Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 5754322, 9 pages
https://doi.org/10.1155/2021/5754322

Research Article

Artificial Intelligence- (AI-) Enabled Internet of Things (IoT) for Secure Big Data Processing in Multihoming Networks

Geetanjali Rathee,[1] **Adel Khelifi**,[2] **and Razi Iqbal**[3]

[1]*Department of Computer Science and Engineering, Netaji Subhas University of Technology, Dwarka, Sector-3, Delhi, India*
[2]*Department of Computer Science and Information Technology, College of Engineering, Abu Dhabi University, UAE*
[3]*Department of Computer Information Systems, University of the Fraser Valley, Canada*

Correspondence should be addressed to Razi Iqbal; razi.iqbal@ieee.org

Received 11 June 2021; Revised 11 July 2021; Accepted 3 August 2021; Published 15 August 2021

Academic Editor: Daniel G. Reina

The automated techniques enabled with Artificial Neural Networks (ANN), Internet of Things (IoT), and cloud-based services affect the real-time analysis and processing of information in a variety of applications. In addition, multihoming is a type of network that combines various types of networks into a single environment while managing a huge amount of data. Nowadays, the big data processing and monitoring in multihoming networks provide less attention while reducing the security risk and efficiency during processing or monitoring the information. The use of AI-based systems in multihoming big data with IoT- and AI-integrated systems may benefit in various aspects. Although multihoming security issues and their analysis have been well studied by various scientists and researchers; however, not much attention is paid towards big data security processing in multihoming especially using automated techniques and systems. The aim of this paper is to propose an IoT-based artificial network to process and compute big data processing by ensuring a secure communication multihoming network using the Bayesian Rule (BR) and Levenberg-Marquardt (LM) algorithms. Further, the efficiency and effect on multihoming information processing using an AI-assisted mechanism are experimented over various parameters such as classification accuracy, classification time, specificity, sensitivity, ROC, and *F*-measure.

1. Introduction

A surge in utilization of smart systems has significantly enhanced efficient processing, reliable communication, and secure transmissions via wireless systems. However, augmentation of data may still encounter various computational and communicational risks in the network. In order to perform an efficient and smooth processing of huge records, a big data term came into existence. Big data is defined as the huge collection of records or information in volume that is exponentially growing with the time [1]. Hence, the traditional data management techniques are not able to perform efficiently. Big data along with certain platforms such as Hadoop and cloud servers may organize and manage the online processing or transmission of records; however, the collection of information from various networks may further lead to various complexity and security risks [2].

The involvement of multiple networks while processing or managing the enormous records introduces a new term known as multihoming networks [3]. It is defined as the involvement of various types of networks while clustering the records of information at a single place [4]. The multihoming is considered an emerging mechanism for clustering multiple records in a network. In addition, the processing and management of big data may further introduce complexity, processing, and security of networks and records while processing at a single place [5].

Numbers of smart-based big data schemes for managing or processing the large-size datasets have been proposed by a number of authors/scientists. Cloud-based Internet of Things (IoT) and Artificial Neural Network (ANN) schemes have been used in big data, network clustering, and multihoming schemes for an efficient and automated control systems [6–9]. Furthermore, a number of schemes in multihoming

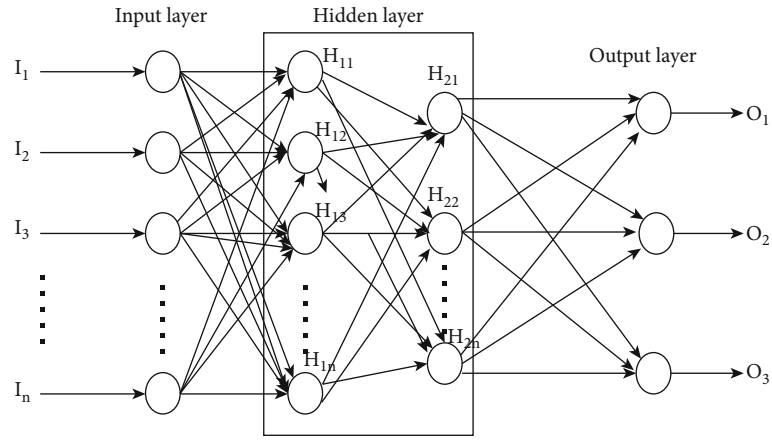

Figure 1: Multilayered perceptron architecture network (this figure is reproduced from Rathee et al. [27]).

and their analysis are proposed by various studies. However, not much attention is given to the automated multihoming schemes for managing, processing, and securing the big data information. In addition, the use of automated and artificial intelligence- (AI-) based smart systems in multihoming networks for securing and processing the information may reduce various security and management risks by enhancing the large-size data distributions, multiple network clustering, and data processing and managing [10]. Further, the AI-enabled proposed mechanism in multihoming for managing, securing, and processing big data provides vast implications for business, research, and future activities [11].

