Studies in Autonomic,
Data-driven and Industrial Computing

Rajeev Mathur · C. P. Gupta ·
Vaibhav Katewa · Dharm Singh Jat ·
Neha Yadav *Editors*

Emerging Trends in Data Driven Computing and Communications

Proceedings of DDCIoT 2021

Springer

Studies in Autonomic, Data-driven and Industrial Computing

The book series Studies in Autonomic, Data-driven and Industrial Computing (SADIC) aims at bringing together valuable and novel scientific contributions that address new theories and their real world applications related to autonomic, data-driven, and industrial computing. The area of research covered in the series includes theory and applications of parallel computing, cyber trust and security, grid computing, optical computing, distributed sensor networks, bioinformatics, fuzzy computing and uncertainty quantification, neurocomputing and deep learning, smart grids, data-driven power engineering, smart home informatics, machine learning, mobile computing, internet of things, privacy preserving computation, big data analytics, cloud computing, blockchain and edge computing, data-driven green computing, symbolic computing, swarm intelligence and evolutionary computing, intelligent systems for industry 4.0, as well as other pertinent methods for autonomic, data-driven, and industrial computing.

The series will publish monographs, edited volumes, textbooks and proceedings of important conferences, symposia and meetings in the field of autonomic, data-driven and industrial computing.

More information about this series at http://www.springer.com/series/16624

Rajeev Mathur · C. P. Gupta · Vaibhav Katewa ·
Dharm Singh Jat · Neha Yadav
Editors

Emerging Trends in Data Driven Computing and Communications

Proceedings of DDCIoT 2021

Springer

Editors
Rajeev Mathur
Department of Electronics
and Communication Engineering
Geetanjali Institute of Technical Studies
Udaipur, India

Vaibhav Katewa
Department of Electronics
and Communication Engineering
Indian Institute of Science Bangalore
Bengaluru, India

Neha Yadav
Department of Mathematics
National Institute of Technology
Hamirpur, Himachal Pradesh, India

C. P. Gupta
Department of Computer Science
and Engineering
Rajasthan Technical University
Kota, India

Dharm Singh Jat
Department of Computer Science
Namibia University of Science
and Technology
Windhoek, Namibia

ISSN 2730-6437 ISSN 2730-6445 (electronic)
Studies in Autonomic, Data-driven and Industrial Computing
ISBN 978-981-16-3914-2 ISBN 978-981-16-3915-9 (eBook)
https://doi.org/10.1007/978-981-16-3915-9

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

Data-Driven Computing is the process of computational analysis using available database in any form to derive predictive output. Data-driven computing needs to be explored more extensively with theories and principles other than mainstream computing. A structured database obtained by various processes can be used for further predictions after computational analysis and intelligent manipulation.

The next step is going to be Data-Driven Manufacturing/Industrial Computing, wherein industrial manufacturers will be able to make decisions based on the prediction after data-driven computing. Industries are expected to utilise Internet of Things, Artificial Intelligence, Machine Learning and other technologies to make manufacturing more automated, autonomic, smart and data-driven. Internet of Things (IoT) and the use of sensors in big data and analytics have evolved a new dimension for next generation manufacturing.

This Book on **Emerging Trends in Data Driven Computing and Communications—Proceedings of DDCIoT 2021** addresses design, development and algorithmic aspects of artificial intelligence, machine learning, deep learning, edge computing, communication and networking. A variety of peer-reviewed papers related to wide applications in various fields like industrial IoT, smart systems, healthcare systems, autonomous systems and various other aligned areas are included. The book is a compilation of papers presented in the International Conference on Data Driven Computing & IOT-DDCIoT-2021, Organised by Department of Electronics and Communications and Department of Computer Science Engineering of Geetanjali Institute of Technical Studies, Udaipur, and Rajasthan Technical University, Kota, during 20–21 March 2021. The Conference was sponsored by AICTE and TEQIP-III, India.

The conference was focused to encourage various scholastic revolutionary researchers, scientists and industrial engineers from all around the world and provides them a platform to present the proposed new technologies, share their experiences and discuss emerging trends in Data-Driven and Industrial Computing and IoT-based Smart Systems

In the conference, 130 papers were received; we have selected 30 papers on the basis of blind reviews, quality and originality of the work and research study. All the papers have been carefully reviewed.

This book could be referred to by academicians, researchers, programmers, system infrastructure designers and industrial hardware developers. This book could also be very useful for manufacturers, entrepreneurs and investors.

Udaipur, India
Windhoek, Namibia
Kota, India
Bengaluru, India
Hamirpur, India
May 2021

Prof.(Dr.) Rajeev Mathur
Prof. Dharm Singh Jat
Dr. C. P. Gupta
Dr. Vaibhav Katewa
Dr. Neha Yadav

Contents

About the Editors

Dr. Rajeev Mathur is serving as Professor and Dean in Geetanjali Institute of Technical Studies, Udaipur, Rajasthan, India. He received his Ph.D. from Jaipur, Masters in Engineering from NITTTR, Chandigarh, India, and B.E. degree in Electronics from VRCE (now VNIT), Nagpur University, in 1991. He joined industry Punjab Wireless System Ltd. Mohali, Chandigarh, and was working as City Manager for 6 Years. He served as Assistant Professor, Associate Professor, and Head at Engineering Institute at Alwar, Jodhpur. He was Founder Member, Head & Associate Prof. in Faculty of E & T, "Jodhpur National University," Jodhpur and Member of Board of management of the University. He was Director & Principal of Marwar Engineering College & Research Centre, Jodhpur, Rajasthan, India. He is "CMI level 5 certified in Management & Leadership by CMI Royal Chapter, UK." He is Senior Member of professional bodies IEEE, Charted Management Institute-UK, ATMS, and Lions International. He has published more than 50 papers in international journals including SCI/SCOPUS indexed journals. He also published 3 book chapters. He had been Keynote Speaker, Advisor in many conferences & Editor, and Reviewer of many international journals & international conferences. He also have published one patent in his name. His research interests are IoT, data driven computing, advanced antenna techniques, metamaterials, and evaluating nature of electromagnetic waves.

