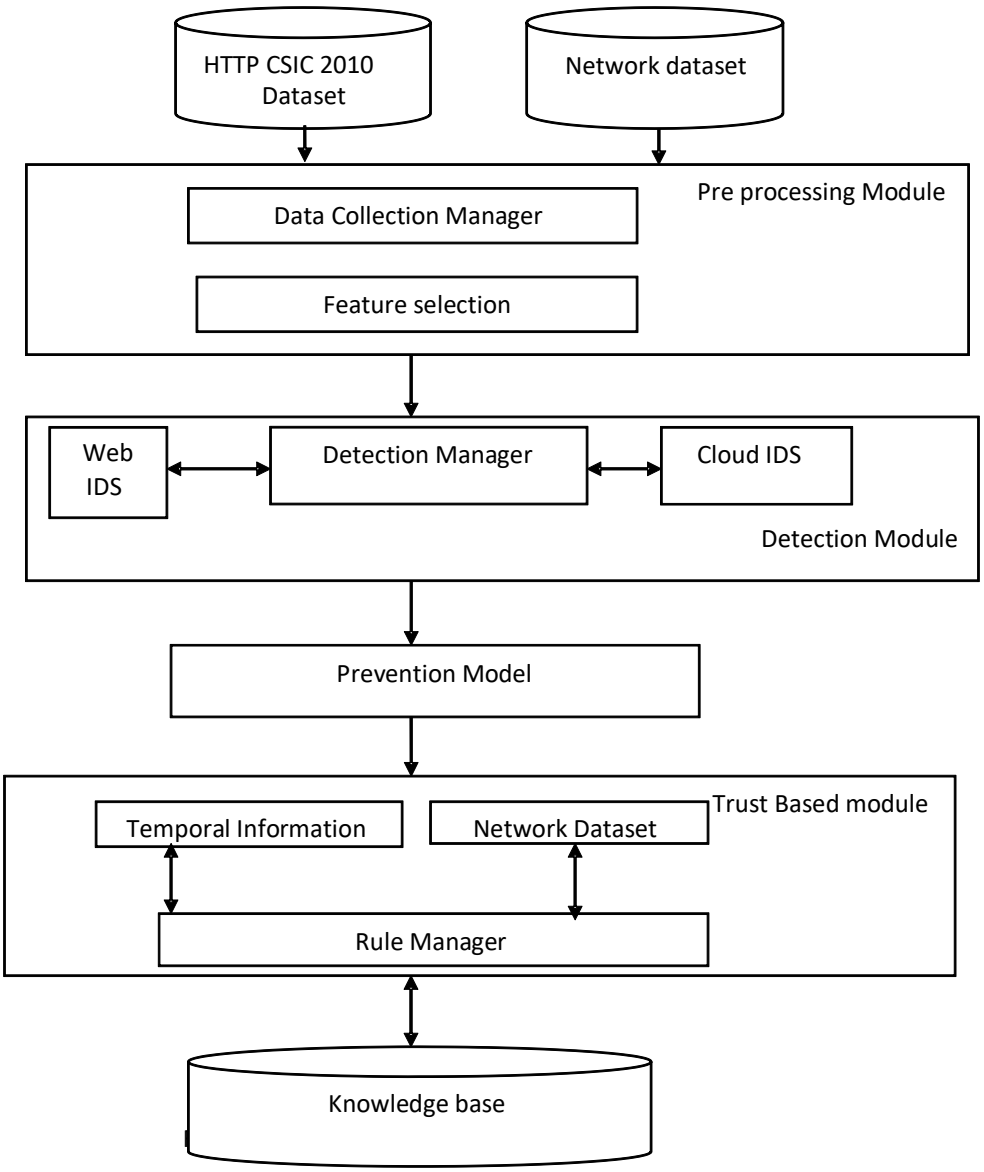

Figure 1 Architecture of proposed system

In the Pre-processing module, if any values of records are having null values and incorrect (or) missing data are also deleted from the dataset. This module contains component decision manager and feature selection. This module helps to select records from the dataset.This data collection is used in two types of environment web and cloud. These datasets are used as the input dataset for the decision support system. Decision manager module The overall process of this proposed system is monitor by the decision manager. For feature selection and classification based on the rules of knowledge base and decision manager to make decision. Feature selection In this module optimal features which

