Hindawi
Security and Communication Networks
Volume 2020, Article ID 8830903, 10 pages
https://doi.org/10.1155/2020/8830903

Research Article

Convolution Neural Network-Based Higher Accurate Intrusion Identification System for the Network Security and Communication

Zhiwei Gu,[1] **Shah Nazir**,[2] **Cheng Hong**,[1] **and Sulaiman Khan**[2]

[1]*State Grid Quzhou Power Supply Company, Quzhou 324000, China*
[2]*Department of Computer Science, University of Swabi, Ambar, Pakistan*

Correspondence should be addressed to Zhiwei Gu; quzhouguzhiwei@163.com

Received 22 June 2020; Revised 17 July 2020; Accepted 25 July 2020; Published 28 August 2020

Academic Editor: Amir Anees

With the development of communication systems, information securities remain one of the main concerns for the last few years. The smart devices are connected to communicate, process, compute, and monitor diverse real-time scenarios. Intruders are trying to attack the network and capture the organization's important information for its own benefits. Intrusion detection is a way of identifying security violations and examining unwanted occurrences in a computer network. Building an accurate and effective identification system for intrusion detection or malicious activities can secure the existing system for smooth and secure end-to-end communication. In the proposed research work, a deep learning-based approach is followed for the accurate intrusion detection purposes to ensure the high security of the network. A convolution neural network based approach is followed for the feature classification and malicious data identification purposes. In the end, comparative results are generated after evaluating the performance of the proposed algorithm to other rival algorithms in the proposed field. These comparative algorithms were FGSM, JSMA, C&W, and ENM. After evaluating the performance of these algorithms and the proposed algorithm based on different threshold values ranging, L_p norms, and different parametric values for c, it was concluded that the proposed algorithm outperforms with small L_p values and high Kitsune scores. These results reflect that the proposed research is promising toward the identification of attack on data packets, and it also reflects the applicability of the proposed algorithms in the network security field.

1. Introduction

The technology is ever playing an important role in human life and made things easy. With the developments of technology, security remains one of the major concerns for communication and interaction [1–10]. Since the last few decades, the attacks on information security become raised and intruders are trying to capture ordination important information for their own benefits. Such attacks on network and information can drastically put the owner of information and network into big loss. The information security of an organization is highly dependent on different types of information of the organization [10–13].

Now a day, the communication is made through Internet of Things (IoT) and a number of devices are connected through a network. The smart devices are connected to communicate, process, compute, and monitor diverse real-time scenarios. The concept of IoT came with the challenges of privacy and security, as the conventional security protocol does not fit the devices of IoT. Different security approaches and measures are used to secure the information communication and to secure the network. This measure includes firewalls, logical access, control, authentication, identification, and encryption and decryption. To build a full-secure system is difficult to manage and none of these security measures alone can secure the communication inside network.

Keeping in view the severity of security, the proposed research has adopted convolution neural network (CNN) approach for intrusion detection. The CNN architecture is

capable of automatic recognition of data within an acceptable range. Whenever new data is fed to these algorithms, they learn and optimize their operations to improve performance, developing "intelligence" over time. The dataset used for the proposed research is available at UCI Machine Learning Repository (https://archive.ics.uci.edu/ml/datasets/Kitsune+Network+Attack+Dataset). The method shows success in identification of attacks on data packets for secure end-to-end communication.

The rest of the paper is organized as follows: Section 2 presents the related work to the current research and a systematic mapping of the similar work reported in the association of computation machinery (ACM) digital library. Section 3 briefly shows the research method followed for the development of an accurate intrusion detection system. Section 4 shows the results and discussions of the proposed research. The paper is concluded in Section 5.

2. Background Study

This section of the paper explains the relevant work reported in the proposed field and a systematic mapping to check the contribution of the work in the ACM digital library.

2.1. Related Work. Diverse approaches and techniques are used to tackle the issue of security from different perspectives. Kotenko and Chechulin [14] presented a framework for security assessment and attack modelling in security information and event management system. Subsorn and Limwiriyakul [15] examined the security of Internet banking of 16 Australian banks for finding the deficiencies which were probably affecting the confidentiality of the bank customers. Furthermore, the study investigated 12 Thai commercial banks and compared the results with the previous research. Kotenko and Chechulin [16] proposed a method for the attack of computer modelling and evaluation of security to realize in security information and event management system. The authors proposed a quantitative approach to security risk for information systems which is extendable, systematic, and modular. The study aims to effectively evaluate security threat in a comprehensive way [9].

Manjiatahsien et al. [17] presented an overview of the IoT architecture with a detailed review of machine learning algorithms, significance of IoT security with diverse types of attacks. The study proposed a model of the associated information management factors for the information security of organization. Firstly, they surveyed 136 articles to identify the information security factors, and, secondly, a series of interviews were held with 19 experts from the industry to evaluate the relevancy of these factors. In third step, a complete model was developed [18]. The security identification has significant role in the field like Internet of Things in smart city. The authors [19] conducted a detailed survey of the state-of-the-art IoT security, deep learning, and big data technology. Deep learning plays a key role from natural language processing to other recognition and security fields [20]. Zhang et al. [7] proposed an approach for crowed assessing the security and trustworthiness of open social networks based on signaling theory.