Dr. C. P. Gupta is presently serving at Rajasthan Technical University, Kota, Rajasthan, India, as Associate Professor. He pursued his Ph.D. from University of Kota, Kota in Wireless Sensor Network in 2014, Master of Technology from Indian Institute of Technology, Delhi, India, and Engineering degree from Malviya National Institute of Technology, Jaipur, India, in 1990. His research interests include computer networks, information, security, and wireless sensor networks. He is also an ISO 27000 certified professional. He has published several papers in international & national journals and international conferences. He is appointed as Chief Editor in Seventh International Conference on Recent Trends in Information, Telecommunication and Computing. He is Member of professional society INSTICC.

Dr. Vaibhav Katewa is working as Assistant Professor, Department of Electrical Communication Engineering, and Associate Faculty, Robert Bosch Center for Cyber-Physical Systems, Indian Institute of Science, Bangalore, India. He has also served as Post-Doctoral Scholar in University of California Riverside, USA, in Dec. 2019, as Research Assistant, Department of Electrical Engineering, University of Notre Dame, USA, from May 2010 to Aug. 2015, and as Research Intern in Department of Electrical and Electronic Engineering at University College Cork, Ireland, from May 2006 to July 2006. He also has 3 years of industrial experience as Research Engineer in Ethernet Development Tejas Networks, Bangalore, India, and Senior Research Associate, Intellectual Property Division at Evalueserve, Delhi, India. He pursued his Ph.D. in Electrical Engineering from University of Notre Dame, USA, in 2016, M.S. in Electrical Engineering in May 2012 from University of Notre Dame, USA, and B.Tech in Electrical Engineering from Indian Institute of Technology Kanpur, India, in 2007. He has published more than 35 papers in international journals of repute and two book chapters. He is Reviewer for many conferences and journals and is Guest Editor in Special Issue on "Swarm Intelligence Techniques for Optimum Utilization of Resources in Grid and Utility Computing," International Journal of Grid and Utility Computing, 2019, and Special Issue on "Smart Computing and Optimization," Journal of Information, and Optimization Sciences, 38(6), 2017.

Prof. Dharm Singh Jat is Professor, Department of Computer Science at Namibia University of Science and Technology (NUST), NAMIBIA. He is the author of more than 150 peer-reviewed articles and the author or editor of more than 20 books. He has been the recipient of more than 19 prestigious awards, such as Eminent Scientist Award, Distinguished Academic Achievement, Eminent Engineering Personality, CSI Chapter Patron, CSI Significant Contribution, Best Faculty Researcher, Best Technical Staff, Outstanding University Service Award, and Distinguished ACM Speaker award. Prof. Dharm Singh is Fellow of The Institution of Engineers (I), Fellow of Computer Society of India, Chartered Engineer (I), Senior Member IEEE, and Distinguished ACM Speaker.

Dr. Neha Yadav received her Ph.D. in Mathematics from Motilal Nehru National Institute of Technology, (MNNIT) Allahabad, India, in the year 2013. She completed her post-doctorate from Korea University, Seoul, South Korea. She is a receiver of Brain Korea (BK-21) postdoctoral fellowship given by Government of Republic of Korea. Prior to joining NIT Hamirpur, she taught courses and conducted research at BML Munjal University, Gurugram, Korea University Seoul, S. Korea, and The NorthCap University, Gurugram. Her major research area includes numerical solution of boundary value problems, artificial neural networks, and optimization. She has published more than 15 journal articles and also authored books and editorials.

Chapter 1
Hybrid Deep Learning Model for Real-Time Detection of Distributed Denial of Service Attacks in Software Defined Networks

Auther Makuvaza, Dharm Singh Jat, and Attlee M. Gamundani

Abstract The growth of network devices has brought a lot of problems in managing the networks. The ill-managed networks create different vulnerabilities which attackers can exploit. The attackers take advantage of open-source tools and low-priced Internet to use the networks. Software Defined Networking (SDN) is a good networking architecture that can be managed centrally. The decoupled SDN architecture has the flexibility of programming network devices from the central controller. There is no doubt that SDN addresses the problem of network management; however, SDN comes with a security concern. SDN controller has a vulnerability of a single point of failure. This vulnerability makes the controller vulnerable to different network attacks, including Distributed Denial of Service (DDoS) attacks, among others. To get the best out of SDN, the controller needs security that can protect it from cyber-attacks. The Deep Learning (DL) approach enhanced the selection of the relevant features from the dataset for classification in an unsupervised manner. This paper proposed the hybrid DL model that utilises Long Short-Term Memory (LSTM) and Convolutional Neural Network (CNN) for DDoS attack detection. The proposed hybrid model produced a detection accuracy of 99.72%.

Keywords CNN · Long short-term memory · IDS · Deep learning · DDoS · SDN

1 Introduction

As new technology redefines the digital world, attackers also have their attacking methods by using multiple attacking vectors [1]. Novel technology has changed the human lifestyle and security landscape; this change threatens the security of different

A. Makuvaza (✉) · D. S. Jat · A. M. Gamundani
Namibia University of Science and Technology, Windhoek, Namibia

D. S. Jat
e-mail: dsingh@nust.na

A. M. Gamundani
e-mail: agamundani@nust.na

R. Mathur et al. (eds.), *Emerging Trends in Data Driven Computing and Communications*,
Studies in Autonomic, Data-driven and Industrial Computing,
https://doi.org/10.1007/978-981-16-3915-9_1

networks and other Information Technology services. According to [2], the privacy challenges come with novel technologies and can endanger and disturb everyday activities in the networking environment. The legacy network lacks the scalability, which is required by the ever-growing networks; however, SDN has proven to be the future of networking because of its centralised controller which is used to program the whole network. The decoupled SDN architecture has attracted a lot of cyber-attacks [3]. Cyber-attackers target the SDN controller to bring the network down because of the single point failure vulnerability.

With the advancement of technology, DDoS attacks can be launched by different computers within a botnet. Attackers can attack the SDN controller by launching DDoS attacks. According to [1], DDoS attacks are currently the most sophisticated network threat to organisations, and they are difficult to detect and prevent. According to [4], attackers are now using multi-vector attacks to attack the complex network. Attackers can automatically or dynamically change the attacking vectors based on the defence mechanisms they encounter during the attack. According to [4], multi vector attacks are increasing by 13% every year, which brings the debate on which DDoS attack detection mechanism organisations should use. Figure 1 below shows the relationship between artificial intelligence, machine learning and deep learning.

