Hindawi
Security and Communication Networks
Volume 2021, Article ID 1852466, 11 pages
https://doi.org/10.1155/2021/1852466

Research Article

Acquiring Data Traffic for Sustainable IoT and Smart Devices Using Machine Learning Algorithm

Yi Huang,[1] Shah Nazir,[2] Xinqiang Ma,[1] Shiming Kong,[1] and Youyuan Liu[1]

[1]*Institute of Intelligent Computing and Visualization Based on Big Data, Chongqing University of Arts and Sciences, Chongqing, China*
[2]*Department of Computer Science, University of Swabi, Swabi, Pakistan*

Correspondence should be addressed to Shah Nazir; snshahnzr@gmail.com and Xinqiang Ma; xinqma@zju.edu.cn

Received 21 April 2021; Revised 11 May 2021; Accepted 25 May 2021; Published 19 June 2021

Academic Editor: Muhammad Ahmad

Billions of devices are connected via the Internet which has produced various challenges and opportunities. The increase in the number of devices connected to the Internet of things (IoT) is nearly beyond imagination. These devices are communicating with each other and facilitating human life. The connection of these devices has provided opening directions for the smart applications which are one of the growing areas of research. Among these opportunities, security and privacy are considered to be one of the major issues for researchers to tackle. Proper security measures can prevent attackers from interrupting the security of IoT network inside the smart city for secure data traffic. Keeping in view the security consideration of data traffic for smart devices and IoT, the proposed study presented machine learning algorithms for securing the data traffic based on a firewall for smart devices and IoT network. The study has used the dataset of "Firewall" for validation purposes. The experimental results of the approach show that the hybrid deep learning model (based on convolution neural network and support vector machine) outperforms than decision1 rules and random forest by generating a recognition rate of 95.5% for the hybrid model, 68.5% for decision rules, and 78.3% accuracy for random forest. The validity of the proposed model is also tested based on other performance metrics such as f score, error rate, recall, and precision. This high accuracy rate and other performance values show the applicability of the proposed hybrid model to secure data traffic purposes in smart devices. This can be used in many research areas of the smart city for security purposes.

1. Introduction

The world population is growing with the passage of time. Various smart devices such as sensor, actuator, and many other smart devices are installed and linked for smooth communication, solving the issues and needs of daily life. The increase in the number of devices connected to the IoT is beyond imagination. These devices are communicating with each other and facilitating human life. The connection of these devices has provided openings directions for the smart applications which are one of the growing areas of research [1–3]. Among these opportunities, security and privacy are considered to be one of the major issues for researchers to tackle. Smart communication is the direct need of modern societies. The role of IoT is understandable in the smart communication of these devices [4–6]. The technology has mainly focused on efficient well-being of humans and with the protection of environment.

The technologies of IoT has unlimited potentials for developing sustainable and smart devices. The information is generally gathered from physical objects and transmitted through communication media for processing. High computation systems are used for processing of the data for producing meaningful insights and needs. These processes can support the administration of city in providing the essential information for maintaining the services in effective way. The applications of IoT are ensuring the delivery of smart services with efficient utilization of resources. Based on the applications of IoT, a gateway is opened for information processing and facilitating automated governance of

smart cities. So, for maintaining the smooth interaction and communication of the devices in the IoT network, security can be considered as the key part of the IoT network for the smart cities [7].

Various approaches have been practiced for communication of security in the smart cities. Ibrahim et al. [8] developed a framework with the help of the programmed sensor by Arduino board and provided the sensory data into the storage of cloud for gaining access to smart-home connected devices. As security and privacy are the key concerns during the process of personal data collection, Witti and Konstantas [9] proposed a framework for ensuring the security and protection of citizen's privacy in the smart city. Jia et al. [10] elaborated the vulnerabilities in the smart home architecture and devised a threat model and then discussed building a semiautomatic vulnerability detection system for detecting vulnerabilities from all sides before releasing the device. The approach was demonstrated through wide-ranging experiments. Talal et al. [11] presented a study with the aim for establishing security solution of IoT-based smart home for monitoring real-time health in the architecture of telemedicine. Various layers were presented. A detailed review analysis on telemedicine was presented with the focus on the server and client sides, showing the other related studies with applications of smart home for IoT. Sharma et al. [12] offered a model for testing the feasibility and performance of the network in the course of link failure and to switch normal environment. Various parameters were considered for assessing the performance of the offered model. The results of the experiments revealed that the model is capable of detecting the mitigate attacks and can be considered for securing the system and ensure security of users.

Proper security measures is the awful need of smart cities which can prevent attackers from interrupting the security of IoT network inside the smart city and the data of devices inside the network traffic will be safe. Keeping in view the security consideration of data traffic for smart cities and IoT, the proposed study achieved the following contributions:

(i) To present machine learning algorithms for securing the data traffic based on a firewall for smart devices and IoT network

(ii) To use the dataset of "Firewall" for validation purposes of the proposed study

(iii) To show the effectiveness of the proposed approach through experiments of the approach

(iv) The validity of the proposed model is also tested based on other performance metrics such as f score, error rate, recall, and precision

(v) Accuracy rate and other performance values show the applicability of the proposed hybrid model for secure data traffic purposes in smart devices

The organization of the paper is as follows. Section 2 depicts the related work to the proposed study. Section 3 shows the methodology of the proposed study with the background of existing associated analysis of literature. Section 4 shows the results and discussion of the paper with evaluation measures of the proposed study. The paper is concluded in section 5.