The authors [5] presented a detailed overview of the security properties investigation of machine learning algorithms. They have analysed the security model of ML to build up a blueprint for multidisciplinary area of research and, after that, the attack methods and discussed the strategies of defense against them. The study presented an overview of the weaknesses and strengths of the available evaluation methods used for usability and security for the websites of electronic commerce (e-commerce). The evaluation models from 2000 to 2018 have been reviewed for e-commerce [21]. Mao et al. [22] proposed a system for building security dependency to measure the significance of security of system from a wide perspective of the system. The effect of small-world and power-law distribution for the degree of in-and out-degree in security dependency network was observed. Nazir et al. [10] proposed a methodology for evaluating the security of software components using the analytic network process. This technique works in situation of complexity where the dependencies exist among different nodes of network.

2.2. Existing Approaches for Security. Information security plays a significant role in the functionality of a system to smoothly be functional. Data inside a network passes through different packets. Secure communication through these packets can further enhance the efficiency of a system to be reliable. Different approaches and methods are used to secure communication inside and outside the network. To know the details of the literature, the popular libraries were searched. The existing approaches along with their details in terms of years, type of publication, and the areas are given in the figures and tables in this section. Table 1 summarizes some of the techniques used in the literature for security purposes [40].

Table 2 shows the articles with references list proposed for the detection of the different types of malwares [40]. It also contains the information for the different types of techniques to address these certain types of malicious attacks.

Figure 1 shows the total number of publications within the selected range of the years (2016–2020 (a portion of 2020 is included in the systematic search process)). This figure also reflects the type of the research/articles reported during this specific range of the years.

The searched papers were checked to show the year of publication; that is, the particular year in which a paper is published (2016–2020 (a portion of 2020 is included in the systematic search process)). Figure 2 shows the total number of publications in the given year.

Figure 3 shows the journal/magazine name along with the total number of papers published for the search process in the ACM library.

Figure 4 shows publications type of all the publications in the ACM digital library. It also contains the information for a total number of publication type within the ACM digital library. The highest number of journal papers and proceedings represents the contribution of the work in the proposed field.

Table 1: Techniqueswise literature categorization.

Ref. no	Year	Description
[23]	2019	Risk assessment model for addressing the security issues in IoT ecosystem
[24]	2019	Threats and attack based analysis of IoT
[25]	2018	Architecture based analysis in light of security requirements
[26]	2018	Discussing the layer based security analysis of IoT
[27]	2018	Security analysis of mobile device-to-device network using Android operating system
[28]	2018	Security analysis of mobile health applications for testing functionality.
[29]	2018	Threat and attack based analysis of IoT
[30]	2018	Analysis of all security areas in IoT
[31]	2018	Study of the existing and proposed countermeasures in IoT based system
[32]	2017	Proposing a mobile application tool for analysis of IoT threats.
[33]	2017	Presenting a threat categorization based on security dimensions like integrity, confidentiality, etc.
[34]	2017	Proposing a classification model to analyse the relation between potential risk and potential vulnerabilities in home automation devices
[35]	2016	Security analysis of smart phone in IoT
[36]	2016	Analysis of identification of application, threats, and impacts in IoT
[37]	2016	Security issues and challenges of IoT and mobile computing
[38]	2015	Analysing the IoT security challenges, issues, and open problems
[39]	2015	Discussing security aims, goals, and vulnerabilities for IoT

Table 2: Malware detection techniques.

Ref. no.	Description
[41]	It uses four ways to detect malwares. It divides the applications into four types like malicious, benign, aggressive, and risky applications
[42]	Android analysis techniques for evaluating the effectiveness of Android intense
[43]	It uses ADA GRAD optimize algorithm for detecting malware pattern without manual intervention
[44]	It detects malware by using ensemble classifier for malware detection
[45]	It uses the machine learning algorithm which was presented by Waikato environment for knowledge analysis (WEKA)
[46]	It uses machine learning method for Android malware detection
[47]	It detects application features and decides whether malicious or not
[48]	It uses multiflow detection algorithm based on information flow analysis

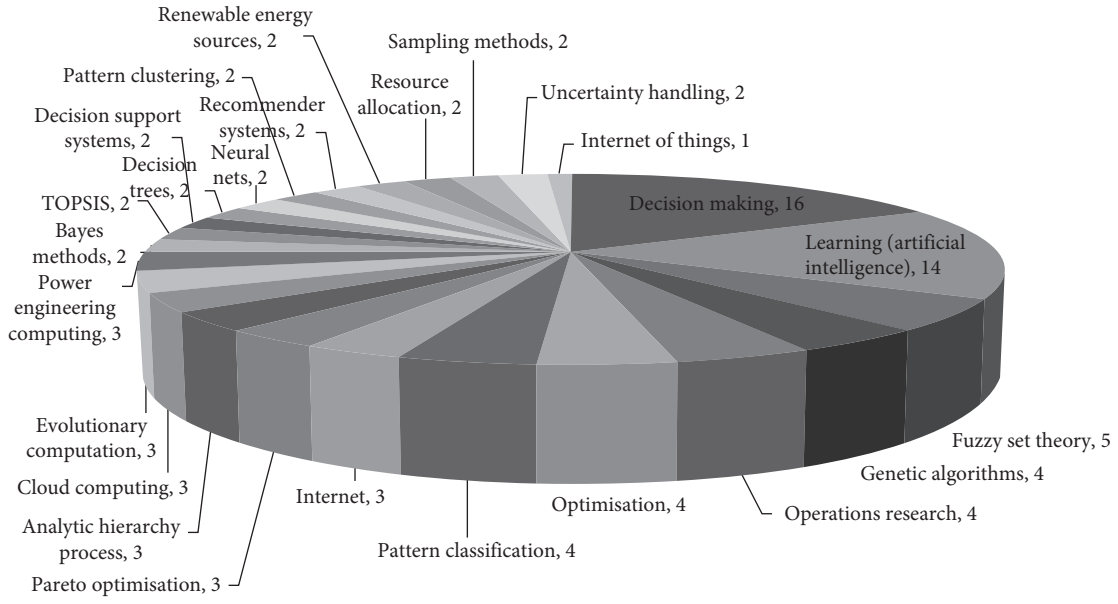

Figure 1: Publication type and total number.

