Hindawi
Complexity
Volume 2020, Article ID 4579495, 6 pages
https://doi.org/10.1155/2020/4579495

Research Article

Developing an Efficient Deep Learning-Based Trusted Model for Pervasive Computing Using an LSTM-Based Classification Model

Yang He,[1,2] **Shah Nazir**,[3] **Baisheng Nie**,[1,2] **Sulaiman Khan**,[3] **and Jianhui Zhang**[4]

[1]*School of Emergency Management and Safety Engineering, China University of Mining &Technology (Beijing), Beijing 100083, China*
[2]*State Key Laboratory Coal Resource and Safe Mining, China University of Mining &Technology (Beijing), Beijing 100083, China*
[3]*Department of Computer Science, University of Swabi, Ambar, Pakistan*
[4]*Postal Savings Bank of China, Beijing 100000, China*

Correspondence should be addressed to Yang He; gzgayou@163.com

Received 16 July 2020; Accepted 20 August 2020; Published 9 September 2020

Academic Editor: M. Irfan Uddin

Mobile and pervasive computing is one of the recent paradigms available in the area of information technology. The role of pervasive computing is foremost in the field where it provides the ability to distribute computational services to the surroundings where people work and leads to issues such as trust, privacy, and identity. To provide an optimal solution to these generic problems, the proposed research work aims to implement a deep learning-based pervasive computing architecture to address these problems. Long short-term memory architecture is used during the development of the proposed trusted model. The applicability of the proposed model is validated by comparing its performance with the generic back-propagation neural network. This model results with an accuracy rate of 93.87% for the LSTM-based model much better than 85.88% for the back-propagation-based deep model. The obtained results reflect the usefulness and applicability of such an approach and the competitiveness against other existing ones.

1. Introduction

The recent advances in information technology has made the world to shift from big desktop computers and have a tendency to powerful and smaller devices to facilitate with large computational and heterogeneous wireless communications interfaces. Weiser [1] referred the concept of pervasive/ubiquitous computing which is the most recent paradigm in the world of computers. Ubiquitous/pervasive computing offers a number of advantages such as making life easier with the support of digital infrastructure and mobile devices accomplished by offering the services distribution to the people. Some of the pervasive and ubiquitous computing facing security-related issues are open for researchers to answer. Devices inside the pervasive systems are embedded and invisible which are operating in pervasive surroundings. The pervasive devices are performing mutual interaction without any identity in advance. So, it becomes complicated for the users to know where such devices are present and to exchange personal information.

The traditional security of computing is mostly relying on the techniques of access control and authentication which provide access to the only registered users of the system. Ubiquitous and pervasive computing systems are very scalable and flexible due to which it is not suitable to adopt such services. The main characteristic of pervasive computing is the development and design of efficient services to the user who sends request for the services and in the context from which the request of service is sent.

The contribution of the proposed research is to develop an efficient deep learning-based model to ensure the generic security issues such as trust, privacy, and authenticity over the Internet. From the selected dataset, only 12% of the data is used for the experimental purposes, and it results in a high accuracy rate of 93.87%. This high accuracy rate for such a small amount of data shows that if the training set increases,

then the proposed model will provide more prominent accuracy rates.

The paper is organized as follows: Section 2 represents the related work to the proposed research. Section 3 briefly shows the materials and method followed for conducting the proposed research. Section 4 shows the experimental results of the proposed study. The paper is concluded in Section 5.

2. Related Work

Different approaches and techniques are proposed by researchers for pervasive computing. Chen et al. [2] proposed an infrastructure of data-centric design to support the applications of context-aware. Their proposed middleware treats sources of contextual data as stream publishers. The system is robust to support self-organizing peer-to-peer overlay to support the services of data-driven. Katsiri and Mycroft [3] proposed a system for simulating pervasive systems through estimated knowledge about its situations and entities involved. The research has improved AESL with the function of higher order predicated to denote estimated knowledge about the possibility of predicted instance with value True for a time reference. Padovitz et al. [4] presented a framework of ECORA for the computing of context-aware for reasoning context about uncertainty and tracing the issues of scalability, usability, communication, and heterogeneity. The system considers an agent-oriented hybrid approach and combining service of centralized reasoning with context-aware, reasoning able mobile software agents. Ahamed et al. [5] presented the S-MARKS design and implementation which consists of resource discovery, device validation, discovery of resource, and privacy of the module.