2. Related Work

Researchers are trying to come across different approaches, techniques, and mechanisms for overcoming various perspectives of smart cities' security. Krichen et al. [13] followed an approach of the model based on consisting of modelling the system with suitable formalism, derivation of suites from the model, applied criteria of convergence for selection of appropriate tests, execution of the tests, and lastly collection of verdicts and their analysis for detection of errors and debug them. The formalism adopted was based on the model of extended timed automata with inputs and outputs. Kaur and Saini [14] described the IoT security challenges, issues, and mechanisms. Le-Dang and Le-Ngoc [15] presented a detailed survey of the architectural design and key technologies of wireless communication for enabling applications of smart city. The study also elaborated the probable threats of security to the devices of IoT in the environment of smart city. Jaafar et al. [16] discussed the literature on the IoT-based smart city from the architecture, platform, technology, and application domain perspectives. Various challenges are raised to the best-effort IoT during the security, end-to-end communication, and energy efficiency. Szymanski [17] surveyed the weaknesses of security of best-effort IoT and, furthermore, presented a secure deterministic industrial tactile IoT core network.

Liu et al. [18] have addressed the attack of traffic analysis for smart homes where the opponents interrupt the traffic from and to the gateway of smart home and profile residents' behavior by digital traces. The traditional tools of cryptography are generally not feasible due to the usefulness of opponents. The study offered a framework for privacy preserved obfuscation for achieving this objective. Several simulations were performed for the effectiveness of the proposed framework. The results elaborated the effectiveness of the framework compared to the existing approaches. Alromaihi et al. [19] analyzed the privacy and security of the healthcare applications for smart cities. Firstly, the study provides a detailed review of the various applications of IoT and their cyber vulnerabilities and then presents a detailed assessment of potential approaches for mitigating the issues of cyber-attacks. Currently, various use cases are available for smart cities. These use cases are in the form of cooperative transportation network, autonomous vehicles, and smart roads for enhancing data propagation. Brincat et al. [20] presented an overview of the scenarios of IoT technology-based smart cities for the intelligent transportation

system. The study has presented the integration of cloud computing with the IoT for big data. The research is attempted for establishing security of the network architecture for enhancing the issues of security [21]. IoT devices are producing traffic based on specific features and variations with respect to traditional devices. Study has been presented for analyzing the possibility of applications of these features for classification of devices. Such classification is better in situation of heterogeneity and dynamic. Total of 41 devices of IoT were used [22]. Research was presented as a secure scenario for operating wireless mobile 6G network to manage big data in smart building [23].

Barbosa et al. [24] proposed a smart card cluster for ensuring message authentication and integration by using hardware signing. The approach is portable, modular, cost-effective, and flexible. With the support of results of the study, it is revealed that the approach outperformed existing solutions. Qureshi et al. [25] presented a framework of detecting version number attack, HELLO-Flood attack, Black hole attack, and Sinkhole attack. Various parameters were used for measuring performance of the framework. These parameters include the true positive rate, detection accuracy rate, false-positive rate, end-to-end delay, and throughput. The results revealed the support of the proposed framework for consideration in the environment of industrial Internet of things. Teng et al. [26] proposed a model of low-cost code dissemination which propagates the update code through mobile vehicles in the city with adoptable style of communication. For code stations, a coverage-based greedy deployment approach was used and algorithm of optimized code selection was used for maximizing code dissemination coverage over the city with low time and cost. Several experiments were performed for validation of the proposed study and the results revealed the effectiveness of the proposed approach. Accurate anomaly detection and identification based on the IoT for traffic identification can be considered as the essential issue for research to tackle. Shafiq et al. [27] proposed an approach of the bijective soft set for feature selection for selecting effective features and then devised approach of CorrACC feature selection metric. Furthermore, the research developed a new technique of features' selection algorithm Corracc based on CorrACC for extracting the most suitable and effective features for the classifier of machine learning through metric of ACC.

3. Analysing the Existing State-of-the-Art Work for Securing Data Traffic of Smart Devices and IoT

The security and privacy aspects are an insinuation of smart city. Research studies in the area have exploited the potential applications and their implications on smart devices. A small number of threats have gained more press in recent times than various ransomware campaigns. The malware and ransomware that encrypt files for denying data access till ransom can be paid by the owner [28]. Alternatives such as cryptolocker, reveton, wannacry, and cryptowall [29] are among the huge number of users paying ransoms. Including a classic ransomware victim, such as loses of personal files or significant work extending from financial information to family pictures [30], there are various victim classes for whom harms are difficult to analyze. The study has presented a detailed survey which focuses on the IoT architecture security and facilitates a comprehensive taxonomy of key issues related with the area and main technologies. Appropriate protocols for infrastructure of IoT and open source tools and platforms for it development are discussed. Issues, challenges, and future directions are given [31]. Research work has been presented with the novel protocol in which the client of IoT can share part of the validation function with the server. Conflict of data at earlier is detected by such clients [32].

Various approaches have been practiced for solving various issues of smart cities. The purpose of this study was to identify the existing research studies in the area. Various popular libraries were searched for achieving the associated details of research. Figure 1 graphically represents the types of articles with the papers published in the ScienceDirect.

Figure 2 depicts the publication titles in the given library.

Figure 3 represents the year of publications. The figure reveals that more articles were published in the year 2020 which further shows that there is a significant growth in research in the given area.