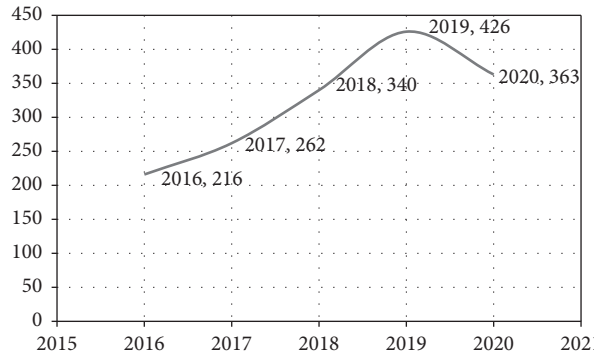

Figure 2: Total number of papers published in the given year.

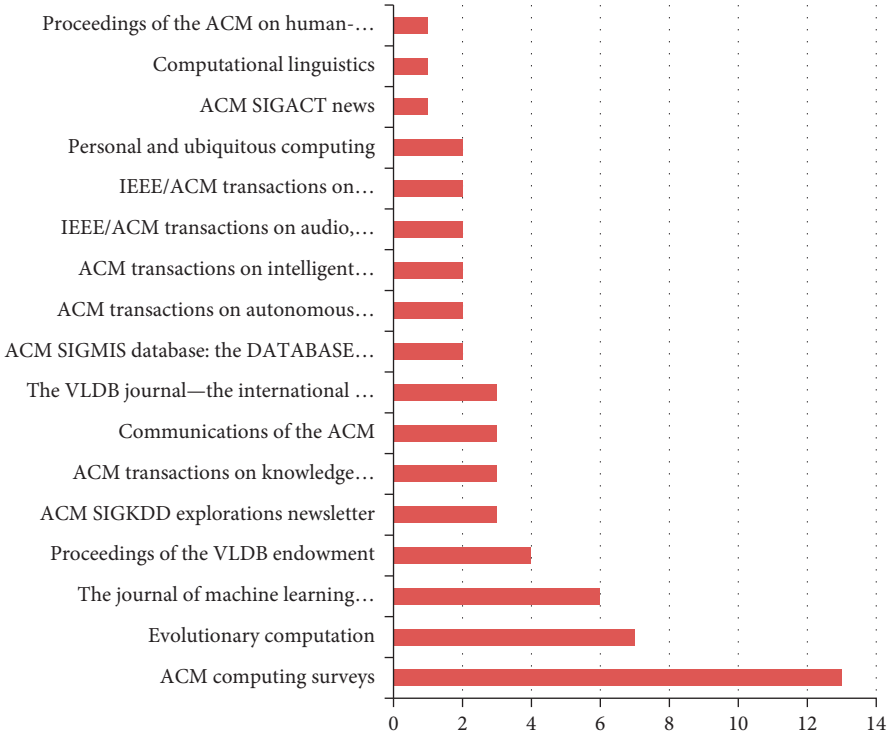

Figure 3: Journal/magazine name and number of publications.

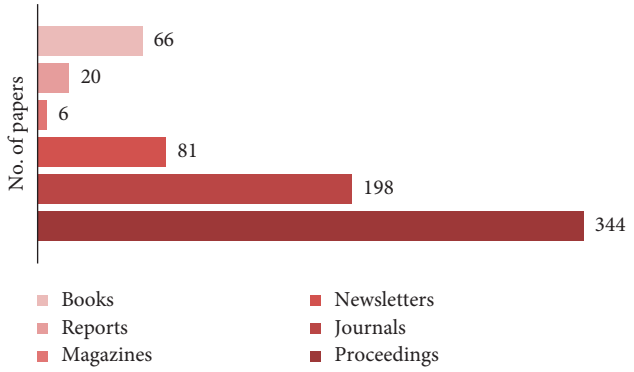

Figure 4: All publications and the total number.

3. The Proposed Methodology

The proposed model consists of an external library (a Kitsune network attack database) developed by Mirsky et al. [49]. This database is used for the simulation and experimental purposes. It consists of nine different attacks depicted in Table 1. It also contains the information about the number of packets selected for the training and test purposes. The experimental setup also contains the feature extractor and feature mapping section. To achieve this goal, the proposed research work uses convolution neural network (CNN) that acts as an automatic feature extractor and classification tool. CNN extracts the features and, based on these features, it generates the output in the form of anomaly detector. In our case, it generates two types of output classes as depicted in

$$\overrightarrow{O(x)} = \begin{bmatrix} \text{Benign} \\ \text{Malicious} \end{bmatrix}, \tag{1}$$

where $\overrightarrow{O(x)}$ represents the corresponding output. This output is generated in the form of malicious and benign data. Finally, the percentile score is generated based on the threshold, N_p norm values, and other parametric values explained in Section 4. Figure 5 shows the experimental setup.