Boukerche and Ren [6] proposed a system of security for management of trust involving development of a trust model, nodes credential assignment, private key updating, managing the trust value, and taking suitable decision about the rights of access nodes. The research demonstrated that a malicious node can efficiently be excluded from the environment of pervasive and ubiquitous computing. Yu et al. [7] surveyed the literature for the comparison and classification framework for the four dimensions of the design concerned application migration: spatial, temporal, entity, and other concerns. Bello Usman and Gutierrez [8] augmented the basic concept of pervasive and mobile computing from different studies of the literature which uses methods and generic conceptual phases for the management of trust. The study covered a wide range of methods, techniques, models, and applications of trust-based protocol. Carullo et al. [9] presented a new approach for the establishment of trust leveraging the profiles of users. The authors [10] presented an approach which is capable of judging the trustworthiness of a device which interacts and behavior of the device with little interaction experience. The existing research in the field of gesture recognition and facial expression in the perspective of intelligent tutoring is analyzed for facilitating educational societies in building an efficient tutoring system [11].

Kurniawan and Kyas [12] presented a statistical decision approach for trust-based access control through Bayesian decision theory for identity management in Internet of Things. Dangelo et al. [13] presented the generic issues of pervasive computing architecture. The system integrated the techniques of artificial intelligence for achieving similar resemblance with the decision making which is human-like. Apriori algorithm was firstly used to extract the behavioral patterns, and then, Naïve Bayes classifier was used for decision making for trustworthiness of users. Uddin et al. [14] proposed an approach for the detection of terrorist activities. The five models of the deep neural network are used to monitor the behaviors of terrorist activities. The approaches used logistic regression, Naïve Bayes, and Support vector machine algorithms. The authors [15] proposed deep learning and neural networks algorithms for prediction of the behavior of punctuality of employees at the workplace. Khan et al. [16] proposed a variant of SVM, a LinearSVC for answer classification. The chi-square and univariate methods are used for the reduction of the size of the feature space. Deep learning algorithms are used in a variety of problems such as for evolutionary computing models in computer vision [17] and deep ensemble learning for human action recognition in still images [18].

3. Materials and Methods

The following sections show the materials and methods used.

3.1. Dataset. Dataset (Dishonest Internet users dataset.txt) [19] has been used in this study. The dataset has 322 instances and 5 attributes which is available on the UCI machine learning repository.

3.2. Deep Learning-Based Intrusion Detection System. Figure 1 represents the generic diagram of the intrusion detection system. The system of intrusion detection acts like a guard at the objective node to activate a firewall and to alert host devices when an unauthorized access or illegal traffic is detected. In our case, we have used the deep learning-based model to defend the unauthorized access and malicious network traffic.

3.3. Deep Neural Network Backward Propagation Model for the Classification of Trusted and Untrusted Internet Users. To tackle the problem of perceptron, in 1986, Rumelhart et al. [20] defined a new supervised learning technique which is called the Back-Propagation Deep Neural Network (BPDNN) which is mostly used for classification problems. The BPNN is a supervised deep learning model where error variance between the calculated outputs and the desired outputs is back-propagated. This process is repetitive through the learning process for minimizing the errors through weights thought the back-propagation of errors. As a consequence of weight regulations, a hidden unit sets their weight to signify significant features of the task domain. The BPDNN contains three layers which are the hidden layer, inputs layer, and outputs layer. Learning in the BPDNN is a two-step procedure [20, 21].

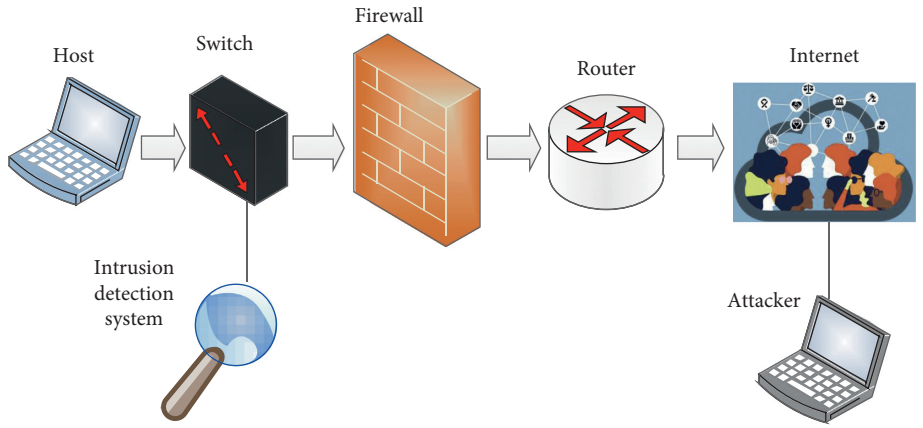

Figure 1: Typical system of intrusion detection positioned to block the host device from abnormal network traffic.