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

influence the attacks are selected. In this module, Intelligent Hybrid based effective feature selection has been proposed and implemented. Detection Module used to identify the attacks and give the intimation to the administrator (or) System Manager. These modules are responsible for applying classification algorithms which are proposed in this research work.(ie) they are used in this work for effective classification of the data. Based on training, they form necessary rules. The rule manager consists of query processor and inference system. It is responsible for firing the rules available in the knowledge base to perform deductive inference using forward chaining inference mechanism. The rules are prioritized and scheduled by the rule manager for execution.

In this work, Intelligent Hybrid Relavent Feature (IHRFA)selection algorithm has been proposed to identify the most relevant features are used to identify the web based attacks. Using this selected features, new classification technique has been proposed to classify accurately the normal and anomaly request. The performance of the proposed algorithm is analysed and compare with the various classification algorithm. The proposed system consists of four phases namely data processing phase, feature selection phase, relevant feature selection phase, classification phase and decision phase.

Table 1HTTP CSIC 2010 Dataset Before and After Reduction

Before removing duplicate instance	After removing duplicate instance	% of reduction
2,23,586	61,000	27.2

5.1 Feature selection phase

Feature selection is used to reduce the dimensionality of dataset. It is also used to remove the noisy (or) irrelevant and redundant data. The feature selection based on the three types of approaches. They are kFilter approach, Wrapper approach and embedded approach.In this work, feature subset are formed based on the information gain ratio raking and knowledge based ranking method and these measures are used to select the optimal number of attributes in the dataset.

5.2 Relevant Feature Algorithm

Relevant feature Algorithm is used to select the optimal features from the dataset. Figure 4.2 shows that the General work flows of relevant feature algorithm. In relevance analysis, features are classify into weak, strong and irrelevant features . Weak features further analysis into redundant and non – redundant features. The objective of is to find the optimal subset.

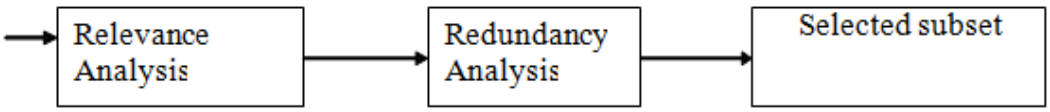

Figure 2 General Work Flow of Features Relevant Analysis

Algorithm 1 : Intelligent Hybrid Relevant Feature Algorithm (IHRFA)
Input: HTTP CSIC 2010 dataset
Output: Reduced ranked dataset R
Step 1: Get all features X in the dataset D
Step 2: Rank the feature set (R)
Step 3: Subset (S) = [1…….d] selected form the feature set.
Step 4: Process repeated until all features are ranked

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

Step 5: compute the weight vector based on the knowledge
Step 6: ranking scores of each features in set is calculate

S: c(i) = $(w(i))^2$

Step 7: compute the smallest ranking score feature with: e = arg min(c(i))
Step 8: Select only top ranking feature S=S-[e]
Step 9 : Stop

In Proposed Intelligent Hybrid Relevant Feature Algorithm, each feature is ranked based on the weight vector. Then ranked all features and select the top ranking in the list and eliminate the remaining. The implementation of the intelligent hybrid relevant feature algorithm, the following features are selected and selected features are listed in the Table 4.