Moreover, the IoT- or ANN-based mechanisms benefitted for processing and monitoring among multihomed sites as depicted in Figure 1. Figure 1 consists of three different layers: input layer, hidden layer, and output layer. The huge amount of data processed by various networks is input in ANN where the processing or analysis of input data is done by the hidden layer. Further, the type of information either trusted or malicious generated by various networks is displayed by the output layer. Furthermore, the ANN-based automated system provides efficient processing, collection, and analysis of huge information while clustering the multiple networks. These techniques may further benefit for preventing, securing, managing, and processing of massive information while ensuring the security in networks [12–14].

1.1. Motivation and Contribution. Numbers of automated schemes have been proposed by various researchers in several applications such as healthcare, IIoT (Industrial Internet of Things), big data, multihoming, and vehicular transportation systems [15]. However, the integration of automated schemes in multihoming networks for managing and processing big data is considered one of the significant research interests. The integration of intelligent techniques while analysing the network algorithms, security, and clustering of multiple networks having various protocols, configurations, and attributes may benefit in a number of techniques. The automated systems may further benefit to manage and store the huge amount of information from heterogenous networks in an efficient way.

The aim of this paper is to propose an efficient and automated AI-based scheme for monitoring and processing various activities, including risk monitoring, processing, and management of big data in multihoming networks. The proposed mechanism is analysed over a simulated synthesized dataset over various processing metrics and parameters such as classification accuracy, classification time, specificity, sensitivity, ROC, and *F*-measure.

The remaining structure of the paper is organized as follows. Section 2 deliberates the number of approaches proposed by various authors/scientists. In addition, the ANN-based proposed phenomenon is detailed in Section 3. Further, Section 4 represents the discussion of results and analysis of the proposed phenomenon against existing mechanisms over various processing metrics. Finally, Section 5 concludes the paper along with future direction.

2. Related Work

The number of schemes proposed by various researchers/scientists is discussed in this section where the technique along with their performance analysis is defined in Table 1. de Santerre et al. [16] have presented an enhanced routing mechanism in multihomed IPv6 terminal sites while dealing with ingress filtering policies. The authors have described a new mechanism for choosing the default route through the packet of the source address. The proposed mechanism resolved the ingress filtering issue without implying Internet service providers. The authors have showed the easy deployment and requirement of changes in terminal nodes during communication. Wang et al. [17] have presented a learning scheme called local mobility anchor by initiating the learning procedures of IP addresses. The proposed mechanism forwarded various interfaces such as active, pending, and home network prefixes at a binding cache entry with learned IP addresses. In order to achieve the IP address, extraction and minimum required messages are detailed and defined by elaborating various charts. Bi et al. [18] have summarized the IPv4 site multihoming limitations and practices by

Table 1: Approaches/schemes proposed by various researchers.

Authors	Technique	Analysis
de Santerre et al. [16]	Enhanced routing mechanism in multihoming	The authors have described a new mechanism for choosing the default route through the packet of the source address
Wang et al. [17]	Learning scheme called local mobility anchor	The proposed mechanism forwarded various interfaces such as active, pending, and home network prefixes at a binding cache entry with learned IP addresses
Bi et al. [18]	IPv4 site multihoming limitations and practices	The authors have discussed various challenges and opportunities to bring up the security and mobility issues in multihoming environment
He et al. [19]	Comprehensive taxonomy of threats	The authors have proposed various criteria for evaluating the data analysis and collection performance
Li et al. [20]	Online IoT security monitoring scheme	An accurate data structural model is proposed to capture the behaviours of smart devices. Further, a hypothesis testing scheme is quantified to monitor the uncertain tasks by resolving the scalability issues
Lin et al. [21]	Network security-related data	The authors have provided the objectives and requirements of information collection with a taxonomy of various data gathering techniques
Wu et al. [22]	Analysis-based architecture	The authors have proposed an authentication mechanism for managing the clusters and enabling the data analysis using a colony optimization scheme
Zhou et al. [23]	Differently private scheme	In order to guarantee the trusted computing, a trust-based mechanism is proposed to evaluate the end user's reliability
Han et al. [24]	Agile confidential transmission strategy	The authors have combined the opportunistic beamforming and driven cluster schemes for managing the huge data collection from various base stations

surveying the current IPv6 multihoming solutions. The authors have discussed various challenges and opportunities to bring up the security and mobility issues in multihoming environment.

