Download   Print   Save to PDF   Save to list   Create bibliography

View more ⌄

Deep Learning-Based Intrusion Detection Model for Network Security

Pande, Sagar Dhanraj[a] ✉ ; Lanke, Govinda Rajulu[b]; Soni, Mukesh[c]; Kulkarni, Mukund Anant[d];

Maaliw, Renato R.[e] ✉ ; Singh, Pavitar Parkash[f] ✉

Save all to author list

[a] School of Computer Science and Engineering, VIT-AP University, Andhra Pradesh, Amaravati, India

[b] Data Science and Engineering, Birla Institute of Technology and Science, Rajasthan, Pilani, India

[c] University Centre for Research and Development Chandigarh University, Punjab, Mohali, 140413, India

[d] Bharati Vidyapeeth (Deemed to Be University), Institute of Management, Kolhapur, India

View additional affiliations ⌄

Full text options ⌄   Export ⌄

Abstract

Author keywords

Indexed keywords

SciVal Topics

Metrics

Abstract

Since it serves as a potent means of network security defence, intrusion detection technology is an essential component of the network security system. As the Internet has grown quickly, so too have network data volumes and threats, which are now more sophisticated and diversified. Modern intrusion detection equipment cannot reliably recognize different types of attacks. A CBL_DDQN intrusion detection model based on an upgraded double deep Q network is suggested based on deep reinforcement learning to address the imbalance of regular traffic and attack traffic data in the actual

Cited by 0 documents

Related documents

Valentina Emilia Balas
Vijay Bhaskar Semwal
Anand Khandare   *Editors*

Intelligent Computing and Networking

Proceedings of IC-ICN 2023

Springer

Lecture Notes in Networks and Systems

Volume 699

Deep Learning-Based Intrusion Detection Model for Network Security

Sagar Dhanraj Pande, Govinda Rajulu Lanke, Mukesh Soni, Mukund Anant Kulkarni, Renato R. Maaliw, and Pavitar Parkash Singh

Abstract Since it serves as a potent means of network security defence, intrusion detection technology is an essential component of the network security system. As the Internet has grown quickly, so too have network data volumes and threats, which are now more sophisticated and diversified. Modern intrusion detection equipment cannot reliably recognize different types of attacks. A CBL_DDQN intrusion detection model based on an upgraded double deep Q network is suggested based on deep reinforcement learning to address the imbalance of regular traffic and attack traffic data in the actual network environment as well as the low detection rate of attack traffic. This model integrates the feedback learning and policy-generating methods of deep reinforcement learning with a one-dimensional convolutional neural network and a bidirectional long-term, short-term memory network to train agents to attack different types of samples. Classification, to some extent, lessens the reliance on data labels during model training. The Borderline-SMOTE algorithm reduces data imbalance, thereby improving the detection rate of rare attacks. The NSL KDD and UNSW NB15 data sets are used to assess the model's efficacy. The findings demonstrate that

S. D. Pande (✉)
School of Computer Science and Engineering, VIT-AP University, Amaravati, Andhra Pradesh, India
e-mail: sagarpande30@gmail.com

G. R. Lanke
Data Science and Engineering, Birla Institute of Technology and Science, Pilani, Rajasthan, India

M. Soni
University Centre for Research and Development Chandigarh University, Mohali 140413, Punjab, India

M. A. Kulkarni
Bharati Vidyapeeth (Deemed to Be University), Institute of Management, Kolhapur, India

R. R. Maaliw
College of Engineering, Southern Luzon State University, Lucban, Quezon, Philippines
e-mail: rmaaliw@slsu.edu.ph

P. P. Singh
Department of Management, Lovely Professional University, Phagwara, India
e-mail: pavitar.19476@lpu.co.in

the model has performed well with respect to the three indices of accuracy, precision, and recall, and the detection effect is significantly superior to Adam BNDNN, KNN, SVM, etc. The detection method is an efficient network intrusion detection model.

1 Introduction

"Network intrusion detection system (network intrusion detection systems, NIDS)," as a proactive defense technology, is the primary means to discover potential network threats in time and formulate reasonable defense strategies and is an integral part of the network security technology system [1–4]. It can detect attacks in time and reduce network security threats by collecting and analyzing relevant network data.

