TAF
Journal of Advances in Technology and Engineering Research
JATER
2021, 7(2): 39-47

PRIMARY RESEARCH

A review on the impact of AI as big data in computer network environment

Mariam Ayub [1], Asia Mumtaz [2], Usman Ahmad [3*], Muhammad Abdullah [4]

[1, 2, 4] Department of Computer Science and Information Technology, University of Sialkot, Punjab, Pakistan

[3] Department of Creative Computing, Bath Spa University, Academic Center RAK, Ras Al-Khaimah, UAE

Keywords

Laser coloring
Stainless steel
Artificial Intelligence
Big Data
Computer Network Technology
Network Security
Intrusion Detection System
Long Short Term Memory

Received: 08 July 2021
Accepted: 03 September 2021
Published: 18 December 2021

Abstract

The rapid growth of Artificial Intelligence (AI) with the evolution of network technology has improved and progressed to meet the needs of people. Big data place an important role in the field of AI due to enhanced utilization in computer networks. Many applications are used for big data-based AI in a computer network environment. The problems and the attacks (such as Ransomware, Phishing attacks, and AI attacks) occurring in Network Technology are widely associated with AI as big data along with the solutions such as detection and identification of given attacks and malicious activities. The computer network technology environment is used on a large scale and varies widely with the use of AI in the context of Big Data. However, more advanced technologies are applied with AI to ensure the security of Computer networks. Due to the vast amount of traffic occurring in networks, the result leads to the occurrence of damage in the network, and intrusion detection is a process that proved to be the most essential to ensure the security provided to the system. The defined attacks are specified as the main issues and will prevent vulnerable and malicious activities. The network requires a system to detect intrusions, which is further used to observe and identify the system and networks for anomalies and malicious intrusions as Intrusion Detection System (IDS), Firewall, Encryption, and Anti-spam technologies are used to identify any malicious activity and prevent it. For these attacks, Long Short Term Memory (LSTM) is used in deep learning, and many other technologies such as Machine learning and Data mining are associated with LSTM to detect intrusions. The computer networks with the application of big data as AI were made highly secure and efficient systems by implementing the proposed LSTM method.

I. INTRODUCTION

Today, the applications of intelligent systems and big data are spread throughout the world [1]. The concept of "Big Data" is based on high-speed criteria, mainly used for processing a huge quantity of compound information [2]. A large amount of real-time production data is gathered, and big data is applied to workshop techniques, including fault tracking, optimization of the process, and workshop scheduling [3]. AI is a process used to simulate human awareness, which leads to the development of various human-like technologies. It includes various fields in development, such as robotics and image recognition [4].

Additionally, Big data AI customizes the business processes and makes better decisions by improving the efficiency of decision-making [5]. It is essential in network technology to organize a processing technology to avoid any discontinuity for network monitoring [6]. Alternatively, the increasing development of society has enhanced the progress in the evolution of the computer network environment [7]. As a result, economics, education, and even industrial applications have introduced advancements in big data-based AI technologies [8]. The combination has been holding up many business activities such as finance, marketing, etc. [9]. While discussing AI, in terms of computer network technology, it improves information processing potential [7]. Furthermore, with the occurrence of big data, the issue of network security has become a matter of concern [10]. For AI in a computer network environment, various technologies

*Corresponding author: Usman Ahmad
†email: usman@bathspa.ae

such as Intrusion detection technology, Anti-spam technology, Encryption technology, Network Segmentation technology, and Firewall technology [11].

Moreover, the association of AI with other technologies produces interactions in machines with humans and machines [12, 13]. While evaluating the values from data, AI distributed the services using meters and sensors to increase the system's potential [14, 15]. When combined with Big Data, AI provides sustainability in business processes to strategize and engage systems [16]. On the other hand, artificial intelligence has widely developed its successful position by producing a smart manufacturing system by constructing intelligent and smart factories [17, 18]. It extends the level of cyber-attack prevention in systems [19]. For the provision of security, the application of wireless sensors is used based on big data in an environmental system [20]. Nowadays, the use of AI in network security is also indulged along with the daily routine devices and gadgets in a scientific view [21]. The AI-based big data is utilized in audit increase by gathering the audit information and technology [22]. Therefore, AI, big data, and other technologies have led to its exposure by providing opportunities for human beings in a social environment [23].

Therefore, the most used techniques to solve these problems are machine learning [24], and data mining is also used for related issues [25, 26]. Various methods are used in these techniques, such as traditional data processing methods, AI, and big data analysis methods, which are applied in the industry [3]. This paper proposes a big data method based on real-time processing known as LSTM [3, 27]. The method is used for processing the production of data, and it also predicts the plan of production in case it should be scheduled again and helps for the completion on time. Further, the experiment-based results are compared with K Nearest Neighbor 'KNN', Decision Tree 'DT,' and Recurrent Neural Network 'RNN' model for the classification of binary and multiclass classification models [3, 28].