Intrusion Detection Systems (IDS) are used to detect network attacks; however, to detect anomaly-based attacks, the IDS should be trained, tested and evaluated. Cybersecurity is the leading driving force of Artificial intelligence [5]. Deep learning has proven to be one of the best methods cybersecurity officers can use to detect DDoS attacks in SDN. However, DL cannot do the job alone, a flow-based dataset is needed for the SDN environment. CICIDS 2017 dataset is a flow-based dataset, and it has more than 11 different network attacks, with DDoS included.

Deep learning models come with problems of false positives and false negatives. A model can incorrectly predict a positive and negative class [6]. To get the correct accuracy from deep learning models, accuracy should be measured by comparing the model results with the ground truth. According to [1], confusion matrix and standard evaluation parameters can be used to measure the accuracy of a model. This paper will discuss the background of the study and related work, methodology, results analysis and conclusion.

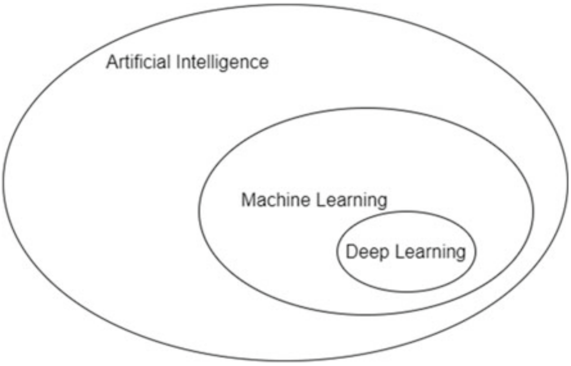


Fig. 1 Relationship between artificial intelligence, machine learning and deep learning

1.1 Background and Related Work

Software-defined networks have changed the game of networking with their flow-based protocol and decoupled architecture [7]. Previously, intrusion detection systems were implemented based on traditional network protocol which is the Internet Protocol (IP). With SDN using OpenFlow protocol, the IP-based intrusion detection systems faced some challenges in detecting DDoS attacks in the SDN environment because of the volume traffic and attack vectors [8]. SDN simplified networking by having a centralised controller where all devices can be programmed and configured from one point [2]. According to [9], recent cybersecurity experts and researchers have designed anomaly intrusion detection systems to detect various network attacks. This direction has seen neural networks being used in this direction of intrusion detection systems.

According to [10], the best way to protect software-defined networks is through intrusion detection systems. Deep learning intrusion systems can provide the last line of defence to software-defined networks. They went on and stated that CNN intrusion systems produce an accuracy of 95% when detecting DDoS attacks in SDN. Reference [11] state that SDN architecture attracts a lot of cyber-attackers because of the vulnerability of the controller. However, an anomaly detection method was used to detect DDoS attacks in SDN. Reference [12] proposed DNN deep learning model for DDoS attack detection in SDN. The proposed DNN intrusion detection system produced an accuracy of 87%.

1.2 Deep Learning

Deep learning has emerged as an effective approach that enables the use of datasets to detect network intrusions [13]. According to [14], deep learning approach has become popular in the field of cybersecurity. Studies have shown that deep learning-based intrusion detection system has surpassed tradition methods [14]. According to [15], deep learning has received a lot of research attention in different fields, including network security. Deep learning has the potential to secure computer networks and information systems [15]. According to [16], traditional machine learning security mechanism faced some difficulties in detecting DDoS attacks due to the high volume of network traffic; however, deep learning has come as a solution to machine learning problems and has shown success in different big data sections.

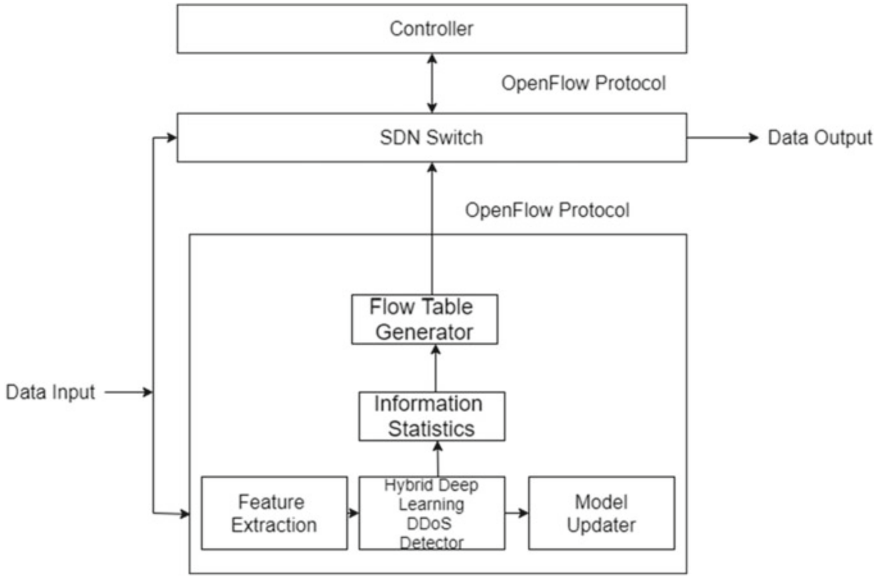


Fig. 2 IDS placement

Figure 2 shows the proposed model placement and traffic flow of the SDN.

Figure 2 shows how the hybrid deep learning IDS was used to detect DDoS attacks in SDN. The communication between the controller and SDN switch was facilitated by OpenFlow protocol. The model has two inputs, one for feature extraction and one for SDN switch. The model has one data output at the SDN switch.

2 Methodology

Feature selection, data distribution, training and testing the classifier and evaluation will be discussed in this section. The proposed model used CICIDS 2017 dataset. The study used literature review [1] to select four best features out of 86 features. Figure 4 shows the hybrid deep learning model block diagram.

Figure 3 shows the proposed model flow diagram. The first step is training, then followed by testing. On the training side, the first step is normalisation. Training of the model follows normalisation. During training, they are forward propagation and weight updates. After training, the model is then tested to detect DDoS attacks.

Figure 3 shows the proposed model flow diagram. The first step is training, then followed by testing. In the training side, the first step is normalisation. Training of the model follows normalisation. During training, they are forward propagation and weight updates. After training, the model is then tested to detect DDoS attacks.