Signature-based NIDS relies on an attack signature database for detection. It has a high detection rate for existing data in the database but cannot detect new attacks [5–8], and the database needs to be updated frequently. Anomaly-based NIDS identifies hidden attacks in computers by analyzing unusual traffic distributions and can be used to detect new types of attacks. The system uses configuration files to store all normal behaviors of users, hosts, network connections, and applications. This approach compares current activity to the configuration file and flags any significant deviations as anomalies [9–12]. This data sensitivity effectively prevents various malicious behaviors. However, this sensitivity advantage can lead to high false favorable rates, leading to unnecessary panic and overreaction [13–15].

Machine learning algorithms, such as Bayesian networks [16] and support vector machines [17], are widely employed in anomaly-based NIDS. Small-scale traffic data detection challenges have been successfully tackled by these methods. Performance of classic intrusion detection methods, however, is facing considerable hurdles in dealing with huge high-dimensional data due to the ongoing advance of network technology and the ongoing expansion of network scale.

Representing representation learning, deep learning can automatically learn high-level data features directly from complex original features, doing away with the requirement for specialized knowledge in the manual feature extraction procedure. As a result, the deep Model architecture is the basis for the vast majority of modern intrusion detection systems. Among the most popular deep models are the autoencoder [18], the convolutional neural network (CNN) [19, 20], the recurrent neural network (RNN) [21], etc. Literature [22] proposes to use CNN for network intrusion detection and uses CNN to select features to classify traffic. Compared with traditional algorithms, it has a good effect but ignores the connection in the time sequence of traffic data; Literature [23] proposes to use LSTM (extended short-term memory network) is used in intrusion detection and has achieved good classification results, but without considering the spatial characteristics of the data, there is still room for improvement in classifier performance. To fully extract the features of

network traffic data, literature [24] proposes to use CNN and LSTM in combination, use CNN to learn the parts of network packets, and then use LSTM to learn the details of network traffic, compare with using LSTM, CNN or LSTM alone. The upgraded model is more efficient and produces more accurate results when classifying traffic data. These models rely on large amounts of labeled data samples, even though the neural network model is capable of powerful feature extraction. Still, there is a lot of data that needs labeling, and doing it manually is a costly and time-consuming process.

Reinforcement learning (RL) is an active solution to the aforementioned issues. Traditional RL is based on the Markov decision process (MDP) to create algorithms; however, it can only examine small-scale problems. Moreover, the natural environment is often complex and changeable. Therefore, it is problematic for traditional RL methods to obtain effective solutions when solving practical problems. Literature [25] combines reinforcement learning with deep learning. It proposes deep reinforcement learning (DRL), which approximates the complex data space and mapping relationship in reinforcement learning with neural networks, significantly expanding the application range of reinforcement learning. This is because coupled with its unique feedback mechanism; reinforcement learning also has an extensive range of applications in classification problems application. Literature [26], for the first time, equates the classification problem to the continuous decision-making process of the agent (agent) and proposes a classification task solution based on reinforcement learning, with an accuracy rate of 87.4% in the eight UCI data sets. Literature [27] proposed an AE-DQN model based on adversarial multi-agents for the problem of network intrusion detection and achieved good detection results. Although the above-mentioned deep reinforcement learning model shows unique advantages in solving the classification problem with imperfect labels, the selection of the deep learning network model cannot whether the selection of the deep learning model is mainly appropriate to determine the classifier's performance. Therefore, the focus of the above models is only on the generation of agent strategies [28, 29].

Uneven data is another common issue. The classifier can obtain higher overall classification accuracy, but the recognition rate of smaller class data is meager, and misclassification of minority classes will bring huge costs. At the algorithm level, by changing the classifier, the existing classifier can strengthen the learning of the minority class [30].

In order to boost the system's detection rate for different types of traffic, this study presents a network intrusion detection model based on the enhanced double Q network. The model incorporates the hybrid network model of CNN and BiLSTM into the learning framework of the deep Q network, simulating the intrusion detection process as the sequential decision-making process of the agent. Improve the classifier's ability to identify different forms of attack flows. Concurrently, an unbalanced processing strategy is offered to improve the detection rate of rare attacks while taking data imbalance into account.

2 CBL_DDQN Model Based on Improved Double Deep Q Network

This paper introduces the mixed CBL model of CNN and BiLSTM into the dual deep Q network framework. To better utilize the CBL network to fit the Q function and the feedback mechanism in the dual deep Q network, a new model for intrusion detection called CBL DDQN is developed and optimization strategy to optimize the CBL network, and finally, realize the correct classification of traffic.

