Intrusion Detection System to Secure a Network using ACNN Model and Machine Learning

Ruchika Dungarani, Satish Narayan Gujjar

***Abstract:** -As cyber threats continue to evolve in sophistication and diversity, the need for robust Intrusion Detection Systems (IDS) becomes paramount to safeguarding network integrity. This research explores the application of an innovative approach by integrating an Attention-based Convolutional Neural Network (ACNN) model with machine learning techniques to enhance the accuracy and efficiency of intrusion detection. The proposed system leverages the ACNN's ability to capture contextual dependencies in network traffic data, enabling the extraction of intricate patterns indicative of potential intrusions. The ACNN's attention mechanism focuses on relevant features within the data, improving the model's discriminative power and adaptability to dynamic cyber threats. To achieve optimal performance, the ACNN is complemented with a machine learning framework that includes feature engineering, dimensionality reduction, and classification algorithms. This integrated approach allows the system to adapt and learn from evolving attack vectors, providing a proactive defense mechanism against both known and unknown threats. The research evaluates the proposed ACNN-based IDS using benchmark datasets and real-world network traffic scenarios. Comparative analysis against traditional IDS models showcases the superiority of the ACNN in terms of detection accuracy, false positive rates, and computational efficiency. Furthermore, the system's adaptability to emerging threats is demonstrated through continuous learning and retraining mechanisms. Results indicate that the ACNN-based IDS not only exhibits superior performance but also demonstrates resilience against evasion techniques employed by malicious actors. The research findings contribute to the advancement of network security by presenting a cutting-edge solution that combines deep learning and machine learning for effective and adaptive intrusion detection.*

***Keywords:** -Intrusion Detection System, ACNN Model, Machine Learning, Network Security, Cyber Threats, Attention Mechanism, Deep Learning, Information Security*

I. INTRODUCTION

Intrusion detection system (IDS)A security system called an intrusion detection system (IDS) is made to spot unapproved activities on a network. Such activity may include, but is not limited to, attempts to access sensitive information, unauthorized access to systems, or malicious activities, such as spam email [1].

Manuscript received on 05 June 2024 | Revised Manuscript received on 13 June 2024 | Manuscript Accepted on 15 June 2024 | Manuscript published on 30 June 2024.
**Correspondence Author(s)*

Ruchika Dungarani*, Research Scholar, Department of Computer Science & Engineering, University of Technology, Jaipur (R.J), India. E-mail: Ruchika.dungarani@gmail.com, ORCID ID: 0000-0002-1498-7964

Dr. Satish Narayan Gujjar, Professor, Department of Computer Science & Engineering, University of Technology, Jaipur (R.J), India. E-mail: satishgujjar@gmail.com

A typical intrusion detection system is based on a variety of sensors, such as network intrusion detection systems (NIDSs) that rely on passive data collection from monitoring devices, host-based intrusion detection systems (HIDSs) that actively probe hosts for anomalous activity, and anomaly detection systems (ADSs) that detect changes outside of normal activity patterns [11]. In order to identify intrusions, the intrusion detection system typically compares current activity against a baseline. If the activity does not match the baseline, it is likely an intrusion has occurred [20].

There are many different models of intrusion detection systems, some of which are more effective at detecting certain types of intrusions than others. For example, protocol analyzers are often effective at detecting SYN floods and other forms of network attacks, and web application-specific intrusion detection signatures are more likely to detect attacks that exploit vulnerabilities in these applications [15]. Your intrusion detection system should be set up to monitor all network traffic for troubling activities in order to ensure network security [2][21][22][23].

A security system called an intrusion detection system (IDS) is created to identify hostile or illegal actions such system intrusions or malicious code. In order to identify malicious behavior, it tracks and examines network traffic, system logs, and other sources of data. An IDS can be used to restrict malicious traffic as well as notify system administrators of any unusual activities [1],[19].

In order to monitor and catch any malicious activity or policy breaches on a network, intrusion detection systems are utilized [11]. To find and notify administrators of any suspicious or malicious behavior, the IDS combines signature-based detection, anomaly-based detection, and heuristic-based detection methods [19].