He et al. [19] have presented a comprehensive taxonomy of threats according to long-term evolution and advanced network structure. The authors have proposed various criteria for evaluating the data analysis and collection performance. All the traditional schemes and methods have discussed and analysed evaluation criteria by presenting various research and open issues for simulating the schemes. In addition, the authors have proposed a security measurement for analysis and collection of information in long-term evolution and advanced networks. Li et al. [20] have proposed an online IoT security monitoring scheme for distributed networks by selecting an advanced point influential operational abstract. An accurate data structural model is proposed to capture the behaviours of smart devices. Further, a hypothesis testing scheme is quantified to monitor the uncertain tasks by resolving the scalability issues. The authors have committed the cyberthreats to an IoT system for sensing the testbed using various strengths and patterns. The proposed algorithms claimed the efficient monitoring and detection of cyberthreats in IoT-based systems. Lin et al. [21] have introduced the network security-related data having different characteristics and definitions. The authors have provided the objectives and requirements of information collection with a taxonomy of various data gathering techniques. In addition, the authors have reviewed various traditional collection tools, nodes, and mechanisms in terms of security-related and data collection based on proposed objectives and requirements towards high-quality related security. Further, the authors have proposed various open challenges by concluding the paper with suggested future directions. Wu et al. [22] have proposed an analysis-based architecture for big data secure clustering management for the control planes. The authors have proposed an authentication mechanism for managing the clusters and enabling the data analysis using a colony optimization scheme. The comparative and simulated results increased the feasibility and efficiency of the proposed framework in control planes. Zhou et al. [23] have proposed a differently private scheme to preserve the data among edge nodes and users while communicating the information in various networks. In order to guarantee the trusted computing, a trust-based mechanism is proposed to evaluate the end user's reliability. The experimental results supported the increasing multimedia big data information while striking the balance among trustworthy, privacy-preserving and caching multimedia contents and big data collection prediction. Han et al. [24] have investigated an agile confidential transmission strategy for securing the big data information transmission. The authors have combined the opportunistic beamforming and driven cluster schemes for managing the huge data collection from various base stations. For the purpose of a secure and confidential transmission among clusters, the authors have combined the beamforming and driven clusters for reliable and efficient changing in network environment. In order to evaluate and validate the proposed scenario, the results have performed average secrecy of sum capacity and number of authorized users while accessing the systems.

Though numbers of approaches have been proposed by various researchers and scientists alone, very few of them have focused on an IoT-based artificial network to process and compute big data by ensuring a secure communication multihoming network. The number of smart techniques that can be helpful for monitoring the data processing, transmission, and communication of big data in multihoming by monitoring their nodes is still unexplored in the literature. In addition, the integration of automated schemes for

managing and processing big data is considered one of the significant research interests. Further, the integration of intelligent techniques while analysing the network algorithms, security, and clustering of multiple networks having various protocols, configurations, and attributes may benefit in a number of techniques. The automated systems may further need to manage storing the huge amount of information from heterogenous networks in an efficient way. The aim of this paper is to propose an efficient IoT-based artificial network to process and compute big data by ensuring a secure communication multihoming network approach with optimum evaluation results using the Bayesian Rule (BR) and Levenberg-Marquardt (LM) algorithms [25]. In addition, the proposed scheme is validated through a set of synthesized datasets against various monitoring and value processing results.

2.1. Proposed Approach. Presently, a number of machine learning, trust-based, and artificial intelligence algorithms have been proposed by various researchers and scientists. The smart and AI-based schemes in IoT benefitted in various phases of application while ensuring a secure transmission or communication among nodes in the network. In this paper, we have proposed an IoT-based artificial network to process and compute big data by ensuring a secure communication multihoming network. An IoT-based ANN is termed as an automated computational and processing scheme inspired by numerous neurons based on the concept of the biological neural network. The general definition of a neuron is defined as the lexeme cell as an assortment of numerous biological neurons referred to as the base for modelling an automated AI-based architecture [26]. An IoT-based ANN is defined as a mathematical model for processing the classification of data, nonlinear function, and regression schemes. It is capable of generating an automated decision model via multilayered perceptron. Figure 1 presents a multistage perceptron IoT-based ANN architecture having input through various smart sensors, hidden layers used for processing and computing the inputs, and an output layer used to generate the final output depending upon the provided input. An IoT-based ANN consists of a set of "o" number of outputs, H_h number of hidden/middle layers, and I_i number of inputs as defined in

$$\alpha_r(t) = \sum_{\alpha=1}^{H_h} W^2{}_{rs} F(.) \sum_{\gamma_{=1}} I_i W^1{}_{\alpha r} \alpha_s(t)^0 + b^1{}_{\alpha}, \quad \text{where } 1 \le r \le 0, \tag{1}$$

where W_{rs} and W_{ar} denote the connection of edges via weights among input, middle, and output layers. In addition, the function $F(.)$ in this equation represents an activation function (AF) that is defined as a sigmoid function to determine an appropriate processing and computation of trust values by evaluating the probabilities using the ANN algorithm. Further, the values in W_{rs} and W_{ar} denote an appropriate scheme using the Levenberg-Marquardt (LM) and Bayesian Rule (BR) principle for an optimum and efficient mechanism. The involvement of the AI-based scheme in the IoT system for processing or securing the multihoming network data can further benefit the system in a variety of ways. The following sections detailed the LM and BR classification for generating an accurate analysis of output results.

