Intelligent Network Intrusion Prevention Feature Collection and Classification Algorithms

Deepaa Selva [1], Balakrishnan Nagaraj [2],*, Danil Pelusi [3], Rajendran Arunkumar [2] and Ajay Nair [2]

[1] Department of Electronics and Communication Engineering, Karpagam University, Coimbatore 641021, Tamil Nadu, India; deepaa.selva@gmail.com
[2] Rathinam Group of Institution, Rathinam Technical Campus, Coimbatore 641021, Tamil Nadu, India; r.arunkumar@rathinam.in (R.A.); ajaynair707@gmail.com (A.N.)
[3] Faculty of Communication Sciences, University of Teramo, 64100 Teramo, Italy; dpelusi@unite.it
* Correspondence: nagaraj@rathinam.in

Abstract: Rapid Internet use growth and applications of diverse military have managed researchers to develop smart systems to help applications and users achieve the facilities through the provision of required service quality in networks. Any smart technologies offer protection in interactions in dispersed locations such as, e-commerce, mobile networking, telecommunications and management of network. Furthermore, this article proposed on intelligent feature selection methods and intrusion detection (ISTID) organization in webs based on neuron-genetic algorithms, intelligent software agents, genetic algorithms, particulate swarm intelligence and neural networks, rough-set. These techniques were useful to identify and prevent network intrusion to provide Internet safety and improve service value and accuracy, performance and efficiency. Furthermore, new algorithms of intelligent rules-based attributes collection algorithm for efficient function and rules-based improved vector support computer, were proposed in this article, along with a survey into the current smart techniques for intrusion detection systems.

Keywords: selection techniques; intrusion detection; neural networks; fuzzy concepts

1. Introduction

Recently, the Internet became an integral part of everyday life. The existing web-based data processing systems are subject to numerous attacks, resulting in substantial losses of multiple types of injury [1]. The importance of security of information, therefore, evolves rapidly. Information security is most importantly designed to develop defense systems that are locked against unauthorized use, alteration, disruption, or destruction, access, and disclosure [2]. Cyber management minimizes the threats regarding secrecy, honesty, and quality relevant to the three main protection goals.

In the past, different systems were developed to detect and block attacks from the Internet. Mortgage detection systems (MDS) are essential systems because they can effectively withstand external attacks [3]. Besides, MDSs deliver a security wall that overcomes the assault on the Internet on computer systems. If a traditional firewall is not good, MDS has been used to detect dissimilar types of occurrences on the networking and the workstation system [4]. The identification of intrusion is expected to vary from the legal user in the actions of intruders. MDS is generally divided into two types such as misuse detection and anomaly based on its methods of exposure [5]. The analysis of anomaly intrusions decides how defects from the standard patterns of use can be identified as intrusions. Issue detection systems, of effectively distinguish destructions of permissions [6]. Smart agents and classification techniques can be used to build intrusion detection systems. Most MDS s operate in two phases, namely intrusion detection and pre-processing step on developing an intrusion prevention system, the intrusions identified the MDS has been effectively prohibited. The main feature of this paper is a smart technique survey suggested in MDS

development [7]. It discusses a new MDS industrialized using two future algorithms such as smart rule-based collection algorithms and smart rules-based improved multiclass vector provision machines.

Smart MDS are the smart computer programs in the network, which evaluate the flexibly function and environment to improve the precision of the identification [8]. These programmers, both through environmental learning and through inference rules, are used to calculate actions to be carried out in the environment. Smart MDSs are in a position to take decisions and to test restrictions. In most smart programs, laws are either shot or decision-making agents are included. Besides, static agents and a number of mobiles have been used to realize a particular objective. Smart intrusion detection systems were developed through the provision of intelligent pre-processing and effective classification techniques [9]. In comparison with other approaches, such MDSs provided a better detection rate.

Classification is used to learn from many labeled data instances called training a model called a classifier and classified a test example the classes utilizing an educated ideal known as analysis. Classification-based on techniques for variance finding work similarly in two phases. The course segment will teach a classifier with the characterized training statistics available [10]. The test segment uses the classificatory to classify a test instance as normal or abnormal. Classification variance detection techniques operate either under one or more classes. One-class-specific variance recognition performances are based on the statement that only one class label exists for each training instance. Both methods use a one-gender classification algorithm to know a biased boundary across standard cases. Any test instance not within the studied limits is considered to be "anomalous" in a multi-class anomaly detection process. The training data suggest that there are classified instances in different ordinary classes [11]. The classificatory is directed to vary between every normal course and the rest of classes such methods of anomaly detection. A test instance is treated as abnormal if any of the classifiers do not recognize it as natural. In this subcategory, some techniques associate the trust with the classification prediction. If neither of the classifiers is sure that the test instance is labeled as natural, the situation is anomalous.

In two groups, wired networks and wireless networks are classified as communication networks. Wired systems are linked via copper wires, or certain forms of cables are linked. Satellite and wireless connections link wireless networks. Either with wired networking or with a wireless network may be handheld computer devices. For smartphones and cell telephones emerging, personal computing and cellular networks is used the most. Wireless networks are classified into two types: technology-based networks and networks without technology [12]. Both nodes are considered to be mobile in service-based wireless networks and linked as an interface to base station. In a situation like this, any form of contact in a system based on this base station is only carried out via the so-called base station. Mobile nodes are connected without depending on the infrastructural structure and therefore all mobile nodes communicatively without the control of the base station in the wireless network commonly called Mobile Ad Hoc Networks.

2. Literature Review

Several research on classification methods and rule-based strategies for the production of smart intrusion detection systems have in the past been carried out [13]. However, the literature only took into account the standard data set to build IDS for most applications. Nonetheless, IDS may be made more reliably if both the simulation dataset and actual dataset are checked. Besides, benchmark datasets for wired networking, such as KDD Cup are created [14]. In a given situation, IDS built for MANET will initially be checked using benchmark data set or with actual ad-hoc network trace data.