Table 4: Selected Features

S.No	Feature Name
1.	Method
2.	Content length
3.	Host
4.	Content type
5.	Connection
6.	User Agent
7.	Payload
8.	Referrer

Table 5: Comparison of Feature Selection from the Dataset

S.NO	Dataset	Feature Selector	Selected Feature	Total no of Features selected
1	HTTP CSIC 2010	Information Gain Ratio Based Feature Selector	16,1,17,3,14,2,12,15,6,4,5,10,13,11,7,9,8	18
2		Intelligent Hybrid Relevant Feature Algorithm (IHRFA)	2,5,9,10,11,12,13,14,	8

The Table 5 shows that the comparison of existing IGR based feature selection algorithm and IHRFA based feature selection from the HTTP CSIC 2010 dataset are listed.

5.4 Classification and decision phase

Classification technique is used to classify the dataset effectively as normal and abnormal dataset. In this work, one new classification technique is called Enhanced Temporal Detection Tree classifier has been proposed for classifying HTTP CSIC2010 dataset. For analysis the performance of new classifier, an existing classification method also used in this work.

5.4.1: The Proposed Enhanced Temporal Decision Tree Algorithm

The proposed Enhanced Temporal Decision Tree Algorithm is as shown in figure 4.5 used for classifying normal and abnormal attacks. The Sp has been chosen to develop the decision tree for classification from attributes set A_i.In this proposed algorithm, Sp condition used to select search direction. Decision parameters based on time and web attacks related attributes are used to grow the tree.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

Algorithm 3 Enhanced Temporal Decision Tree Algorithm
Input: Reduced HTTP CSIC 2010 Dataset
Output: Web request are classified based on their Class labels
Step 1: read input data
Step 2: set of attributes *values* $SA = \{A_1, A_2, ..., A_n\}$, and set the point values(PV) at the time [t1, t2]
Step 3: From the attribute set select the root node and convert its value into point value(PV)
PV ={ p1, p2 p3**….**pn}
Step 4: Check the condition $Ci \in C$, where *C* Set of class labels and Compute the point values for each attributes A_i,
Step 5: from the web request assign Input values as *inputval*,
where *inputval* set of input values
Step 6: Based on *inputval*and temporal constraints place the tuples into two subset 'left' and 'right'
Step 7: If $inputval \leq Sv$
Grow the left child
Else
Grow the Right child
Step 8: To avoid testing error, pruning level set at point of the node 7.
Step 9: From the web request check for *Ci*and temporal constraints.
Step 10: steps 1 to 9 Repeated until all the web request classified
In this dataset, a normal class label is set as '0' and abnormal label is set as '1'. For each, the inputval compare with pv, where inputval is input value from record. The decision tree construct based on spv and temporal constraints the attributes are placed left or right. In this work the pruning level is 7. At each level, this algorithm is checking for class labels.

IV. VALIDATION PARAMETERS

A confusion matrix contains information about the number of normal and an abnormal instance predicted correctly and incorrectly by a classification model and is given in Table 6 it is used to evaluate the performance of a classifier.

Table6 Confusion Matrix of a Classifier

Confusion Matrix		**Predicated Class**	
		Normal	**Abnormal**
Actual Class	Normal	TP	TN
	Abnormal	FP	FN

Using the above confusion matrix IDS performance is evaluated, with respect to their capabilities.True Positive (TP): The number of abnormal record that is correctly identified.False Positive (FP): The number of normal records incorrectly classified. False Negative (FN): The number of abnormal record incorrectly classified.True Negative (TN): The number of normal records that are correctly classified. Using the above terms the performance metrics calculated as follows. Detection Rate (DR), Classification Accuracy, False Alarm Rate and Specificity.

6.1 Detection rate

Detection Rate (True Positive Rate) is the percentage of the number of abnormal record correctly classified and is calculated using Equation (5). The term is synonymous with sensitivity and recall.

$$\text{Detection rate} = TP/TP+TN \quad (5)$$

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

6.2 False alarm rate

False Alarm Rate (False Positive Rate) is the percentage of the number of normal record incorrectly classified and is calculated using Equation (6).