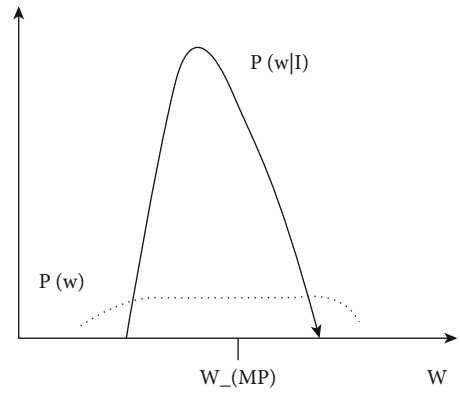

Figure 2: Prior to posterior weight changing process.

2.1.1. Levenberg-Marquardt (LM) Algorithm. LM is a deterministic and gradient-based local optimum algorithm. The benefit of using the LM algorithm while training the multistage perceptron architecture is the fast and average convergence rate by providing the stability in the system. Similar to the quasi-Newton scheme, LM was developed for a second-order derivation training speech approach without computing the Hessian matrix. The Hessian matrix is approximated while performing the function of sum of squares as

$$H_M = Q^T Q, \tag{2}$$

where the gradient can be evaluated as

$$G = Q^T \sigma, \tag{3}$$

where Q is defined as the Jacobian matrix containing the first derivations of error with respect to biases and weights. In addition, σ denotes the vector of errors in a network. The Jacobian matrix can be evaluated using a standard BR technique where the expected outputs through hidden layers are represented as

$$\alpha_q(t) = F'(I_i(t)) \sum_q \sigma^r{}_q(t) W^2{}_{rq}(t-1), \tag{4}$$

where q is the number of hidden layer neurons having r number of layers. Further, the LM algorithm uses the approximation to the Hessian matrix as

$$\text{delta}w = -\left[Q^T Q + \mu I\right]^{-1} Q^T \sigma, \tag{5}$$

where w represents the differential weights and μ denotes the controlling parameters. Whenever the mu is scaled to zero, then it is defined as Newton's method using the Hessian matrix approximation. However, when mu is large, then it becomes gradient descent having small step size. Newton's

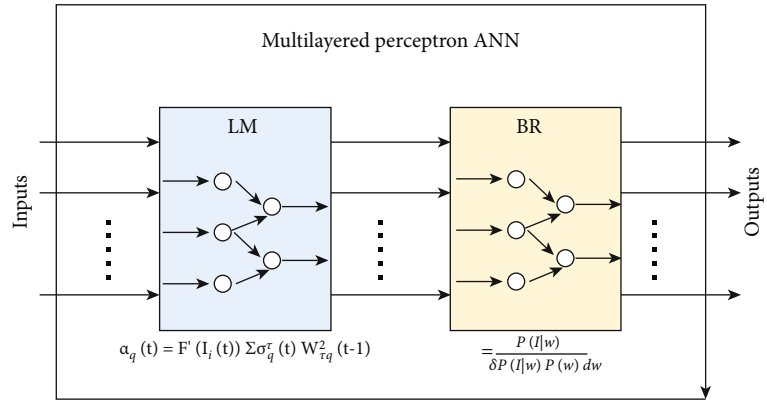

Figure 3: Prior to posterior weight changing process.

method is much accurate and faster near an error minimum. Therefore, the value of mu is decreased after every successful process and increased only when the step increases the performance function.

2.1.2. Bayesian Rule (BR) Algorithm. Later on, the LM algorithm is integrated with the BR method in order to further optimize the processed data. The BR algorithm is defined as

$$P(x \mid I) = \frac{P(I \mid x)}{P(I)}, \tag{6}$$

where $P(x)$ represents the prior probability of parameter x before actually seeing the processed information and $P(x \mid I)$ represents the likelihood where the probability of information I is. The BR was basically used to illustrate the posterior probability of x given the information I. In common, BR provides an entire distribution over all possible x values. This process was applied to a neural network by coming up with the probability distribution over weights w upon giving the training data as $P(w \mid I)$.

The posterior distributions upon weights are determined as

$$P(w \mid I) = \frac{P(I \mid w)P(w)}{P(I)}, \tag{7}$$

$$P(w \mid I) = \frac{P(I \mid w)}{\delta P(I \mid w)P(w)dw}. \tag{8}$$

Further, in the BR rule formulation, the learning of weights changes the beliefs about prior $P(w)$ and posterior $P(w \mid I)$ weights as consequences of seeing the information represented in Figure 2. As depicted in Figure 2, the weights of the learning rates are changes as per the information received and processed from various inputs. The inputs received from malicious nodes are analysed through their energy consumption and distribution ratio in the network. The nodes having malicious behaviour will always process false or alternate information with a number of generated errors.