The utilization of the concept of AI as big data will be used to provide security of networks at a higher level of enhancement. However, the critical analysis of the year, authors, and title of previous research related to the specified concepts included in this paper is provided in the next section of the paper, known as the literature review. Therefore, the discussion of a literature review is necessary to be added as the information evaluation of related research is efficiently used for the innovative implementation of terms in the present study.

II. LITERATURE REVIEW

The literature to identify the critical analysis as the previous research methodologies details along with the problem statement, methodologies, gaps, solutions, and conclusions are described as the titles of the previous study as follows:

TABLE 1
LITERATURE REVIEW PAPERS INFORMATION

Sr#	Year	Author	Title
1)	2018	Stahl and Wright	Ethics and Privacy in AI and Big Data: Implementing Responsible Research and Innovation [29].
2)	2019	Wang and Lu	Research on Application of AI in Computer Network Technology [30].
3)	2019	Allam and Dhunny	On big data, artificial intelligence, and smart cities [31].
4)	2019	Duan et al.	Artificial intelligence for decision making in the era of Big Data–evolution, challenges, and research agenda [32].
5)	2020	Zhu et al.	Big data and artificial intelligence modeling for drug discovery [33].
6)	2020	Singh et al.	Block IoT intelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence [34].
7)	2021	Gao et al.	An introduction to a key technology in artificial intelligence and big data-driven e-learning and e-education [35].
8)	2021	Zhang et al.	Big data and artificial intelligence-based early risk warning system of fire hazards for smart cities [36].
9)	2022	Manivannan et al.	Artificial intelligence databases: turn-on big data of the SMBs [37].
10)	2022	Muheidat et al.	Emerging Concepts Using Blockchain and Big Data [38].

ISSN: 2414-4592
DOI: 10.20474/jater-7.2.3

In Table 1, the critical analysis of previous research is given to associate those with the current and upcoming research for developing a productive system.

After the literature review analysis, the various attacks of AI as big data occurring in a computer network along with each of their solutions are elaborated in tabular form and are defined in a well-organized form. Furthermore, the methodology known as LSTM is proposed by applying for protection from upcoming attacks and threats while discussing the working of the proposed methodology. Therefore, in this way, it will be able to eradicate intrusions by proposing a protected mechanism for computer networks.

III. ISSUES & SOLUTIONS OF AI AS BIG DATA IN COMPUTER NETWORK

The issues and solutions of security occurring in AI as Big Data and computer network environment is described as follows:

TABLE 2
ISSUES & SOLUTIONS OF AI AS BIG DATA IN COMPUTER NETWORK

Sr#	Issues	Description	Year	Solutions	Description	Year
1)	Malware/ Ransomware	The business field is more possibly affected [39].	2018	Ransomware Solution	After restarting the system, download the security-ensured application and start a full scan of the system [40].	2021
2)	Phishing Attacks	Access private information [41].	2019	Phishing Attacks Solution	An anti-phishing filter should be applied to prevent access to vulnerable websites, even if the user accidentally clicks on an unknown URL [42].	2021
3)	DDoS	Attack online operations [43].	2020	DDoS Solution	The solution is to confirm to decrease the nodes attainable for attacks and concentrate on reducing the strength of attacks [44].	2021
4)	Distributed Data	Increase the number of security problems [45].	2020	Distributed Data Solution; Encrypting Big Data	The mechanism for big data encryption must be secured at a large level [46].	2021
5)	Endpoint Vulnerabilities	Illegal access to processing systems [47].	2021	Endpoint Vulnerabilities Solution; Controlling Access	User access control is security's main and fundamental networking mechanism [48].	2021
6)	AI Attacks	Due to the use of AI in developing systems, hackers urge to attack using AI technology.	2022	DNS Protection	It applies firewalls that ensure DNS queries during the processing of any attack.	2022
7)	Zeus Virus	It steals personal information, such as backs, by bypassing centralized servers.	2021	Trojan Discharge Tool	The trojan tool is the best possible approach to eradicate Zeus by the safe mode scanning mechanism.	2022
8)	Fleeceware	It is used to charge a large amount of money from app users even after the deletion of those apps.	2021	Automated Software	It is used to avoid the apps being downloaded from the google play store by utilizing automation.	2022

In Table 2, the various possible problems in AI as big data along with their solutions are given for the knowledge of which type of attacks can occur in a network environment and how to fight back against them when needed.