A five-layered CNN architecture is used for the experimental purposes. It consists of an input and output layer and three hidden layers. A "relu" is used as an activation function. This architecture is tested for varying training and test sets. The CNN models are prominent in classifying spatial data.

4. Results and Discussion

The dataset used for the proposed experimental work is selected from the feature vector dataset (https://archive.ics.uci.edu/ml/datasets/Kitsune+Network+Attack+Dataset) developed by Mirsky et al. [49]. They developed this dataset after recording the network traffic on two different networks such as (a) a commercial IP-based camera video surveillance network on which they conducted 8 attacks that affect the availability and integrity of the video uplinks; (b) a noisier IoT network comprised of 9 IoT devices and 3 PCs; one of the devices was infected with the MIrai botnet attacks (malware). From each of these input vectors (in the dataset), we extracted a segment of consecutive packets. These packets are accordingly separated into training and test sets as depicted in Table 3.

Kitsune's developers mostly evaluate the deep learning based intrusion detection systems against a series of attacks based on different networks. In the case of the proposed study, accuracy of the system is dependent relative to the value of threshold, T. when deploying the system this threshold describes the boundary of decision and makes it a crucial parameter.

The following two metrics are followed to access the performance of a certain threshold parameter:

(a) False negative: the percentile of malicious data that is considered/classified as benign data

(b) False positive: the percentile of benign inputs that are considered/classified as malicious data

The false positives rate is associated with the network reliability, while the rate of false negatives accounts for the effectiveness of the network intrusion detection system (NIDS). Therefore, to achieve an ideal situation, both these parameters should be minimized. However, dealing with Kitsune settings, the value of T acts as a trade-off in between both false positives and false negatives parameters.

The functional range of the threshold values ranging from 0 to 15 is investigated for a given training and test set parameters as shown in Table 1. 100% false negatives are recorded for the false negatives on the given feature vector. Figure 6 shows the two threshold parameters versus the accuracy of the proposed system.

It can be observed from Figure 6 that, in the middle, both the parameters (false positives and false negatives) remain unchanged. Furthermore, it can also be concluded from Figure 6 that if we minimize one parameter, the other parameter significantly increases. Finally, the accuracy of the proposed system remains unchanged for a threshold value below 10 (which reflects that most of the data belongs to the benign inputs).

A receiver operating characteristic (ROC) is shown in Figure 7 to represent the effectiveness of the proposed algorithm for the Kitsune network attack dataset.

Two of the significant attacking objectives that are availability and integrity violation are in machine learning techniques. The violations of availability try to make benign traffic appear malicious.

The violations of integrity try to construct malicious traffic which escapes detection.

The network attacks containing the information differ from the images that are most commonly used in generic machine learning techniques.

One of the definitions for examples of adversarial, assisted by the architecture of Kitsune, is to adopt the features extracted as an indication of the difference be observed. So, the distance of L_P is adopted on the space feature between the perturbed input and original input as the distance metric. The L_0 norm correlates to altering a small number of extracted features, which might be a better metric than other L_P norms.

The proposed algorithm is also evaluated against generic NIDS to test the applicability of the proposed algorithm. These generic algorithms include Fast Gradient Sign Method (FGSM), Jacobian Base Saliency Map (JSMA), Carlini and Wagner (C&W), and Elastic Net Method (ENM). A description of these techniques is given as follows:

(i) FGSM**:** over the L1 norm, this technique is strictly optimal (i.e., it reduces the maximum perturbation on any input data (feature)) by selecting a single step to each element of $\sim x$ in the opposite direction to the gradient [50]

(ii) JSMA**:** this type of attack minimizes the L_0 norm by iteratively calculating a saliency map and then perturbing the feature that will have the highest effect [51]

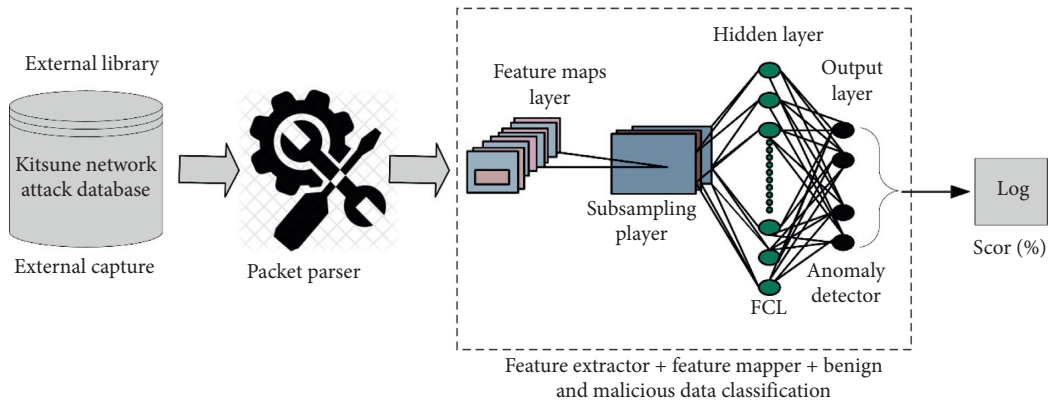

Figure 5: Experimental setup.

Table 3: Characteristics of the IoT network attack and commercial IP camera dataset [49].