Table 2: Simulation parameters.

Multilayered network	Training (%)	Testing (%)	Time (secs)
Bayesian Rule (BR)	63.52	36.48	8.562
Levenberg-Marquardt (LM)	66.89	33.11	2.598
IoT nodes	150	50	60 sec

Table 3: Synthesized simulated results.

Class	Proposed mechanism	Basic mechanism
Specificity	0.081	0.075
Sensitivity	0.912	0.0873
Accuracy	98.58	97.46
F-measure	1.19	1.10
ROC (receiver operator characteristic)	0.87	0.83

3. Working of the Proposed Approach Using LM and BR Algorithms

The working of the proposed mechanism using the BR and LM algorithm is explained through a diagram as presented in Figure 3. The above-mentioned BR and LM algorithms are used for ensuring a secure and efficient communication transmission while processing the data. The input in terms of received signals/information is passed into the ANN multilayered perceptron. Initially, the LM algorithm is applied on the inputs for computing the convergence rate and weights (trust) of each node's input while mentioning the error. Each node including hidden nodes will evaluate the gradient and Jacobian matrix. The errors while analysing the weights from various input nodes will be handled using the controlling parameters as depicted in equations (4) and (5). In addition, Newton's method is further analysed to ensure the fast and accurate results while minimizing the errors.

Now, in order to ensure an efficient processing and computation of weights after analysing or computing the weights from each node, the BR algorithm is applied over LM to

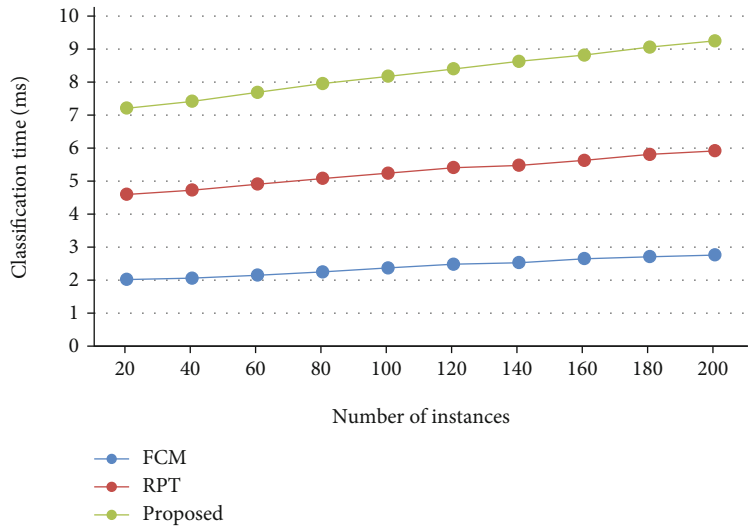

Figure 4: Classification time.

optimize the processed or recorded information from the inputs. The input is probabilistically distributed to the various nodes for computing and processing the efficient distribution of information while stabilizing the system. The posterior distribution of weights using the BR algorithm is computed using equations (7) and (8).

3.1. Performance Analysis. The proposed IoT-based artificial network, to process and compute big data by ensuring a secure communication multihoming network mechanism, is validated and experimented over an existing smart mechanism against several security threats. The proposed phenomenon is analysed over a synthesized dataset with a conventional smart-based scheme where the number of instances or inputs to the network is taken as 20-200 using a MATLAB simulator. The number of instances is input in the network where BR and LM algorithms are used to analyse and process the incoming data. Table 2 depicts the measured simulation results with several analysed values where the proposed approach having BR and LM algorithms is used to process the information. The number of input information is passed through both the mechanisms where the data is divided into training and testing analysis for optimizing or processing the information. Further, the input is probabilistically distributed to the various nodes for computing and processing the information distribution while stabilizing the system. The weights of posterior distribution using the BR algorithm is further computed using various equations.

The simulated results are analysed over various security measures as follows:

Accuracy: the accuracy is defined as the number of values required to produce accurate results.

Specificity: it is defined as the false-positive rates to categorize the weights of each node that are designed incorrectly. In the multihoming network where the data is recorded and processed from various networks, the probability of false-positive rates may be very high.

F-measure and ROC (receiver operator characteristic): they are used to determine and illustrate the classification accuracy of the proposed phenomenon. It is used to compute the *F*1 score of each node by recognizing precision and recall. The classification accuracy measures the efficient and trusted behavior of the network while processing various inputs of heterogenous networks.

Sensitivity: it determines the true-positive results which are correctly recognized by the system.

The synthesized simulation results are represented in Table 3.