As discussed earlier, the problems and solutions of AI as big data in a computer network have multiple other mechanisms. By observing the network traffic, the intrusion Detection and Prevention System allows the security teams to provide security to a big data plan of action through malicious activities. In contrast to IDS, IPS mostly works and examines directly following the firewall to isolate the intrusions before the actual damage occurs [49]. Along with all

ISSN: 2414-4592
DOI: 10.20474/jater-7.2.3

the solutions, anti-spam technology and firewall technology are used to overcome many network security issues [30]. Moreover, to access in an illegal way to avail and utilize the information from the network, the intruder intrudes or performs malicious activity in the system [49]. As a result, the intruders perform various malicious activities to gain access, including unauthorized access to anything available on the Internet and network servers, systems, etc. [50]. Many types of attacks come under cyber-attacks, including Hacking, Denial of Services, Malware, Phishing, and Theft [51]. Apart from this, an IDS is a system known to manage security information. IDS is mainly comprised of signature-based and anomaly-based detections, whereas there are various other types known as Network Intrusion Detection System (NIDS), Host, Perimeter, and VM-based IDS [52].

IV. LSTM

As discussed earlier in the introduction, network security problems became a matter of concern, and the most used techniques to solve these problems are machine learning and data mining [3]. However, machine learning is the study of algorithms that are improved automatically, and data mining is the study that is mainly focused on exploring data analysis through unsupervised learning [25, 26]. Therefore, the method introduced in this research is a real-time-based big data processing method known as LSTM method [3].

A. LSTM

LSTM is a particular type of artificial construction of a Recurrent Neural Network. It is applied within the deep learning field. Although, the feedback connections originated to avert depending for a long time and are used for the sequencing of knowledge-based data points [53].

The functions also include recognizing speed and detecting problems. A unit of LSTM contains four basic parts; a cell, input, output, and forget gate [54]. These are used to normalize the flow of data/information. On the other hand, LSTM networks also exist, which are used to process, classify and predict depending on the data of time sequence [55].

B. Working of LSTM

The paper describes the ever-increasing critical problems while developing the concept of industry-based, industrialized Internet [56]. Though, it mainly explains the overall review of the latest technologies in the application of various methods, the enhanced computer-aided and assisted learning regarding cyber security issues [57]. In this case, the given LSTM method is comprised of designing and constructing vectors in the form of code, and the neural network is instructed to disclose the orderly formed abstractions for testing and to examine to detect the availability of malicious activities [58]. However, the basic functionalities for examining the software-based code to detect vulnerable problems and activities use LSTM within the neural network [59, 60].

Moreover, LSTM involves analyzing security-ensured networks based on the future network by sampling data predicting problems [61]. The various network security attacks identified are comparable to the properties of data and categorization of algorithms by comparing many algorithms and settlement of hyper-parameters [62]. Although, the LSTM is used to detect intrusions [54].

Therefore, the LSTM method is applied to identify the intrusions in a network system [59]. Various steps are carried out in the proposed method defined in the table above [63]. As a result, the proposed LSTM model method is utilized for indicating results as the output classification, known as Binary Classification, which is used to detect normal and malicious activities, and the other is known as Multiclass Classification, which is used to give five outputs including R2L, Probe, Normal, DOS, U2R [54].

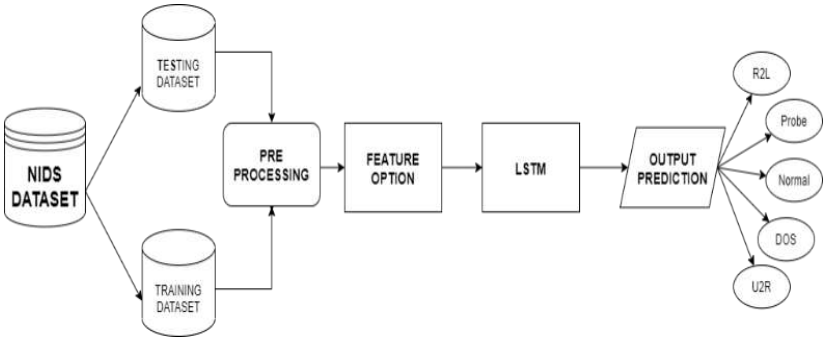

Fig. 1. The proposed method of LSTM

ISSN: 2414-4592
DOI: 10.20474/jater-7.2.3

In Fig. 1, the proposed methodology named as LSTM Method is represented briefly, along with the steps required to identify attacks of different types.

V. RESULTS

While discussing the assessment of the proposed and applied approach of LSTM methodology, with the use of RNN, the prediction of attacks through LSTM is further proved with the application of the confusion matrix approach.

The results indicated that the LSTM method is used to classify data. As a result, it is then applied for eradicating the malicious data. The confusion matrix of the binary classification model is applied for splitting the data as true positive, true negative, false positive, and false negative. In the malicious part, the malicious is alike to the normal which represents true positive value, while the normal over the malicious part represents the negative values as shown in the table below [54].

