Cloud Computing Environment: An Effective New Intrusion Detection System

[1]Adapa Uma Devi, [2]Dr.Angajala Srinivasa Rao

[1]M. Tech Student, Department of CSE, Kallam Haranadhareddy Institute of Technology (Autonomous), Guntur, umadevikanala05@gmail.com
[2]Professor, Department of CSE, Kallam Haranadhareddy Institute of Technology (Autonomous), Guntur, rao1966@gmail.com

ABSTRACT: Rife acceptance of Cloud Computing has made it bull's eye for the hackers. Intrusion detection System (IDS) plays a vibrant role for it. Researchers have done marvelous works on the development of a competence IDS. But there are many challenges still exists with IDS. One of the biggest concerns is that the computational complexity and false alarms of the IDS escalates with the increase in the number of features or attributes of the dataset. Hence, the concept of Feature Selection (FS) contributes an all-important role for the buildout of an efficacious IDS. New FS algorithm is put forward which is the modified Firefly Algorithm in which Decision Tree (DT) classifier is used as the classification function. We have used the hybrid classifier which is the combination of neural network and DT. We have used CSE CIC IDS 2018 dataset and simulated dataset for performance assessment. Our examination pragmatic that the performance of proposed architecture is better than the state-of-the-art algorithms.

I. INTRODUCTION

Cloud Computing (CC) acquires countless value today. It has on-demand and scalable services. It is satisfying the demand of its users by reducing overall cost and complexities [1]. Diverse types of cloud provide diverse services which fascinates sundry hackers. Intrusion Detection System (IDS) is very imperative. Due to huge traffic generation, cloud computing is becoming an eye-catching target for the attackers. The foremost security concern in this domain is to protect it from different network attacks. IDS ranges from anti-virus software to the well-developed monitoring system. Large data produced by the cloud is a biggest concern [2].

The intrusions concoct the system capricious for the network traffic due to its nonlinear behavior. It is a proactive technology which monitors the malicious activities in the network and provides a protective mechanism. There is urgent need of providing good techniques for detecting attacks. It observes, collects and analyzes the network traffic, log files and actions of users for discovering the malicious activities in the network. Figure 1 represents different IDSs. On the basis of objective for the protection, there are two types of IDSs that are Host-Based IDS and Network-Based IDS where former is monitoring specific hosts and latter is monitoring network for the detection of malicious activities. On the basis of detection technique, there are two types of IDSs that are Anomaly-based and Signature-based where former is for the detection of attacks which are unknown or known and latter is used for known attack detection. IDS related to cloud can be applied to mobile e-health and resource-limited devices. Data mining and Machine Learning (ML) are used by various researchers [3]. Machine classifiers are usually used for binary classification into normal and attack packets [4].

Neural Networks (NNs) are widely used as they can perform very well on incomplete datasets [5]. While each service model in CC has its own benefits, they also encounter particular obstacles. In the case of Infrastructure as a Service (IaaS), virtualization is essential for infrastructure provisioning but has its limitations, and the value of IaaS services may decrease over time. Platform as a Service face challenges related to interoperability, host sensitivity, confidentiality, authorization, reliability, and extensibility. On the other hand, Software as a Service deal with security concerns regarding authorization, authentication, data protection, reliability, and network monitoring. Cloud companies need to tackle these security challenges head-on. Feature Selection (FS) is a basic pre-processing step when the concept of Machine Learning (ML) comes. FS is important for an IDS as it enhances the performance and accuracy and it diminishes the number of features of the dataset or the network record [6], [7]. With the increase in the data accumulation in the databases and data warehouses, the dimensionality problem is becoming a big expostulation for the ML chores [8].

For making an efficacious IDS, there is an exigency of identification of the noteworthy features before the detection of attacks in the network. But the recognition of the significant features is a complicated task because the features can be relevant, extraneous or excessive which hikes the computation complexity for the detection of the attacks or intrusions [9], [10], [11]. Different techniques are used by researchers for developing good attack finding system in by using neural networks.

FS is aiming at retaining the relevant features which are required for building a strong model. For developing an IDS, it is vital to get rid of the irrelevant features so that the accuracy of the IDS increases. The highlights of our contributions are as follows:

- Discerned the various FS techniques and IDSs linked with the CC.
- Proposed a novel FS algorithm by modifying the Firefly Algorithm.
- Proposed a novel architecture for the detection of various attacks affecting CC.
- Latest intrusion detection dataset CSE-CIC-IDS 2018 and simulated dataset are used for the experiment and evaluation.

II. LITERATURE REVIEW

Title: “Intrusion detection systems in cloud comput ing paradigm: Analysis and overview”
Author: P. **Rana, I. Batra, A. Malik, A. L. Imoize, Y. Kim, S. K. Pani, N. Goyal, A. Kumar, and S. Rho**

Cloud computing paradigm is growing rapidly, and it allows users to get services via the Internet as pay-per-use and it is convenient for developing, deploying, and accessing mobile applications. Currently, security is a requisite concern owning to the open and distributed nature of the cloud. Copious amounts of data are responsible for alluring hackers. Thus, developing efficacious IDS is an imperative task. This article analyzed four intrusion detection systems for the detection of attacks. Two standard benchmark datasets, namely, NSL-KDD and UNSW-NB15, were used for the simulations. Additionally, this study highlights the proliferating challenges for the security of sensitive user data and gives useful recommendations to address the identified issues. Finally, the projected results show that the hybridization method with support vector machine classifier outperforms the existing techniques in the case of the datasets investigated.