Step 1. Forward propagation: this step depends on the input and present weights, and the output is computed. For such computations, each hidden unit and output unit calculates net excitation which depends on these conditions:

(i) Values of earlier layer units that are linked to the unit in deliberation

(ii) Weights between the unit in consideration and the previous layer unit

(iii) Threshold value on the consideration unit

This net excitation is accomplished by activation function returning the calculated output value for that unit. This activation function must be differentiable and continuous. Several activation functions can be used in the BPDNN. Sigmoid is an extensively used activation function.

Step 2. Backward propagation of error: in this step, the error is computed by variance between the actual output of each output unit and targeted output. This error is back-propagated to the former layer that is the hidden layer. Error at that node is calculated for each unit in the hidden layer N. In a similar way, error at each node of the previous hidden layer that is N-1 is calculated. Forward and backward steps are repetitive until the error is reduced up to the predictable level. The parameters of BPDNN are shown in Table 1.

The BPDNN graphically represented in Figure 2 contains three layers, the inputs layer, hidden layer, and outputs layer.

3.4. Cross Validation Method. For data classification using hold-out methods: 70% for training and 73% for testing in this study.

3.5. Performance Evaluation Metrics. Accuracy, model execution time, and ROC-AUC have been used as performance evaluation metrics to evaluate the performance of the model.

4. Experimental Results

The backward propagation deep learning-based different networks have been trained and tested with essential parameters and reported in Table 1. The deep propagation

Table 1: BPDNN parameters.

S. no.	Parameter
1	Rate learning
2	Initial weights
3	Number of hidden units
4	Overtraining and initial stopping criteria
5	Number of instances
6	Function of activation
7	Inputs normalization

neural network model has been used for the classification of trusted and untrusted Internet users. In the dataset, there are 322 instances and 5 attributes. During preprocessing, the missing instances have been removed from the dataset. A hold-out method has been used for training and testing of the models. Additional performance evaluation metrics such as accuracy, processing time, and AUC have been computed for models performance evaluations. According to Table 2, BPNN4 achieved high performance as compared to other deep back-propagation networks. The BPNN4 classification accuracy was 88.88%, AUC was 88.78%, and model computation time was 165 seconds under the reported parameters for BPNN1.

The accuracy and processing time and ROC-AUC of different BPDN networks have been graphically presented in Figures 3 and 4, respectively. It is concluded from Figure 3 that the back-propagation neural network generates an accuracy rate of 85.88% for the proposed problem, while the LSTM-based classification and recognition model outperforms by generating an accuracy rate of 93.87% as depicted in Figure 5.

The back-propagation neural network is good in sequence learning problems but fails in retaining the information used long before [22]. To address the problem of retention in back-propagation neural networks, Hochreiter and Schmidhuber proposed a modified version of the back-propagation neural network in 1997 known as long short-term memory (LSTM) [23]. This model provided prominent results for many machine learning problems such as text recognition, speech recognition, network attack detection problems, and many others. This high applicability of the

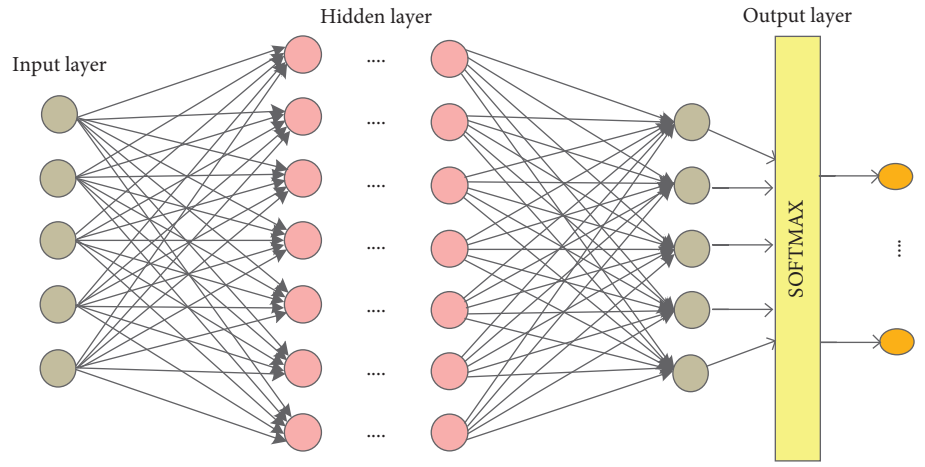

Figure 2: BPDNN flowchart.