Artificial neural network development has a major advantage in providing intelligent decision rules and was developed through the structure and operation of the human brains [15]. In such a case, the ANN is designed to contain many neurons with a resemblance to the human brain that are interconnected synapses, consisting of millions and

millions of tiny units that are called neurons for input, processing, and output. In the past, several soft computation techniques have been developed, either separately or in collaboration with other soft calculation techniques, expanding the fuzzy set theory [16].

In many applications, including data extraction, search algorithms, capacity planning, and developing shortest path algorithms, genetic algorithms (GAs), are used [17]. The literature contains many works using neural networks for many reasons of course including selecting features, image processing, categorization, and interference detection because they converge very quickly and offer the ideal solution within a limited time. The author suggested a new fugitive genetic method for the mining of association rules to examine transaction help and trust [18]. In this scenario, genetic algorithms are used to help locate K-item collections, which allow less storage, which tests quite quickly. Genetic algorithms have been assessed for an optimum solution with a cost function known as fitness. The genetic algorithm can, therefore, be used independently or in conjunction with other soft-calculation techniques to develop smart decision-making systems.

In developing a feature selection algorithm, there are two main approaches, namely filtering and wrapping methods. The wrapping approach tries a prediction with an optimization feature to choose the next step. Besides, filter methods rely on the existence of the data sets [19]. The wrapper strategies, on the other hand, have more significant outcomes when all facets of the selection process are addressed. A filter system or wrapper method may be used to create IDS. The confidence modeling method suggested is an efficient trust-based method for safe routing. This model classifies users as neighboring nodes and other nodes, it is easy to find trusted neighbors [20].

A modern statistical identification anomaly algorithm has been developed for the creation of IDS based on Markov classification chains. Their model has been able to preview intrusions in advance because they use the Markov chain building algorithm, which analyzes the data set efficiently. Proposed new IDS installed on each MANET node to provide adequate network protection. As their concept, they suggested to be solved as an optimization process, a strategy for reducing the actual length of the IDSs deployed in all MANET nodes [21]. Besides, the authors developed a new model of cooperative games to represent the different interactions between IDSs that are deployed around all the nodes. This model's main advantage is that it extends to heterogeneous networks and optimizes energy detecting and preventing intrusion.

Multi-agent structures may be used in this way [22]. Multiple agents for security surveillance and communication operations are employed in hosts and networks within this scenario. Many literatures have utilized co-operative agents who prepare in advance to achieve optimum cooperation and communication in the identification of intrusions [23]. The project requires a modern, multi-agent framework for controlling the network for co-ordinated analysis to provide efficient system stability among the works available in the literature for multi-agent systems. They proposed a modern multi-agent focused method for the creation of a multi-agent intelligent intrusion detection program named multi-agent dependent [24]. In their model, they used a learner who learned new rules and applied the rules to decide on intrusion detection effectively.

The multiclass vector machine support algorithm (MSVM) can perform multi-parameter classification [25]. Various forms of threats may be more easily categorized using multiclass SVM when designing an intrusion detection program [26]. In the past, such IDS were developed to provide greater detection accuracy integrating the decision tree algorithm with the multiclass SVM—the new abuse-oriented IDS proposed the multilevel and hybrid algorithm of classification. To detect intrusions more efficiently, their system combines the decision tree classificatory and clustering algorithms.

3. The Architecture of System ISTID

The machine design contains the eight critical elements suggested in this work. The following include intrusion detection module, cup data set, network trace data agent,

decision manager, data preprocessing module, trust-based routing module, and knowledge data collection agent, as shown in Figure 1.
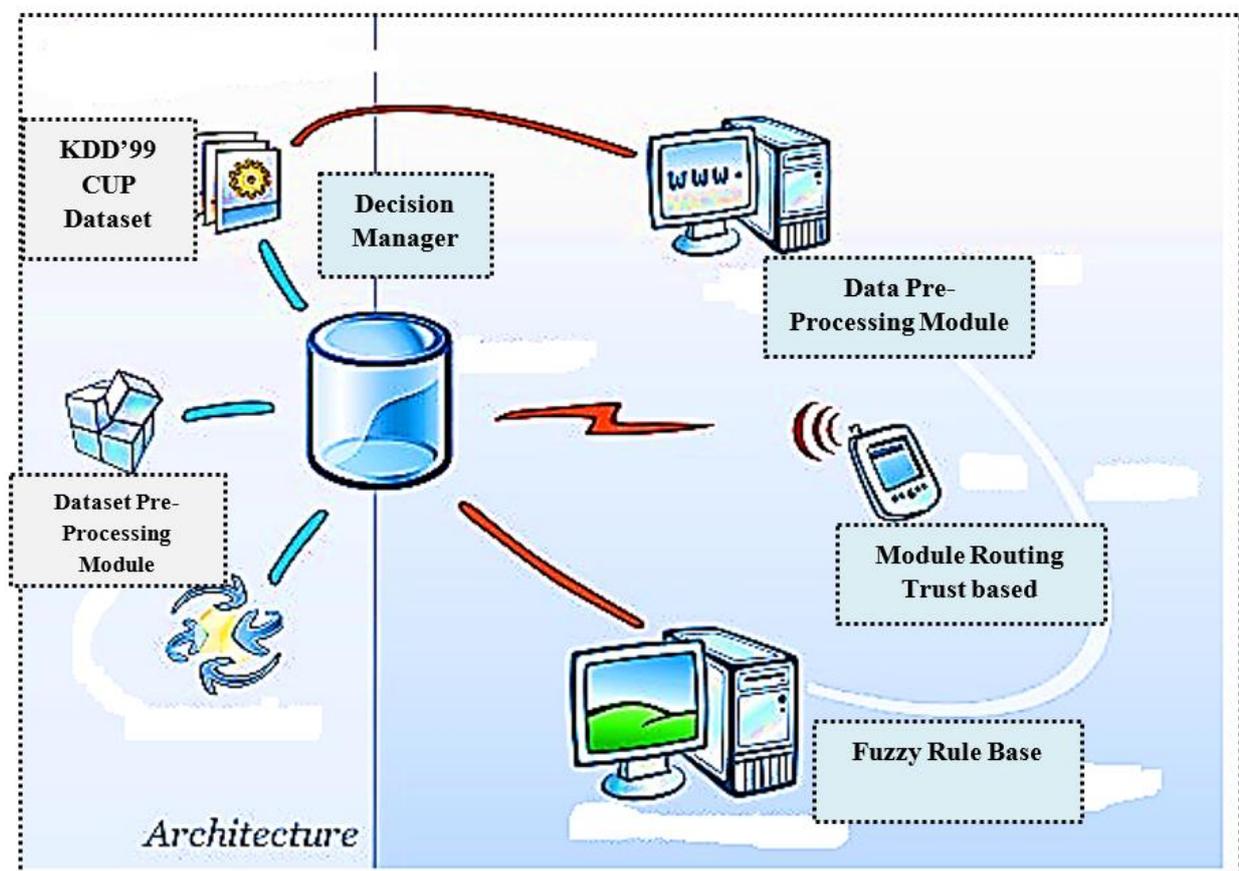
Figure 1. Architecture of System ISTID.