Network traffic data is a sequence with a time step, which has both spatial and temporal characteristics [13–16]. Because both CNN and BiLSTM are very good at extracting features from input, we create a CNN-BiLSTM hybrid model, the CBL model, by fusing a one-dimensional convolutional network with a bidirectional long-term, short-term memory network (see Fig. 1).

The parameters are discretized in the highest pooling layer to shorten training time and prevent overfitting; middle-layer parameters are normalized with batch normalization to speed up training; and the BiLSTM layer is used to learn onward and rearward time series data. One way to improve understanding is to utilize two BiLSTM layers that each learn at a different granularity. One-dimensional convolutional neural network with long-term time-dependent feature correlation; network

Fig. 1 CBL model framework
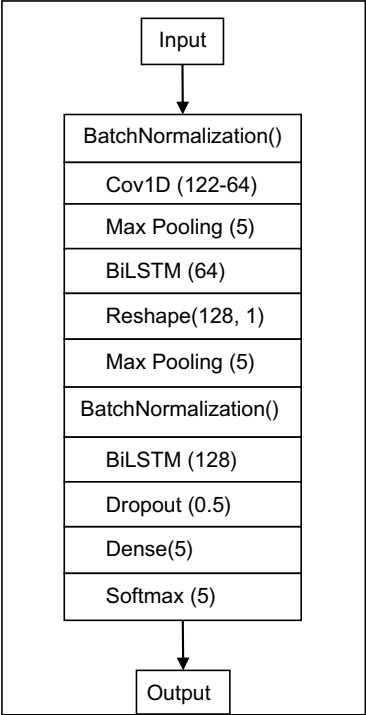
layer between BiLSTM layers to extract features efficiently and speed up training; Dropout layer to prevent model overfitting; and Softmax function for probability matrix output.

3 Selection and Processing of Data Sets

3.1 Dataset Selection and Preprocessing

In this study, the CBL DDQN model is validated using simulation tests on two public intrusion detection datasets NSL KDD and UNSW NB15. Tables 1 and 2 detail the two datasets, respectively.

Data preprocessing mainly includes the following three parts: character feature medicalization, one-hot encoding, and numerical normalization.

(1) Numericalization of character features

The category features of standard records and different attack records are converted from character type to digital label, and the label distribution after conversion is shown in Tables 1 and 2.

Table 1 Attack category information of NSL_KDD dataset

Attack category	Quantity	Convert tag
Normal	077,054	0
Dos	053,385	1
Probing	014,077	2
R2L	003,749	3
U2R	000,252	4

Table 2 Attack category information of UNSW_NB15 dataset

Attack category	Quantity	Convert tag
Normal	93,000	0
Generic	2677	1
Exploit	2329	2
Fuzzers	16,353	3
Dos	44,525	4
Reconaissance	24,246	5
Analysis	58,871	6
Backdoor	13,987	7
Shellcode	1511	8
Worms	174	9

(2) One-hot encoding

With one-hot encoding, the distance calculation between components can be more realistic.

(3) Numerical normalization

After one-hot encoding, to reduce the impact of the value of each dimension attribute feature on the subsequent network, each dimension attribute feature is normalized according to formula (1), and the normalized interval is [0,1]:

$$\dot{x} = (x - x_{min}) / (x_{max} - x_{min})$$

3.2 Experimental Results and Analysis

In this paper, two network traffic data sets, NSL_KDD and UNSW_NB15, are used for experiments. The details of the dataset are described in Sect. 3.1. In the experiment, set all the data of the entire training set as one epoch, set the maximum epoch to 30, make statistics on the classification results of the model every five ages of training, and use the control experiment to test the system before and after using the Borderline-SMOTE algorithm. The recognition rate of the data. The classification results after statistical training for 30 epochs are shown in Figs. 2 and 3.

Figures 2 and 3 show that the classifiers' performances are steadily rising as the training process progresses. If you compare the model introduced with the Borderline-SMOTE algorithm to the same training, you'll see that the latter has a greater classification accuracy. Within a certain threshold of repetitions, the accuracy of the original data set can be direct.

It can be seen visually that the introduction of the imbalance processing algorithm has a more significant role in promoting the convergence of the model.