False Alarm Rate = FP/(TN+FN) (6)

6.3 Specificity

Specificity (True Negative Rate) is the percentage of the number of normal record are correctly classified and is calculated using Equation (7)

Specificity = TN/(TP+FN) (7)

6.4 Sensitivity

Sensitivity is used to measures the actual positives record which are correctly identifiedis calculated using Equation (8)

Sensitivity = TP/(TP+FN) (8)

6.5 Accuracy

Accuracy is defined as of the overall number of records correctly classified and is calculated using Equation (9)

Accuracy = TP+TN/TP+FP+TN+FN (9)

V. RESULT AND DISCUSSIONS

5.3 Experimental tool used

The proposed technique is implemented using the Weak 3.7.7 machine learning tool. There are two important objects an attribute evaluator and search method are consider for evaluation because attribute evaluator is used to assign a worth to each subset of features and search method is used to search all the way through the space of feature subset. The selected features are used to identify the web based attacks. For the implementation purpose, in this work 10–fold cross validation technique is used. The data are divided randomly into 10 parts (sets). 10 % of full dataset is used for evaluation and remaining 90 % is used for training. The result of ten iteration (10–folds) are averaged to yield an overall error estimate. Using the proposed Enhanced Temporal Decision Tree Algorithm, the web requests are classified according to their Point Values. The labels *A*1*, A2…. An* are represented as attributes. In this work, 8 attributes were selected using feature selection algorithm. Each leaf node represents the class labels. It is classified as 0 for normal web request and 1 as abnormal web request. To avoid test error, pruning level is taken as 7. The experimental result in the Table7 shows that based on the IGR based feature selection algorithm with Enhanced Temporal Decision Tree Algorithm, the detection rate of abnormal data from the HTTP CSIC 2010 dataset. Compare to other classifier, proposed Enhanced Temporal Detection Tree Algorithm gives the more detection rate.

Table 7 : IGR based Detection Rate

Classifier	**Detection Rate (TP in percentage)**
Random Tree	78.97
PART	79.84
J48	87.27
Enhanced temporal decision tree Algorithm	89.65

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

Table 8 shows that based on the IHRFA based feature selection algorithm with Enhanced Temporal Decision Tree Algorithm and the detection rate of abnormal data from the HTTP CSIC 2010 dataset. Compare to other classifier, proposed Enhanced temporal detection tree algorithm gives the more detection rate.

Table 8: IHRFA based Detection Rate

Classifier	Detection rate (TP in percentage)
Random Tree	85.97
PART	89.84
J48	92.65
Enhanced temporal decision tree Algorithm	94.27

The results obtained from the classification algorithm have been measured in terms of sensitivity, specificity and accuracy. The best five experimental results have been tabulated in the Table 9, Table 10 and Table 11. The performance of the proposed Temporal Decision Tree is compared with other decision trees. From the experimental results, it has been observed that the proposed Temporal Decision Tree Algorithm provides better results when it is compared with other existing algorithms.

Table.9 Performance Analysis with Sensitivity (In Percentage)

Exp. No.	Random Tree	Part	J48	Enhanced temporal decision tree Algorithm
1	82.3	85.5	90.27	90.27
2	85.6	82.3	88.02	92.02
3	87.5	81.5	91.21	94.21
4	81.5	83.2	89.10	95.10
5	84.5	84.2	91.23	92.23
Average	**84.28**	**83.34**	**89.97**	**92.77**

Table.10Performance Analysis with Specificity (In Percentage)

Exp. No	Random Tree	Part	J48	Enhanced temporal decision tree Algorithm
1	81.3	82.5	91.23	92.3
2	84.2	80.4	90.04	95.5
3	84.5	82.4	90.43	96.5
4	82.4	86.8	93.02	95.5
5	80.3	87.3	90.43	96.4
Average	**82.54**	**83.88**	**91.03**	**95.24**

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

Table.11 Performance Analysis with Accuracy (In Percentage)

Exp. No.	Random Tree	Part	J48	Enhanced temporal decision tree Algorithm
1	81.9	81.5	90.27	93.4
2	82.8	83.5	91.24	95.3
3	84.2	85.6	90.63	96.6
4	85.3	85.3	91.34	93.4
5	87.7	86.2	92.78	91.5
Average	**84.38**	**84.42**	**91.25**	**94.04**

Table 12 shows that the comparative analysis of performance of algorithm with metrics sensitivity, specificity and accuracy and the enhanced temporal decision tree Algorithm with IHRF Algorithm give the best results.