In the user experience module, the data from the databases would be stored. These data are transmitted to the data preparation module. The preprocessing module incorporates preprocessing approaches, such as normalizing with the min-max and incremental feature selection algorithms, for efficient preprocessing. For successful classification of the dataset, the intrusion detection module uses algorithms of classification. The decision manager monitors the overall work of this system. The decision manager takes decisions on selecting, classifying, and routing functions using rules.

Finally, there are two components in the trust-based routing module, namely the component cluster and routing subsystems. The clustering sub-system is the clustering method of the network nodes. This module covers the formation of groups, cluster heading choices and the routing of these cluster heads after calculation and trust values. The routing module is responsible for the phase of path.

3.1. Proposed Algorithm

In these works, the intelligent feature selection techniques and intrusion detection (ISTID) is proposed to be the new smart classification algorithm. This algorithm optimizes rule generation during the training stage and stores the optimum rules in a knowledge base that is indexed according to time intervals. In the next step, the input fluctuates and genetic operations are carried out to conduct the classification of intrusion data used for processing. The fused input corresponds to the fused genetic regulations established in the basis of knowledge, and validation is controlled for time constraints. Finally, for each input information, the classification algorithm decides the class.

Let 'E' be the 'n' data records database. The database is split into the testing dataset (E1) and the evaluation dataset (E2) in two sections. The genetic time fuzzy rules are produced, and the training datasets are used. This device is checked ten times over. Therefore, 92% of data sets are for preparation, and 8% are for research purposes. The data sets are included. This is done until all records have been tested. This research translates all attributes of the data set into a standard format using the numerical values from zero to one which is simple to compare during classification. For that reason, the minimum and maximum value is known as the limits for each attribute, and the interval between the maximum and minimum values is determined the attribute duration. The standardized cost is calculated using an equation formula:

$$Normalize\ value\ (J) = \frac{Value\ of\ Given\ (J)}{maximum\ value - minimum\ value} \tag{1}$$

Equation (1) where the *Jth*data record is indicated, given value is current, normalized value is the computed value between zero and one, the max value is the maximum value for the specific attribute, and the minimum value is the maximum value for the specific attribute.

3.2. Pre-Processing Normalized Data

On every record, the input data is standardized splitting a maximum value into the maximum value, and therefore all data in a single format with a range of values from zero to one. This preparation assists in making easier comparisons in the decision-making process. A new pre-processing algorithm is suggested for this reason, which is named the normalized intelligent GA-based techniques and intrusion detection (ISTID) algorithm. Furthermore, a more pre-processing algorithm called ISTID in these research papers is suggested. This is called the intelligent agent-based incremental sorting algorithm. These two methods for pre-processing are often used to pick attributes from a dataset.

Fitness is an analytical tool used to determine the right benefit. applying the following formula, the fitness function is calculated:

$$g_j\left(B_k,\ E_k^b\right) = \begin{cases} \frac{1}{b+1} & if\ B_k = E_k \\ \frac{1}{b} & Otherwise \end{cases} \tag{2}$$

Equation (2) where B_k—is a rule precedent and E_k—is the database fact. Each record is rotated here such that once the first, twice the second and so on, the first record is rotated. Now, due to migration rotation, the chromosomes are arranged differently.

A crossover process takes place between two parent chromosomes to receive a new chromosome. A new child allele is selected depending on the fusion rate C r. the parent chromosomes are chosen. The fitness feature is added to the child chromosome after a new chromosome is produced. The crossover rate calculation formula is as follows:

$$Rate\ of\ Crossover\ (D_s) = \frac{Gene\ crossing\ number\ Number}{Length\ of\ the\ chromosome} \tag{3}$$