3.2. Baseline Approach. For analysing the performance measure, the proposed phenomenon is compared against a baseline approach proposed by Wu et al. [22] which generated an analysis-based architecture for big data secure clustering management for the control planes. The authors have proposed an authentication mechanism for managing the clusters and enabling the data analysis using a colony optimization scheme. The comparative and simulated results increased the feasibility and efficiency of the proposed framework in control planes. In addition, the comparative results are analysed over various AI-based schemes such as Fuzzy *C* Means (FCM) and REPTree (RPT) methods. The proposed mechanism is analysed against various existing decision-making schemes to measure the accuracy and security of the processed information in multihoming networks.

4. Results and Discussion

Numbers of classified algorithms are evaluated and analysed based upon two statistical values, namely, accuracy and time of classified values. The classification time as shown in Figure 4 of the AI-based scheme is analysed over the existing mechanism against various data formats. Figure 4 shows the classification time that shows better results as compared to the existing scheme. The classification time of the proposed approach is better as compared to the existing AI-based schemes because of the optimized and discrete LM algorithm that trains the multistage perceptron architecture in a faster and average convergence rate by providing the stability in

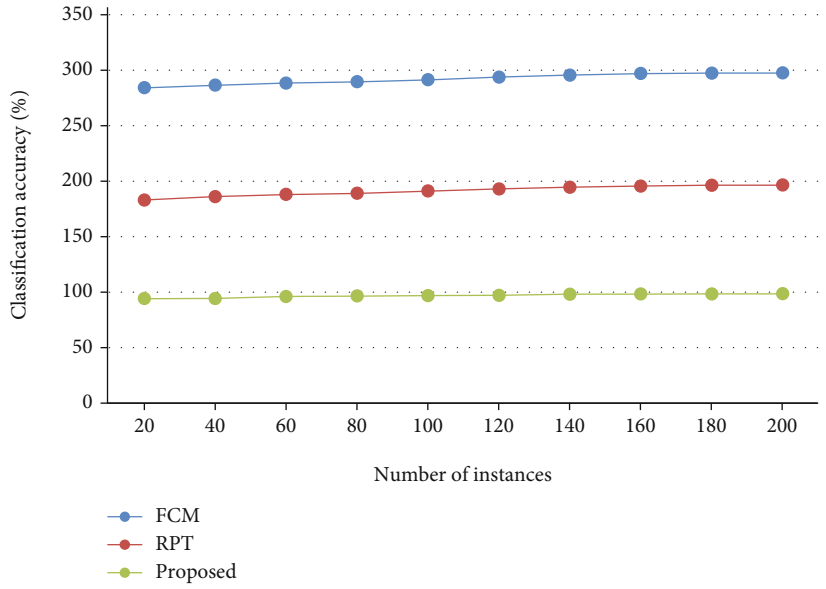

Figure 5: Classification accuracy.

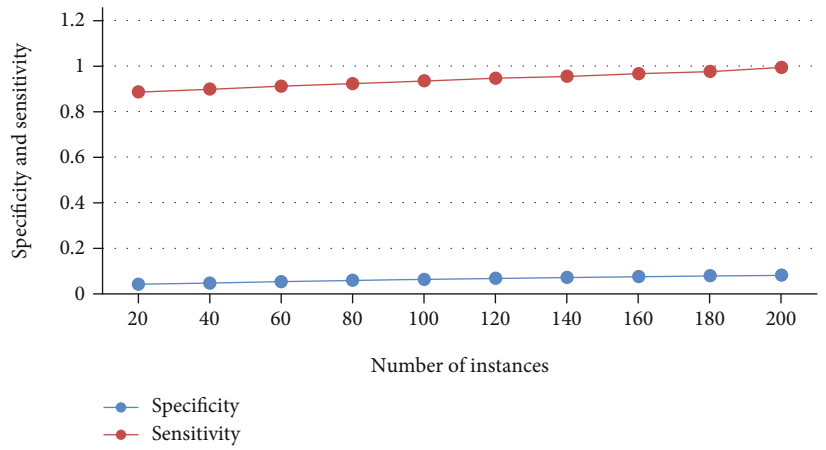

Figure 6: Specificity and sensitivity.

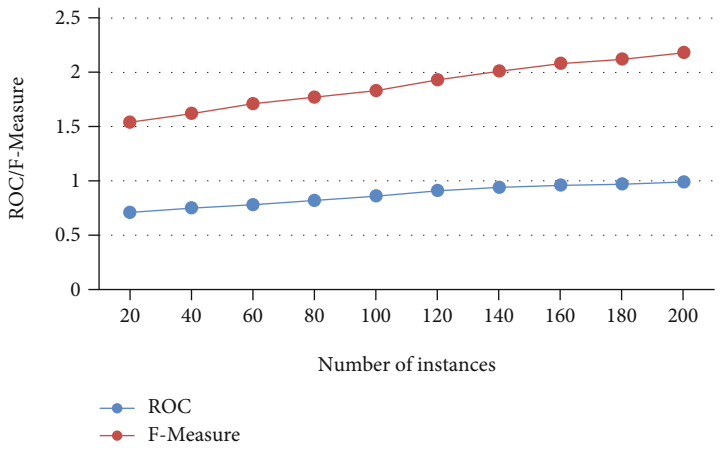

Figure 7: *F*-measure and ROC.

the system. In addition, Figure 5 depicts the classification accuracy of the proposed scheme that performs in a relative manner to the existing mechanism.