S/no.	Type of attacks	Training set (packets)	Test set (packets)	Malicious test packets
(1)	OS Scan	7000	12,500	1499
(2)	Fuzzing SFuzz	1300	8900	1199
(3)	ARP MitM	7000	12,500	1499
(4)	Video Inj.	5000	8000	1199
(5)	Mirai	7000	8000	1199
(6)	SYN DoS	1300	8900	1199
(7)	SSDP Flood	7000	13,500	1499
(8)	SSL Reneg	7000	12,500	1499
(9)	Wiretap	1300	8900	1199

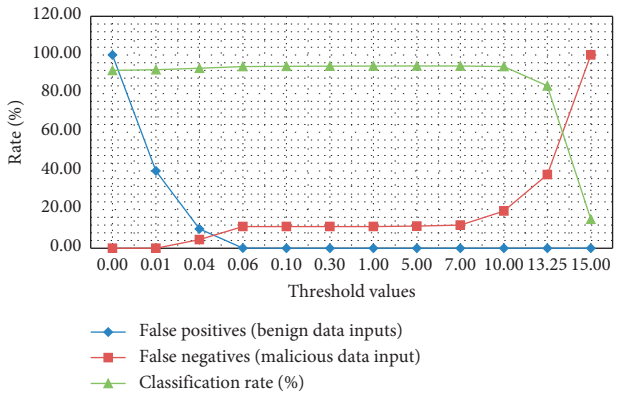

Figure 6: Threshold parameters versus the accuracy of the proposed system.

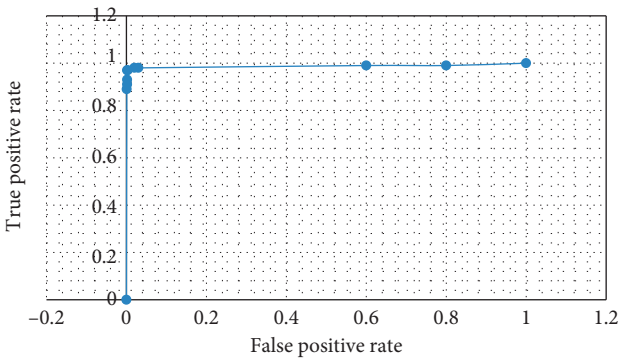

Figure 7: ROC curve for Kitsune.

(iii) C&W: Carlini and Wagner's adversarial framework, as discussed earlier, can either minimize the L_2, L_0, or L_1 distance metric [52]

(iv) ENM: **e**lastic net attack is an algorithm that restricts the total absolute perturbation across the input space. The ENM constructs the adversarial examples by expanding an iterative L_2 attack with an L_1 regularizer [53]

To check the validity of the proposed algorithm, the experimental results are carried out for the selected generic algorithms based on different threshold values ranging from 0.05 to 1 to test the Kitsune score. The experimental results are depicted in Table 4.

From Table 4, it is evident that our algorithm performs well compared to the other generic algorithms. The experimental results are carried out on the input vectors selected from the Kitsune network attack dataset as depicted in Table 1. The simulated results are shown in Figure 8.

For the same threshold values used in Table 2, the availability attacks on the Kitsune network are processed. Different training sets are selected for the simulation purposes as shown in Table 1. The input vectors (training sets) that yield closest output scores to the threshold were selected. Table 5 shows the experimental results. The normalizers were trained on benign inputs; several malicious input values would be normalized outside the typical range between 0.05 and 1.

Table 4: Integrity attacks on Kitsune network.

S/no.	Algorithms	Threshold value	Kitsune score (%)	L_p distances			
				L_0	L_1	L_2	L_∞
(1)	FGSM	1.0	100	100	102	9.7	1.5
(2)	JSMA	1.0	100	1.98	9.23	6.29	4.10
(3)	C&W	1.0	100	100	6.89	3.23	3.46
(4)	ENM	1.0	100	1.02	4.09	2.98	3.98
(5)	Our algorithm	1.0	100	0.87	3.33	1.09	3.45

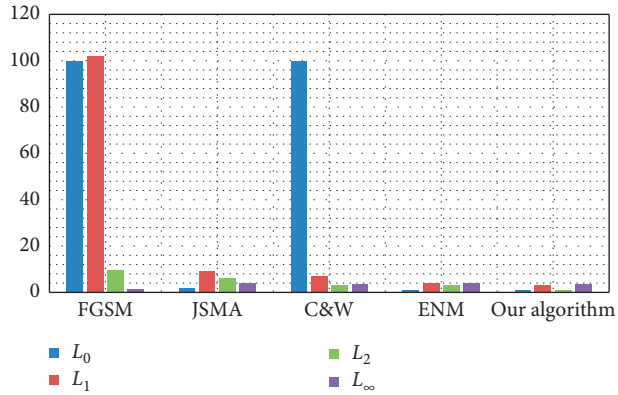

Figure 8: Integrity attack on Kitsune network.

Table 5: Availability attacks on Kitsune network.

S/no.	Algorithms	Threshold value	Kitsune score (%)	L_p distances			
				L_0	L_1	L_2	L_∞
(1)	FGSM	1.0	4	100	76.53	7.03	0.69
(2)	JSMA	1.0	0	—	—	—	—
(3)	C&W	1.0	100	100	21.32	7.98	5.46
(4)	ENM	1.0	100	7.85	20.09	7.48	3.68
(5)	Our algorithm	1.0	100	5.87	13.33	6.09	2.45

From Table 5, it is depicted that our algorithm outperforms for the availability attacks as well using the Kitsune network attack dataset. The comparative results are also shown in Figure 9. From Figure 9, it is concluded that our algorithm outperforms very well compared to the other generic algorithms in the proposed field.