Equation (3), the mutation rate N_s—is determined based on the number of mutations per database N_Q—is the length of the chromosome where O_M—is the mutation point. The mutation risk estimation rule is:

$$rate\ of\ Mutation\ (N_s) = \frac{N_Q}{O_M} \tag{4}$$

In this analysis, the triangular membership feature was chosen to pass the input data to the fused label, as shown in Figure 2. The method for the estimation of membership values is therefore seen below in Equation (4):

$$g(y) = \begin{cases} 0 & if\ y \le b \\ \frac{y-b}{c-b} & if\ b \le y \le c \\ \frac{d-y}{d-c} & if\ c \le y \le d \\ 0 & if\ y \ge d \end{cases} \tag{5}$$
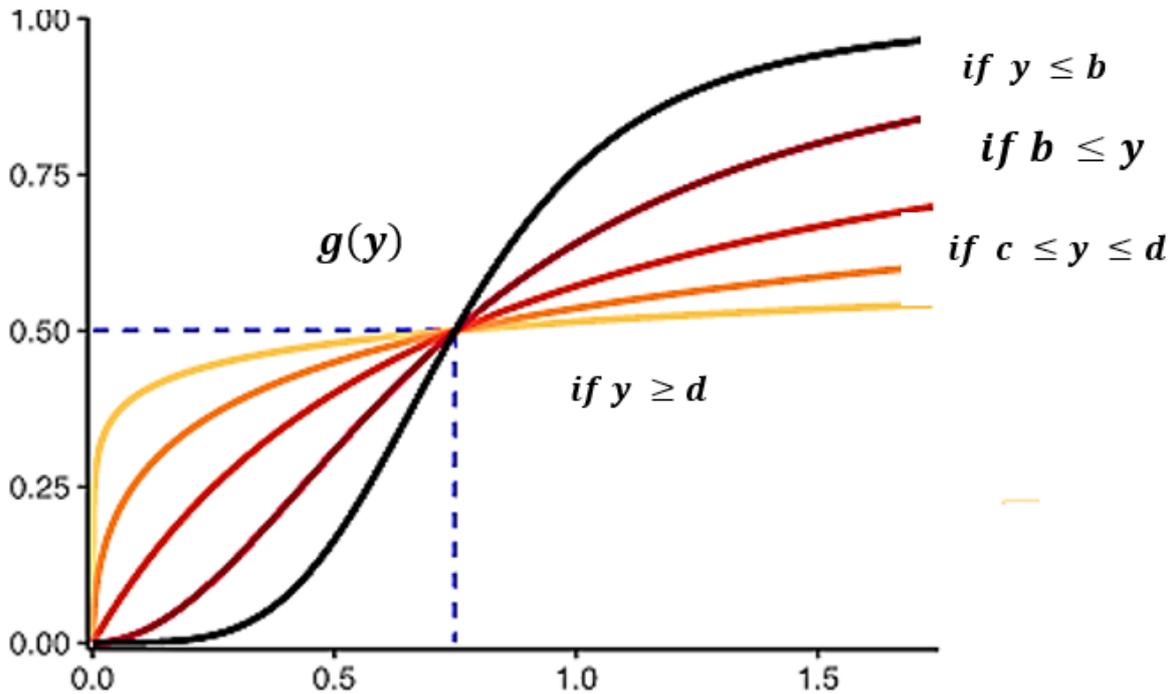
Figure 2. Estimation of Membership.

In this scenario, the codes for the kind of attacks are low, medium, and large. This research was carried out for three-way participation as shown in Figure 3. The basis of knowledge consists of rules generated from the genetic and fugitive operation and trained using the proposed algorithm of classification, which is subject to time constraints. The rules are IF ... BEFORE declarations that are compared internally and overlapping members. Membership features depict a fuzzy set graphically. The x-axis is the discourse universe, and the y-axis shows membership levels inside the [0, 1] interval. To create membership functions, simple functions are utilized. The membership function of a fluid set is to generalize the indicators for traditional sets in mathematics. It is an extension of appraisal, in futile reasoning, of truth.
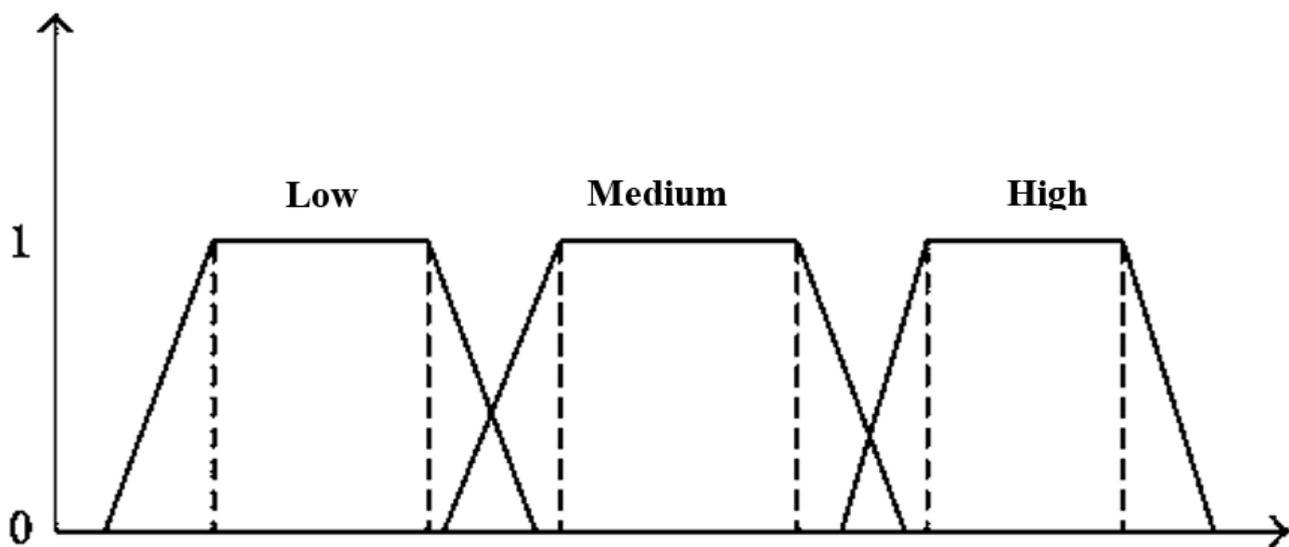
Figure 3. Function with Given Parameter Triangular Membership.