The confusion matrix of the multiclass-based classification model is indicated to result in the same values. The only thing that is changed is that giving a large number of values to each class makes it complex to calculate. The formula difficulty and complication in the confusion matrix of the multiclass classification model are expanded in contrast to the confusion matrix of a binary classification model. However, all values and the DOS (Denial of Service) attack over DOS possessing positive values are considered negative values for the DOS class and other classes [54].

Therefore, the tabular form of results as the binary and multiclass classification is shown in Table 3 as follows.

TABLE 3
BINARY AND MULTICLASS CLASSIFICATION

Blocks	Binary Classification	Multiclass Classification
Malicious	Positive	-
Normal	Negative	-
DOS	-	Negative
U2R	-	Negative
R2L	-	Negative
Probe	-	Negative
Normal	-	Negative

In Table 3, the results after the application of the confusion matrix in association with LSTM are shown by the classification of a binary and multiclass classifier.

Therefore, the paper results as giving 99.2% accuracy for the Binary classification model and 96.9% accuracy for the Multiclass classification model based on classifications done by LSTM [54, 63].

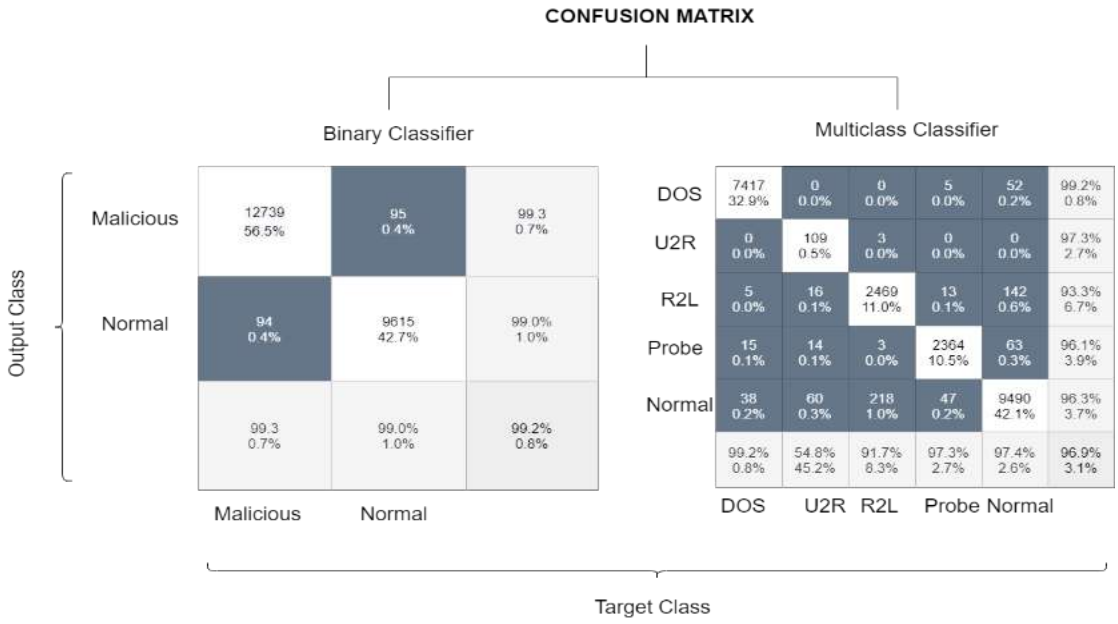

Fig. 2. The confusion matrix of binary classifier and multiclass classifier

In Fig. 2, the confusion matrix is applied under the supervision of the LSTM method which is used to evaluate the performance by the utilization of the classification model with the comparison among binary classifier and multiclass classifier.

ISSN: 2414-4592
DOI: 10.20474/jater-7.2.3

VI. CONCLUSION

AI is now being used in almost every field of technology and the combination of big data AI has provided security to the computer network in efficient and innovative ways. It revealed that the big data-based AI application has greatly enhanced the skills and the capability of network technology and played a very important role in detecting the various attacks and intrusions faced by a computer network. Altogether, the problems of network security in big data AI with the solutions are described. Additionally, the working of the proposed method, the LSTM method is elaborated. However, the proposed LSTM method used for intrusion detection provides security in a network environment, which is utilized for identifying problems. Generally, this method is comprised of binary classification and multiclass classification to calculate detection accuracy. As a result, it gives less accuracy for multiclass classifiers and more accuracy for a binary classifiers. Therefore, by using the deep learning method, intrusions can be detected more effectively. However, today, the application of big data AI in a computer network environment is still facing various challenges and issues which are mainly concerned with the management of a network and scanning of data. Due to the increasing demands of people and users, AI with the union of other technologies is playing an essential role in considering reaching the requirements of people. Moreover, the researchers should work and research more on the application of big data AI technology and other newer technologies for more advanced improvements.