Table 2: Training parameters of the backward propagation deep neural network.

Network	BPNN1	BPNN2	BPNN3	BPNN4	BPNN5	BPNN6
Training instances	220	220	220	220	220	220
Validating instances	100	100	100	100	100	100
Learning rate	0.001	0.0001	0.0001	0.01	0.0001	0.001
Activation function	relu	relu	relu	relu	relu	relu
Epochs	200	600	800	900	1000	1200
Training time (s)	130	150	160	165	200	250
Accuracy (%)	78.00	81.02	88.88	85.88	87.30	88.76
AUC (%)	78.23	81.45	88.78	85.78	86.22	88.76

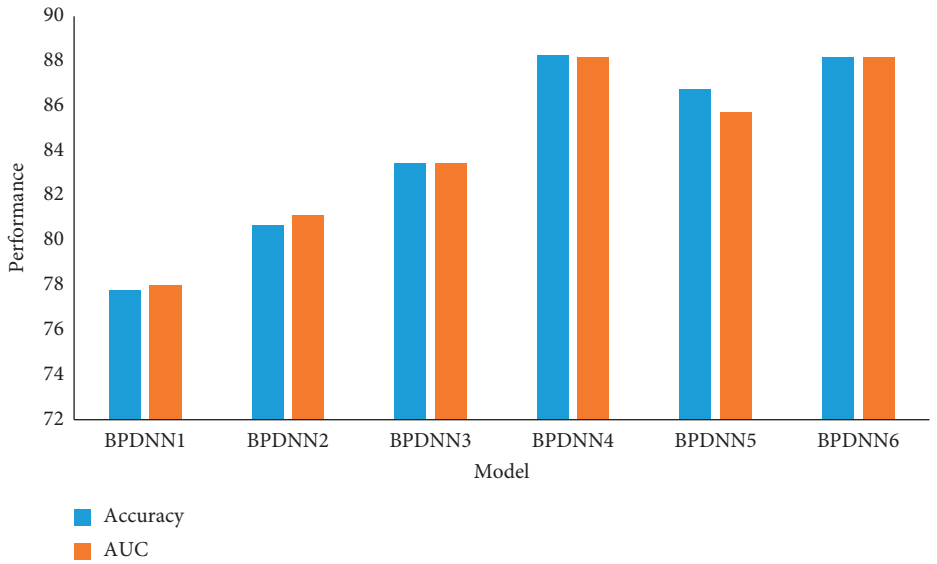

Figure 3: Performance of the BPDNN models.

LSTM represents the outperformance to the vanilla recurrent neural networks (back-propagation, feed-forward propagation, and so on) significantly. The applicability of the proposed algorithm is also tested using the LSTM model. The performance results of the LSTM-based model are depicted in Figure 5, and it generates an accuracy rate of 93.87% for the proposed problem. This high accuracy rate for the LSTM-based recognition model reflects the application of the proposed model for the said issue.

After testing the LSTM model for varying training and test sets, it is concluded from Figure 5 that the LSTM shows