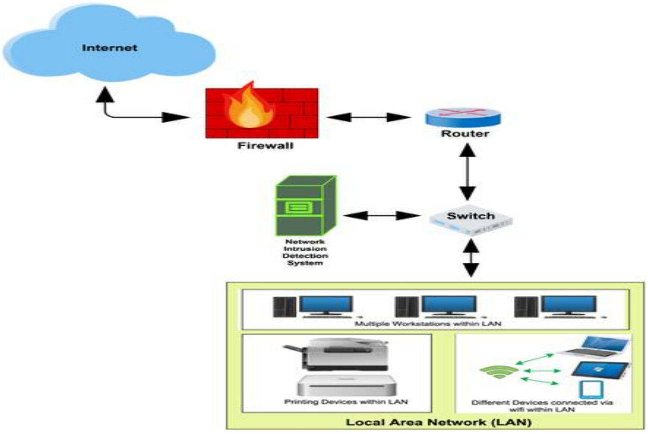
Internet
Firewall
Router
Switch
Network Intrusion Detection System
Multiple Workstations within LAN
Printing Devices within LAN
Different Devices connected via wifi within LAN
Local Area Network (LAN)

Fig: 1.1 Intrusion Detection System in Network

Intrusion detection is a security technique used to detect unauthorized access to computer systems, networks, or websites. Intrusion detection systems (IDS) are designed to detect malicious activity, such as network attacks, malicious software, and suspicious user behavior [19]. They can also detect attempts to gain access to sensitive information, such as passwords and financial data. IDSs use a variety of techniques, including signature-based detection, anomaly-based detection, and heuristics [8]. They may also use machine learning algorithms to detect patterns that indicate malicious activity. Intrusion detection systems can be used to alert administrators of suspicious activity and help them take appropriate action [1]. Machine learning is a type of artificial intelligence that allows software applications to become more accurate in predicting outcomes without being explicitly programmed. It uses statistical analysis to identify patterns in data that can then be used to make decisions and predictions based on new or unseen data [12][17].

Machine learning is a branch of artificial intelligence that uses algorithms to learn from data and improve its performance over time. It is used to develop computer programs that can access data and use it to make predictions or decisions without explicit instructions [13]. Machine learning is used in a variety of applications, such as image recognition, natural language processing, and robotics [3].

II. CNN model

CNN is a network security model designed to protect systems and data. This model is based on the concepts of risk management and incident response.The first step in the CNN model is risk assessment. A process that helps administrators identify risks associated with systems and data. Administrators then use risk mitigation strategies to reduce the risk posed by the system [13] [25]. Finally, administrators use incident response procedures to respond to threats and incidents.CNN models are supported by tools and resources. It includes standard protocols and tools used to secure networks, as well as databases that track incidents and threats [6]. An adaptive convolutional neural network (ACNN)-based fault line selection method is proposed for a distribution network. This method improves the feature extraction ability of the network by improving the pooling model. Compared with deep belief networks (DBN), it can improve the accuracy of fault classification by 7. 86% and training time by 42.7%. Based on this, the secondary defect location was identified using the bipolar defect localization principle, and in this study, the defect data obtained through Simulink simulation was used as a training set, and the ACNN model was built on the TensorFlow platform [4],[5].

III. LITERATURE REVIEW

Network security is significantly influenced by Network Intrusion Detection Systems (NIDS). To stop network infiltration, detect malicious traffic. Machine learning techniques like support vector machines, Bayesian classification, decision trees, and k-means have been employed in conventional procedures [14]. Conventional machine learning techniques have apparent drawbacks and initially require manual feature selection. We suggest a novel NIDS system based on convolutional neural networks in this study. Use both the retrieved features and the original network traffic to train a deep learning search model [3]. Do rigorous tests utilizing reference data sets that are well-known. The results demonstrate that models trained on raw traffic are more accurate than those trained using extracted characteristics, validating the system's effectiveness [6].