The use of AI as big data should be introduced in various systems of the environment for the social improvement in human and socio-economic development. This will be able to serve society in many ways to secure their systems for privacy enhancement. It can be further facilitated with various other technologies such as blockchain and machine learning technology.

REFERENCES

[1] H. Liu, ``Application analysis of artificial intelligence technology in computer network based on big data era,'' in *Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC),* Dalian, China, 2020. doi: https://doi.org/10.1109/IPEC49694.2020.9115152

[2] Z. Lv, W. Deng, Z. Zhang, N. Guo, and G. Yan, ``A data fusion and data cleaning system for smart grids big data,'' in *Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom),* Xiamen, China, 2019. doi: https://doi.org/10.1109/ISPA-BDCloud-SustainCom-SocialCom48970.2019.00119

[3] W. Du, Z. Zhu, C. Wang, and Z. Yue, ``The real-time big data processing method based on LSTM for the intelligent workshop production process,'' in *5th IEEE International Conference on Big Data Analytics (ICBDA),* Xiamen, China, 2020. doi: https://doi.org/10.1109/ICBDA49040.2020.9101345

[4] W. Sun, C. Li, and R. Ren, ``Artificial intelligence and its application in computer network technology,'' *Journal of Physics: Conference Series*, vol. 1237, no. 2, pp. 1-5, 2019. doi: https://doi.org/10.1088/1742-6596/1237/2/022142

[5] S. Dilmaghani, M. R. Brust, G. Danoy, N. Cassagnes, J. Pecero, and P. Bouvry, ``Privacy and security of big data in ai systems: A research and standards perspective,'' in *IEEE International Conference on Big Data (Big Data),* Los Angeles, CA. IEEE, 2019. doi: https://doi.org/10.1109/BigData47090.2019.9006283

[6] J. Zuo, C. Zhang, J. Chen, Y. Wu, Z. Liu, and Z. Li, ``Artificial intelligence prediction and decision evaluation model based on deep learning,'' in *International Conference on Electronic Engineering and Informatics (EEI),* Nanjing, China, 2019. doi: https://doi.org/10.1109/EEI48997.2019.00102

[7] Y. Feng, ``Research on the application of big data and artificial intelligence technology in computer network technology,'' in *International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS),* Vientiane, Laos, 2020. doi: https://doi.org/10.1109/ICITBS49701.2020.00117

[8] Z. Wang, ``Exploring different notions of literacy: A literature review analysis of literacy research related to artificial intelligence and big data application,'' in *IOP Conference Series: Materials Science and Engineering,* Guangzhou, China, 2020. doi: https://doi.org/10.1088/1757-899X/806/1/012023

[9] M. Obschonka and D. B. Audretsch, ``Artificial intelligence and big data in entrepreneurship: A new era has begun,'' *Small Business Economics*, vol. 55, no. 3, pp. 529-539, 2020. doi: https://doi.org/10.1007/s11187-019-00202-4

[10] H. Xu, ``Application of artificial intelligence in computer network technology under the background of big data era,'' *Journal of Physics: Conference Series*, vol. 1550, no. 3, pp. 1-5, 2020. doi: https://doi.org/10.1088/1742-6596/1550/3/032033

ISSN: 2414-4592
DOI: 10.20474/jater-7.2.3

[11] L. Yang, ``Research on application of artificial intelligence based on big data background in computer network technology,'' *IOP Conference Series: Materials Science and Engineering*, vol. 392, no. 6, pp. 1-6, 2018. doi: https://doi.org/10.1088/1757-899X/392/6/062185

[12] V. Galaz, M. A. Centeno, P. W. Callahan, A. Causevic, T. Patterson, I. Brass, S. Baum, D. Farber, J. Fischer, D. Garcia *et al.*, ``Artificial intelligence, systemic risks, and sustainability,'' *Technology in Society*, vol. 67, pp. 1-10, 2021. doi: https://doi.org/10.1016/j.techsoc.2021.101741

[13] T. Kabudi, I. Pappas, and D. H. Olsen, ``Ai-enabled adaptive learning systems: A systematic mapping of the literature,'' *Computers and Education: Artificial Intelligence*, vol. 2, pp. 1-12, 2021. doi: https://doi.org/10.1016/j.caeai.2021.100017

[14] S. Barja-Martinez, M. Aragüés-Peñalba, Í. Munné-Collado, P. Lloret-Gallego, E. Bullich-Massagué, and R. Villafafila-Robles, ``Artificial intelligence techniques for enabling big data services in distribution networks: A review,'' *Renewable and Sustainable Energy Reviews*, vol. 150, pp. 1-25, 2021. doi: https://doi.org/10.1016/j.rser.2021.111459

[15] A. Chehri, I. Fofana, and X. Yang, ``Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence,'' *Sustainability*, vol. 13, no. 6, pp. 1-19, 2021. doi: https://doi.org/10.3390/su13063196

[16] S. J. Bickley, A. Macintyre, and B. Torgler, ``Artificial intelligence and big data in sustainable entrepreneurship,'' Zurich, Switzerland: Center for Research in Economics, Management and the Arts (CREMA), CREMA working paper no. 2021-11, 2021.