Title: “Enhanced mechanism to detect and mitigate economic denial of sustainability (EDoS) attack in cloud computing environments”
Authors: P. S. Bawa et al.,

Cloud computing (CC) is the next revolution in the Information and Communication Technology arena. CC is often provided as a service comparable to utility services such as electricity, water, and telecommunications. Cloud service providers (CSP) offer tailored CC services which are delivered as subscription-based services, in which customers pay based on the usage. Many organizations and service providers have started shifting from traditional server-cluster infrastructure to cloud- based infrastructure. Nevertheless, security is one of the main factors that inhibit the proliferation of cloud computing. The threat of Distributed Denial of Service (DDoS) attack continues to wreak havoc in these cloud infrastructures. In addition to DDoS attacks, a new form of attack known as Economic Denial of Sustainability (EDoS) attack has emerged in recent years. DDoS attack in conventional computing setup usually disrupts the service, which affects the client reputation, and results in financial loss. In CC environment, service disruption is very rare due to the auto-scalability (Elasticity), capability, and availability of service level agreements (SLA). However, auto scalability utilizes more computing resources in event of a DDoS attack, exceeding the economic bounds for service delivery, thereby triggering EDoS for the organization targeted. Although EDoS attacks are small at the moment, it is expected to grow in the near future in tandem with the growth in cloud usage. There are few EDoS detection and mitigation techniques available but they have weaknesses and are not efficient in mitigating EDoS. Hence, an enhanced EDoS mitigation mechanism (EDoS-EMM) has been proposed. The aim of this mechanism is to provide a real-time detection and effective mitigation of EDoS attack.

Title: "A survey of mitigation techniques against economic denial of sustainability (EDoS) attack on cloud computing architecture"
Authors: P. Singh, S. Manickam, and S. U. Rehman,
Cloud computing is the next revolution in the Information and Communication Technology arena. It is a model in which computing is delivered as a commoditized service similar to electricity, water and telecommunication. Cloud computing provides software, platform, infrastructure and other hybrid models which are delivered as subscription-based services in which customers pay based on usage. Nevertheless, security is one of the main factors that inhibit the proliferation of cloud computing. Economic Denial of Sustainability (EDoS) is a new breed of security and economical threats to the cloud computing. Unlike the traditional Distributed Denial of Service (DDoS) which brings down a particular service by exhausting the resources of the server in traditional setup, EDoS takes advantage of the elasticity of the cloud service. This causes the resources to dynamically scale to meet the demand (as a result of EDoS attack) resulting in a hefty bill for the customer. In this survey, we review various EDoS mitigation techniques that have been introduced in recent years.

Title: "A novel hybrid KPCA and SVM with GA model for intrusion detection"
Author: F.Kuang,W.Xu,andS.Zhang
A novel support vector machine (SVM) model combining kernel principal component analysis (KPCA) with genetic algorithm (GA) is proposed for intrusion detection. In the proposed model, a multi-layer SVM classifier is adopted to estimate whether the action is an attack, KPCA is used as a preprocessor of SVM to reduce the dimension of feature vectors and shorten training time. In order to reduce the noise caused by feature differences and improve the performance of SVM, an improved kernel function (N-RBF) is proposed by embedding the mean value and the mean square difference values of feature attributes in RBF kernel function. GA is employed to optimize the punishment factor C, kernel parameters and the tube size ε of SVM. By comparison with other detection algorithms, the experimental results show that the proposed model performs higher predictive accuracy, faster convergence speed and better generalization.

Title: "Enhanced intrusion detection and prevention system on cloud environment using hybrid classification and OTS generation"
Author : V.Balamurugan andR.Saravanan
Cloud environment is an assembly of resources for furnishing on-demand services to cloud customers. Here access to cloud environment is via internet services in which data stored on cloud environment are easier to both internal and external intruders. To detect intruders, various intrusion detection systems and authentication systems was proposed in earlier researches which are primarily ineffective. Many existing researchers were concentrated on machine learning approaches for detecting intrusions using fuzzy clustering, artificial neural network, support vector machine, fuzzy with neural network and etc., which are not furnishing predominant results based on detection rate and false negative rates. Our proposed system directed on intrusion detection system and it uses cloudlet controller, trust authority and virtual machine management in cloud environment. We propose two novel algorithms such as (i) *packet scrutinization algorithm* which examines the packets from the users and (ii) hybrid classification model called "NK-RNN" which is a combination of *normalized K-means* clustering algorithm with *recurrent neural network*. For preventing the user from intruders, we propose a *one time signature* for cloud user in order to access the data on cloud environment. Our proposed classifier effectively detects the intruders which are experimentally proved by comparing with existing classification models. Thus our proposed results are expressed by packet loss ratio, average packet delay, throughput, detection rate, false positive rate and false negative rate.

III. A. EXISTING SYSTEM

In [12], a model called Game Theory-based Cloud Security Deep Neural Network (GT-CSDNN) was proposed. This model incorporates both defender and attacker techniques using game theory principles. The main goal is to classify a network administrator to be aware of the nature of such traffic in order to effectively block and terminate any intrusive network connections. To achieve this, the Binary-Based Particle Swarm Optimization (BPSO) technique was utilized to identify the most relevant network features, while the Standard-Based Particle Swarm Optimization (SPSO) was used to fine-tune the control parameters of the Support Vector Machine (SVM).