Table 12: Comparative Analysis of Performance

Algorithm / Measures	Random Tree	Part	J48	Enhanced Temporal Decision Tree Algorithm
Sensitivity	84.28	83.34	89.97	92.77
Specificity	86.54	83.88	91.03	95.24
Accuracy	84.38	84.42	91.25	94.04

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

The Figure 3 shows the performance analysis of all algorithms. The proposed Enhance Temporal Decision Tree Algorithm shows good results among all algorithms

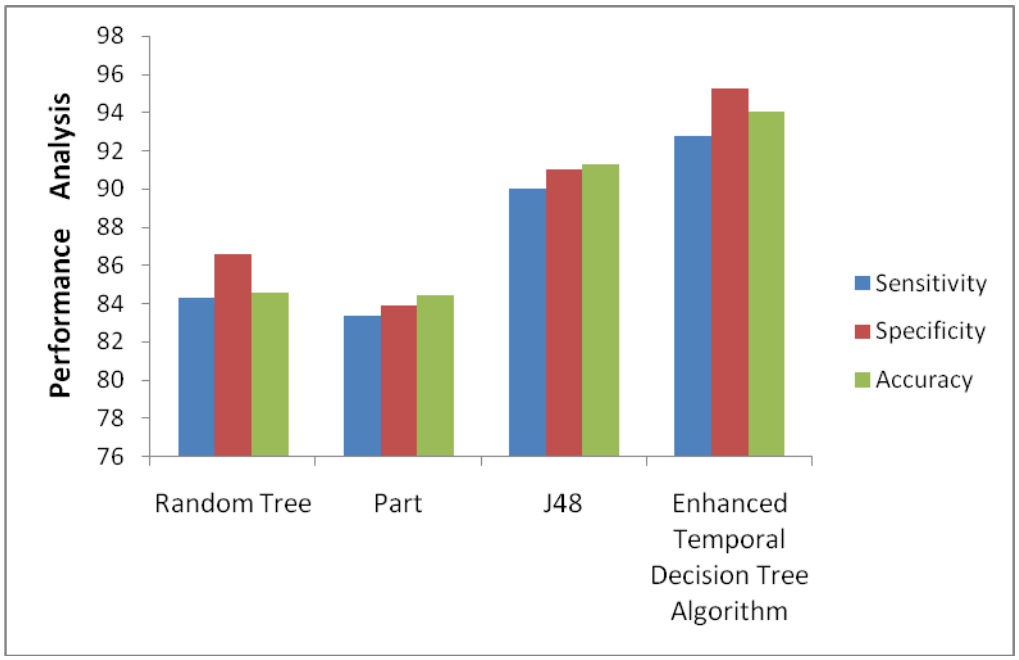

Figure 3 Performance Analysis of various algorithms

VI. CONCLUSION AND FUTURE WORK

In this paper, Intelligent Hybrid Relevant Feature Algorithm has been proposed and implemented. The proposed features selection algorithm is used to select the optimal number of features from HTTP CSIC2010 dataset and they are used to classify the normal and abnormal HTTP web request. Using weak tool and new Enhanced Temporal Decision Tree classification algorithm is implemented and gives the best result with minimum false alarm using 10-fold cross validation method.