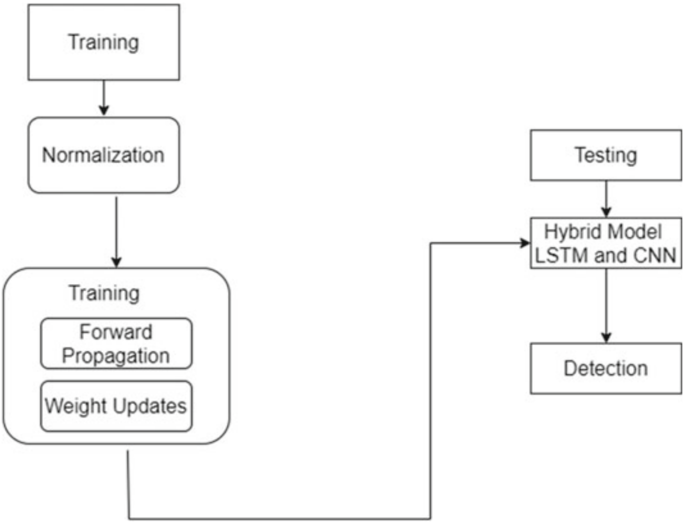


Fig. 3 LSTM and CNN block diagram

For the proposed model to accurately detect DDoS attacks, only relevant features were used to train and test a hybrid DDoS intrusion detection system. According to [1], the following features are the four best features used to build the classifier: [Backward Packet Length Standard Deviation, Flow Duration, Average Packet Size, Forward Inter Arrival Time Standard Deviation].

2.1 Data Distribution

The dataset distribution of the proposed algorithm used an 80:20 ratio, where 80% is the training set and 20% is the testing set.

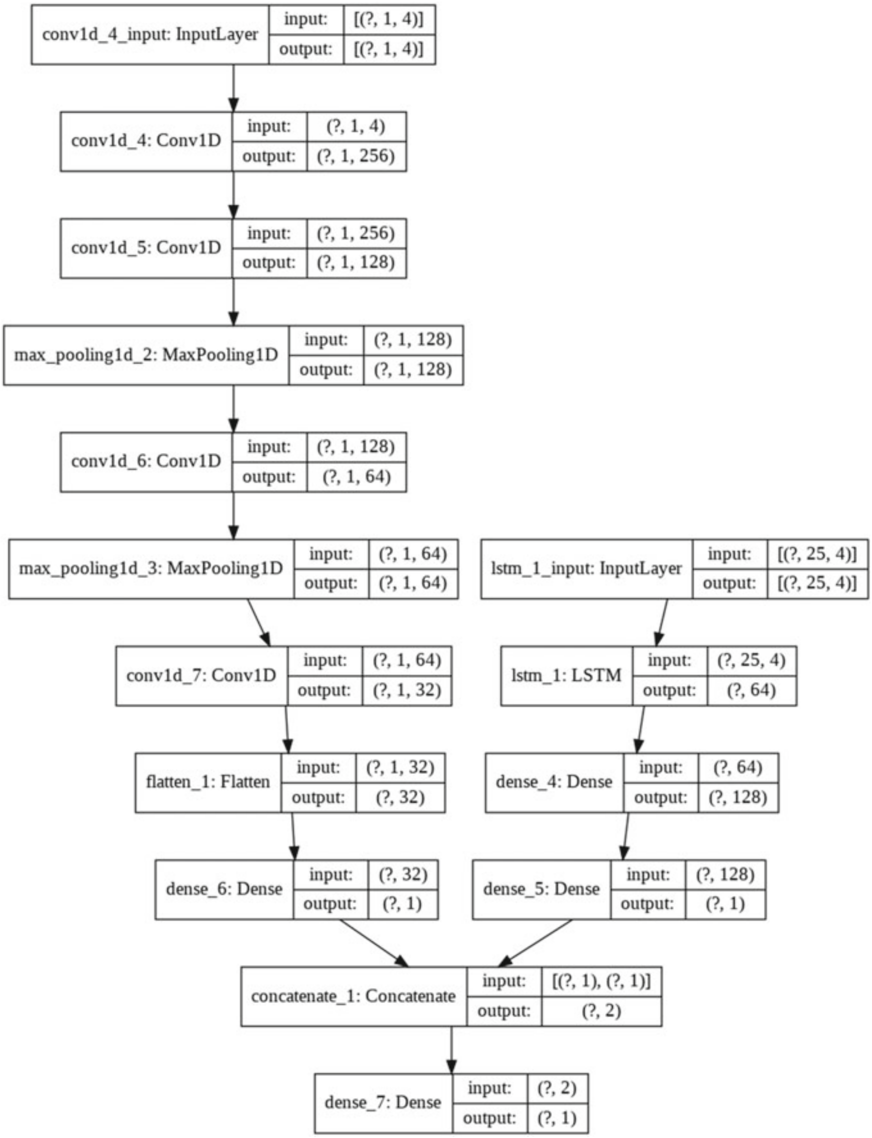


Fig. 4 Proposed model semantic

2.2 Algorithm

```
Input: Four best features
   Splitting (Training set 0.8 and Testing data 0.2
          Train LTM model
         Train CNN model
           Merge the predictions from LSTM and CNN
          Test the model
         Decision using decision tree
        Evaluation
      Benign traffic
  Else
    DDoS traffic
```

2.3 Proposed Deep Learning Model

The study proposed a hybrid deep learning model of LSTM and CNN for real-time DDoS attack detection in SDN. Below is the layout of the proposed model (LSTM and CNN).

The hybrid LSTM and CNN model has five layers; the input layer has an input of 64 neurons for CNN and four input neurons for LSTM. CNN has an output of 64 neurons and LSTM has an output of four neurons. The output of CNN, which is 64 neurons, is loaded into the second layer, which produced an output of 32, and LSTM produced an output of 64 neurons. Thirty-two neurons of CNN are then loaded into the next hidden layer, which produced an output of 32 neurons, and the input of LSTM 64 neurons produced 128 neurons. The fourth layer of CNN moved the output of 32 neurons to the next layer, which produced one and 128 neurons of LSTM, then moved to the next hidden layer, which produced the output of one. At this stage, the two models were then joined to form a hybrid model. The input is one and the hybrid produced the result, which is either 0 or 1, where 0 is benign traffic, and 1 is DDoS traffic.

2.4 Evaluation

The study used accuracy, precision, recall and F1-Score as standard evaluation parameters of the hybrid DL distributed denial of service attack detection in SDN.