In [17], authors evaluated and presented a detector based on Radial Basis Function Neural Network (RBF-NN) for detecting DDoS attacks. However, the resulting network structure can often be insufficient or unnecessarily complex, requiring manual configuration through a trial-and-error approach. This study proposes the use of the Bat Algorithm (BA) to automatically configure the RBF-NN network structure. In [18], authors introduced a highly effective approach called the Dragonfly-Improved Invasive Weed Optimizerbased Shepard CNN (DIIWO-based ShCNN) for detecting intruders and mitigating attacks in the cloud paradigm. This approach also enables the detection of intruders using ShCNN.

In another study [19], a powerful Intrusion Detection System (IDS) was proposed using the Sailfish Dolphin Optimizer-based Deep RNN (SFDO-based Deep RNN) to identify anomalies in the cloud framework. The SFDO algorithm combines the Sailfish Optimizer (SFO) with the Dolphin Echolocation (DE) technique. The ChicWhale technique can be utilized forVirtual Machine (VM) migration and cloud data management.

In [20] conducted a study on an IDS (Intrusion Detection System) using a Fisher Kernel-Based PCA dimensional reduction technique and a Grey Wolf Optimizer (GWO)- based weight dropped Bi-LSTM technique (FKPCA-GWO WDBiLSTM). Firstly, they combined the data record with PCA to achieve linearly separable dimensionality reduction by using the fisher kernel with fisher score as input. Secondly, they employed the WDBiLSTM network to retain long-term dependencies while eliminating features from both forward and backward directions. In another study [21], a novel Deep Learning (DL) approach incorporating CNNs Convolutional Networks and Recurrent Neural Networks was developed for cloud security in IDS. With this DL technique, technique, they were able to prevent some detected but unauthorized traffic from accessing the server in the cloud.

DISADVANTAGES

- ➢ An existing system didn’t explore Implementation of Decentralized Identifiers.
- ➢ An existing system didn't implement Token-Based Access Control.

B. PROPOSED SYSTEM

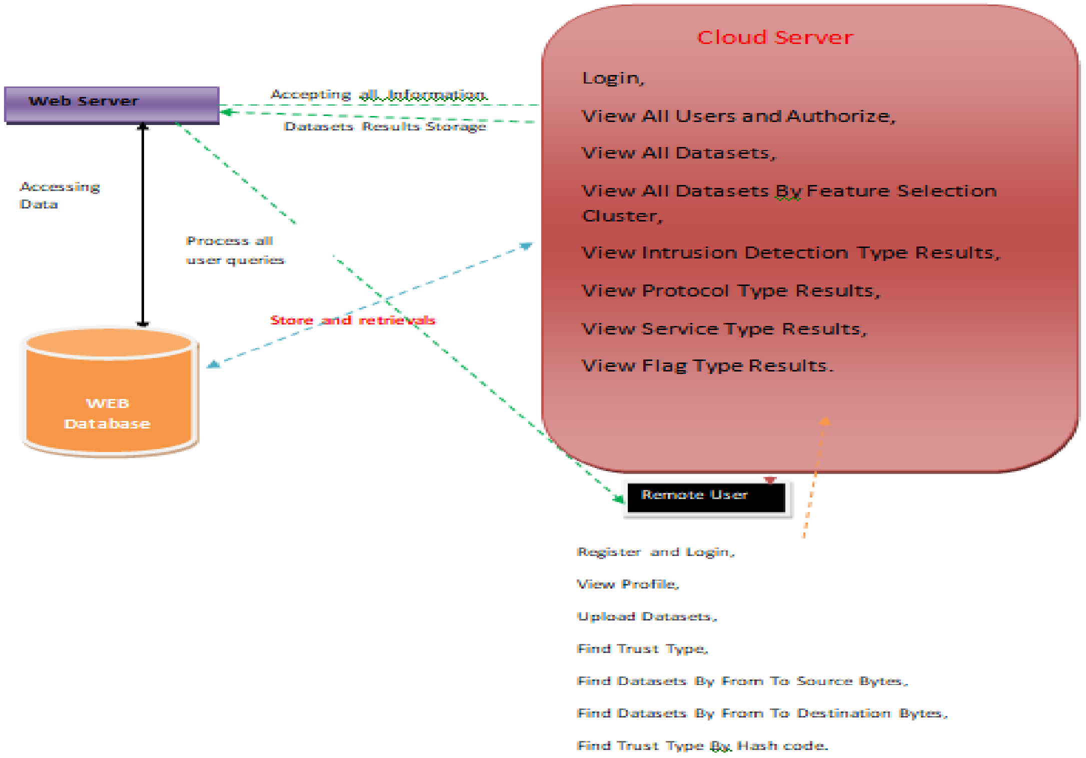
FS is aiming at retaining the relevant features which are required for building a strong model. For developing an IDS, it is vital to get rid of the irrelevant features so that the accuracy of the IDS increases. The highlights of our contributions are as follows:

- Discerned the various FS techniques and IDSs linked with the CC.
- Proposed a novel FS algorithm by modifying the Firefly Algorithm.
- Proposed a novel architecture for the detection of various attacks affecting CC.
- Latest intrusion detection dataset CSE-CIC-IDS 2018 and simulated dataset are used for the experiment and evaluation.