This method is incorporated with the suggested classification model, named the intelligent sequential adaptive genetic techniques and intrusion detection (ISTID)) described in Algorithm 1. The technique is used and the full phases of the algorithm proposed are as follows:

Algorithm 1

Input; Dataset $E_j = \{S_1, S_2, \ldots . S_n\}$
Output: Groups of Classifications
Step 1—Choose the first chromosomes.
Step 2—Submit fuzzy chromosome membership function
Step 3—Assess the fitness of chromosomes
Step 4—Using threshold values to pick a new population
Step 5—Apply time restrictions
Step 6—While the population is present
  i. Compare the process immediately
  ii. Place the ranking comparing values instantaneously
  iii. Comparison of performance interval
  iv. Forms weight population
Step 7—Crossover with the next community for every community of weight
Step 8—Again, add exercise
Step 9—When *fitness value > threshold,*
                Mutate performance
                    Else
Step 10—Form policy based on conduct

Genetic Fuzzy Cognitive Temporal Adaptive Algorithm

This research has established and applied the algorithm of classification of the intelligent temporal adaptive genetic fuzzy. A modern exercise feature has been used for this reason, which helps to make decisions. In the case of instant comparison and period compare procedures, time constraints are often added. Finally, in this algorithm, a triangular membership function based on fuzzy logic has been applied for flushing and deflation. The essential advantage of the proposed algorithm is the usage of time limits, dynamic logic, and genetic algorithms as an efficient decision-making tool.

In this model, two datasets were used to check the suggested IDS: the KDD cup dataset and the network trace dataset. The dataset module for the KDD cup consists of the data from the MIT Lincoln laboratory. This data set is a benchmark data set that is accepted in standard data sets to test intrusion detection systems. During this research study, the cup

data collection for the KDD 1999 is used for the testing of the proposed algorithms because it is more widely used for the measurement of algorithms for intrusion detection. This dataset contains 41 attributes, and each is useful to explain the network behavior. These attributes have 38 numerical characteristics as well as 3 typical characteristics that give a total of 41.

A one hour-long simulation of 15 min to produce and track attacks took place in the actual networks. The trace data collection was collected. The KDD cup dataset is the initial check for all the algorithms proposed in this research, and they are checked with network trace knowledge. The intrusion detection rates of the proposed algorithms are identical when they are performed with this dataset and with actual network trace datasets in low mobility and medium-mobility scenarios in this work.

4. Result and Discussion

This section discusses data sets, performance measurements, and experimental findings. The reasons why the proposed system is being achieved are presented here.

4.1. Performance Analysis

In this study, the precision of the identification of intrusion was developed using the following measures to test the device proposed. Since the detection exactness is affected these metrics, recall, and G-measure are as follows:

4.2. Precision

Precision is specified as the data ratio conditioned to the data related to the detection. The calculation is computed in Equation (6).

$$Precision = \frac{PT}{PT + PF} \tag{6}$$

4.3. Recall

The partnership with data necessary for the practical identification of data. The formula can be computed in Equation (7).

$$Recall = \frac{PT}{PT + NP} \tag{7}$$

4.4. G-Measure

The G-measure is used to be the fraction of accuracy minus reminder. It has a beta value which is typically 1:

$$G - Measure = \frac{\left(1 + \propto^2\right) \times Precision \times Recall}{\propto \left(Precision + Recall\right)} \tag{8}$$

In Equation (8), the performance evaluation is based on the number, time, accuracy, and false-positive rates of the generated detectors (rules). The ISTID test dataset is used during each repeated improvement iteration. The accuracy of the rating and the false positive rate (FPR) is calculated as follows:

$$Accuracy = \frac{PT + NT}{PT + PF + NF + NT} \tag{9}$$

Equation (9), where true positive (PT) samples are classified as naturally valid, and false positive (PF) samples are wrongly classified as an irregular, real negative (NT) samples are appropriately classified as a different sample and false negative (NF).

The tests are conducted utilizing the new method with the same data set, and the actual framework is shown in Table 1. Such experiments were conducted to identify attacks from Study, DoS, S2M or V2S. Table 1, with respect to precision, recall, and G-measure,

shows the results obtained for all four different types of attacks. Although the ISTID utilizes the same collection of data as the current IGS, the exact classification with the usage of intelligent agents and the time restrictions are outlined in Table 1. A technically adaptive genetic fugitive method is used.

Table 1. Analysis of Attacks.

Attacks	Precision (%)	Recall (%)	G-Measure (%)	Performance Analysis (%)
DoS	88.62	92.31	91.25	92.35
S2M	92.65	94.62	93.52	94.52
Probe	94.52	92.16	96.14	93.64
V2S	92.36	96.72	94.25	97.25
ISTID	99.14	98.36	99.26	98.62

In Table 1, the precision, reminder, and F-measurement of the data are improved when the proposed ISTID is classified. That is because ISTID utilizes rational agents and time constraints to make judgments. The system proposed is compared with the existing ISTID (and decision tree classification methods). It has been observed from the experiments carried out that ITAGFS is better able to detect accuracy than the other two techniques. The main reason for this improvement is that the ISTID proposed not only insists on the use and use of the smart agents as well as the knowledge basis to make effective decisions on genetic operations and fugitive time regulations.

The efficiency review is demonstrated five separate tests for the identification of four attack types: Probe, DoS, S2M and V2S. The suggested method of intrusion detection is conducted.