To minimize the attacks on the Kitsune network, Cleverhans implementations are followed. These implementations use a simple gradient descent optimizer to minimize the function that is represented using

$$c.\max\{F(\vec{x})_i - Y, 0\} + \beta\vec{x} - \vec{x}_0 1 + \vec{x} - \vec{x}_0 2, \quad (2)$$

where $F(\vec{x})_i$ is the logit output of the target classifier, Y is the logit target output, and $\vec{x}_0$ is the original network input data. It can be seen that there are two regularization parameters, c and β. These parameters help in determining the contribution of the several metrics to the attacking algorithms, the success rate and L_1 distance with respect to changes in the regularization parameter, c.

The parameter, c, helps in determining the contribution of the adversarial misclassification objectives at the cost of diminishing the two LP normalization terms. For $\beta = 1$ and c the parametric values range from 0 to 500. And it is concluded from Figures 10 and 11 that 500 is the optimal parametric value for c that results in 100% success rate with a small perturbation. It can also be seen

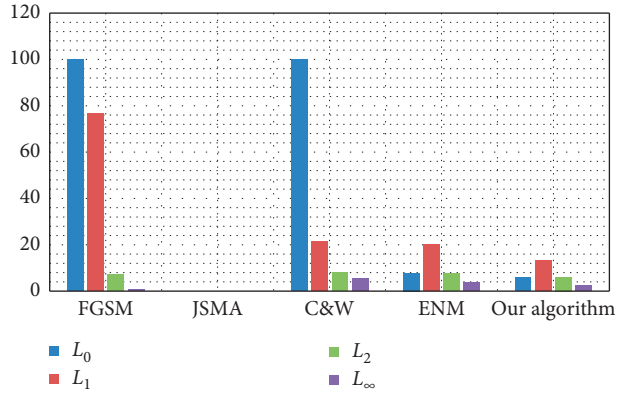

Figure 9: Availability attacks on Kitsune network.

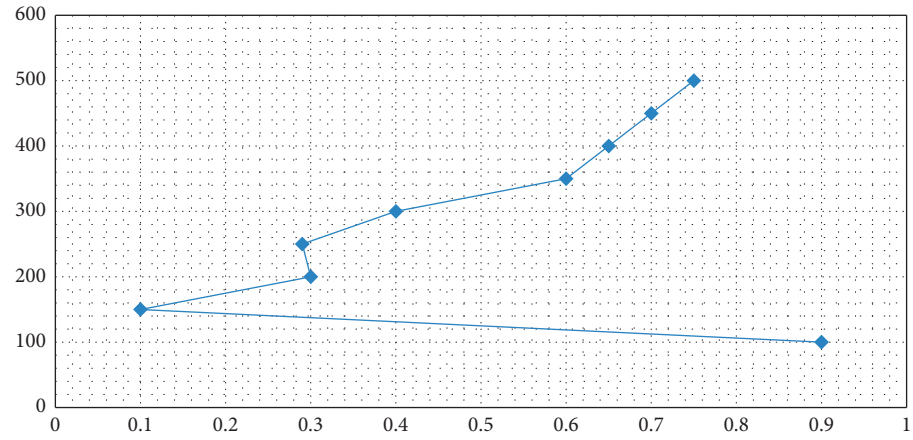

Figure 10: L_1 distance.

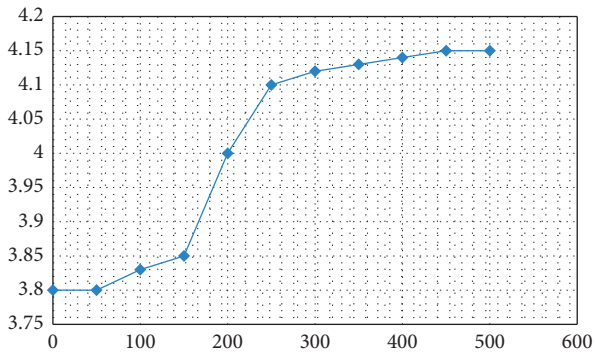

Figure 11: Success rate.

in Figure 10 that the generated L_1 distance does not directly correlate with the selection of parametric c values.

5. Conclusion

Security of components plays an important role in the functionality of a system to properly function. Different security approaches and measures are used to secure the information communication and to secure the network. This measure includes firewalls, logical access, control, authentication, identification, and encryption and decryption. A convolution neural network based approach is followed for the feature classification and benign and malicious data identification purposes. In the end, comparative results are generated after evaluating the performance of the proposed algorithm to other rival algorithms in the proposed field. These algorithms include FGSM, JSMA, C&W, and ENM. After assessing the performance of these algorithms and the proposed algorithm based on different threshold values ranging, L_p norms, and different parametric values for c, it was derived that the proposed algorithm outperforms with small L_p values and high Kitsune scores. These results show that the proposed research is capable of identifying intrusion and replicating the application of the proposed algorithms in the field of network security.

Data Availability

The proposed study has used the data avaliable online in the UCI Machine Learning Repository.

Conflicts of Interest

The authors declare no conflicts of interest regarding this paper.

References

[1] H. H. Song, "Testing and evaluation system for cloud computing information security products," in *Proceedings of the 3rd International Conference on Mechatronics and Intelligent Robotics (ICMIR-2019)*, pp. 84–87, Kunming, China, May 2020.

