International Journal of Electrical and Electronics Engineering Studies, 11(1), 15-26, 2025
ISSN 2056-581X (Print),
ISSN 2056-5828(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Review of the Development of an AI-Enabled Powerline Security System Using Infrared Image Processing and a Fuzzy Logic Threat Classification for Real-Time Intrusion Detection

A.I Musa[1], Y.S Haruna[2], B.H Mamman[3], and H.S Miya[4]
[1,2,3,4]Department of Electrical and Electronics Engineering Faculty of Engineering and Engineering Technology Abubakar Tafawa Balewa university Bauchi State, Nigeria.

doi: https://doi.org/10.37745/ijeees.14/vol11n11526 Published November11, 2025

Citation: Musa A.I., haruna Y.S., MammanB.H., and Miya H.S. (2025) Review of the Development of an AI-Enabled Powerline Security System Using Infrared Image Processing and a Fuzzy Logic Threat Classification for Real-Time Intrusion Detection, *International Journal of Electrical and Electronics Engineering Studies*, 11(1), 15-26

Abstract: *This paper introduces an all-in-one, smart, surveillance system to protect high-voltage transmission lines with a combination of infrared (IR) thermal imaging, artificial intelligence (AI)-based object detection, fuzzy logic-based threat classification, geolocation tagging, and real-time wireless alerts. The framework solves the endemic problem of ensuring that remote and low visibility transmission routes are not intruded, vandalized and sabotaged- problems which traditional security mechanisms find hard to control. Using deep learning models like YOLOv8 and Convolutional Neural Network (CNNs), the suggested system is able to improve detection and situational awareness even in various environmental parameters. An interpretation fuzzy inference system also puts the detected events more into context by evaluating proximity, time at which events take place, and thermal intensity, which reduces false alarms. The paper is a critical review of the contemporary developments in AI-aided thermal surveillance, existing gaps in the existing methodologies, and the viability of implementing real-time, edge-enabled thermal surveillance systems on a large-scale power network. The study is a contribution to the emerging body of intelligent infrastructure protection since it indicates how AI-based systems can be used to change reactive security-focused systems into proactive ones.*

Keywords: AI-enabled powerline security system, infrared image processing, fuzzy logic threat classification, real-time intrusion detection

INTRODUCTION

The protection of electrical transmission infrastructure is becoming a fundamental principle of energy resiliency and economic stability at the national level. Transmission towers and high-

voltage lines take up a significant and remote location and hence are susceptible to vandalism, metal theft, sabotage, and natural threat. They cause energy distributions disruption and can cause systemic grid outages with severe economical and safety effects [1]. Conventional security systems like manual patrols, closed-circuit television (CCTV), and motion sensors have range constraints, visibility constraints and cost constraints when implemented in large transmission systems. Moreover, they are too reliant on human supervision, which adds delays and inconsistencies in response [2]. The lack of real time situational awareness and intelligent automation underscores the need to have new surveillance paradigms which have the capability to work independently in situations of low visibility and resource scarcity. Thus, the improvement of the system that incorporates the modern sensing, artificial intelligence (AI), and geolocation technologies is not only better but a requirement to secure the modern energy systems.

The traditional surveillance systems are also based much on the optical cameras which can be constrained by the environment like low lighting, fog, and rain. These systems also have difficulties in distinguishing between human intrusion and benign activity, which leads to high false alarm [3]. The motion sensors are cheap but have limited coverage and are prone to noise in the environment whereas the periodic patrol is labor intensive and cannot be deployed on a large scale. Also, legacy systems are usually silo-based and lack the capability to integrate data or geolocate therefore their situational intelligence is minimal [4]. The growth of critical infrastructure to remote or hostile areas makes these shortcomings make traditional surveillance more and more outdated. The shift to autonomous, sensor-fused surveillance solutions, in particular, the ones that use thermal scanning and AI, has therefore become a crucial approach to infrastructure protection in the future [5]. This study is a direct reaction to this development as it combines AI-aided infrared thermal imaging with contextual threat detection to provide intelligent, scalable, and real-time surveillance.

According to the recent years, IR thermal imaging has become notorious due to its ability to identify human thermal features regardless of the visibility of light. In contrast to optical imaging, the IR technology is capable of working well at night, during fog, or during partial obstructions, and it is more reliable to use in various environments [6]. Its use in inspection of industries and surveillance of the military has proved to be a stable performer as well as not prone to environmental interference. Thermography has already been applicable in the power systems, where it is used in detecting faults, such as hotspots in insulators, conductors, and connector [7]. Nonetheless, its use in intrusion detection of humans is still little explored, and the majority of studies concentrate on condition monitoring and not on the security-sensitive applications [8]. The proposed research builds on this literature by using thermal imaging to monitor and identify, as well as categorize illegal human presence near the transmission towers. This passive inspection to active threat detection is a change in itself, which can be considered an innovative thermography evolution in energy infrastructure protection.