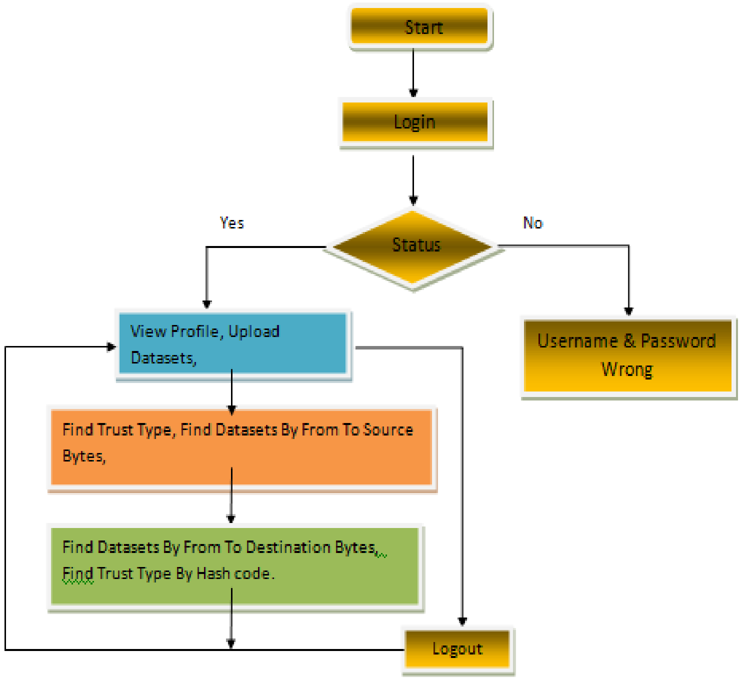
ADVANTAGES

1. FFA is used in modified form for
2. FS.
3. Latest attacks are detected by proposed work. Latest dataset is used for validation of dataset.
4. Simulated dataset is created for the checking the performance of the proposed work.
5. Hybridization is done in FS module and classification module for the development of an efficient IDS.

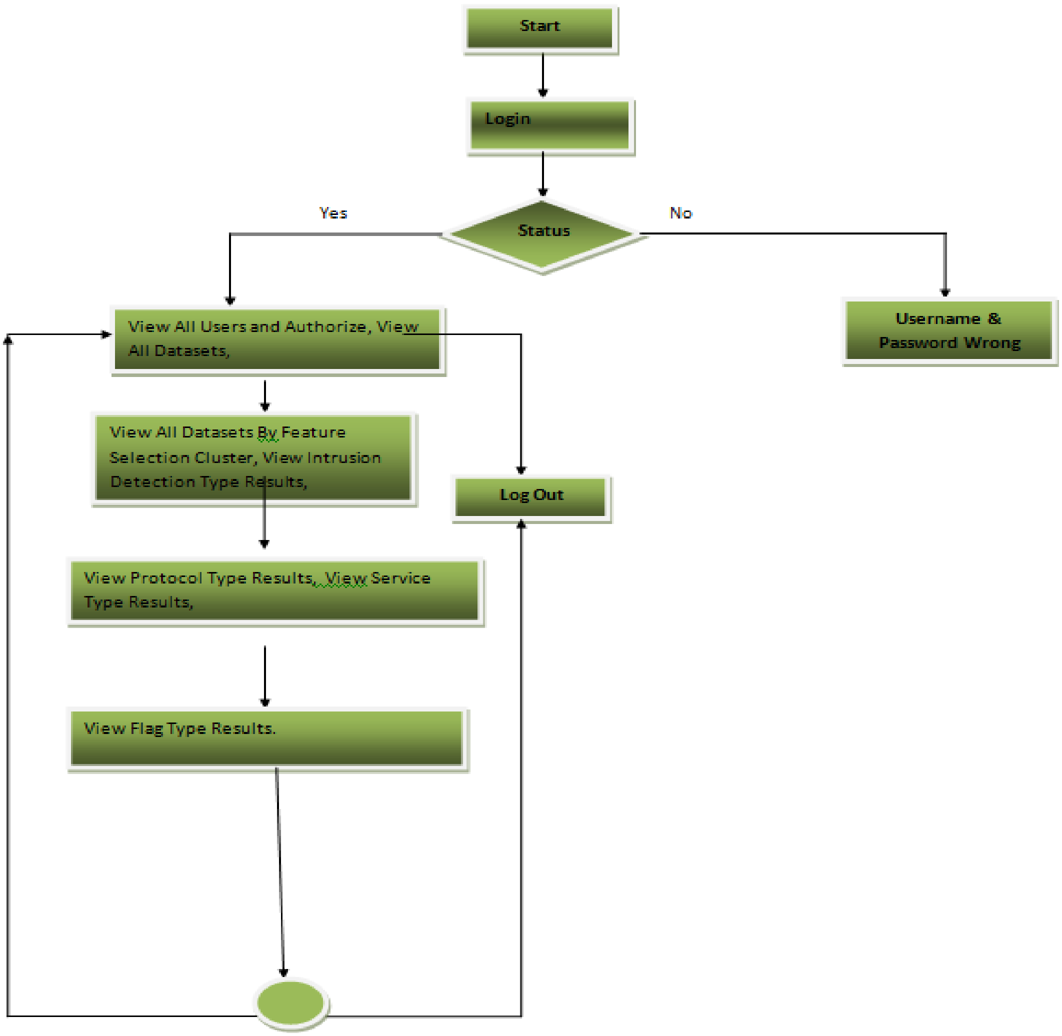
IV. PROPOSED SYSTEM ARCHITECTURE:


Cloud Server
Login,
View All Users and Authorize,
View All Datasets,
View All Datasets By Feature Selection Cluster,
View Intrusion Detection Type Results,
View Protocol Type Results,
View Service Type Results,
View Flag Type Results.
Web Server
Accepting all Information
Datasets Results Storage
Accessing Data
Process all user queries
Store and retrievals
WEB Database
Remote User
Register and Login,
View Profile,
Upload Datasets,
Find Trust Type,
Find Datasets By From To Source Bytes,
Find Datasets By From To Destination Bytes,
Find Trust Type By Hash code.