[17] S. K. Jagatheesaperumal, M. Rahouti, K. Ahmad, A. Al-Fuqaha, and M. Guizani, ``The duo of artificial intelligence and big data for industry 4.0: Applications, techniques, challenges, and future research directions,'' *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 12 861-12 885, 2021. doi: https://doi.org/10.1109/JIOT.2021.3139827

[18] F. Zou, L. Ye, Y. Liu, and Y. Zhou, ``The application of big data technology in computer artificial intelligence technology,'' in *Journal of Physics: Conference Series,* Dalian, China, 2021.

[19] T. Ahmad, D. Zhang, C. Huang, H. Zhang, N. Dai, Y. Song, and H. Chen, ``Artificial intelligence in sustainable energy industry: Status quo, challenges and opportunities,'' *Journal of Cleaner Production*, vol. 289, pp. 1-31, 2021. doi: https://doi.org/10.1016/j.jclepro.2021.125834

[20] H. Lin, B. Weng, J. Pan, C. Lin, and Q. Yang, ``Application of wireless sensor networks in the sensitive data security of intelligent data center under the big data environment,'' in *Journal of Physics: Conference Series,* Chongqing, China, vol. 1982, 2021. doi: https://doi.org/10.1088/1742-6596/1982/1/012017

[21] Y. Li, G. Liu, J. Hou, Y. Sun, and Y. Yuan, ``Application of artificial intelligence in computer network technology,'' in *Application of Intelligent Systems in Multi-modal Information Analytics*, V. Sugumaran, Z. Xu, and H. Zhou, Eds. Cham, UK: Springer, 2021.

[22] G. Zhou, ``Research on the problems of enterprise internal audit under the background of artificial intelligence,'' in *Journal of Physics: Conference Series,* Zhuhai, China, 2021. doi: https://doi.org/10.1088/1742-6596/1861/1/012051

[23] S. Zhang, L. T. Yang, J. Feng, W. Wei, Z. Cui, X. Xie, and P. Yan, ``A tensor-network-based big data fusion framework for cyber-physical-social systems (cpss),'' *Information Fusion*, vol. 76, pp. 337-354, 2021. doi: https://doi.org/10.1016/j.inffus.2021.05.014

[24] M. M. Rathore, S. A. Shah, D. Shukla, E. Bentafat, and S. Bakiras, ``The role of ai, machine learning, and big data in digital twinning: A systematic literature review, challenges, and opportunities,'' *IEEE Access*, vol. 9, pp. 32 030-32 052, 2021. doi: https://doi.org/10.1109/ACCESS.2021.3060863

[25] L. Geng, ``Research on artificial intelligence visualization application under internet of things big data,'' in *International Conference on Artificial Intelligence and Advanced Manufacturing (AIAM),* Dublin, Ireland, 2019. doi: https://doi.org/10.1109/AIAM48774.2019.00046

[26] A. Massaro, A. Calicchio, V. Maritati, A. Galiano, V. Birardi, L. Pellicani, M. Gutierrez Millan, B. Dalla Tezza, M. Bianchi, and G. Vertua, ``A case study of innovation of an information communication system and upgrade of the knowledge base in industry by ESB, artificial intelligence, and big data system integration,'' *International Journal of Artificial Intelligence and Applications (IJAIA)*, vol. 9, no. 5, pp. 27-43, 2018. doi: https://doi.org/10.5121/ijaia.2018.9503

[27] R. K. Behera, M. Jena, S. K. Rath, and S. Misra, ``Co-LSTM: Convolutional LSTM model for sentiment analysis in social big data,'' *Information Processing & Management*, vol. 58, no. 1, pp. 389-390, 2021. doi: https://doi.org/10.1016/j.ipm.2020.102435

ISSN: 2414-4592
DOI: 10.20474/jater-7.2.3

[28] G. Rathee, A. Khelifi, and R. Iqbal, ``Artificial Intelligence-(AI-) Enabled Internet of Things (IoT) for secure big data processing in multihoming networks,'' *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1-9, 2021. doi: https://doi.org/10.1155/2021/5754322

[29] B. C. Stahl and D. Wright, ``Ethics and privacy in AI and big data: Implementing responsible research and innovation,'' *IEEE Security & Privacy*, vol. 16, no. 3, pp. 26-33, 2018. doi: https://doi.org/10.1109/MSP.2018.2701164