The detection precision may be observed for the identification of four forms of attacks in the different experiments. However, the precise identification of DoS attacks in both tests is higher than the precision of the identification of certain forms of aggression. The false-positive intravenous identification method and current classifiers study as seen in Figure 4.
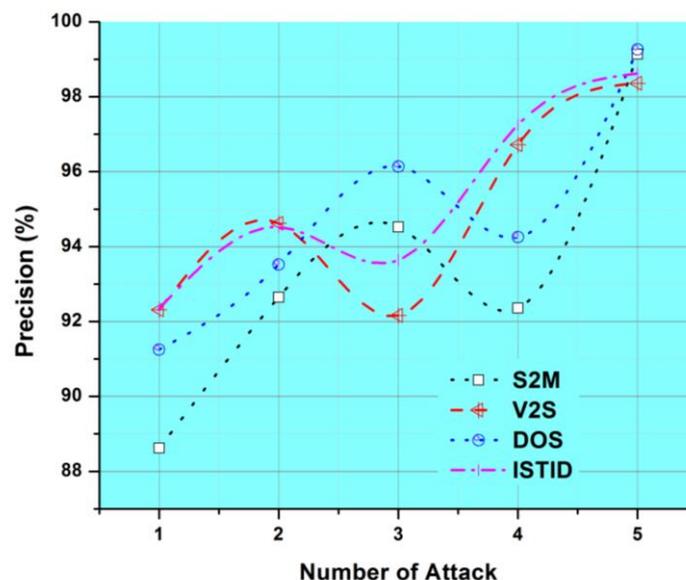
Figure 4. Number of Attacks vs. Precision (%).

The precision of measurement of the device suggested is determined using Equation (5). The study of precision in the identification of attack forms Review, Probe, DoS, S2M and V2S on the proposed method and the current classifiers. It is noted that ISTID is

much better than Probe and other classifiers' performance. Compared to this existing Probe directional system and the different decision-making bodies such as D 6.3 and Enhanced D5.6 the most impressive part of ISTID is a significant improvement.

There are several explanations of why ISTID has improved detection precision. Second, only chosen features are included, as shown in Figure 5. Third, it utilizes transient and pointless laws shot into successful decision-making rational agents. Third, for optimized rules, genetic operations are used. Finally, it calls temporary constraints in the implementation of logic.
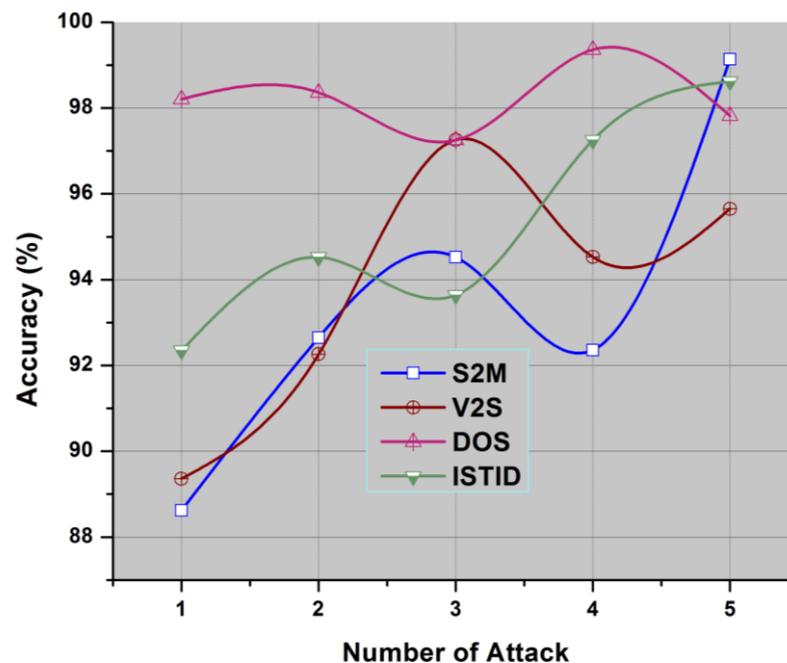
Figure 5. Number of Attacks vs. Accuracy (%).

The efficiency of the proposed program is higher as opposed to current systems can be seen in Figures 5 and 6. The use of most essential features selected the feature selection algorithm, which uses intelligent agents for decision making, enhances the accuracy of the classification process leading to an increase of intrusion detection using temporal constraints, bizarre rules and genetic algorithms.

Table 2 shows an optimum set of functionality chosen the proposed function selection algorithms called the Min-Max Function Selection ISTID Normalized Intelligent GA Algorithm. It is noted in Table 2 that only 14 features from a collection of 32 features present in the KDD cup dataset have been picked from the suggested uniform Intelligent Genetic Fuzzy Cognitive Temporal Adaptive feature selection algorithm. It was evident that as compared to the current frameworks, it increases the efficiency of the proposed ISTID Algorithm. The use of most essential features selected the feature selection algorithm, which uses smart machines for decision making, enhances the accuracy of the classification process leading to an increase of intrusion detection using temporal constraints, bizarre rules, and genetic algorithms.
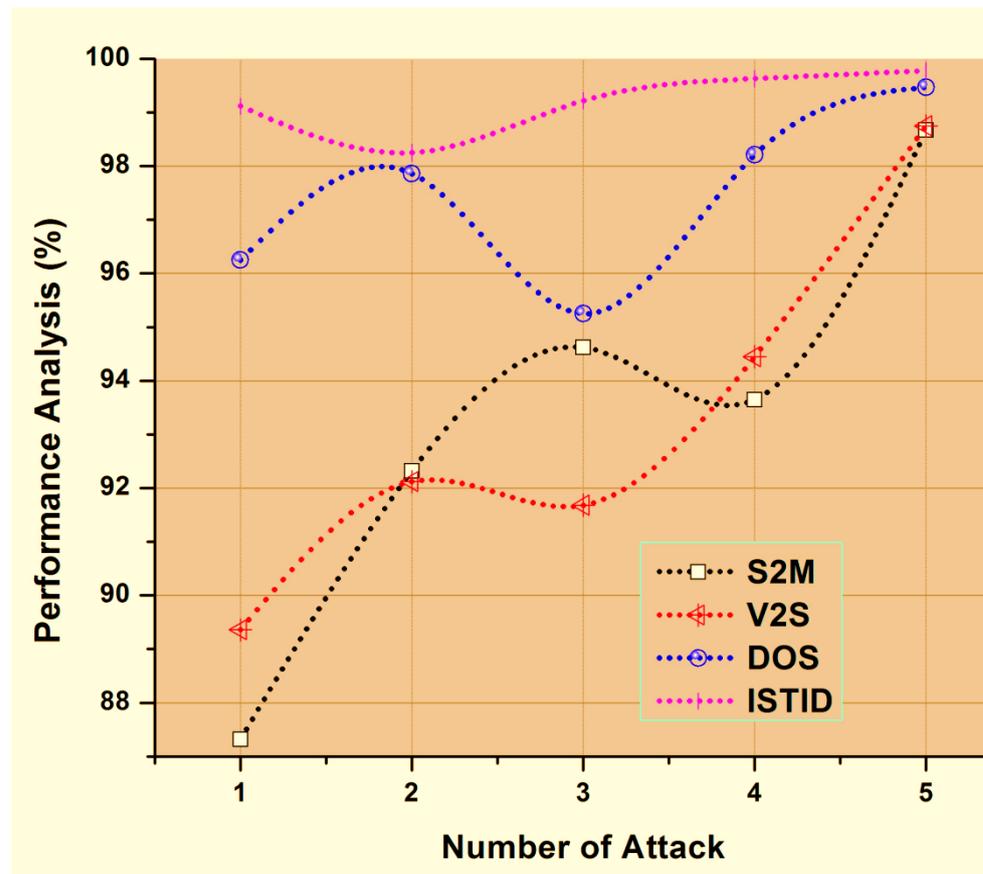
Figure 6. Number of Attacks vs. Performance Analysis (%).