Figure 4 depicts disciplines of the publications in the given library. It was shown in the figure that more articles were published in the field of Computer Science.

The Springer library was searched for analyzing the existing research in the area. Figure 5 briefly describes the disciplines covered in the area with total of publications.

Figure 6 describes the publication types with the total of publications in the given area.

The ACM library was searched for obtaining the relevant materials for the analysis process. Figure 7 depicts the publication types and papers in the given library.

Figure 8 depicts the conference held with the total of papers in the given area.

Figure 9 represents the types of contents in the given library.

The analysis was explored for further in-depth study of the materials in the given area of research. Figure 10 represents the media format with the publications in the library mentioned.

The IEEE library was searched and the associated results for analysis were obtained. Figure 11 depicts the publication types with the number of papers in the IEEE.

This library was further explored in order to obtain more results of the search. Figure 12 represents the location of conferences held.

The study analyzed the publication topics covered by the current study and identified a list of topics which are shown in Figure 13.

4. Results and Discussion

The experimental and simulation results are carried out on the dataset downloaded from Kaggle "Internet Firewall." The experimental work was performed using the Python tool.

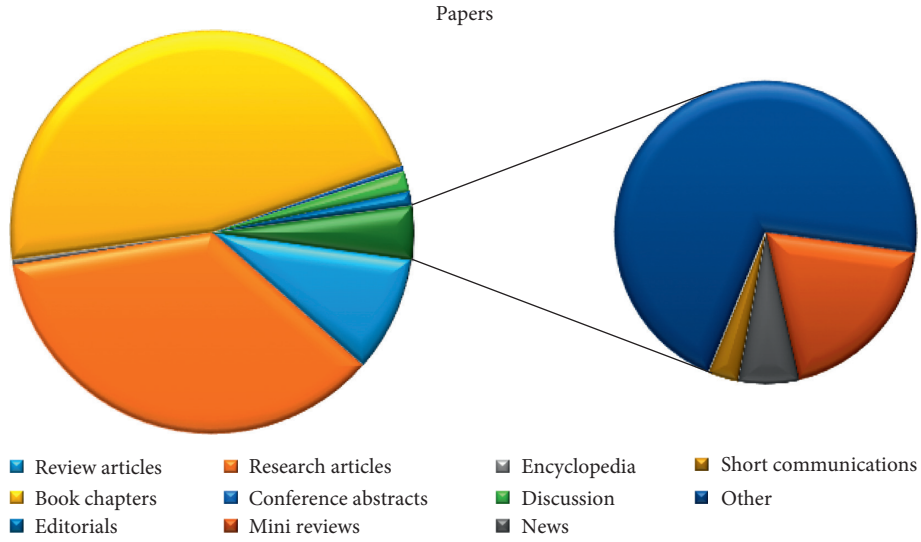

Figure 1: Article types.

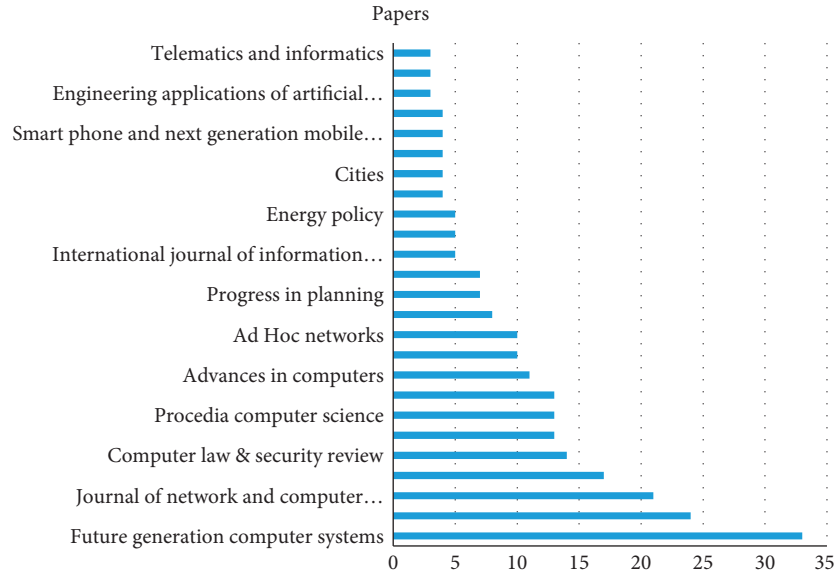

Figure 2: Publication titles.

This research work proposes the uses of a hybrid deep learning model based on convolution neural network (CNN) and support vector machine (SVM). The CNN is used for the classification purposes, while the SVM is used for the recognition and prediction purposes. The performance comparison in between these algorithms is depicted in Figure 14.

After assessing the planned hybrid model for various performance metrics such as misclassification rate, specificity, F measure, precision, recall, and accuracy, it was concluded that the hybrid model outperforms very well among other classification algorithms as depicted in Figure 15. The other two generic techniques random forest and decision rules are used to

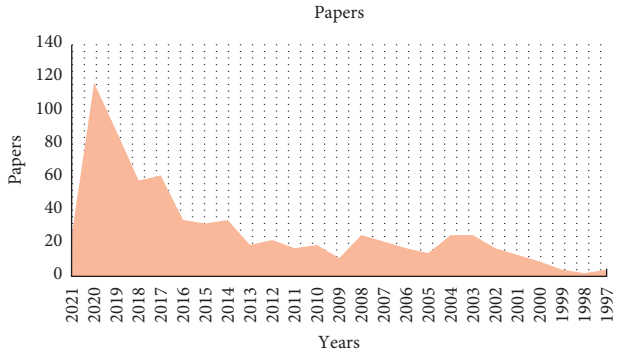

Figure 3: Years of publication.