The accuracy of the proposed phenomenon is approximately 98% which is improved as compared to that of the existing scheme. The significant outperformance of the proposed phenomenon is due to the BR method that optimizes the processed data to improve the accuracy of the overall system in the network. Figure 6 outperforms while monitoring and analysing the activities of each and every individual. Further, Figure 6 represents the specificity and sensitivity of the proposed phenomenon using AI-based architecture where the values are analysed and processed over smart devices. As depicted in Figure 6, the specificity and sensitivity of the proposed record are improved as a huge amount of information from various networks is processed via the LM mechanism that may enhance the multistage architectural processing, management, and security of records in multihoming networks. Furthermore, Figure 7 represents the ROC and *F*-measure of the proposed phenomenon to determine the accuracy and monitoring against various existing schemes. Figure 7 determines the optimum value results of the proposed approach. The significant improvement of the proposed phenomenon as compared to the existing scheme is due to BR and LM schemes that manage and optimize the huge number of generated records from various types of networks into a single environment.

The processing of big data is optimized through a deterministic and gradient-based local optimum algorithm while training the multistage perceptron architecture through a fast and average convergence rate by providing the stability in the system.

5. Conclusions

This paper proposes an AI-based secure multihoming mechanism for ensuring a secure transmission and processing of big data using the Bayesian Rule (BR) and Levenberg-Marquardt (LM) algorithms. For an efficient monitoring and processing of big data risks while communicating, the LM and BR mechanisms processed the various inputs from heterogenous networks and analyse the weights of each node. The hybrid of the LM and BR algorithm in multihoming networks ensured the efficiency and security while processing the huge information from various networks. The proposed approach efficiently processed the classification of data, nonlinear function, accuracy, and regression schemes in multihoming networks. In addition, the proposed mechanisms are capable of generating an automated decision model via multilayered perceptron using the hybrid of LM and BR schemes. Further, the proposed phenomenon significantly processes and monitors the processed data while proving the security with optimal time delay. The validity and verification of the proposed scheme are experimented over various simulating results against various monitoring and processing parameters such as accuracy, specificity, sensitivity, *F*-measure, and ROC.

The number of automated controlling schemes such as explainable artificial intelligence to further analyse the huge processed records in an efficient and secured manner in multihoming networks by monitoring their activities can be considered in future communication. In addition, the concept of backpropagation in the proposed mechanism is not considered at this stage where instead of computing the gradient of lost function, we have calculated the error propagation ratio and accuracy from the input information in the network.

Data Availability

This paper does not need any online data for the simulation. The present study is based on synthesized data generated randomly by the authors based on some parameters mentioned in the above text.

Conflicts of Interest

The authors declare that they have no conflicts of interest to report regarding the present study.

Acknowledgments

This work is supported by the Netaji Subhas University of Technology, India, and University of the Fraser Valley, Canada. The work was funded by the Abu Dhabi University (Faculty Research Incentive Grant 19300483—Adel Khelifi), United Arab Emirates (https://www.adu.ac.ae/research/research-at-adu/overview).

References

[1] S. Madden, "From databases to big data," *IEEE Internet Computing*, vol. 16, no. 3, pp. 4–6, 2012.

[2] Z. S. Ageed, S. R. Zeebaree, M. M. Sadeeq et al., "Comprehensive survey of big data mining approaches in cloud systems," *Qubahan Academic Journal*, vol. 1, no. 2, pp. 29–38, 2021.

[3] K. A. Bryan and J. S. Gans, "A theory of multihoming in rideshare competition," *Journal of Economics and Management Strategy*, vol. 28, no. 1, pp. 89–96, 2019.

[4] C. Cennamo, H. Ozalp, and T. Kretschmer, "Platform architecture and quality trade-offs of multihoming complements," *Information Systems Research*, vol. 29, no. 2, pp. 461–478, 2018.

[5] A. Sharma, G. Rathee, R. Kumar et al., "A secure, energy- and SLA-efficient (SESE) E-healthcare framework for quickest data transmission using cyber-physical system," *Sensors*, vol. 19, no. 9, pp. 2011–2119, 2019.

[6] Q. Xu, Z. Su, Q. Zheng, M. Luo, B. Dong, and K. Zhang, "Game theoretical secure caching scheme in multihoming edge computing-enabled heterogeneous networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4536–4546, 2018.