REFERENCES

1. Scholte, T, Robertson, W, Balzarotti, D &Kirda, E 2012, 'An empirical analysis of input validation mechanisms in web applications and languages', Proceedings of the 27th Annual ACM Symposium on Applied Computing, pp. 1419-1426.
2. Frajt, K, Bureš, M &Jelínek, I 2014, 'Reducing user input validation code in web applications using Pex extension', International Conference on Computer Systems and Technologies - CompSysTech'14 Reducing, pp. 302-308
3. Kirit& Patel 2015, 'Detection and Prevention of Input Validation Attacks: Survey and Strategies', International Journal of Emerging Research in Management &Technology, vol. 9359, no. 12, pp. 116-120.
4. Cao, LC 2006, 'Detecting web-based attacks by machine learning', Proceedings of the 2006 International Conference on Machine Learning and Cybernetics, vol. 2006, no. August, pp. 2737-2742.
5. Kumar, P &Pateriya, RK 2013, 'Enhanced Intrusion Detection System for Input Validation Attacks in Web Application', IJCSI International Journal of Computer Science Issues, vol. 10, no. 1, pp. 435-441.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 12, December 2017

6. He, Q, Wang, Y, Linlin, Y & Key, QK 2013, 'P2PRPIPS: A P2P and reverse proxy based web intrusion protection system', Research Journal of Applied Sciences, Engineering and Technology, vol. 5, no. 7, pp. 2439-2444.
7. Livshits, VB & Lam, MS 2005, 'Finding Security Vulnerabilities in Java Applications with Static Analysis', Architecture, pp. 18-18.
8. Artzi, S, Kiezun, A, Dolby, J, Tip, F, Dig, D, Paradkar, A & Ernst, MD 2010, 'Finding bugs in web applications using dynamic test generation and explicit-state model checking', IEEE Transactions on Software Engineering, vol. 36, no. 4, pp. 474-494.
9. Manmadhan, S &Manesh, T 2012, 'A Method of Detecting SQL Injection Attack To Secure Web Applications', International Journal of Distributed and Parallel Systems, vol. 3, no. 6, pp. 1-8.
10. Yeole, AS & Meshram, BB 2011, 'Analysis of different technique for detection of SQL injection', Proceedings of the International Conference & Workshop on Emerging Trends in Technology - ICWET '11, vol. 1, no. Icwet, pp. 963-963.
11. Kruegel, C &Vigna, G 2003, 'Anomaly detection of web-based attacks', Proceedings of the 10th ACM conference on Computer and communications security, vol. 03, no. November, pp. 251-251.
12. Fonseca, J, Seixas, N, Vieira, M & Madeira, H 2014, 'Analysis of field data on web security vulnerabilities', IEEE Transactions on Dependable and Secure Computing, vol. 11, no. 2, pp. 89-100.
13. Pack, DJ, Streilein, W, Webster, S & Cunningham, R 2002, 'Detecting HTTP Tunneling Activities', Proceedings of the 2002 IEEE Workshop on Information Assurance, pp. 1-8.
14. **Maheswari KG** & Anita R 2015 "Generalization of minkowski distance metrics in mixed case analysis for web intrusion detection" in **International Journal of Soft Computing,** vol. 10, no. 4, pp. 274-278, ISSN ISSN 1816-9503.
15. **Maheswari KG** & Anita R 2015 "A dynamic tool for detection of xss attacks in a real time environment" **ARPN Journal of Engineering and Applied Science**, vol. 10, no. 10, pp. 4627- 4634, ISSN 1819-6608.
16. **Maheswari KG** & Anita R 2016 'A dynamic virtual machine security scheme against co resident attack in cloud computing' **Asian Journal of Information Technology**, vol. 15, no. 13, pp. 2116-2122, ISSN 1682-3915.
17. G. Nalinipriya, P.J.Varalakshmi, K.G.Maheswari, R. Anita, 'An Extensive Survey on Co- Resident Attack in Dynamic Cloud Computing Environment" published in **International Journal of Applied Engineering Research ,** ISSN 0973-4562 , Volume 11, Number 5 , pp 3019-3023 , **2016.**