Table 2. Analysis of Attacks.

Attacks	Precision (%)	Recall (%)	G-Measure (%)	Performance Analysis (%)
DoS	91.23	88.12	88.24	98.25
S2M	94.62	96.35	96.23	99.64
Probe	97.85	94.62	97.82	99.72
V2S	98.67	99.82	99.25	99.29
ISTID	95.62	98.26	99.75	99.32

It can be shown that if it is compared with existing ISTID, the performance of the trusted ISTID will perform well. This is because the confidential, secure routing algorithm only uses the trusted routing nodes. The packet delivery ratio in the safe routing model is improved compared to the conventional attack scenario ISTID.

The delay analysis of ISTID and trusted ISTID is shown in Figure 7. Figure 7 demonstrates that using trust values to define the honest nodes and route the trustworthy nodes decreases the latency as opposed to the routing utilizing the traditional ISTID algorithm, as shown in Figure 7. This is because untrustworthy nodes are not taken into consideration in the ISTID. On the opposite, untrustworthy delays are avoided the security method suggested.
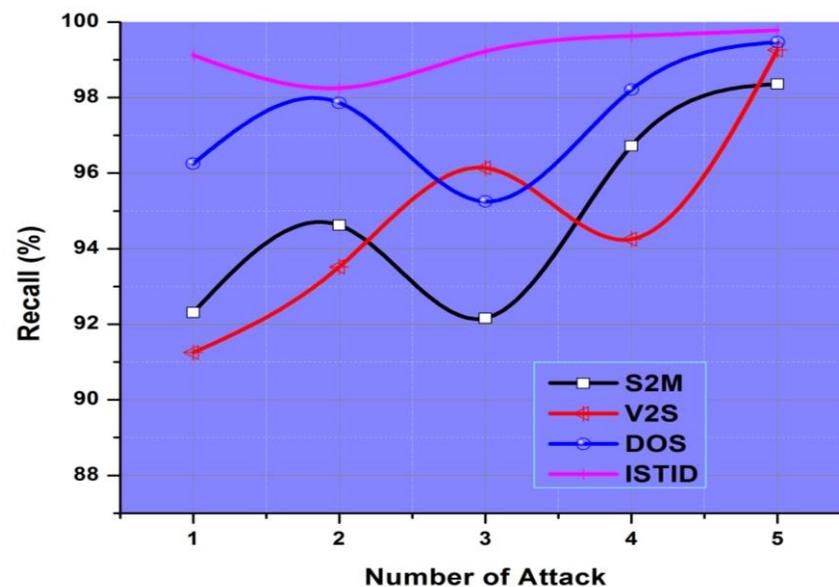
Figure 7. Number of Attacks vs. Recall (%).

The usage of trust scores increases the packet delivery ratio 3.5 percent one point. It is further increased to a boost in the packet delivery ratio of overall 4.32 percent on ISTIDs, while the routing process requires clustering and confidence management.

5. Conclusions

A new protected routing algorithm focused on the cluster, and confidence is suggested in this study. The reliability of routing is ensured in this algorithm increasing the packet returns using IDS feedback. Two new selection algorithms, IAIFSA and ISTIDs were proposed for the development of this intelligent ID. Besides, the idea is to improve the precision of intrusion detection leading to increased reliability of communication utilizing two intelligent classification algorithms ISTIDs and DoS, S2M, and V2S. In comparison, the efficient routing algorithm based on confidence and cluster improves the distribution ratio of packets. It reduces the latency to improve the efficiency of routing utilizing the proposed algorithm.

Author Contributions: Methodology, D.S.; Resources, P.D.; Supervision, B.N.; Writing—original draft, A.N.; Writing—review & editing, A.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Sultana, N.; Chilamkurti, N.; Peng, W.; Alhadad, R. Survey on SDN based network intrusion detection system using machine learning approaches. *Peer Peer Netw. Appl.* **2019**, *12*, 493–501. [CrossRef]
2. Nguyen, T.G.; Phan, T.V.; Nguyen, B.T.; So-In, C.; Baig, Z.; Sanguanpong, S. Search: A Collaborative and Intelligent NIDS Architecture for SDN-Based Cloud IoT Networks. *IEEE Access* **2019**, *7*, 107678–107694. [CrossRef]
3. Selvakumar, B.; Muneeswaran, K. Firefly Algorithm Based Feature Selection for Network Intrusion Detection. *Comput. Secur.* **2019**, *81*, 148–155.
4. Wang, Q.; Lu, P. Research on Application of Artificial Intelligence in Computer Network Technology. *Int. J. Pattern Recognit. Artif. Intell.* **2019**, *33*, 1959015. [CrossRef]