Accuracy—is used to find the portion of correctly classified values, and it tells how often the classifier is suitable [17].

Precision—The ability of the model to classify positive values correctly [17].

Recall—used to calculate the ability of the model to predict positive values. It shows how often the model predicts the correct positive values [17].

F1-Score—is the average of recall and precision. It is useful when both recall and precision are being used [17].

3 Results

The results section presents and interprets the results of the experiment. Accuracy, Precision, Recall and F1-Score are calculated as:

Accuracy (%)

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} * 100$$

Accuracy = 99.72%

Precision (%)

$$Precision = \frac{TP}{TP + FP} * 100$$

$$\boldsymbol{Precision = 99.75\%}$$

Recall (%)

$$Recall = \frac{TP}{TP + FN} * 100$$

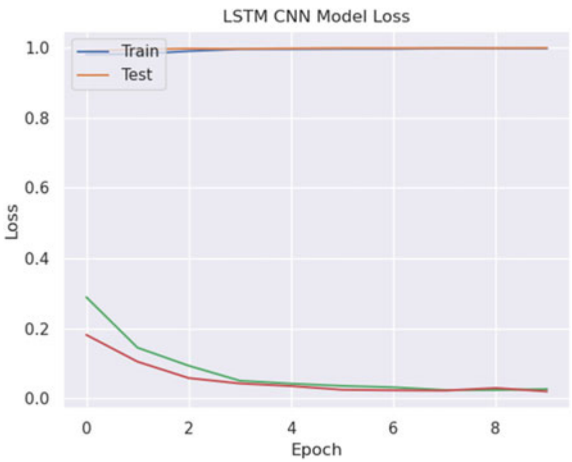
$$\boldsymbol{Recall = 99.82\%}$$

F1-Score (%)

$$F1Score = \frac{2 * TP}{2 * TP + FN} * 100$$

$$\boldsymbol{F1Score = 99.9\%}$$

Fig. 5 Proposed model loss



3.1 Loss

Figure 5 shows the epoch vs loss graph for the proposed model. The training loss of the proposed model is 0.3, and the test loss of the proposed model is 0.2.

3.2 Accuracy

The accuracy of the proposed model is shown in Fig. 6, and it was compared with models which are already in the market.

Fig. 6 Accuracy of the proposed model

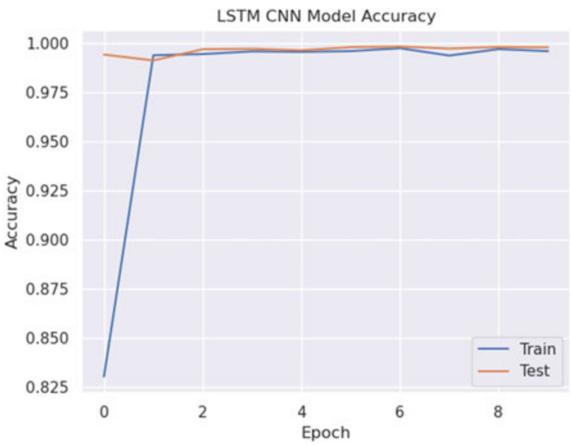


Table 1 Accuracy comparison table

Model	Accuracy %	Reference
LSTM and CNN (Proposed model)	99.72	–
RNN	68.55	[14]
GRU and RNN	89	[18]
RNN	84	[19]
KNN	98.3	[20]
CNN	97.2	[21]

Figure 6 shows how the proposed model performed in detecting DDoS attacks in SDN. The proposed model produced 99.72% accuracy.

Table 1 and Fig. 7 show the comparison of the proposed model and other existing models. The proposed model (LSTM and CNN) achieved 99.72% accuracy, which is better than existing models.

Figure 8 shows the confusion matrix of the proposed model. The model detects 12,724 instances classified as true positive for benign attacks and 58 instances misclassified as DDoS attacks. The model detects 41 instances of misclassified false positive for DDoS as benign attacks, and the model detects 23,172 instances classified as benign attacks.

Figure 9 shows the value of the evaluation parameters of the proposed model. The proposed model achieved an accuracy of 99.72%, precision 99.73%, recall 99.52% and F1-score 99.9%.