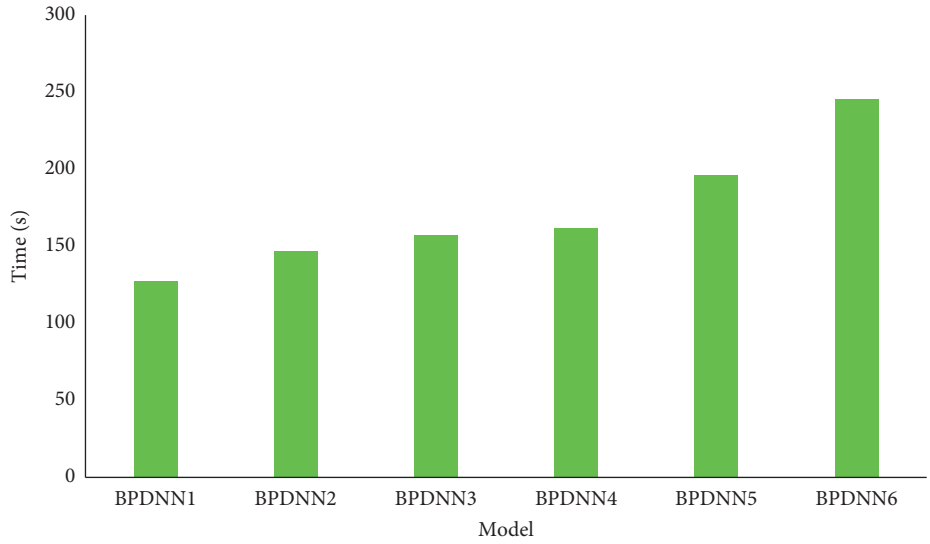

Figure 4: Processing time of the back-propagation-based model.

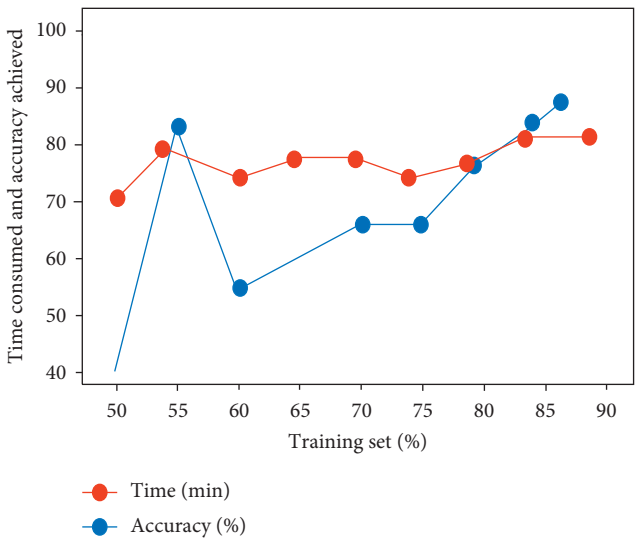

Figure 5: LSTM-based accuracy results.

an average highest accuracy rate of 93.87% for a training set of 70% and the remaining is selected as a test set. This high-accuracy value reflects the applicability of the LSTM model for the proposed problem. It is also concluded from Figure 5 that when the training set increases, the calculated time consumption also increases accordingly. The highest accuracy value of the LSTM model in Figure 5 reflects the solution to the nonretaining problem (forgetting/destroying the values used long before) of the back-propagation model.

5. Conclusions

Pervasive and ubiquitous computing is one of the advance paradigms in the area of information technology. The recent advances in information technology has made the world to shift from big desktop computers and have a tendency to powerful and smaller devices to facilitate with large computational and heterogeneous wireless communications interfaces. The role of pervasive computing is foremost in the field where it provides ability to distribute computational services to the surroundings where people work and leads to make issues such as trust, privacy, and identity. To provide an optimal solution to these generic problems, the proposed research work aims to implement a deep learning-based pervasive computing architecture to address these problems. Long short-term memory architecture is used during the development of the proposed trusted model. The applicability of the proposed model is validated by comparing its performance with the rival back-propagation neural network. This model results with an accuracy rate of 93.87% for the LSTM-based model much better than 85.88% for the back-propagation-based deep model. The obtained results reflect the usefulness and applicability of such approach and the competitiveness against other existing ones. In the future, the proposed research can be expanded for the recognition of unfair recommenders and its implementations on portable devices in order to validate it for real-world scenarios.

Data Availability

The research has used the dataset which is available online.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding this paper.

Acknowledgments

This work was sponsored in part by the Key Research and Development Program and the standard system and norm of hierarchical management in coal mine safety supervision (2018YFC0808301).

References

[1] M. Weiser, "The computer for the 21st century," *Mobile Computing and Communications Review*, vol. 3, pp. 3–11, 1999.

[2] G. Chen, M. Li, and D. Kotz, "Data-centric middleware for context-aware pervasive computing," *Pervasive and Mobile Computing*, vol. 4, no. 2, pp. 216–253, 2008.

[3] E. Katsiri and A. Mycroft, "Linking temporal first-order logic with Bayesian networks for the simulation of pervasive computing systems," *Simulation Modelling Practice and Theory*, vol. 19, no. 1, pp. 161–180, 2011.