FLOW CHART DIAGRAM: User


Start
Login
Status
Yes
No
View Profile, Upload Datasets,
Username & Password Wrong
Find Trust Type, Find Datasets By From To Source Bytes,
Find Datasets By From To Destination Bytes, Find Trust Type By Hash code.
Logout

FLOW CHART DIAGRAM: Cloud Server


Start
Login
Yes
Status
No
View All Users and Authorize, View All Datasets,
Username & Password Wrong
View All Datasets By Feature Selection Cluster, View Intrusion Detection Type Results,
Log Out
View Protocol Type Results, View Service Type Results,
View Flag Type Results.

V. IMPLEMENTATION

MODULES:

Cloud Server

In this module, the admin has to login by using valid user name and password. After login successful he can do some operations such as View All Users and Authorize, View All Datasets, View All Datasets By Feature Selection Cluster, View Intrusion Detection Type Results, View Protocol Type Results, View Service Type Results,   View Flag Type Results.

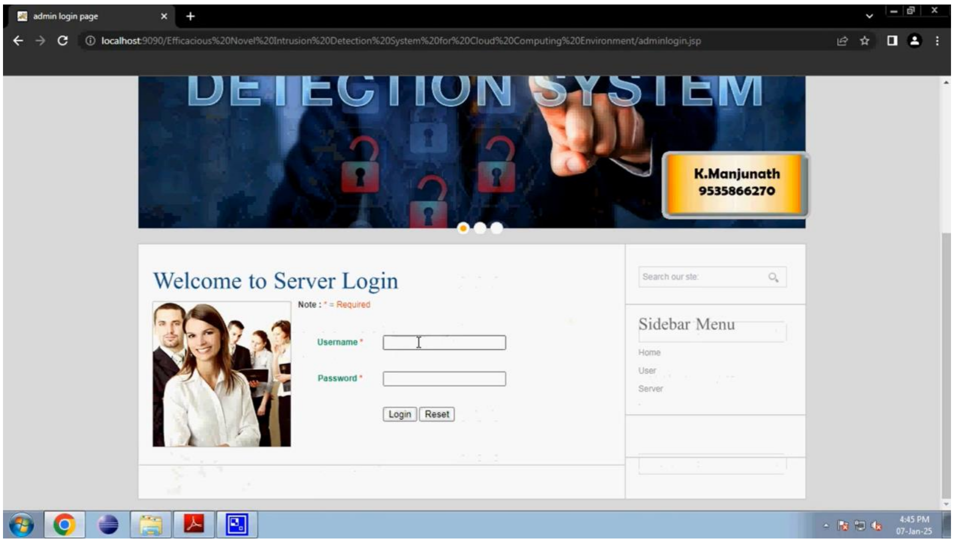
View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorize the users.

User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like   Register and Login, View Profile, Upload Datasets, Find Trust Type, Find Datasets by From To Source Bytes, Find Datasets By From To Destination Bytes, Find Trust Type By Hash code.

VI. RESULTS



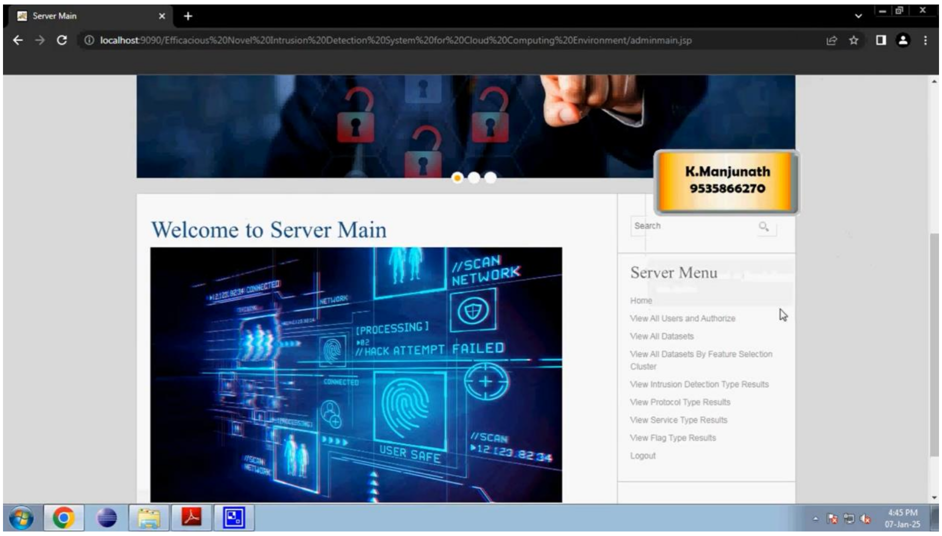
admin login page
localhost:9090/Efficacious%20Novel%20Intrusion%20Detection%20System%20for%20Cloud%20Computing%20Environment/adminlogin.jsp
DETECTION SYSTEM
K.Manjunath
9535866270
Search our site
Sidebar Menu
Home
User
Server
Login
Reset
4:45 PM
07-Jan-25