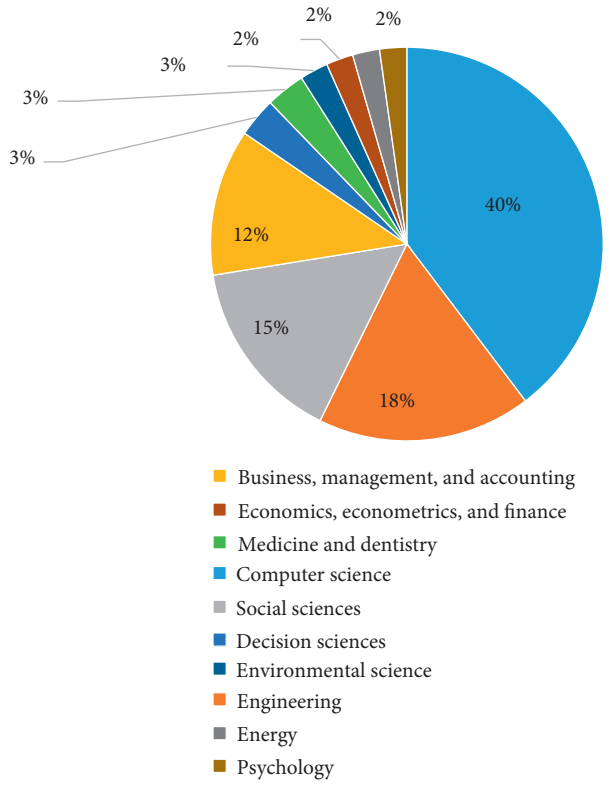

Figure 4: Disciplines of publication.

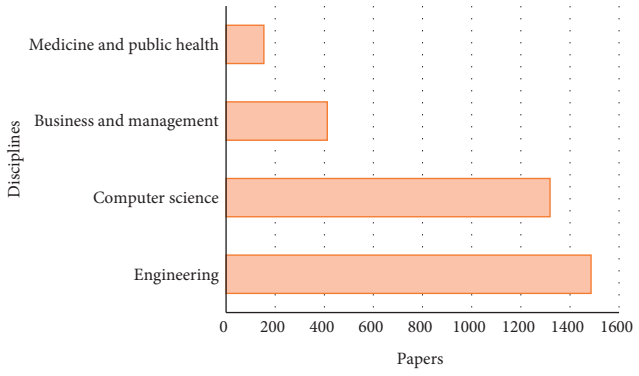

Figure 5: Disciplines and number of articles.

validate the applicability of the hybrid model in the recognition and classification task:

(i) Hybrid model results: Figure 15 shows the experimental results of the proposed hybrid model. The CNN is considered as one of the best technique among deep architectures to accurately classify different objects.

(ii) Random forest-based results: Figure 16 depicts the recognition capabilities of the random forest-based model based on different performance metrics.

(iii) Decision rules: using different performance metrics, the recognition capabilities of decision rule-based recognition model is depicted in Figure 17.

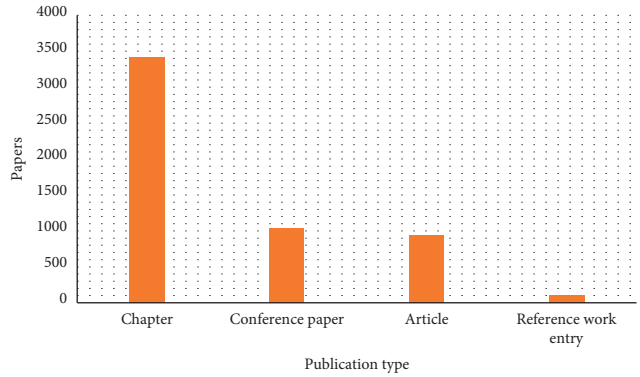

Figure 6: Publication types and papers.

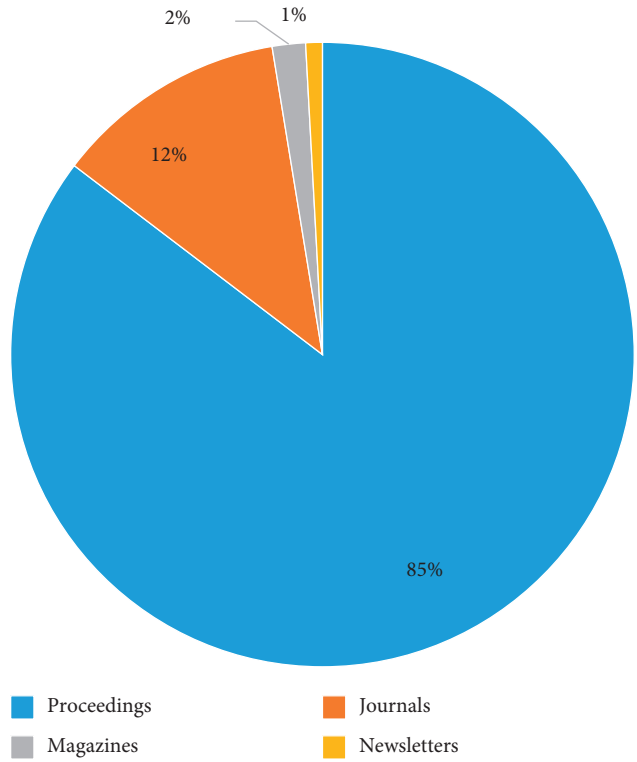

Figure 7: Publication types and papers.