Accuracy, recall, and precision of six approaches were evaluated to further validate the model described in this research. Table 9 and Table 10 display the statistical
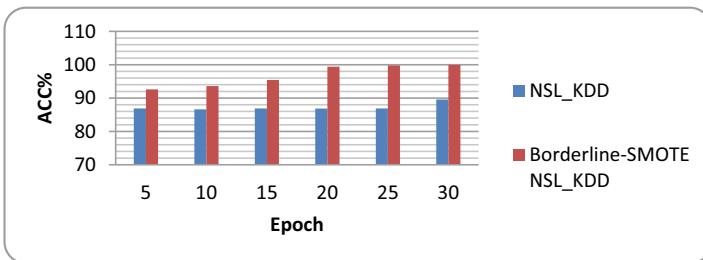

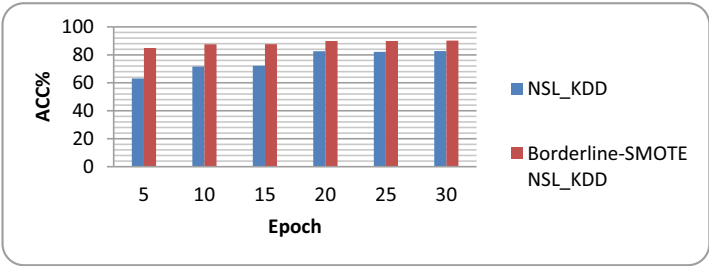**Fig. 2** The recognition rate of the model for NSL_KDD

Fig. 3 The recognition rate of the model for UNSW_NB15

outcomes of Adam BNDNN [18, 18], DQN [19, 30], RF [19], SVM [19], MLP [19], and Adaboost [20], where the data in bold is the optimal value of this performance index.

For intuition, the data is drawn in a bar graph, and the result is shown in Fig. 4.

With the help of Fig. 4, it is clear that the CBL DDQN model suggested in this paper has a substantial detection effect on the NSL KDD dataset. All performance parameters are higher than prior similar studies, with precision at 99.96%, recall at 99.97%, and precision at 99.79%.

Similarly, for the sake of intuition, the data drawn in bar charts, and the results are shown in Fig. 5.
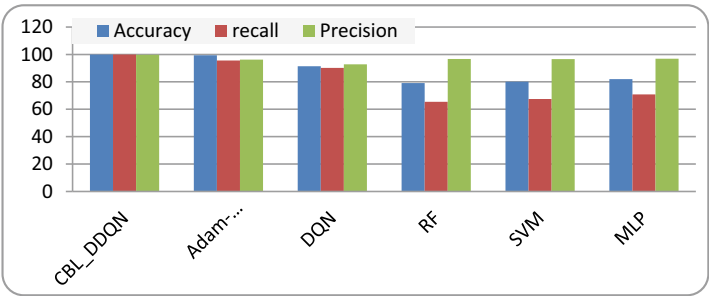

Fig. 4 Classification performance of each model for NSL_KDD
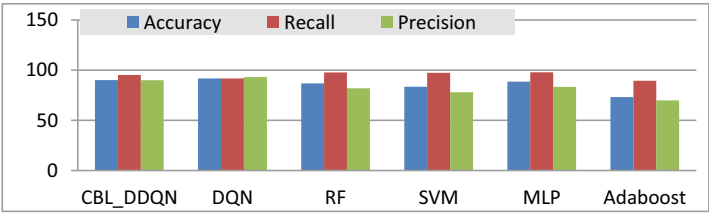

Fig. 5 Classification performance of each model for UNSW_NB15

Taken together, Table 4 and Fig. 5 show that the UNSW NB15 detection results using this paper's model have an overall identification accuracy rate of 90.12%, recall of 95.20%, and precision of 89.93%. On the downside, it does not perform as well as its counterparts. After cautiously considering a number of performance factors, the model suggested in this research is able to produce a good intrusion detection impact.

The above two sets of experimental results demonstrate that the upgraded dual deep Q network model suggested in this paper may effectively address the intrusion detection problem.

4 Conclusion

The purpose of this paper is to present the CBL DDQN network intrusion detection model, which incorporates the hybrid network CBL network of CNN and BiLSTM into the DDQN framework to enhance the model's performance. In comparison to more standard deep learning algorithms, this one reduces or eliminates the need for labeled data. In this way, it outperforms deep learning algorithms in terms of classification accuracy. Moreover, the Borderline-SMOTE technique is used to increase the number of unusual attack samples because of the fact that the disparity between the data makes it hard for the classifier to understand the data features properly. Based on these findings, it appears that the imbalanced processing technique helps the model become more accurate in classifying data.