[2] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet of Things*, vol. 11, Article ID 100227, 2020.

[3] J. Yuan and X. Luo, "Regional energy security performance evaluation in China using MTGS and SPA-TOPSIS," *Science of the Total Environment*, vol. 696, Article ID 133817, 2019.

[4] X. Wu, S. Liu, Y. Sun, Y. An, S. Dong, and G. Liu, "Ecological security evaluation based on entropy matter-element model: a case study of Kunming city, southwest China," *Ecological Indicators*, vol. 102, pp. 469–478, 2019.

[5] X. Wang, J. Li, X. Kuang, Y.-A. Tan, and J. Li, "The security of machine learning in an adversarial setting: a survey," *Journal of Parallel and Distributed Computing*, vol. 130, pp. 12–23, 2019.

[6] M. Marwan, A. Kartit, and H. Ouahmane, "Security enhancement in healthcare cloud using machine learning," *Procedia Computer Science*, vol. 127, pp. 388–397, 2018.

[7] Z. Zhang, J. Wen, X. Wang, and C. Zhao, "A novel crowd evaluation method for security and trustworthiness of online social networks platforms based on signaling theory," *Journal of Computational Science*, vol. 26, pp. 468–477, 2018.

[8] Y. Cherdantseva, J. Hilton, O. Rana, and W. Ivins, "A multifaceted evaluation of the reference model of information assurance & security," *Computers & Security*, vol. 63, pp. 45–66, 2016.

[9] M. Jouini, L. B. A. Rabai, and R. Khedri, "A multidimensional approach towards a quantitative assessment of security

threats," *Procedia Computer Science*, vol. 52, pp. 507–514, 2015.

[10] S. Nazir, S. Shahzad, M. Nazir, and H. U. Rehman, "Evaluating security of software components using analytic network process," in *Proceedings of the 11th International Conference on Frontiers of Information Technology (FIT)*, pp. 183–188, IEEE, Islamabad, Pakistan, December 2013.

[11] M. Li, S. Nazir, H. U. Khan, S. Shahzad, and R. Amin, "Modelling features-based birthmarks for security of end-to-end communication system," *Security and Communication Networks*, vol. 2020, Article ID 8852124, 9 pages, 2020.

[12] 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 *Lecture Notes in Networks and Systems*, pp. 964–974, Springer, Berlin, Germany, 2020.

[13] S. Nazir, S. Shahzad, S. Mahfooz, and M. N. Jan, "Fuzzy logic based decision support system for component security evaluation," *International Arab Journal of Information and Technology*, vol. 15, pp. 1–9, 2015.

[14] I. Kotenko and A. Chechulin, "Common framework for attack modeling and security evaluation in SIEM systems," in *Proceedings of the 2012 IEEE International Conference on Green Computing and Communications*, pp. 94–101, Besancon, France, November 2012.

[15] P. Subsorn and S. Limwiriyakul, "A comparative analysis of internet banking security in Thailand: a customer perspective," *Procedia Engineering*, vol. 32, pp. 260–272, 2012.

[16] I. Kotenko and A. Chechulin, "Computer attack modeling and security evaluation based on attack graphs," in *Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS)*, pp. 614–619, Berlin, Germany, September 2013.

[17] S. Manjiatahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of things (IoT): a survey," *Journal of Network and Computer Applications*, vol. 161, Article ID 102630, 2020.

[18] R. Diesch, M. Pfaff, and H. Krcmar, "A comprehensive model of information security factors for decision-makers," *Computers & Security*, vol. 92, Article ID 101747, 2020.

[19] M. A. Amanullah, R. A. A. Habeeb, F. H. Nasaruddin et al., "Deep learning and big data technologies for IoT security," *Computer Communications*, vol. 151, pp. 495–517, 2020.

[20] S. Khan, H. Ali, Z. Ullah, N. Minallah, S. Maqsood, and A. Hafeez, "KNN and ANN-based recognition of handwritten pashto letters using zoning features," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 10, pp. 570–577, 2018.

[21] N. A. B. Mohd and Z. F. Zaaba, "A review of usability and security evaluation model of ecommerce website," *Procedia Computer Science*, vol. 161, pp. 1199–1205, 2019.

[22] W. Mao, Z. Cai, D. Towsley, Q. Feng, and X. Guan, "Security importance assessment for system objects and malware detection," *Computers & Security*, vol. 68, pp. 47–68, 2017.

[23] G. George and S. M. Thampi, "Vulnerability-based risk assessment and mitigation strategies for edge devices in the internet of things," *Pervasive and Mobile Computing*, vol. 59, Article ID 101068, 2019.

[24] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: internet of threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182–8201, 2019.

[25] M. Ammar, G. Russello, and B. Crispo, "Internet of things: a survey on the security of IoT frameworks," *Journal of Information Security and Applications*, vol. 38, pp. 8–27, 2018.

[26] M. A. Khan and K. Salah, "IoT security: review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[27] K. Liu, W. Shen, Y. Cheng et al., "Security analysis of mobile device-to-device network applications," *IEEE Internet of Things Journal*, vol. 6, pp. 2922–2932, 2018.

[28] A. Papageorgiou, M. Strigkos, E. Politou, E. Alepis, A. Solanas, and C. Patsakis, "Security and privacy analysis of mobile health applications: the alarming state of practice," *IEEE Access*, vol. 6, pp. 9390–9403, 2018.