Welcome to Server Login

Note : * = Required

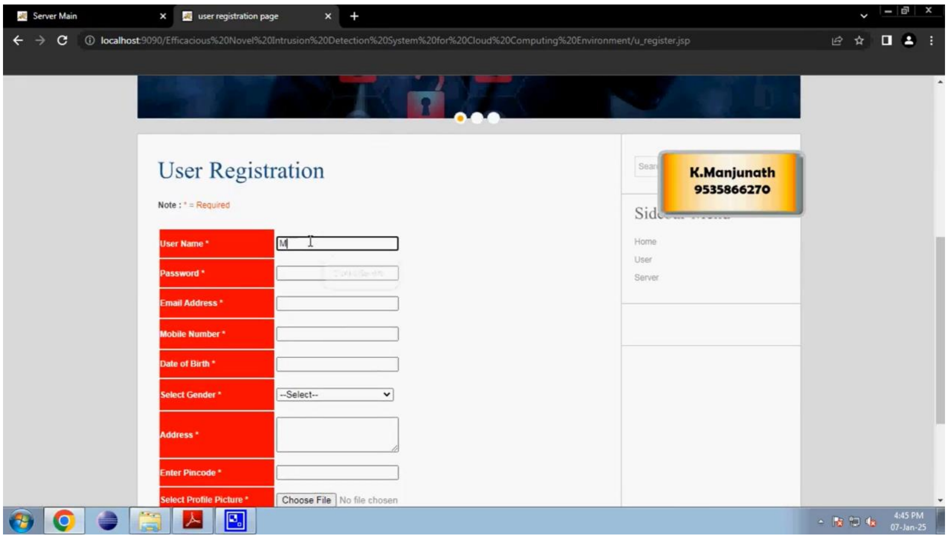
Username *

Password *



Server Main
localhost:9090/Efficacious%20Novel%20Intrusion%20Detection%20System%20for%20Cloud%20Computing%20Environment/adminmain.jsp
K.Manjunath
9535866270
//SCAN NETWORK
[PROCESSING]
//HACK ATTEMPT FAILED
USER SAFE
//SCAN
12.123.82.34
Search
Server Menu
Home
View All Users and Authorize
View All Datasets
View All Datasets By Feature Selection Cluster
View Intrusion Detection Type Results
View Protocol Type Results
View Service Type Results
View Flag Type Results
Logout
4:45 PM
07-Jan-25

Welcome to Server Main

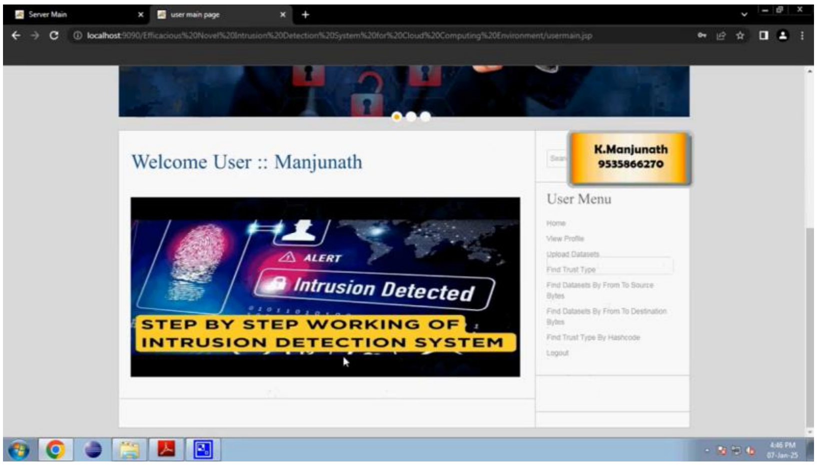


Server Main
user registration page
localhost:9090/Efficacious%20Novel%20Intrusion%20Detection%20System%20for%20Cloud%20Computing%20Environment/u_register.jsp
K.Manjunath
9535866270
Sear
Sid
Home
User
Server
Choose File
4:45 PM
07-Jan-25

User Registration

Note : * = Required

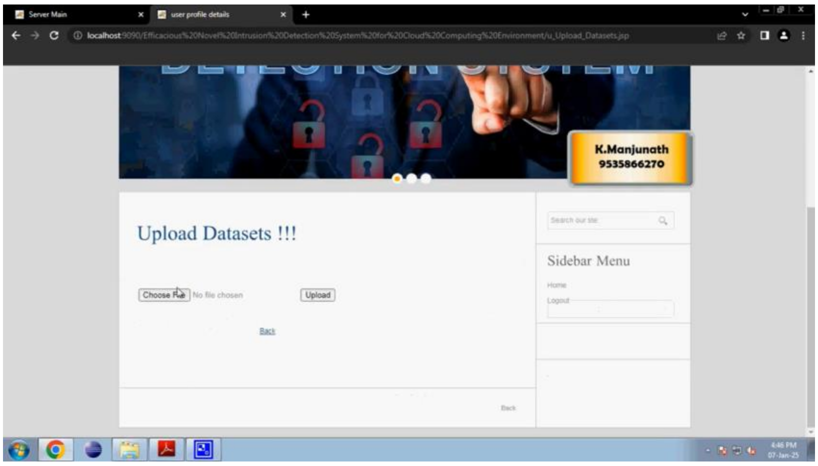
User Name *	M
Password *	
Email Address *	
Mobile Number *	
Date of Birth *	
Select Gender *	--Select--
Address *	
Enter Pincode *	
Select Profile Picture *	No file chosen