In conclusion, the suggested model in this paper has good results in the imbalanced data classification challenge. Its overall performance is higher than that of the enhanced DQN network and other deep learning networks, suggesting a novel approach to deep reinforcement learning.

References

1. Haghighat MH, Li J (2021) Intrusion detection system using voting-based neural network. Tsinghua Sci Technol 26(4):484–495. https://doi.org/10.26599/TST.2020.9010022
2. Zhong W, Yu N, Ai C (2020) Applying big data based deep learning system to intrusion detection. Big Data Mining Analyt 3(3):181–195. https://doi.org/10.26599/BDMA.2020.9020003
3. Ullah I, Mahmoud QH (2021) Design and development of a deep learning-based model for anomaly detection in IoT networks. IEEE Access 9:103906–103926. https://doi.org/10.1109/ACCESS.2021.3094024
4. Oseni A et al (2023) An explainable deep learning framework for resilient intrusion detection in IoT-enabled transportation networks. IEEE Trans Intell Transp Syst 24(1):1000–1014. https://doi.org/10.1109/TITS.2022.3188671
5. Xie G, Yang LT, Yang Y, Luo H, Li R, Alazab M (2021) Threat analysis for automotive CAN networks: a GAN model-based intrusion detection technique. IEEE Trans Intell Transp Syst 22(7):4467–4477. https://doi.org/10.1109/TITS.2021.3055351

6. Wang Z, Zeng Y, Liu Y, Li D (2021) Deep belief network integrating improved kernel-based extreme learning machine for network intrusion detection. IEEE Access 9:16062–16091. https://doi.org/10.1109/ACCESS.2021.3051074

7. Shu J, Zhou L, Zhang W, Du X, Guizani M (2021) Collaborative intrusion detection for VANETs: a deep learning-based distributed SDN approach. IEEE Trans Intell Transp Syst 22(7):4519–4530. https://doi.org/10.1109/TITS.2020.3027390

8. Naseer S et al (2018) Enhanced network anomaly detection based on deep neural networks. IEEE Access 6:48231–48246. https://doi.org/10.1109/ACCESS.2018.2863036

9. Khan FA, Gumaei A, Derhab A, Hussain A (2019) A novel two-stage deep learning model for efficient network intrusion detection. IEEE Access 7:30373–30385. https://doi.org/10.1109/ACCESS.2019.2899721

10. Abdel Wahab O (2022) Intrusion detection in the IoT under data and concept drifts: online deep learning approach. IEEE Internet Things J 9(20):19706–19716, https://doi.org/10.1109/JIOT.2022.3167005

11. Zhang Y, Li P, Wang X (2019) Intrusion detection for IoT based on improved genetic algorithm and deep belief network. IEEE Access 7:31711–31722. https://doi.org/10.1109/ACCESS.2019.2903723

12. Yang H, Qin G, Ye L (2019) Combined wireless network intrusion detection model based on deep learning. IEEE Access 7:82624–82632. https://doi.org/10.1109/ACCESS.2019.2923814

13. Nie L et al (2022) Intrusion detection for secure social internet of things based on collaborative edge computing: a generative adversarial network-based approach. IEEE Trans Comput Soc Syst 9(1):134–145. https://doi.org/10.1109/TCSS.2021.3063538

14. Zhang C, Costa-Pérez X, Patras P (2022) Adversarial attacks against deep learning-based network intrusion detection systems and defense mechanisms. IEEE/ACM Trans Netw 30(3):1294–1311. https://doi.org/10.1109/TNET.2021.3137084

15. Yang J, Li T, Liang G, He W, Zhao Y (2019) A simple recurrent unit model based intrusion detection system With DCGAN. IEEE Access 7:83286–83296. https://doi.org/10.1109/ACCESS.2019.2922692

16. Halbouni A, Gunawan TS, Habaebi MH, Halbouni M, Kartiwi M, Ahmad R (2022) CNN-LSTM: hybrid deep neural network for network intrusion detection system. IEEE Access 10:99837–99849. https://doi.org/10.1109/ACCESS.2022.3206425

17. Alkadi O, Moustafa N, Turnbull B, Choo K-KR (2021) A deep Blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. IEEE Internet Things J 8(12):9463–9472, https://doi.org/10.1109/JIOT.2020.2996590

18. Kim A, Park M, Lee DH (2020) AI-IDS: application of deep learning to real-time web intrusion detection. IEEE Access 8:70245–70261. https://doi.org/10.1109/ACCESS.2020.2986882