[7] Z. Zhang, "Artificial neural network," in *Multivariate Time Series Analysis in Climate and Environmental Research*, pp. 1–35, Springer, Cham, 2018.

[8] G. Rathee, S. Garg, G. Kaddoum, and B. J. Choi, "A decision-making model for securing IoT devices in smart industries," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 4270–4278, 2020.

[9] J. Arshad, M. A. Azad, R. Amad, K. Salah, M. Alazab, and R. Iqbal, "A review of performance, energy and privacy of

intrusion detection systems for IoT," *Electronics*, vol. 9, no. 4, pp. 1–24, 2020.

[10] G. Rathee, H. Saini, and G. Singh, "Aspects of trusted routing communication in smart networks," *Wireless Personal Communications*, vol. 98, no. 2, pp. 2367–2387, 2018.

[11] H. Gao, Y. Xu, X. Liu et al., "Edge4Sys: a device-edge collaborative framework for MEC based smart systems," in *2020 35th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, pp. 1252–1254, New York, NY, USA, 2020.

[12] G. Rathee, M. Balasaraswathi, K. P. Chandran, S. D. Gupta, and C. S. Boopathi, "A secure IoT sensors communication in industry 4.0 using blockchain technology," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 533–545, 2021.

[13] J. S. Warm, W. N. Dember, and P. A. Hancock, "Vigilance and workload in automated systems," in *Automation and Human Performance: Theory and Applications*, pp. 183–200, CRC Press, 2018.

[14] D. Ferraioli, A. Meier, P. Penna, and C. Ventre, "Automated optimal OSP mechanisms for set systems," in *International Conference on Web and Internet Economics*, pp. 171–185, Springer, Cham, 2019.

[15] R. Mamlook, O. F. Khan, M. M. Haddad, H. S. Koofan, and S. M. Tabook, "Controlling future intelligent smart homes using wireless integrated network systems," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 15, no. 2, 2017.

[16] E. G. de Santerre, S. Jammoul, and L. Toutain, "Solving the ingress filtering issue in an IPv6 multihomed home network," in *Ninth International Conference on Networks*, pp. 272–278, Menuires, France, 2010.

[17] L. Wang, H. Guo, Y. Su, and C. Liu, "A reactive learning mechanism for multihoming MN on PMIPv6," in *2010 2nd International Asia Conference on Informatics in Control, Automation and Robotics (CAR 2010)*, vol. 3, pp. 76–79, Wuhan, China, 2010.

[18] J. Bi, P. Hu, and L. Xie, "Site multihoming: practices, mechanisms and perspective," in *Future Generation Communication and Networking (FGCN 2007)*, vol. 1, pp. 535–540, Jeju, Korea (South), 2007.

[19] L. He, Z. Yan, and M. Atiquzzaman, "LTE/LTE-a network security data collection and analysis for security measurement: a survey," *IEEE Access*, vol. 6, pp. 4220–4242, 2018.

[20] F. Li, R. Xie, Z. Wang et al., "Online distributed IoT security monitoring with multidimensional streaming big data," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4387–4394, 2020.

[21] H. Lin, Z. Yan, Y. Chen, and L. Zhang, "A survey on network security-related data collection technologies," *IEEE Access*, vol. 6, pp. 18345–18365, 2018.

[22] J. Wu, M. Dong, K. Ota, J. Li, and Z. Guan, "Big data analysis-based secure cluster management for optimized control plane in software-defined networks," *IEEE Transactions on Network and Service Management*, vol. 15, no. 1, pp. 27–38, 2018.

[23] P. Zhou, K. Wang, J. Xu, and D. Wu, "Differentially-private and trustworthy online social multimedia big data retrieval in edge computing," *IEEE Transactions on Multimedia*, vol. 21, no. 3, pp. 539–554, 2018.

[24] S. Han, S. Xu, W. Meng, and C. Li, "An agile confidential transmission strategy combining big data driven cluster and OBF," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10259–10270, 2017.

[25] J. Adnan, N. N. Daud, S. Ahmad et al., "Heart abnormality activity detection using multilayer perceptron (MLP) network," in *AIP Conference Proceedings (Vol. 2016, No. 1, p. 020013)*, AIP Publishing LLC, 2018.

[26] F. Anifowose, J. Labadin, and A. Abdulraheem, "Ensemble model of artificial neural networks with randomized number of hidden neurons," in *IEEE 8th International Conference on Information Technology in Asia (CITA)*, pp. 1–5, Kota Samarahan, Malaysia, 2013.

[27] G. Rathee, S. Garg, G. Kaddoum, Y. Wu, D. N. K. Jayakody, and A. Alamri, "ANN assisted-IoT enabled COVID-19 patient monitoring," *IEEE Access*, vol. 9, pp. 42483–42492, 2021.