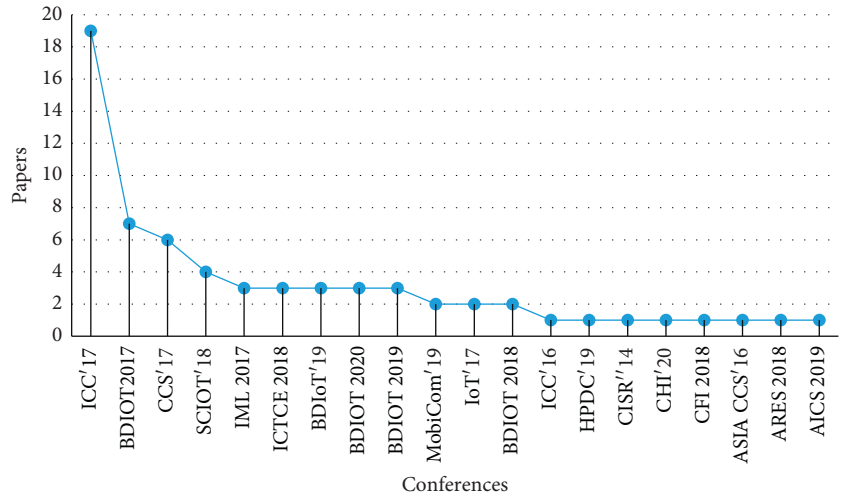

Figure 8: Conference location and papers.

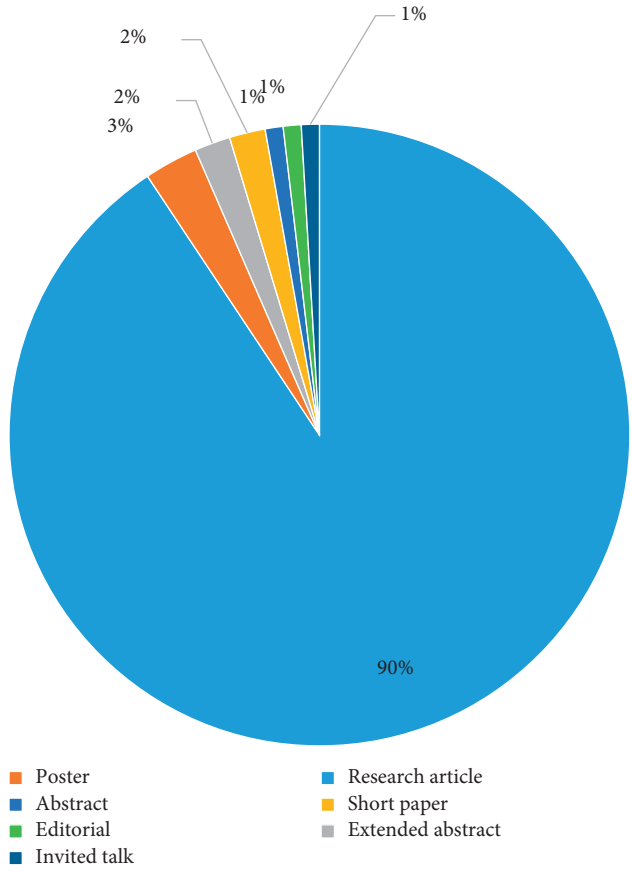

Figure 9: Content type.

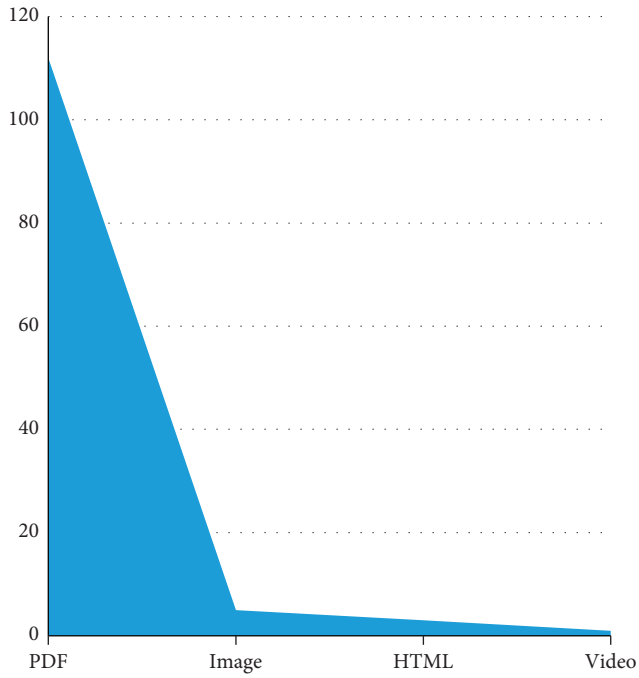

Figure 10: Media format.