[4] A. Padovitz, S. W. Loke, and A. Zaslavsky, "The ECORA framework: a hybrid architecture for context-oriented pervasive computing," *Pervasive and Mobile Computing*, vol. 4, no. 2, pp. 182–215, 2008.

[5] S. I. Ahamed, H. Li, N. Talukder, M. Monjur, and C. S. Hasan, "Design and implementation of S-MARKS: a secure middleware for pervasive computing applications," *Journal of Systems and Software*, vol. 82, no. 10, pp. 1657–1677, 2009.

[6] A. Boukerche and Y. Ren, "A trust-based security system for ubiquitous and pervasive computing environments," *Computer Communications*, vol. 31, no. 18, pp. 4343–4351, 2008.

[7] P. Yu, X. Ma, J. Cao, and J. Lu, "Application mobility in pervasive computing: a survey," *Pervasive and Mobile Computing*, vol. 9, no. 1, pp. 2–17, 2013.

[8] A. Bello Usman and J. Gutierrez, "Toward trust based protocols in a pervasive and mobile computing environment: a survey," *Ad Hoc Networks*, vol. 81, pp. 143–159, 2018.

[9] G. Carullo, A. Castiglione, G. Cattaneo, A. De Santis, U. Fiore, and F. Palmieri, "Feeltrust: providing trustworthy communications in ubiquitous mobile environment," in *Proceedings of the 2013 IEEE 27th International Conference on Advanced Information Networking and Applications (AINA)*, pp. 1113–1120, Barcelona, Spain, March 2013.

[10] M. K. Denko, T. Sun, and I. Woungang, "Trust management in ubiquitous computing: a Bayesian approach," *Computer Communications*, vol. 34, no. 3, pp. 398–406, 2011.

[11] M. Ivanova, "Researching affective computing techniques for intelligent tutoring systems," in *Proceedings of the 2013 International Conference on Interactive Collaborative Learning (ICL)*, pp. 596–602, Kazan, Russia, September 2013.

[12] A. Kurniawan and M. Kyas, "A trust model-based Bayesian decision theory in large scale Internet of things," in *Proceedings of the 2015 IEEE Tenth International Conference on Intelligent Sensors*, Sensor Networks and Information Processing (ISSNIP), Singapore, Singapore, pp. 1–5, April 2015.

[13] G. Dangelo, S. Rampone, and F. Palmieri, "An artificial intelligence-based trust model for pervasive computing," in *Proceedings of the 2015 10th international conference on P2p, parallel, grid, cloud and internet computing (3pgcic)*, pp. 701–706, Krakow, Poland, November 2015.

[14] M. I. Uddin, N. Zada, F. Aziz et al., "Prediction of future terrorist activities using deep neural networks," *Complexity*, vol. 2020, 16 pages, 2020.

[15] S. A. Ali Shah, I. Uddin, F. Aziz, S. Ahmad, M. A. Al-Khasawneh, and M. Sharaf, "An enhanced deep neural network for predicting workplace absenteeism," *Complexity*, vol. 2020, 12 pages, 2020.

[16] A. Khan, I. Ibrahim, M. I. Uddin et al., "Machine learning approach for answer detection in discussion forums: an application of big data analytics," *Scientific Programming*, vol. 2020, 2020.

[17] L. Zhang, C. P. Lim, and J. Han, "Complex deep learning and evolutionary computing models in computer vision," *Complexity*, vol. 2019, Article ID 1671340, 2019.

[18] X. Yu, Z. Zhang, L. Wu et al., "Deep ensemble learning for human action recognition in still images," *Complexity*, vol. 2020, Article ID 9428612, 2020.

[19] https://archive.ics.uci.edu/ml/datasets/Dishonest+Internet+users+Dataset Access 11-07-2020.

[20] D. E. Rumelhart, G. E. Hinton, and R. J. Williams, "Learning representations by back-propagating errors," *Nature*, vol. 323, no. 6088, pp. 533–536, 1986.

[21] B. Shah and B. Trivedi, "Optimizing back propagation parameters for anomaly detection," in *Proceedings of the IEEE - International Conference on Research and Development Prospectus on Engineering and Technology (ICRDPET)*, Nagapatnam, Tamil Nadu, March 2013.

[22] 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," 2019, https://arxiv.org/abs/1904.03391.

[23] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.