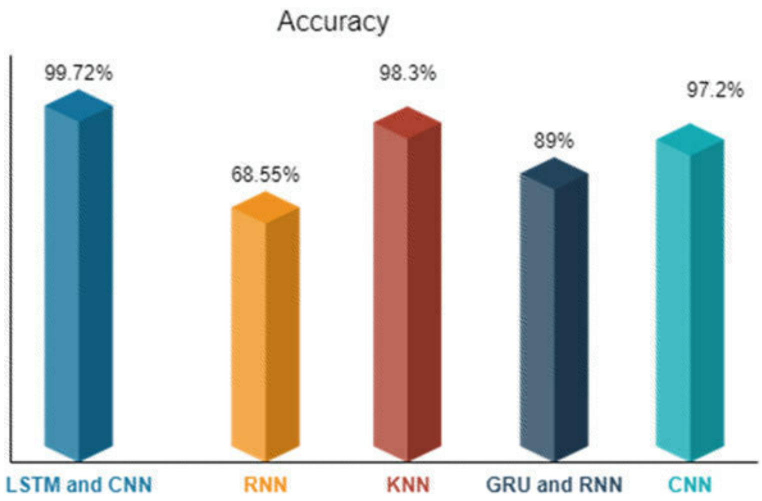


Fig. 7 Comparison graph

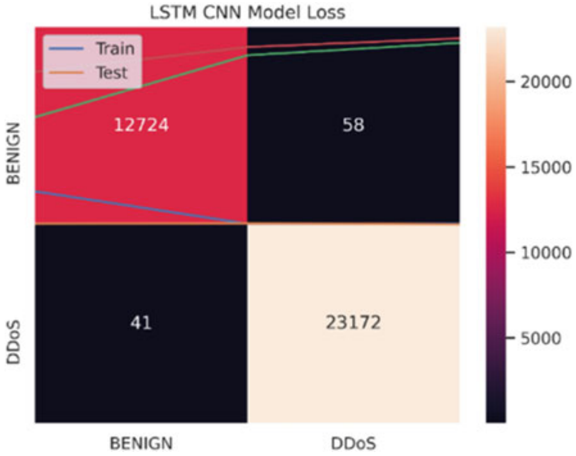


Fig. 8 Confusion matrix of the proposed model

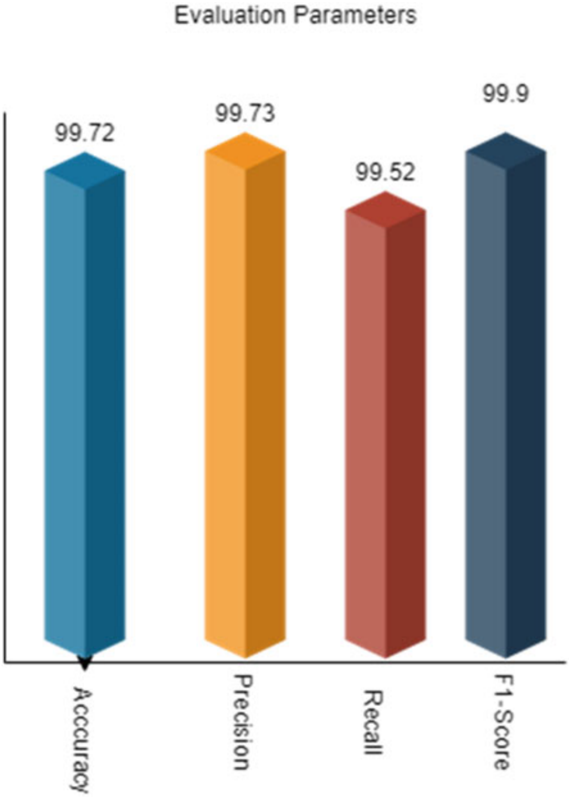


Fig. 9 Evaluation parameters of the proposed model

4 Conclusion

Software-defined networks have shown great potential in changing the networking architecture. Its decoupled architecture has become a significant target of cyber-attacks. To protect SDN architecture from cyber-attacks, the proposed hybrid deep learning DDoS intrusion detection system has shown a strong ability to detect DDoS attacks in SDN. The model is cost-effective and has a high accuracy detection rate. The flow-based dataset CICIDS 2017 has been utilised in this model. This proposed model has shown great potential by producing 99.72% accuracy using less computation power and less training time.

References

1. Haider S et al (2020) A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks 8
2. Haider S, Akhunzada A, Ahmed G, Raza M (2019) Deep learning based ensemble convolutional neural network solution for distributed denial of service detection in SDNs. In: 2019 UK/China Emerging Technologies, pp 1–4. https://doi.org/10.1109/UCET.2019.8881856
3. Ujjan RMA, Pervez Z, Dahal K (2019) Suspicious traffic detection in SDN with collaborative techniques of snort and deep neural networks. In: Proceedings—20th international conference on high performance computing and communications; 16th international conference on smart city; 4th international conference on data science and systems HPCC/SmartCity/DSS 2018, pp 915–920. https://doi.org/10.1109/HPCC/SmartCity/DSS.2018.00152
4. Dimolianis M, Pavlidis A, Kalogeras D, Maglaris V (2019) Mitigation of multi-vector network attacks via orchestration of distributed rule placement. In: 2019 IFIP/IEEE symposium on integrated network and service management IM 2019, vol 731122, no 731122, pp 162–170
5. Learning M, Cookbook R Title: a short review on applications of deep learning for cyber security, no Dl
6. Hwang RH, Peng MC, Huang CW, Lin PC, Nguyen VL (2020) An unsupervised deep learning model for early network traffic anomaly detection. IEEE Access 8(February):30387–30399. https://doi.org/10.1109/ACCESS.2020.2973023
7. Li C et al (2018) Detection and defense of DDoS attack–based on deep learning in OpenFlow-based SDN. Int J Commun Syst 31(5):1–15. https://doi.org/10.1002/dac.3497
8. Santos Da Silva A, Wickboldt JA, Granville LZ, Schaeffer-Filho A (2016) ATLANTIC: a framework for anomaly traffic detection, classification, and mitigation in SDN. In: Proceedings NOMS 2016–2016 IEEE/IFIP network operations and management symposium, no Noms, pp 27–35. https://doi.org/10.1109/NOMS.2016.7502793
9. Garg S, Kumar N, Rodrigues JJPC, Rodrigues JJPC (2019) Hybrid deep-learning-based anomaly detection scheme for suspicious flow detection in SDN: a social multimedia perspective. IEEE Trans Multimed 21(3):566–578. https://doi.org/10.1109/TMM.2019.2893549
10. Čeponis D, Goranin N (2019) Evaluation of deep learning methods efficiency for malicious and benign system calls classification on the AWSCTD. Secur Commun Netw 2019. https://doi.org/10.1155/2019/2317976
11. Hafizah S et al (2018) A review of anomaly detection techniques and distributed denial of service (DDoS) on software defined network (SDN). Technol Appl Sci Res 8(2):2724–2730. https://www.researchgate.net/publication/324830666
12. Dey SK, Rahman MM (2018) Flow based anomaly detection in software defined networking: a deep learning approach with feature selection method. In: 2018 4th international conference

on electrical engineering and information & communication technology, pp 630–635. https://doi.org/10.1109/CEEICT.2018.8628069.