Welcome User :: Manjunath

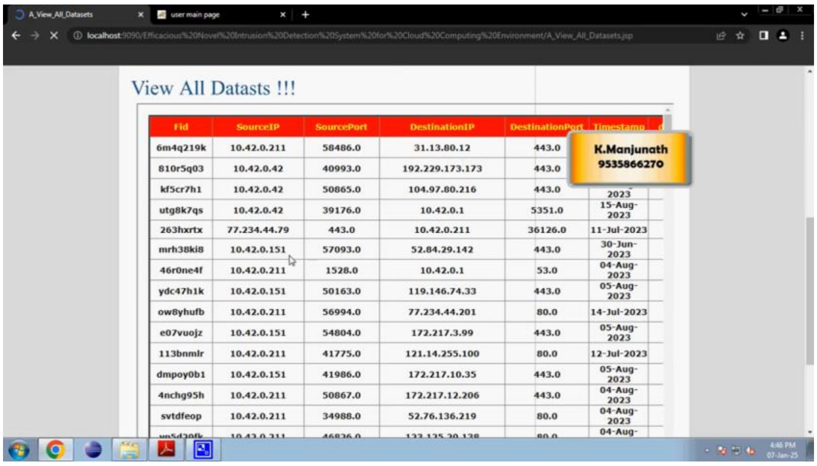
K.Manjunath
9535866270

Server Main
user main page
ALERT
Intrusion Detected
STEP BY STEP WORKING OF INTRUSION DETECTION SYSTEM
User Menu
Home
View Profile
Upload Datasets
Find Trust Type
Find Datasets By From To Source Bytes
Find Datasets By From To Destination Bytes
Find Trust Type By Hashcode
Logout



Upload Datasets !!!

K.Manjunath
9535866270



View All Datasts !!!

K.Manjunath
9535866270

Fid	SourceIP	SourcePort	DestinationIP	DestinationPort	Timestamp
6m4q219k	10.42.0.211	58486.0	31.13.80.12	443.0	
810r5q03	10.42.0.42	40993.0	192.229.173.173	443.0	
kf5cr7h1	10.42.0.42	50865.0	104.97.80.216	443.0	2023
utg8k7qs	10.42.0.42	39176.0	10.42.0.1	5351.0	15-Aug-2023
263hxrtx	77.234.44.79	443.0	10.42.0.211	36126.0	11-Jul-2023
mrh38ki8	10.42.0.151	57093.0	52.84.29.142	443.0	30-Jun-2023
46r0ne4f	10.42.0.211	1528.0	10.42.0.1	53.0	04-Aug-2023
ydc47h1k	10.42.0.151	50163.0	119.146.74.33	443.0	05-Aug-2023
ow8yhufb	10.42.0.211	56994.0	77.234.44.201	80.0	14-Jul-2023
e07vuojz	10.42.0.151	54804.0	172.217.3.99	443.0	05-Aug-2023
113bnmlr	10.42.0.211	41775.0	121.14.255.100	80.0	12-Jul-2023
dmpoy0b1	10.42.0.151	41986.0	172.217.10.35	443.0	05-Aug-2023
4nchg95h	10.42.0.211	50867.0	172.217.12.206	443.0	04-Aug-2023
svtdfeop	10.42.0.211	34988.0	52.76.136.219	80.0	04-Aug-2023
[illegible]	10.42.0.211	46826.0	[illegible]	80.0	04-Aug-

VII. CONCLUSION

A unique approach for creating an intrusion detection system was presented in this study. The method involves combining the hybrid firefly algorithm with the hybrid classifier. The recent CSE CIC IDS 2018 dataset and simulated dataset were used to assess the effectiveness of the proposed architecture. Novel feature selection algorithm is proposed which is the combination of the firefly algorithm with the decision tree. The proposed feature selection performs better than the PSO and GA. We have studied in the literature review that FFA is performing better than PSO and GA. Also we observed this by performing practically that results are better with the proposed feature selection algorithm. Hybrid classifier is used which is the hybridization of neural network with the DT. The proposed architecture outperforms the other state-of the-art techniques for finding attacks in the cloud computing environment.

The future directions related to proposed work is itemized below:

- Adaptive attack detection system is a good future scope in the field of security of clouds. Dynamic conditions can be controlled by developing an adaptive detection system. Dynamic network condition include change in the environmental configurations, computation resources and different locations where attack detection systems are deployed. Dynamic conditions can be controlled by developing an adaptive detection system.
- Another future direction can be developing an IDS which expands or contracts according to the virtual machines of the cloud. Vulnerabilities can be detected by discovering an efficient detection system.