19. Su T, Sun H, Zhu J, Wang S, Li Y (2020) BAT: deep learning methods on network intrusion detection using NSL-KDD dataset. IEEE Access 8:29575–29585. https://doi.org/10.1109/ACCESS.2020.2972627

20. Wei P, Li Y, Zhang Z, Hu T, Li Z, Liu D (2019) An optimization method for intrusion detection classification model based on deep belief network. IEEE Access 7:87593–87605. https://doi.org/10.1109/ACCESS.2019.2925828

21. Abdelmoumin G, Rawat DB, Rahman A (2022) On the performance of machine learning models for anomaly-based intelligent intrusion detection systems for the internet of things. IEEE Internet Things J 9(6):4280–4290, https://doi.org/10.1109/JIOT.2021.3103829

22. Zhang L, Yan X, Ma D (2022) A Binarized neural network approach to accelerate in-vehicle network intrusion detection. IEEE Access 10:123505–123520. https://doi.org/10.1109/ACCESS.2022.3208091

23. Prasath S, Sethi K, Mohanty D, Bera P, Samantaray SR (2022) Analysis of continual learning models for intrusion detection system. IEEE Access 10:121444–121464. https://doi.org/10.1109/ACCESS.2022.3222715

24. Benaddi H, Ibrahimi K, Benslimane A, Jouhari M, Qadir J (2022) Robust enhancement of intrusion detection systems using deep reinforcement learning and stochastic game. IEEE Trans Veh Technol 71(10):11089–11102. https://doi.org/10.1109/TVT.2022.3186834

25. Han D et al (2021) Evaluating and improving adversarial robustness of machine learning-based network intrusion detectors. IEEE J Sel Areas Commun 39(8):2632–2647. https://doi.org/10.1109/JSAC.2021.3087242

26. Liu C, Gu Z, Wang J (2021) A hybrid intrusion detection system based on scalable K-means+ random forest and deep learning. IEEE Access 9:75729–75740. https://doi.org/10.1109/ACCESS.2021.3082147

27. Lei S, Xia C, Li Z, Li X, Wang T (2021) HNN: a novel model to study the intrusion detection based on multi-feature correlation and temporal-spatial analysis. IEEE Trans Netw Sci Eng 8(4):3257–3274, https://doi.org/10.1109/TNSE.2021.3109644

28. Zhang Y, Chen X, Guo D, Song M, Teng Y, Wang X (2019) PCCN: parallel cross convolutional neural network for abnormal network traffic flows detection in multi-class imbalanced network traffic flows. IEEE Access 7:119904–119916. https://doi.org/10.1109/ACCESS.2019.2933165

29. Mauro MD, Galatro G, Liotta A (2020) Experimental review of neural-based approaches for network intrusion management. IEEE Trans Netw Serv Manage 17(4):2480–2495. https://doi.org/10.1109/TNSM.2020.3024225

30. Zhao R et al (2021) An efficient intrusion detection method based on dynamic Autoencoder. IEEE Wirel Commun Lett 10(8):1707–1711. https://doi.org/10.1109/LWC.2021.3077946

CERTIFICATION OF PERCENTAGE CONTRIBUTION

(Research Output with Multiple Authors)

Title of Research: Deep Learning-Based Intrusion Detection Model for Network Security
Type of Research Output: Book Chapter (Scopus-Indexed, Publisher: Springer Nature)

Instruction: Supply ALL the names of the authors involved in the publication of Research output and indicate the contribution of each author in percentage. Each author shall sign the conforme column if he/she agrees with the distribution. The conforme should be signed by all the authors in order to be considered. Please prepare separate Certification for each output.

	Name of Authors	Current Affiliation	% Contribution	Conforme *(Sign if you agree with the % distribution)*
1	Sagar Pande	LD College of Engineering	16.67%	
2	Govinda Lanke	LD College of Engineering	16.67%	
3	Mukesh Soni	Chandigarh University	16.67%	
4	Mukund Kulkarni	Tashkent Institute	16.67%	
5	Renato R. Maaliw III	SLSU	16.67%	*RM3*
6	Pavitar Parkash Singh	AlMaarefa University	16.67%	

* Should have a total of 100%   100.00%

Prepared by: Certified by:

RM3

Renato R. Maaliw III, DIT   **Nicanor L. Guinto, Ph.D**
(Name and Signature)   (Name and Signature)
Faculty   Director, Office of Research Services