[30] Q. Wang and P. Lu, ``Research on application of artificial intelligence in computer network technology,'' *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 33, no. 05, pp. 1-12, 2019. doi: https://doi.org/10.1142/S0218001419590158

[31] Z. Allam and Z. A. Dhunny, ``On big data, artificial intelligence and smart cities,'' *Cities*, vol. 89, pp. 80-91, 2019. doi: https://doi.org/10.1016/j.cities.2019.01.032

[32] Y. Duan, J. S. Edwards, and Y. K. Dwivedi, ``Artificial intelligence for decision making in the era of big data-evolution, challenges and research agenda,'' *International Journal of Information Management*, vol. 48, pp. 63-71, 2019. doi: https://doi.org/10.1016/j.ijinfomgt.2019.01.021

[33] H. Zhu, ``Big data and artificial intelligence modeling for drug discovery,'' *Annual Review of Pharmacology and Toxicology*, vol. 60, pp. 573-589, 2020. doi: https://doi.org/10.1146/annurev-pharmtox-010919-023324

[34] S. K. Singh, S. Rathore, and J. H. Park, ``Blockiotintelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence,'' *Future Generation Computer Systems*, vol. 110, pp. 721-743, 2020. doi: https://doi.org/10.1016/j.future.2019.09.002

[35] P. Gao, J. Li, and S. Liu, ``An introduction to key technology in artificial intelligence and big data driven e-learning and e-education,'' *Mobile Networks and Applications*, vol. 26, no. 5, pp. 2123-2126, 2021. doi: https://doi.org/10.1007/s11036-021-01777-7

[36] Y. Zhang, P. Geng, C. Sivaparthipan, and B. A. Muthu, ``Big data and artificial intelligence based early risk warning system of fire hazard for smart cities,'' *Sustainable Energy Technologies and Assessments*, vol. 45, pp. 1-10, 2021. doi: https://doi.org/10.1016/j.seta.2020.100986

[37] P. Manivannan, D. Prabha, and K. Balasubramanian, ``Artificial intelligence databases: Turn-on big data of the SMBs,'' *International Journal of Business Information Systems*, vol. 39, no. 1, pp. 1-16, 2022.

[38] F. Muheidat, D. Patel, S. Tammisetty, A. T. Lo'ai, and M. Tawalbeh, ``Emerging concepts using blockchain and big data,'' *Procedia Computer Science*, vol. 198, pp. 15-22, 2022. doi: https://doi.org/10.1016/j.procs.2021.12.206

[39] G. Cusack, O. Michel, and E. Keller, ``Machine learning-based detection of ransomware using sdn,'' in *Proceedings of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization,* Tempe, AZ, 2018. doi: https://doi.org/10.1145/3180465.3180467

[40] T. McIntosh, A. Kayes, Y.-P. P. Chen, A. Ng, and P. Watters, ``Dynamic user-centric access control for detection of ransomware attacks,'' *Computers & Security*, vol. 111, pp. 1-22, 2021. doi: https://doi.org/10.1016/j.cose.2021.102461

[41] K. Demertzis and L. Iliadis, ``Cognitive web application firewall to critical infrastructures protection from phishing attacks,'' *Journal of Computations & Modelling*, vol. 9, no. 2, pp. 1-26, 2019.

[42] Y. Al-Hamar, H. Kolivand, M. Tajdini, T. Saba, and V. Ramachandran, ``Enterprise credential spear-phishing attack detection,'' *Computers & Electrical Engineering*, vol. 94, pp. 1-13, 2021. doi: https://doi.org/10.1016/j.compeleceng.2021.107363

[43] B. Wang and X. Zhang, ``Construction of compound DDOS network security system based on PKI and CA authentication,'' in *Data Processing Techniques and Applications for Cyber-Physical Systems (DPTA 2019)*. Singapore: Springer, 2020.

[44] M. Snehi and A. Bhandari, ``Vulnerability retrospection of security solutions for software-defined cyber-physical system against DDoS and IoT-DDoS attacks,'' *Computer Science Review*, vol. 40, pp. 1-23, 2021. doi: https://doi.org/10.1016/j.cosrev.2021.100371

[45] J. Liu, Y. Tian, Y. Zhou, Y. Xiao, and N. Ansari, ``Privacy preserving distributed data mining based on secure multi-party computation,'' *Computer Communications*, vol. 153, pp. 208-216, 2020. doi: https://doi.org/10.1016/j.comcom.2020.02.014

[46] P. Matta, M. Arora, and D. Sharma, ``A comparative survey on data encryption techniques: Big data perspective,'' *Materials Today: Proceedings*, vol. 46, pp. 11 035-11 039, 2021. doi: https://doi.org/10.1016/j.matpr.2021.02.153

[47] D. Adame, ``Managing and securing endpoints: A solution for a telework environment,'' California State University, San

Bernardino, CA, Master thesis, 2021.