In order to improve our daily activities, interconnectedness and interoperability of computing systems are now widely used. In addition, it creates a conduit to weaknesses that are far beyond the reach of human control. Due to the weaknesses, communication exchange must now include cyber-security measures [20]. Secure communication needs improvements to security measures to counter evolving security threats as well as security measures to battle the threats. In order to identify and categorize network attacks, this study suggests using deep learning architectures to build an adaptable and robust network intrusion detection system (IDS). Information security has recently seen increased use of machine learning techniques. Because of unexpected behavior and undiscovered flaws, traditional rule-based security solutions are susceptible to sophisticated assaults [18]. It is possible to create intrusion detection systems (IDS) based on anomaly detection rather than abuse detection using machine learning techniques. When anomalies are found, machine learning can also be utilized to resolve threshold issues. The data set for network intrusion detection is quite tiny in comparison to the data set for malware [7]. There are several security problems as the world becomes more sophisticated and computerized with Internet of Things (IoT) devices. One of the most important and intricate security risks to have evolved with the emergence of the heterogeneous Internet of Things is the distributed denial of service (DDoS) assault [15]. Large-scale DDoS assaults have shown how damaging they can be by repeatedly breaking different infrastructures, resulting in huge losses, and endangering the overall availability of the digital world. This study's main objective is to recognize and counteract different DDoS assaults on HetIoT. [8].

As society and the Internet become more interconnected although the way people live, learn, and work is changing because to the Internet, the myriad security dangers we face are become more serious. A major, inescapable technical difficulty is how to recognize different network attacks, particularly unanticipated attacks. An intrusion detection system (IDS), a crucial development in information security, can spot intrusions that are currently taking place as well as intrusions that have already happened [19]. The difficulty of identifying whether network traffic behavior of the is normal or deviant, or classifying into five categories: (U2R), Probe (probing), and R2L are examples of classification jobs that are similar to intrusion detection (Root to Local). In essence, the basic goal of intrusion detection () is to efficiently detect intrusions while increasing the classifier's accuracy [1]. In cybersecurity, machine learning techniques are frequently employed. However new research has revealed that hostile instances can exploit machine learning algorithms. This puts essential cybersecurity applications at risk in new ways. Cybersecurity adversarial practices currently exist, although they are not fully understood [3],[5].In this article, we offer a fresh technique known as the brute force attack approach to more accurately evaluate the security of machine learning classifiers.

The suggested technique is straightforward to build and just requires the output of the target classifiers to produce adversarial examples. It operates in a black-box manner and addresses several shortcomings of the current adversarial attack methods based on generative adversarial networks.[We use our method to create adversarial examples against popular machine learning-based security systems in cybersecurity, such as host intrusion detection systems, Android malware detection systems, and network intrusion detection systems, in order to have a thorough evaluation of the attack performance of the proposed method [12][19]. We contrast the attack effectiveness of the suggested strategy against various security systems with that of cutting-edge adversarial attack strategies based on generative adversarial networks [9][24]. The preliminary experimental findings demonstrate that the proposed approach, which is more computationally efficient and outperforms state-of-the-art attack methods based on generative adversarial networks, can be used to assess the resilience of different machine learning-based cybersecurity systems against adversarial examples [20].

When a distribution network experiences a single-phase ground fault, it is typically permitted to continue operating for one to two hours despite the fault, which could cause it to worsen and possibly jeopardize the power system's ability to function safely. Therefore, when a small current system has a ground fault, it must be quickly diagnosed to shorten the time of operation with fault. In this paper, an adaptive convolutional neural network (ACNN)-based fault line selection method is proposed for a distribution network [13]. This method improves the feature extraction ability of the network by improving the pooling model. Compared with deep belief network (DBN), it can improve the accuracy of fault classification by 7. 86% and training time by 42.7%. Based on this, the secondary defect location was identified using the bipolar defect localization principle, and in this study, the defect data obtained through Simulink simulation was used as a training set, and the ACNN model was built on the Tensor-Flow platform [4], [5]. In order to increase the efficiency of image analysis techniques, it is essential to take into account past information of the layout and structure of organs. Dictionaries can be particularly helpful when images are distorted and have artifacts as a result of the restrictions in the image collecting process [6]. Learning-based approaches can effectively capture a very small number of anatomical object's features. Unfortunately, it is unclear how to apply this prior information to the most recent, promising techniques, including segmentation based on CNN [10]. In the state-of-the-art method, the learning objective ignores the structure and interdependencies of the output data and behaves as a pixel-by-pixel classifier [14].