5. Chaabouni, N.; Mosbah, M.; Zemmari, A.; Sauvignac, C.; Faruki, P. Network Intrusion Detection for IoT Security Based on Learning Techniques. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2671–2701. [CrossRef]

6. Salo, F.; Nassif, A.B.; Essex, A. Dimensionality reduction with IG-PCA and ensemble classifier for network intrusion detec-tion. *Comput. Netw.* **2019**, *148*, 164–175. [CrossRef]

7. Chapaneri, R.; Shah, S. A Comprehensive Survey of Machine Learning-Based Network Intrusion Detection. In *Blockchain Technology and Innovations in Business Processes*; Springer Science and Business Media LLC: Berlin, Germany, 2018; pp. 345–356.

8. Khan, F.A.; Gumaei, A.; Derhab, A.; Hussain, A. A novel two-stage deep learning model for efficient network intrusion detection. *IEEE Access.* **2019**, *7*, 30373–30385. [CrossRef]

9. Faris, H.; Ala'M, A.Z.; Heidari, A.A.; Aljarah, I.; Mafarja, M.; Hassonah, M.A.; Fujita, H. An intelligent system for spam de-tection and identification of the most relevant features based on evolutionary random weight networks. *Inf. Fusion* **2019**, *48*, 67–83. [CrossRef]

10. Zhang, W.; Zhang, Z.; Chao, H.C.; Guizani, M. Toward Intelligent Network Optimization in Wireless Networking: An Au-to-Learning Framework. *IEEE Wirel. Commun.* **2019**, *26*, 76–82. [CrossRef]

11. Rajagopal, S.; Kundapur, P.P.; Hareesha, K.S. A Stacking Ensemble for Network Intrusion Detection Using Heterogeneous Datasets. *Secur. Commun. Netw.* **2020**, *2020*, 4586875. [CrossRef]

12. Liu, Y.; Zhu, L. A new intrusion detection and alarm correlation technology based on neural network. *EURASIP J. Wirel. Commun. Netw.* **2019**, *2019*, 109. [CrossRef]

13. Adebowale, M.; Lwin, K.; Sánchez, E.; Hossain, M. Intelligent web-phishing detection and protection scheme using integrated features of Images, frames and text. *Expert Syst. Appl.* **2019**, *115*, 300–313. [CrossRef]

14. Alagrash, Y.; Drebee, A.; Zirjawi, N. Comparing the Area of Data Mining Algorithms in Network Intrusion Detection. *J. Inf. Secur.* **2020**, *11*, 96983. [CrossRef]

15. Alazzam, H.; Sharieh, A.; Sabri, K.E. A feature selection algorithm for intrusion detection system based on Pigeon Inspired Optimizer. *Expert Syst. Appl.* **2020**, *148*, 113249. [CrossRef]

16. Ye, K. Key Feature Recognition Algorithm of Network Intrusion Signal Based on Neural Network and Support Vector Machine. *Symmetry* **2019**, *11*, 380. [CrossRef]

17. Xylogiannopoulos, K.F.; Karampelas, P.; Alhajj, R. Detecting DDoS Attacks. In *Developments in Information Security and Cyber-Netic Wars*; IGI Global: Hershey, PA, USA, 2019; pp. 121–139.

18. Cui, Z.; Du, L.; Wang, P.; Cai, X.; Zhang, W. Malicious code detection based on CNNs and multi-objective algorithm. *J. Parallel Distrib. Comput.* **2019**, *129*, 50–58. [CrossRef]

19. Zhiqiang, L.; Mohi-Ud-Din, G.; Bing, L.; Jianchao, L.; Ye, Z.; Zhijun, L. Modeling Network Intrusion Detection System Using Feed-Forward Neural Network Using UNSW-NB15 Dataset. In Proceedings of the 2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE), Ontario, ON, Canada, 12–14 August 2019; Institute of Electrical and Electronics Engineers (IEEE): New York, NY, USA, 2019; pp. 299–303.

20. Papamartzivanos, D.; Marmol, F.G.; Kambourakis, G. Introducing Deep Learning Self-Adaptive Misuse Network Intrusion Detection Systems. *IEEE Access* **2019**, *7*, 13546–13560. [CrossRef]

21. Dwivedi, S.; Vardhan, M.; Tripathi, S.; Shukla, A.K. Implementation of adaptive scheme in evolutionary technique for anomaly-based intrusion detection. *Evol. Intell.* **2019**, *13*, 103–117. [CrossRef]

22. Zhang, Y.; Chen, X.; Jin, L.; Wang, X.; Guo, D. Network Intrusion Detection: Based on Deep Hierarchical Network and Original Flow Data. *IEEE Access* **2019**, *7*, 37004–37016. [CrossRef]

23. Sahingoz, O.K.; Buber, E.; Demir, O.; Diri, B. Machine learning based phishing detection from URLs. *Expert Syst. Appl.* **2019**, *117*, 345–357. [CrossRef]

24. Suresh, A.; Udendhran, R.; Balamurgan, M.; Varatharajan, R. A Novel Internet of Things Framework Integrated with Real Time Monitoring for Intelligent Healthcare Environment. *J. Med. Syst.* **2019**, *43*, 165. [CrossRef] [PubMed]

25. Pajila, P.J.B.; Julie, E.G. Detection of DDoS Attack Using SDN in IoT: A Survey. In *Advances on P2P, Parallel, Grid, Cloud and Internet Computing*; Springer Science and Business Media LLC: Berlin, Germany, 2019; pp. 438–452.

26. Wang, F.; Jiang, D.; Wen, H.; Song, H. Adaboost-based security level classification of mobile intelligent terminals. *J. Supercomput.* **2019**, *75*, 7460–7478. [CrossRef]