[29] R. Gurunath, M. Agarwal, A. Nandi, and D. Samanta, "An overview: security issue in IoT network," in *Proceedings of the 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, pp. 104–107, Palladam, India, August 2018.

[30] R. Román-Castro, J. López, and S. Gritzalis, "Evolution and trends in iot security," *Computer*, vol. 51, no. 7, pp. 16–25, 2018.

[31] X. Su, Z. Wang, X. Liu, C. Choi, and D. Choi, "Study to improve security for IoT smart device controller: drawbacks and countermeasures," *Security and Communication Networks*, vol. 2018, Article ID 4296934, 14 pages, 2018.

[32] A. Rodríguez-Mota, P. J. Escamilla-Ambrosio, J. Happa, and E. Aguirre-Anaya, "GARMDROID: IoT potential security threats analysis through the inference of android applications hardware features requirements," in *Applications for Future*, pp. 63–74, Springer, Berlin, Germany, 2017.

[33] F. Loi, A. Sivanathan, H. H. Gharakheili, A. Radford, and V. Sivaraman, "Systematically evaluating security and privacy for consumer IoT devices," in *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, pp. 1–6, Dallas, TX, USA, November 2017.

[34] M. Capellupo, J. Liranzo, M. Z. A. Bhuiyan, T. Hayajneh, and G. Wang, "Security and attack vector analysis of IoT devices," in *Proceedings of the International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, pp. 593–606, Guangzhou, China, December 2017.

[35] M. H. Khan and M. A. Shah, "Survey on security threats of smartphones in internet of things," in *Proceedings of the 2016 22nd International Conference on Automation and Computing (ICAC)*, pp. 560–566, Colchester, UK, September 2016.

[36] J. Ahamed and A. V. Rajan, "Internet of things (IoT): application systems and security vulnerabilities," in *Proceedings of the 2016 5th International Conference on Electronic Devices, Systems and Applications (ICEDSA)*, pp. 1–5, Ras Al Khaimah, UAE, December 2016.

[37] A. Kamilaris and A. Pitsillides, "Mobile phone computing and the internet of things: a survey," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 885–898, 2016.

[38] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things," in *Proceedings of the 2015 IEEE World Congress on Services*, pp. 21–28, New York, NY, USA, June 2015.

[39] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: security vulnerabilities and challenges," in *Proceedings of the 2015 IEEE Symposium on Computers and Communication (ISCC)*, pp. 180–187, Larnaca, Cyprus, July 2015.

[40] 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.

[41] V. G. Shankar, G. Somani, M. S. Gaur, V. Laxmi, and M. Conti, "AndroTaint: an efficient android malware detection framework using dynamic taint analysis," in *Proceedings of the 2017 ISEA Asia Security and Privacy (ISEASP)*, pp. 1–13, Surat, India, January 2017.

[42] A. Feizollah, N. B. Anuar, R. Salleh, G. Suarez-Tangil, and S. Furnell, "Androdialysis: analysis of android intent effectiveness in malware detection," *Computers & Security*, vol. 65, pp. 121–134, 2017.

[43] H. Liang, Y. Song, and D. Xiao, "An end-to-end model for android malware detection," in *Proceedings of the 2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 140–142, Beijing, China, July 2017.

[44] F. Ghaffari, M. Abadi, and A. Tajoddin, "AMD-EC: anomaly-based android malware detection using ensemble classifiers," in *Proceedings of the 2017 Iranian Conference on Electrical Engineering (ICEE)*, pp. 2247–2252, Tehran, Iran, May 2017.

[45] E. Gandotra, D. Bansal, and S. Sofat, "Zero-day malware detection," in *Proceedings of the 2016 Sixth International Symposium on Embedded Computing and System Design (ISED)*, pp. 171–175, Patna, India, December 2016.

[46] P. Palumbo, L. Sayfullina, D. Komashinskiy, E. Eirola, and J. Karhunen, "A pragmatic android malware detection procedure," *Computers & Security*, vol. 70, pp. 689–701, 2017.

[47] D. Li, Z. Wang, L. Li, Z. Wang, Y. Wang, and Y. Xue, "FgDetector: fine-grained android malware detection," in *Proceedings of the 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC)*, pp. 311–318, Shenzhen, China, June 2017.

[48] F. Shen, J. Del Vecchio, A. Mohaisen, S. Y. Ko, and L. Ziarek, "Android malware detection using complex-flows," *IEEE Transactions on Mobile Computing*, vol. 18, pp. 1231–1245, 2018.

[49] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune network attack dataset data set," 2019, https://archive.ics.uci.edu/ml/datasets/Kitsune+Network+Attack+Dataset.

[50] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," 2014, https://arxiv.org/abs/1412.6572.

[51] N. Papernot, P. Mcdaniel, S. Jha, M. Fredrikson, Z. B. Celik, and A. Swami, "The limitations of deep learning in adversarial settings," in *Proceedings of the 2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 372–387, Saarbrucken, Germany, March 2016.

[52] N. Carlini and D. Wagner, "Towards evaluating the robustness of neural networks," in *Proceedings of the 2017 IEEE Symposium on Security and Privacy (sp)*, pp. 39–57, San Jose, CA, USA, May 2017.

[53] P.-Y. Chen, Y. Sharma, H. Zhang, J. Yi, and C.-J. Hsieh, "EAD: elastic-net attacks to deep neural networks via adversarial examples," in *Proceedings of the Thirty-Second AAAI Conference on Artificial Intelligence*, New Orleans, LA, USA, February 2018.