We provide a generic learning technique that combines CNN's anatomical prior information with a fresh regularization model that learns end-to-end in order to get over this constraint. With the help of a non-linear representation of the acquired shape, the new structure helps the model to adhere to the general anatomical characteristics of the underlying anatomy (such as shape and mark structure) [16]. We show that the suggested method may be used to solve a variety of analytical issues (such as picture enhancement and segmentation) and raise the predicted accuracy of cutting-edge models. Our method's usefulness is demonstrated in multimodal cardiac datasets and freely accessible tests. We also illustrate the interpretation and application of the trained 3D geometric depth model as a diagnostic for categorizing heart diseases [11].

There are many survey papers in the literature that provide some implementation details on the IDS. Our article is different from the other review articles11-16 from three aspects: (i) We followed a systematic article selection process to obtain more focused articles on NIDS design considering AI tools [20]. While the other studies reviewed the general IDS system without using the systematic approach. (ii) Our study reviewed the articles published between 2017 and April 2020. So it provides more updated information and the recent trends followed in the design of AI-based NIDS. (iii) In our study, an extensive review of the recent NIDS based on ML and DL approach is provided where they are critically analyzed according to their methods, techniques, datasets, and evaluation metrics [15]. The focus is to provide researchers with more updated knowledge on AI-based NIDS in one place, where they can find the recent trends and potential research areas in the domain to start exploring it. A detailed comparison of this article with other review articles is provided in Table 1.

TABLE 1. Comparison with other Similar Review Articles: (:Yes, ✗: No)

Review Article	*Year*	*Systematic Study*	*NIDS Focused*	*AI-based Approaches*		*Future Trends*
				ML	**DL**	
Vasilomanolakis et al[11]	2015	✗	✗	➚	✗	➚
Buczak et al[12]	2015	✗	✗	➚	✗	➚
Thomas et al[13]	2018	✗	➚	➚	✗	➚
Liu et al[14]	2019	✗	➚	➚		➚
Khraisat et al[15]	2019	✗	✗	➚	✗	➚
Da Costa et al[16]	2019	✗	✗	➚	➚	➚
This Article		➚	➚	➚	➚	➚

IV. CONCLUSION

The conclusion of the research paper titled "Intrusion Detection System to secure a network using ACNN Model and Machine Learning" emphasizes the significance of robust Intrusion Detection Systems (IDS) in safeguarding network integrity against evolving cyber threats. The study proposes an innovative approach that integrates an Attention-based Convolutional Neural Network (ACNN) model with machine learning techniques to enhance intrusion detection accuracy and efficiency. The research findings demonstrate the superiority of the ACNN-based IDS in terms of detection accuracy, false positive rates, and adaptability to emerging threats compared to traditional IDS models. The system's ability to continuously learn and adapt to evolving attack vectors is highlighted, showcasing its proactive defense mechanism against known and unknown threats. Overall, the research contributes to advancing network security by presenting a cutting-edge solution that combines deep learning and machine learning for effective and adaptive intrusion detection.

DECLRATION STATEMENT

Funding	No, I did not receive.
Conflicts of Interest	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material	Not relevant.
Authors Contributions	All authors have equal participation in this article.