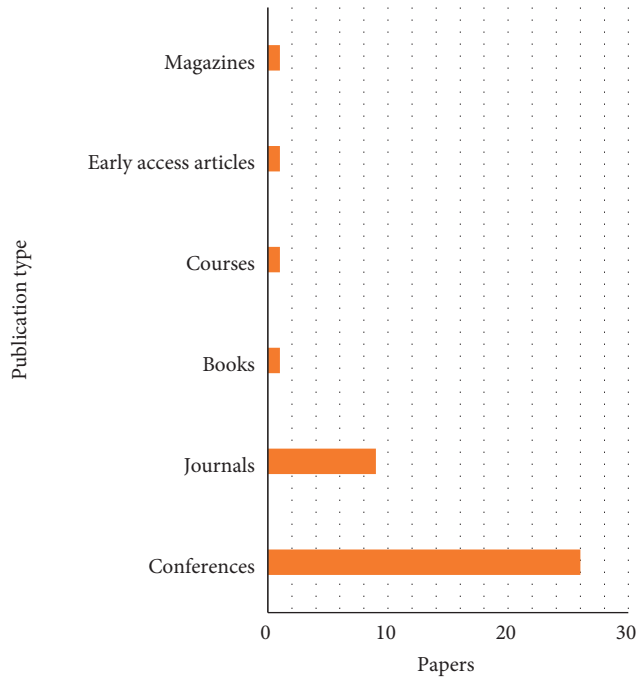

Figure 11: Publication type.

Figure 12: Conference locations.

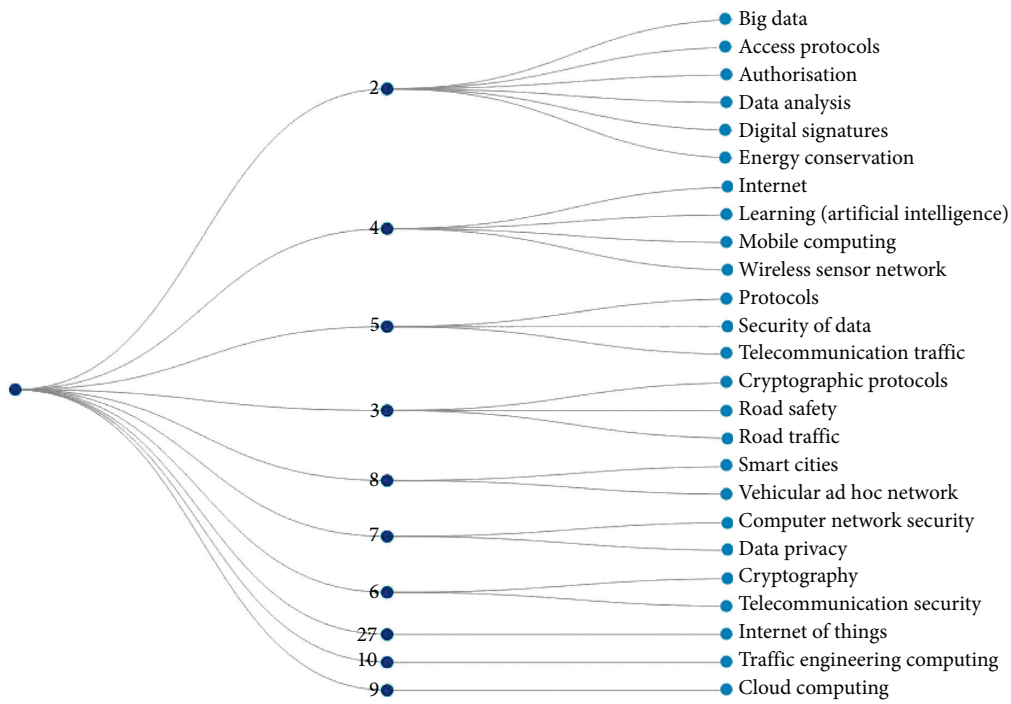

Figure 13: Publication topics and papers.

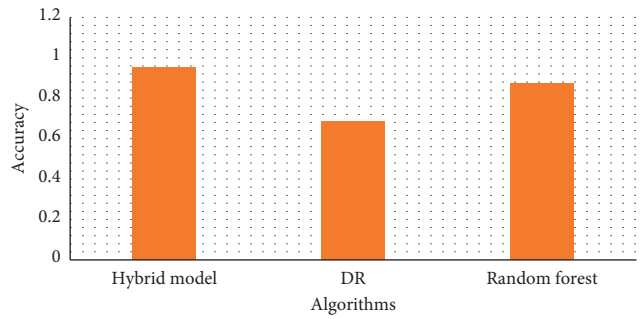

Figure 14: Comparison of algorithms for the planned study.

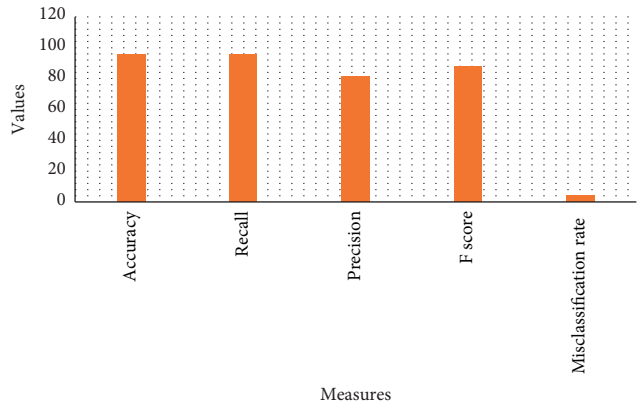

Figure 15: Hybrid model-based classification and recognition results.