VIII. BIBLIOGRAPHY

[1] P. Rana, I. Batra, A. Malik, A. L. Imoize, Y. Kim, S. K. Pani, N. Goyal, A. Kumar, and S. Rho, ''Intrusion detection systems in cloud computing paradigm: Analysis and overview,'' Complexity, vol. 2022, pp. 1–14, Jun. 2022.
[2] P. S. Bawa et al., ''Enhanced mechanism to detect and mitigate economic denial of sustainability (EDoS) attack in cloud computing environments,'' Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 9, pp. 51–58, 2017.
[3] P. Singh, S. Manickam, and S. U. Rehman, ''A survey of mitigation techniques against economic denial of sustainability (EDoS) attack on cloud computing architecture,'' in Proc. 3rd Int. Conf. Rel., INFOCOM Technol. Optim., Oct. 2014, pp. 1–4.
[4] F. Kuang,W. Xu, and S. Zhang, ''A novel hybrid KPCA and SVM with GA model for intrusion detection,'' Appl. Soft Comput., vol. 18, pp. 178–184, May 2014.
[5] V. Balamurugan and R. Saravanan, ''Enhanced intrusion detection and prevention system on cloud environment using hybrid classification and OTS generation,'' Cluster Comput., vol. 22, no. 6, pp. 13027–13039, Nov. 2019.
[6] D.-S. Huang and H.-J. Yu, ''Normalized feature vectors: A novel alignment-free sequence comparison method based on the numbers of adjacent amino acids,'' IEEE/ACM Trans. Comput. Biol. Bioinf., vol. 10, no. 2, pp. 457–467, Mar. 2013.
[7] H. Abusamra, ''A comparative study of feature selection and classification methods for gene expression data of glioma,'' Proc. Comput. Sci., vol. 23, pp. 5–14, Jan. 2013.
[8] K. Zhang, Y. Li, P. Scarf, and A. Ball, ''Feature selection for highdimensional machinery fault diagnosis data using multiple models and radial basis function networks,'' Neurocomputing, vol. 74, no. 17, pp. 2941–2952, Oct. 2011.
[9] T.W. Rauber, F. de Assis Boldt, and F. M. Varejão, ''Heterogeneous feature models and feature selection applied to bearing fault diagnosis,'' IEEE Trans. Ind. Electron., vol. 62, no. 1, pp. 637–646, Jan. 2015.
[10] A. Khotanzad andY. H. Hong, ''Rotation invariant image recognition using features selected via a systematic method,'' Pattern Recognit., vol. 23, no. 10, pp. 1089–1101, Jan. 1990.
[11] D. D. Lewis, Y. Yang, T. G. Rose, and F. Li, ''RCV1: A new benchmark collection for text categorization research,'' J. Mach. Learn. Res., vol. 5, pp. 361–397, Dec. 2004.
[12] P. Varun and K. Ashokkumar, ''Intrusion detection system in cloud security using deep convolutional network,'' Appl. Math. Inf. Sci., vol. 16, pp. 581–588, Jan. 2022.
[13] S. I. Shyla and S. S. Sujatha, ''Cloud security: LKM and optimal fuzzy system for intrusion detection in cloud environment,'' J. Intell. Syst., vol. 29, no. 1, pp. 1626–1642, Dec. 2019.
[14] P. Mishra, V. Varadharajan, E. S. Pilli, and U. Tupakula, ''VMGuard: A VMI-based security architecture for intrusion detection in cloud environment,'' IEEE Trans. Cloud Comput., vol. 8, no. 3, pp. 957–971, Jul. 2020.
[15] Y. Aoudni, C. Donald, A. Farouk, K. B. Sahay, D. V. Babu, V. Tripathi, and D. Dhabliya, ''Cloud security based attack detection using transductive learning integrated with hidden Markov model,'' Pattern Recognit. Lett., vol. 157, pp. 16–26, May 2022.
[16] M. M. Sakr, M. A. Tawfeeq, and A. B. El-Sisi, ''Network intrusion detection system based PSO-SVM for cloud computing,'' Int. J. Comput. Netw. Inf. Secur., vol. 11, no. 3, pp. 22–29, Mar. 2019.
[17] S. Velliangiri and J. Premalatha, ''Intrusion detection of distributed denial of service attack in cloud,'' Cluster Comput., vol. 22, no. 5, pp. 10615–10623, Sep. 2019.
[18] S. S. Sathiyadhas and M. C. V. Soosai Antony, ''A network intrusion detection system in cloud computing environment using dragonfly improved invasive weed optimization integrated shepard convolutional neural network,'' Int. J. Adapt. Control Signal Process., vol. 36, no. 5, pp. 1060–1076, May 2022.
[19] B. V. Srinivas, I. Mandal, and S. Keshavarao, ''Virtual machine migrationbased intrusion detection system in cloud environment using deep recurrent neural network,'' Cybern. Syst., vol. 55, no. 2, pp. 450–470, Feb. 2024.

[20] T. V. Geetha and A. J. Deepa, ‘‘A FKPCA-GWO WDBiLSTM classifier for intrusion detection system in cloud environments,’’ Knowl.-Based Syst., vol. 253, Oct. 2022, Art. no. 109557.
[21] S. Hizal, Ü. Çavusoglu, and D. Akgün, ‘‘A new deep learning-based intrusion detection system for cloud security,’’ in Proc. 3rd Int. Congr. Human-Computer Interact., Optim. Robotic Appl. (HORA), Istanbul, Turkey, Jun. 2021, pp. 1–4.
[22] U. A. Butt, M. Mehmood, S. B. H. Shah, R. Amin, M. W. Shaukat, S. M. Raza, D. Y. Suh, and M. J. Piran, ‘‘A review of machine learning algorithms for cloud computing security,’’ Electronics, vol. 9, no. 9, p. 1379, Aug. 2020.
[23] H. Hourani and M. Abdallah, ‘‘Cloud computing: Legal and security issues,’’ in Proc. 8th Int. Conf. Comput. Sci. Inf. Technol. (CSIT), Amman, Jordan, Jul. 2018, pp. 13–16.
[24] J. Martínez Torres, C. Iglesias Comesaña, and P. J. García-Nieto, ‘‘Review: Machine learning techniques applied to cybersecurity,’’ Int. J. Mach. Learn. Cybern., vol. 10, no. 10, pp. 2823–2836, Oct. 2019.
[25] M. Fouda, R. Ksantini, and W. Elmedany, ‘‘A novel intrusion detection system for Internet of Healthcare Things based on deep subclasses dispersion information,’’ IEEE Internet Things J., vol. 10, no. 10, pp. 8395–8407, May 2023.