REFERENCES

1. L. Chen, X. Kuang, A. Xu, S. Suo, and Y. Yang, “A Novel Network Intrusion Detection System Based on CNN,” *2020 Eighth International Conference on Advanced Cloud and Big Data (CBD)*, pp. 243–247, Dec. 2020, doi:. https://doi.org/10.1109/CBD51900.2020.00051
2. R. Vinayakumar, K. P. Soman, and P. Poornachandrany, “Applying convolutional neural network for network intrusion detection,” *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, vol. 2017-January, pp. 1222–1228, Nov. 2017, doi: 10.1109/ICACCI.2017.8126009. https://doi.org/10.1109/ICACCI.2017.8126009
3. Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017, September). Applying convolutional neural network for network intrusion detection. In *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 1222-1228). IEEE. https://doi.org/10.1109/ICACCI.2017.8126009
4. Liang, J., Jing, T., Niu, H., & Wang, J. (2020). Two-terminal fault location method of distribution network based on adaptive convolution neural network. *IEEE Access*, *8*, 54035-54043. https://doi.org/10.1109/ACCESS.2020.2980573
5. J. Liang, T. Jing, H. Niu, and J. Wang, “Two-Terminal Fault Location Method of Distribution Network Based on Adaptive Convolution Neural Network,” *IEEE Access*, vol. 8, pp. 54035–54043, 2020, doi: https://doi.org/10.1109/ACCESS.2020.2980573
6. L. Ashiku and C. Dagli, “Network Intrusion Detection System using Deep Learning,” *Procedia Comput Sci*, vol. 185, pp. 239–247, Jan. 2021, doi: 10.1016/J.PROCS.2021.05.025. https://doi.org/10.1016/j.procs.2021.05.025
7. J. Kim, Y. Shin, and E. Choi, “An Intrusion Detection Model based on a Convolutional Neural Network,” *J. Multim. Inf. Syst.*, vol. 6, no. 4, pp. 165–172, Dec. 2019, doi: https://doi.org/10.33851/JMIS.2019.6.4.165
8. S. Mahadik, P. M. Pawar, and R. Muthalagu, “Efficient Intelligent Intrusion Detection System for Heterogeneous Internet of Things (HetIoT),” *Journal of Network and Systems Management*, vol. 31, no. 1, pp. 1–27, Mar. 2023, doi:https://doi.org/10.1007/s10922-022-09697-x
9. L. Mohammadpour, T. C. Ling, C. S. Liew, and A. Aryanfar, “A Survey of CNN-Based Network Intrusion Detection,” *Applied Sciences (Switzerland)*, vol. 12, no. 16, Aug. 2022, doi: https://doi.org/10.3390/app12168162
10. Mohammadpour, L., Ling, T. C., Liew, C. S., &Aryanfar, A. (2022). A Survey of CNN-Based Network Intrusion Detection. *Applied Sciences*, *12*(16), 8162. https://doi.org/10.3390/app12168162
11. Vigneswaran, R. K., Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2018, July). Evaluating shallow and deep neural networks for network intrusion detection systems in cyber security. In *2018 9th International conference on computing, communication, and networking technologies (ICCCNT)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICCCNT.2018.8494096
12. L. Chen, X. Kuang, A. Xu, S. Suo, and Y. Yang, “A Novel Network Intrusion Detection System Based on CNN,” *2020 Eighth International Conference on Advanced Cloud and Big Data (CBD)*, pp. 243–247, Dec. 2020, doi: https://doi.org/10.1109/CBD51900.2020.00051
13. R. Vinayakumar, K. P. Soman, and P. Poornachandrany, “Applying convolutional neural network for network intrusion detection,” *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, vol. 2017-January, pp. 1222–1228, Nov. 2017, doi: 10.1109/ICACCI.2017.8126009. https://doi.org/10.1109/ICACCI.2017.8126009
14. Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017, September). Applying convolutional neural network for network intrusion detection. In *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 1222-1228). IEEE. https://doi.org/10.1109/ICACCI.2017.8126009
15. Liang, J., Jing, T., Niu, H., & Wang, J. (2020). Two-terminal fault location method of distribution network based on adaptive convolution neural network. *IEEE Access*, *8*, 54035-54043. https://doi.org/10.1109/ACCESS.2020.2980573
16. J. Liang, T. Jing, H. Niu, and J. Wang, “Two-Terminal Fault Location Method of Distribution Network Based on Adaptive Convolution Neural Network,” *IEEE Access*, vol. 8, pp. 54035–54043, 2020, doi: 10.1109/ACCESS.2020.2980573. https://doi.org/10.1109/ACCESS.2020.2980573
17. L. Ashiku and C. Dagli, “Network Intrusion Detection System using Deep Learning,” *Procedia Comput Sci*, vol. 185, pp. 239–247, Jan. 2021, doi: https://doi.org/10.1016/j.procs.2021.05.025
18. J. Kim, Y. Shin, and E. Choi, “An Intrusion Detection Model based on a Convolutional Neural Network,” *J. Multim. Inf. Syst.*, vol. 6, no. 4, pp. 165–172, Dec. 2019, doi: 10.33851/JMIS.2019.6.4.165. https://doi.org/10.33851/JMIS.2019.6.4.165
19. S. Mahadik, P. M. Pawar, and R. Muthalagu, “Efficient Intelligent Intrusion Detection System for Heterogeneous Internet of Things (HetIoT),” *Journal of Network and Systems Management*, vol. 31, no. 1, pp. 1–27, Mar. 2023, doi: 10.1007/S10922-022-09697-X/TABLES/14. https://doi.org/10.1007/s10922-022-09697-x
20. L. Mohammadpour, T. C. Ling, C. S. Liew, and A. Aryanfar, “A Survey of CNN-Based Network Intrusion Detection,” *Applied Sciences (Switzerland)*, vol. 12, no. 16, Aug. 2022, doi: 10.3390/APP12168162. https://doi.org/10.3390/app12168162
21. Reddy, M. V. K., & Pradeep, Dr. S. (2021). Envision Foundational of Convolution Neural Network. In International Journal of Innovative Technology and Exploring Engineering (Vol. 10, Issue 6, pp. 54–60). https://doi.org/10.35940/ijitee.f8804.0410621
22. Kumar, P., & Rawat, S. (2019). Implementing Convolutional Neural Networks for Simple Image Classification. In International Journal of Engineering and Advanced Technology (Vol. 9, Issue 2, pp. 3616–3619). https://doi.org/10.35940/ijeat.b3279.129219
23. Mandhare, V. V., Pede, D. R., & Vikhe, P. S. (2020). Network Intrusion Detection using a Deep Learning Approach. In International Journal of Recent Technology and Engineering (IJRTE) (Vol. 9, Issue 3, pp. 59–64). https://doi.org/10.35940/ijrte.b4086.099320
24. Dubey, S. K., Sinha, Dr. S., & Jain, Dr. A. (2023). Heart Disease Prediction Classification using Machine Learning. In International Journal of Inventive Engineering and Sciences (Vol. 10, Issue 11, pp. 1–6). https://doi.org/10.35940/ijies.b4321.11101123
25. Mukherjee*, P., Palan, P., & Bonde, M. V. (2021). Using Machine Learning and Artificial Intelligence Principles to Implement a Wealth Management System. In International Journal of Soft Computing and Engineering (Vol. 10, Issue 5, pp. 26–31). https://doi.org/10.35940/ijsce.f3500.0510521