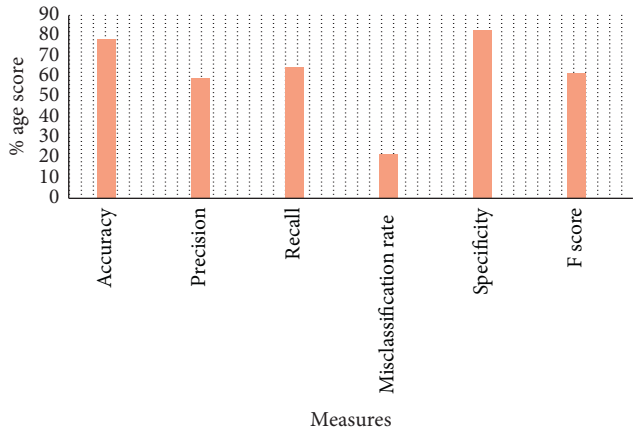

Figure 16: Random forest-based recognition results.

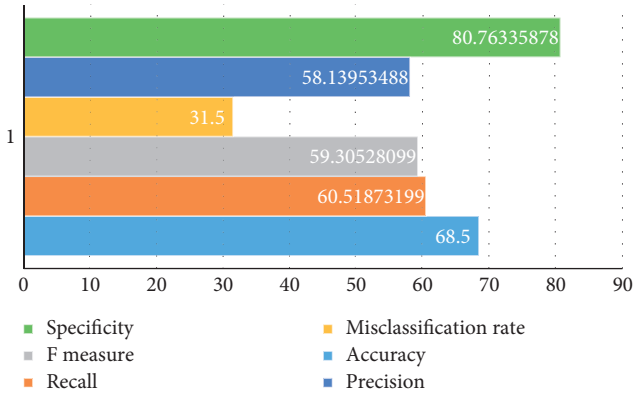

Figure 17: Decision rule-based recognition results.

5. Conclusion

Numerous devices such as sensor, actuator, and many other smart devices are connected and installed for communication, interaction, and solving the issues smart devices. The increase in the number of devices connected to the IoT is rising day by day. The connection of these devices has provided openings' directions for the smart applications which is one of the growing areas of research. Among these opportunities, security and privacy are considered to be one of the major issues for researchers to tackle. Smart communication is the direct need of modern societies. The role of IoT is understandable in the smart communication of these devices. The technology has mainly focused on efficient well-being of humans and with the protection of environment. These devices are communicating with each other and facilitating human life. The connection of these devices has provided openings' directions for the smart applications which is one of the growing areas of research. Proper security measures can prevent attackers from interrupting the security of IoT network inside the smart city for secure data traffic. Keeping in view the security consideration of data traffic for smart cities and IoT, the proposed study presented machine learning algorithms for securing the data traffic based on a firewall for smart devices and IoT network. The study has used the dataset of "Firewall" for validation purposes. The experimental results of the approach shows that hybrid deep learning model (based on convolution neural network and support vector machine) outperforms than decision1 rules and random forest by generating a recognition rate of 95.5% for the hybrid model, 68.5% for decision rules, and 78.3% accuracy for random forest. The validity of the proposed model is also tested based on other performance metrics such as error rate, recall, f score, and precision. This great accuracy rate and other performance values show the influence of the proposed hybrid model for secure data traffic purposes in smart devices.

Data Availability

The data used in this study are not available.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Z. Gu, S. Nazir, C. Hong, and S. Khan, "Convolution neural network based higher accurate intrusion identification system for the network security and communication," *Security and Communication Networks*, vol. 2020, Article ID 8830903, 10 pages, 2020.

[2] H. U. Rahman, A. U. Rehman, S. Nazir, I. U. Rehman, and N. Uddin, "Privacy and security—limits of personal information to minimize loss of privacy," in *Proceedings of the Presented at the Future of Information and Communication Conference*, San Francisco, CA, USA[Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-12385-7_65#citeas, San Francisco, CA, USA, March 2019.

[3] J. Zhang, S. Nazir, A. Huang, and A. Alharbi, "Multicriteria decision and machine learning algorithms for component security evaluation: library-based overview," *Security and Communication Networks*, vol. 2020, Article ID 8886877, 14 pages, 2020.

[4] B. Liao, Y. Ali, S. Nazir, L. He, and H. U. Khan, "Security analysis of IoT devices by using mobile computing: a systematic literature review," *IEEE Access*, vol. 8, pp. 120331–120350, 2020.

[5] L. Ning, Y. Ali, H. Ke, S. Nazir, and Z. Huanli, "A hybrid MCDM approach of selecting lightweight cryptographic cipher based on ISO and NIST lightweight cryptography security requirements for Internet of Health Things," *IEEE Access*, vol. 8, pp. 220165–220187, 2020.

[6] L. Wang, Y. Ali, S. Nazir, and M. Niazi, "ISA evaluation framework for security of internet of health things system using AHP-TOPSIS methods," *IEEE Access*, vol. 8, pp. 152316–152332, 2020.

[7] S. Sivagurunathan, A. Sebastian, and K. Prathapchandran, "Internet of things for developing smart sustainable cities (SSC): a security perspective," in *Connectivity Frameworks for Smart Devices*, pp. 307–331, Springer, New York, NY, USA, 2016.

[8] J. M. Ibrahim, A. Karami, and F. Jafari, "A secure smart home using internet-of-things," in *Proceedings of the 9th International Conference on Information Management and Engineering*, pp. 69–74, Barcelona, Spain, October 2017.