13. Karatas G, Demir O, Koray Sahingoz O (2019) Deep learning in intrusion detection systems. In: 2018 international congress on big data, deep learning and fighting cyber terrorism, pp 113–116. https://doi.org/10.1109/ibigdelft.2018.8625278
14. Yin C, Zhu Y, Fei J, He X (2017) A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access 5:21954–21961. https://doi.org/10.1109/ACCESS.2017.2762418
15. Fadlullah Z, Tang F, Mao B, Kato N et al (2017) State-of-the-art deep learning: evolving machine intelligence toward tomorrow's intelligent network traffic control systems. Surv Tutorials 19(4):2432–2455. https://www.researchgate.net/profile/Imed_Romdhani/post/can_we_use_deep_learning_concepts_in_IoT_security_projects/attachment/5a60c3cbb53d2f0bba4c2b92/AS:584181025361920@1516291018882/download/State-of-the-Art+Deep+Learning+Evolving+Machine+Intelligence+T
16. Diro AA, Chilamkurti N (2018) Distributed attack detection scheme using deep learning approach for Internet of Things. Futur Gener Comput Syst 82:761–768. https://doi.org/10.1016/j.future.2017.08.043
17. Malik J, Akhunzada A, Bibi I, Imran M, Musaddiq A, Kim SW (2020) Hybrid deep learning: an efficient reconnaissance and surveillance detection mechanism in SDN. IEEE Access 8:134695–134706. https://doi.org/10.1109/ACCESS.2020.3009849
18. Tang TA, McLernon D, Mhamdi L, Zaidi SAR, Ghogho M (2019) Intrusion detection in sdn-based networks: deep recurrent neural network approach. IEEE
19. Jakhar K, Hooda N (2019) Big data deep learning framework using keras: a case study of pneumonia prediction, pp 1–5. https://doi.org/10.1109/ccaa.2018.8777571
20. Polat H, Polat O, Cetin A (2020) Detecting DDoS attacks in software-defined networks through feature selection methods and machine learning models. Sustainability 12(3). https://doi.org/10.3390/su12031035
21. Hojjatinia S, Hamzenejadi S, Mohseni H (2019) Android botnet detection using convolutional neural networks, pp 1–6

Chapter 2
CP-ABE Scheme with Decryption Keys of Constant Size Using ECC with Expressive Threshold Access Structure

Rakshit Kothari, Naveen Choudhary, and Kalpana Jain

Abstract With the rapid development of cross-organizational application systems that are geographically distributed, the notion of Virtual Organization (VO) is indispensable. The inevitable existence of global information infrastructure in every field has forced virtual organizations to gain importance as a fitting model for making a large-scale organization of distributed nature. Virtual organization mainly deals with the devolution of responsibilities to other organizations and providing goods and services by having mutual cooperation among organizations. An ancient mechanism is essential to have controlled access to shared resources and proper participation policies. However, this controlled access is challenging in the case of VO because of its distributed nature. Thus, a mechanism which can handle complex access policies is needed. The mechanism is also required to be reasonably scalable and efficient. In this paper, we propose a threshold access structure implemented using Elliptic Curve Cryptography, which is much better in terms of efficiency. Our main contribution is that we propose a threshold access structure that uses ECC and provides constant-size secret keys for the Ciphertext Policy Attribute-based Encryption (CP-ABE) scheme. In essence, we suggest a formal procedure to share secret information using encryption, where secret messages are associated with a policy, and only the users who have this specific attribute set that fulfils the specified policy will be apt to successfully decrypt and gain access to the secret message/information.

Keywords Threshold access structure · Attribute-based encryption · Secret keys of constant size · Ciphertext policy · Distributed system security · Virtual organization · Elliptic curve cryptography

R. Kothari (✉) · N. Choudhary · K. Jain
Department of Computer Science and Engineering, College of Technology and Engineering,
MPUAT, Udaipur, India
e-mail: kalpana_jain2@rediffmail.com

R. Mathur et al. (eds.), *Emerging Trends in Data Driven Computing and Communications*,
Studies in Autonomic, Data-driven and Industrial Computing,
https://doi.org/10.1007/978-981-16-3915-9_2

1 Introduction

Today, distributed computing systems, deployed over the large geographical area, are used as a model to achieve a single task by many different organizations working together with mutual cooperation. These characteristics can be appropriately sketched by Virtual Organization (VO). Virtual organizations can be thought of as both organizationally and geographically distributed organizations [11] which can aptly satisfy the needs like cooperative resource sharing. Virtual organizations can also be thought of as a model for designing distributed systems for an organization that requires complex resource sharing rules, expressive access structure and tangled inter-process interaction. However, the task of defining and enforcing the access scheme is hard because each organization participating in VO can delegate a large number of representatives, who in turn are at different hierarchical levels. Because of accountability and liability issues, the access of users to shared resources should be controlled with a proper access structure, which is flexible enough to facilitate the required functionality. Therefore, the control over sharing of resources using proper and flexible access structure is an extremely important and challenging task in case of VO.

As an illustration, we present a scenario in which VO is an appropriate model to achieve required goals. The outbreak of Coronavirus in the World led to the establishment of epidemiological and virological surveillance and controlled task forces to combat and find the source of infection. In order to control and combat the spreading of this infection, it is required to closely monitor all the key factors that led to the spreading of this infection. For example, it is mandatory to keep track of records of patients who have COVID-19 symptoms, we may also need to retrieve the immigration records of such patients to exactly locate the origin point of infection. COVID-19 is lethal which spreads through droplets generated when the COVID-19 patient coughs, sneezes or speaks. In order to control and combat the spreading of this infection, it is required to closely monitor all the key factors that led to its spreading.

An appropriate encryption scheme is CP-ABE in which the access policy is associated with the plaintext message by the encrypter and only the users who fulfil the specified policy will be able to decipher the ciphertext. The users are related with attributes based on which organization they belong to and what their designation is in that organization. The policy is also specified by a set of attributes. Hence, CP-ABE is acutely appropriate and suitable for implementing controlled resource sharing in Virtual Organizations because it enables the encrypter to decide and impose access policy while encrypting confidential or sensitive information.

1.1 Related Work

In the literature, ABE [25] is an important encryption scheme given by Sahai and Waters, which can be applied to any role-based system to provide data confidentiality

[10]. Identity-based Encryption [5], in particular, changed the classical way of thinking for public key encryption by letting the public key be some string associated with the identity of a receiver, for example, the email address of the receiver. There exist many identity-based encryption schemes that provide shorter keys for decryption, for example, multi-identity single-key decryption [14, 15, 17] and identity-based encryption with traitor tracing [16].

Sahai-Water's seminal work [25] was followed by the development of several KP-ABE schemes [1, 12, 24, 25] and CP-ABE schemes [3, 7, 10, 18, 21, 22, 25, 26]. CP-ABE permits the user to decide the policy of access during execution of encryption; it is more suitable for access control applications which require implicit authorization. CP-ABE schemes come in two flavours, one with constant-size ciphertext [9, 10, 28], and another with constant-size secret keys [10, 13, 23]. All these schemes are built upon bilinear maps and provide an expressive access structure. Bilinear maps are far less efficient when compared with ECC because they require large-sized security parameter. Thus, ECC is more suitable and a better choice as compared to bilinear maps [2, 20, 29].