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

AUTHORS PROFILE

Ruchika P. Dungarani is an Assistant Professor at Swarrnim Startup and Innovation University Gandhinagar, In Computer Science & Engineering Department. Her interests are in Cyber Security, Information Security, Artificial Intelligence, Machine Learning, Internet of Things. She did her M.E. in Computer Engineering from Growmore Faculty of Engineering Under Gujarat Technological University. BE in Computer Engineering from Growmore Faculty of Engineering Under Gujarat Technological University. Currently she is working on Network security in her Phd. She is doing her PhD from University of Technology, Jaipur. She has published 05 international Papers in Cyber Security and Information Security.

Dr. Satish N. Gujar is a Research Guide at Department of Computer Science and Engineering, University of Technology, Rajasthan, India. His interests are in Database, Big Data, Internet of Things, Information Security, Cyber Security, Computer Graphics and Image Processing. He has received Ph.D. in Computer Science & Engineering from Department of Computer Science & Engineering,Sant. Gadgebaba Amravati University, Amravati , India. M.E. in Computer Science & Engineering from Prof. Ram Meghe Institute of Technology and Research, Badnera, Amravati under Sant. Gadgebaba Amravati University, Amravati. And BE in Computer Science and Engineering from Babasaheb Naik College of Engineering, Pusad, Dt. Yavatmal. Under under Sant. Gadgebaba Amravati University, Amravati. He has published 04 patent in IoT and Cyber Security.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.