[9] M. Witti and D. Konstantas, "A secure and privacy-preserving Internet of Things framework for smart city," in *Proceedings of*

the 6th International Conference on Information Technology: IoT and Smart City, pp. 145–150, Hong Kong, December 2018.

[10] X. Jia, X. Li, and Y. Gao, "A novel semi-automatic vulnerability detection system for smart home," in *Proceedings of the International Conference on Big Data and Internet of Thing*, pp. 195–199, London, UK, December 2017.

[11] M. Talal, A. A. Zaidan, B. B. Zaidan et al., "Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: multi-driven systematic review," *Journal of Medical Systems*, vol. 43, no. 3, p. 42, 2019.

[12] P. K. Sharma, J. H. Park, Y.-S. Jeong, J. H. Park, and Applications, "Shsec: sdn based secure smart home network architecture for internet of things," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 913–924, 2019.

[13] M. Krichen, M. Lahami, O. Cheikhrouhou, R. Alroobaea, and A. J. Maâlej, "Security testing of internet of things for smart city applications: a formal approach," in *Smart Infrastructure and Applications*, pp. 629–653, Springer, New York, NY, USA, 2020.

[14] G. Kaur and K. S. Saini, "Securing network communication between motes using hierarchical group key management scheme using threshold cryptography in smart home using internet of things," in *Computing and Network Sustainability*, pp. 201–212, Springer, New York, NY, USA, 2017, Lecture Notes in Networks and Systems.

[15] Q. Le-Dang and T. Le-Ngoc, "Internet of things (IoT) infrastructures for smart cities," in *Handbook of Smart Cities*, pp. 1–30, Springer, New York, NY, USA, 2018.

[16] A. A. Jaafar, K. H. Sharif, M. I. Ghareb, and D. N. A. Jawawi, "Internet of thing and smart city: state of the art and future trends," in *Advances in Computer Communication and Computational Sciences*, pp. 3–28, Springer, New York, NY, USA, 2019.

[17] T. H. Szymanski, "Securing the industrial-tactile internet of things with deterministic silicon photonics switches," *IEEE Access*, vol. 4, pp. 8236–8249, 2016.

[18] J. Liu, C. Zhang, and Y. Fang, "EPIC: a differential privacy framework to defend smart homes against internet traffic analysis," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1206–1217, 2018.

[19] S. Alromaihi, W. Elmedany, and C. Balakrishna, "Cyber security challenges of deploying IoT in smart cities for healthcare applications," in *Proceedings of the 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, pp. 140–145, Barcelona, Spain, August 2018.

[20] A. A. Brincat, F. Pacifici, S. Martinaglia, and F. Mazzola, "The internet of things for intelligent transportation systems in real smart cities scenarios," in *Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, pp. 128–132, Limerick, Ireland, April 2019.

[21] C. Stergiou, K. E. Psannis, B. B. Gupta, Y. Ishibashi, and Systems, "Security, privacy & efficiency of sustainable cloud computing for big data & IoT," *Sustainable Computing: Informatics and Systems*, vol. 19, pp. 174–184, 2018.

[22] I. Cvitić, D. Peraković, and M. Periša, "Ensemble machine learning approach for classification of IoT devices in smart home," in *Proceedings of the 3rd International Conference on Data Intelligence and Security*, pp. 1–24, Texas, TX, USA, June 2020.

[23] C. L. Stergiou and K. E. Psannis, *IoT-based Big Data Secure Management in the Fog over a 6G Wireless Network*, https://ieeexplore.ieee.org/document/9239366, 2020.

[24] G. Barbosa, P. T. Endo, and D. Sadok, "An internet of things security system based on grouping of smart cards managed by field programmable gate array," *Computers & Electrical Engineering*, vol. 74, pp. 331–348, 2019.

[25] K. N. Qureshi, S. S. Rana, A. Ahmed, and G. Jeon, "A novel and secure attacks detection framework for smart cities industrial internet of things," *Sustainable Cities and Society*, vol. 61, Article ID 102343, 2020.

[26] H. Teng, Y. Liu, A. Liu et al., "A novel code data dissemination scheme for Internet of Things through mobile vehicle of smart cities," *Future Generation Computer Systems*, vol. 94, pp. 351–367, 2019.

[27] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "IoT malicious traffic identification using wrapper-based feature selection mechanisms," *Computers & Security*, vol. 94, Article ID 101863, 2020.

[28] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, "Ransomware threat success factors, taxonomy, and countermeasures: a survey and research directions," *Computers and Security*, vol. 74, pp. 144–166, 2018.

[29] N. Hampton and Z. A. Baig, *Ransomware: Emergence of the Cyber-Extortion Menace*, Cowan University Joondalup Campus, Perth, Australia, 2015.

[30] G. O"Gorman and G. McDonald, *Ransomware: A Growing Menace*, Symantec Corporation, Arizona, AZ, USA, 2012.

[31] B. Gupta and M. J. C. Quamara, "C. Practice, and experience an overview of internet of things (IoT): architectural aspects, challenges, and protocols," vol. 32, no. 21, Article ID e4946, 2020.

[32] A. Al-Qerem, M. Alauthman, A. Almomani, and B. B. Gupta, "IoT transaction processing through cooperative concurrency control on fog-cloud computing environment," *Soft Computing*, vol. 24, no. 8, pp. 5695–5711, 2020.