Except EMNOS scheme [10], no other scheme facilitates constant-size ciphertext along with constant-size secret keys. EMNOS scheme [10] facilitates (n, n)-threshold structure which can be restrictive for some practical applications. GSWV scheme [13] provides an access structure of AND-gate and facilitates secret keys of constant size. However, both GSWV scheme [13] and EMNOS scheme [10] are based on computationally expensive bilinear maps. ODG scheme [23] uses ECC instead of bilinear maps, thus achieving efficiency, but provides expressive AND gate access structure which is again too restrictive in some practical instances.

The scheme which we propose in this paper is the only one, which achieves threshold access structure and is based on ECC instead of bilinear maps, thus promising in terms of efficiency, while keeping the secret decryption key size constant. Threshold

Table 1 Comparing various CP-ABE techniques

Scheme	LSK	LCT	Access structure
Waters [26]	$(\mathbb{A} + 2)\mathbb{G}$	$(2\mathbb{P} + 1)\mathbb{G} + \mathbb{G}_t$	LSSS
ODG [23]	$2 \times O(\mathbb{G})$	$(n - \lvert\mathbb{P}\rvert + 3)\mathbb{G} + L$	AND gates
Ours	$2 \times O(\mathbb{G})$	$(2n - \lvert\mathbb{P}\rvert - \lvert\mathbb{A}\rvert + 3)\mathbb{G} + L$	Threshold

Note LSSS: scheme on linear secret sharing; LSK: user secret key length; LCT: ciphertext length; L: length of message of plaintext M; $\mathbb{G}$ and $\mathbb{G}_t$: groups of prime order paring; G: base-point of the curve group which is elliptic; O(G): order of base point of the elliptic curve group access structure is flexible and general enough to meet the needs of some practical problems like resource sharing in the case of virtual organizations. A comparison of different attribute-based encryption is presented in Table 1.

1.2 Our Contributions

Our main contribution are summarized below.

1. We propose an efficient mechanism using CP-ABE and Elliptic Curve Cryptography with an expressive (n, k)-threshold access structure. This is the first scheme that provides a provably secure (n, k)-threshold access structure using ECC.
2. Another major contribution of this paper is that it uncovers an error in the KeyGen phase and Decrypt phase of the ODG scheme [23]. We show that the ODG scheme will not work as expected and we also give appropriate changes to make it work correctly.
3. Our proposed CP-ABE technique also achieves secret keys which are of constant size, i.e., user decryption key size is not dependent on the cardinality of universe attribute set $\mathbb{U}$.
4. It is shown that the achieved (n, k)-threshold access structure is secure under the given model.

2 Definitions and Preliminaries

The section provides an outline of the basic preliminary concepts along with the computational hard problems associated with our scheme, which are used in this paper. The representation used throughout this paper is mentioned in Table 2. In the end of this section, we draw a basic CP-ABE technique for a selective game that defines the selective-security against a chosen ciphertext attack.

2.1 Access Structure and Attribute

We represent the Universe attribute set by $\mathbb{U}$ consisting of n number of attributes. Let $\mathbb{U} = \{A_1, A_2, A_3 ... A_n\}$. We represent the ith attribute by A_i. The attribute set corresponding to a user is denoted by $\mathbb{A} \subseteq \mathbb{U}$. In this paper, attribute set is denoted by n-bit string of binary $a_1 a_2 a_3 ... a_n$; also, this binary string is defined by

$$\begin{cases} a_i = 1 \text{ iff } A_i \in \mathbb{A} \\ a_i = 0 \text{ iff } A_i \notin \mathbb{A} \end{cases}$$

Table 2 Notation used

Symbol	Description
ρ	Security parameter
p	Numbers which are prime and large (160 bits)
$E_p(a, b)$	$y^2 = x^3 + ax + b(mod\ p)$ represents Elliptic curve
G	Order of 160-bit number at point of base in $E_p(a, b)$ in $\mathbb{Z}_p$
xG	$G + G + \cdots + G$ (x times), Elliptic curve multiplication by scalar, $G \in E_p(a, b)$
$P + Q$	Point addition for the curve which is elliptic, $P, Q \in E_p(a, b)$
$\mathbb{G}$	Group of curves which are elliptically generated by G
$\mathbb{Z}_p^*$	$\{1, 2, 3, \ldots, p - 1\}$, p is the prime number
p'	Order of the point of base G in $E_p(a, b)$
MSK	Secret key of master
MPK	Public key of master
α, β, γ	Random numbers which serve as master secret key. $\alpha, \beta, \gamma \in \mathbb{Z}_p$
H_1, H_2, H_3, H_4	Collision-resistant for functions which are hash
KDF	Function of Key Derivation
$\mathbb{U}$	Universe attribute set $A_1, A_2, A_3, \ldots, A_n$ for n number of attributes
n	Cardinality of $\mathbb{U}$
$\mathbb{A}$	$\mathbb{A} \subseteq \mathbb{U}$, user attribute set
a_i	ith bit in the bit representation of attribute set $\mathbb{A}$. $a_i = 1$ iff $A_i \in \mathbb{A}$
$\mathbb{P}$	Access Policy, $\mathbb{P} \subseteq \mathbb{U}$
b_i	ith bit in the bit representation of attribute set $\mathbb{P}$. $b_i = 1$ iff $A_i \in \mathbb{P}$
$\lvert\mathbb{X}\rvert$	Cardinality of the set $\mathbb{X}$.
$\mathbb{S}^x$	Cartesian Product of $\mathbb{S}$, x times, $\mathbb{S}^x = \mathbb{S} \times \mathbb{S} \times \mathbb{S} \times \cdots \times \mathbb{S}$ (x times)
M	Plaintext message
C	Ciphertext corresponding to M
l_σ	Length of string which is random
l_m	Length of the message which is plaintext M
$\oplus$	Bitwise XOR operator
$\{0, 1\}^*$	String which is binary and of arbitrary length
$\{0, 1\}^l$	String which is binary whose length is represented by l
$f(x, \mathbb{P})$	$\prod_{j=1}^{n} (x + H_4(j))^{1-b_j}$
f_j	Coefficient of x^j in $f(x, \mathbb{P})$
$F(x, \mathbb{A}, \mathbb{P})$	$\prod_{j=1}^{n} (x + H_4(j))^{2-a_j-b_j}$
F_j	Coefficient of x^j in $F(x, \mathbb{A}, \mathbb{P})$