[48] R. Dastres and M. Soori, ``A review in recent development of network threats and security measures,'' *International Journal of Information Sciences and Computer Engineering*, vol. 15, no. 1, pp. 75-81, 2021.

[49] Y. Zhang and Z. Rao, ``Research on information security evaluation based on artificial neural network,'' in *3rd International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE),* Shenzhen, China, 2020. doi: https://doi.org/10.1109/AEMCSE50948.2020.00098

[50] G. Xiao, ``Research on computer network information security based on big data technology,'' in *IEEE International Conference on Artificial Intelligence and Information Systems (ICAIIS),* Dalian, China, 2020. doi: https://doi.org/10.1109/ICAIIS49377.2020.9194896

[51] U. Sabeel, S. S. Heydari, H. Mohanka, Y. Bendhaou, K. Elgazzar, and K. El-Khatib, ``Evaluation of deep learning in detecting unknown network attacks,'' in *International Conference on Smart Applications, Communications and Networking (SmartNets),* Sharm El Sheikh, Egypt, 2019. doi: https://doi.org/10.1109/SmartNets48225.2019.9069788

[52] S. A. Althubiti, E. M. Jones, and K. Roy, ``LSTM for anomaly-based network intrusion detection,'' in *28th International Telecommunication Networks and Applications Conference (ITNAC),* Sydney, NSW. IEEE, 2018. doi: https://doi.org/10.1109/ATNAC.2018.8615300

[53] F. Shu, S. Chen, F. Li, J. Zhang, and J. Chen, ``Research and implementation of network attack and defense countermeasure technology based on artificial intelligence technology,'' in *5th Information Technology and Mechatronics Engineering Conference (ITOEC),* Chongqing, China, 2020. doi: https://doi.org/10.1109/ITOEC49072.2020.9141751

[54] S. Shende and S. Thorat, ``Long Short-Term Memory (LSTM) deep learning method for intrusion detection in network security,'' *International Journal of Engineering Research and*, vol. 9, no. 6, pp. 1615-1620, 2020.

[55] M. Li, Z. Yang, J. Zhong, L. He, and Y. Teng, ``Research on network attack and defense based on artificial intelligence technology,'' in *IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC),* Chongqing, China, 2020. doi: https://doi.org/10.1109/ITNEC48623.2020.9085100

[56] S. Wenhui, W. Kejin, and Z. Aichun, ``The development of artificial intelligence technology and its application in communication security,'' in *International Conference on Computer Engineering and Application (ICCEA),* Guangzhou, China, 2020. doi: https://doi.org/10.1109/ICCEA50009.2020.00164

[57] B. Sagar, S. Niranjan, N. Kashyap, and D. Sachin, ``Providing cyber security using artificial intelligence-a survey,'' in *3rd International Conference on Computing Methodologies and Communication (ICCMC),* Erode, India, 2019. doi: https://doi.org/10.1109/ICCMC.2019.8819719

[58] R. K. Vigneswaran, R. Vinayakumar, K. Soman, and P. Poornachandran, ``Evaluating shallow and deep neural networks for network intrusion detection systems in cyber security,'' in *9th International conference on computing, communication and networking technologies (ICCCNT),* Bengaluru, India, 2018. doi: https://doi.org/10.1109/ICCCNT.2018.8494096

[59] C. Zhang, L. Xie, Y. Aizezi, and X. Gu, ``User multi-modal emotional intelligence analysis method based on deep learning in social network big data environment,'' *IEEE Access*, vol. 7, pp. 181 758-181 766, 2019. doi: https://doi.org/10.1109/ACCESS.2019.2959831

[60] K. Liu, Y. Zhou, Q. Wang, and X. Zhu, ``Vulnerability severity prediction with deep neural network,'' in *5th International Conference on Big Data and Information Analytics (BigDIA),* Kunming, China, 2019.

[61] L. Liu, J. Lin, P. Wang, L. Liu, and R. Zhou, ``Deep learning-based network security data sampling and anomaly prediction in future network,'' *Discrete Dynamics in Nature and Society*, vol. 2020, pp. 1-9, 2020. doi: https://doi.org/10.1155/2020/4163825

[62] A. Pechenkin and R. Demidov, ``Application of deep neural networks for security analysis of digital infrastructure components,'' in *SHS Web of Conferences,* St. Petersburg, Russia, 2018. doi: https://doi.org/10.1051/shsconf/20184400068

[63] V. Q. Nguyen, L. Van Ma, J.-y. Kim, K. Kim, and J. Kim, ``Applications of anomaly detection using deep learning on time series data,'' in *16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech),* Athens, Greece, 2018. doi: https://doi.org/10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00078