With the introduction of AI and especially deep learning, image-based detection and classification have been transformed in several fields. The use of CNNs and real-time object detection algorithms

of You Only Look Once (YOLOv8) algorithms have made a remarkable breakthrough in identifying intricate visual patterns in dynamic situations [9]. When used in the thermal imaging task, these algorithms are capable of distinguishing between human intrusion and a background noise or an object that will not cause threat to an individual with unprecedented accuracy [10]. The AI-based systems are more effective than the manual ones as they are capable of analyzing visual data and reporting anomalies unremittingly and with impregnable objectivity. Regardless of these benefits, the field of AI-based model implementation in the power infrastructure monitoring is not thoroughly covered in comparison with other security systems or autonomous vehicles [11]. Besides, the majority of the works done before are aimed at detecting faults or at basic motion detection but not at fine-tuning threat detection. The research will therefore contribute to the existing body of knowledge by designing and training a deep neural network that is directly designed to detect human faces in transmission tower settings using infrared technology.

Although AI can be used to detect, intelligent surveillance also requires a contextual interpretation of the observed phenomenon. The introduction of Global Positioning System (GPS) modules can be used to localize the intrusion incidents in real-time and respond to them accordingly and effectively send the maintenance or security teams to the necessary locations [12]. But bare raw detections with no prioritization run risk of flooding the operators with alerts of low urgency. This paper proposes a threat evaluation system implemented with fuzzy logic that considers several contextual features in categorizing risk levels including the distance of the intruder to the tower, the timing when this occurred, and the signal strength [13]. In contrast to deterministic thresholding, the fuzzy logic enables the reasoning under uncertainties and it simulates human judgment in uncertainties. This is a hybrid technique of perception via AI and fuzzy logic via cognition to fill the gap between the detection and actionable intelligence. It is one of the most fundamental developments of the traditional systems of surveillance that can only recognize objects to the intelligent ones that can reason about the level of threat and its urgency.

Although rapid innovation in thermal imaging, AI and geospatial technologies is being achieved, the lack of specific frameworks ensuring the protection of power transmission infrastructure is evident. The majority of the current literature addresses individual components, including visual AI recognition or GIS-based asset prediction, which are not able to form a coherent multi-layered intelligence [14]. Besides, the constraints of the real-time deployment such as the efficiency of the edge processing, communication bandwidth, and environmental variability are rarely addressed along with the accuracy of detection. The proposed study will address these shortcomings by designing, implementing, and validating a smart, real-time surveillance system that will be an intelligent surveillance system that is a combination of IR thermal imaging, AI-based object identification, fuzzy logic identification, and geolocation tagging. The system will prove the practicability of real-time intrusion detection and contextual threat evaluation in the simulated field conditions, through controlled experiments. This addition does not only improve on the current methodologies, but also provides a model of how other smart grid security systems can be replicated in the future.

This study is theoretically and practically important. In principle, it can apply AI and fuzzy logic to the area of critical infrastructure protection to provide a theoretical basis of the integration of sensory, cognitive, and spatial reasoning modules in the surveillance systems [15]. In practice, it gives an engineering conceptualization of creating cost-effective, autonomous monitoring systems that can be flexible to remote conditions. The research helps to develop the ever-expanding discussion on intelligent energy management and smart infrastructure resilience by showing how the application of multi-sensor fusion and AI can be used in conjunction to improve the perception of threats [16]. It is also consistent with the world sustainability as it enhances proactive maintenance, less physical patrols, and less operational expenses. The research will be of value to scholars, energy regulators, and utility operators who are in search of new ways of mitigating vulnerability of the fundamental power resources in a digitalizing age, which is becoming more susceptible to physical attacks. This study is eventually a move in the right direction toward having resilient, intelligent, and adaptive infrastructure security.

Review of Related Research

Infrared Thermal Imaging and Condition Monitoring

IRT has developed into a non-contact and non-intrusive mechanical systems that have become mature. It offers serious understanding of the temperature aberrations that indicate faults at the initial phases including loose connections, insulation failure, and overloads [17]. The efficiency of the technology is in its ability to visualize patterns of the heat outside the visible spectrum diagnostic tool that is highly used in condition-based monitoring (CBM) of electrical equipment and in allowance of preventive maintenance before disastrous failures take place. In the electrical energy business, IRT has proved to be highly reliable in determining the health of the transformers, substation elements, and transmission lines [18]. The fact that it can be used to do inspections in a load-gagged situation that does not disrupt operations renders it invaluable in predictive maintenance regimes. Nevertheless, even being mature, there are still several operational constraints that deter accuracy and repeatability in an unfavorable weather scenario because sensor calibration drift, reliance on ambient conditions, and a small range of detection are present [19].

In addition, the increased use of Artificial Intelligence (AI) with IRT has made it reach beyond passive surveillance and have been incorporated with smart monitoring of conditions and labeling of anomalies [20]. With the help of AI-based analytics, thermographic data can be automatically analyzed via the detection of defect patterns, heat distribution quantification and fault development forecasting. As an example, the latest reviews include the use of deep neural networks to automatically detect defects based on thermal images, which is significantly less prone to human error [21]. However, the majority of the research has focused on maintenance-based applications-monitoring of overheating parts- as opposed to external security risks including intrusions by unauthorized users or sabotage. [22] observe that although thermal imaging has been seen to work well in fault localization in utility lines, its application in real-time intrusion detection in high-

voltage tower settings is not well studied. The given gap explains why the current research had to focus on the adaptation of IRT to the proactive surveillance in the power transmission realm.

Artificial Intelligence and Deep Learning for Object Detection in Thermal Imagery

AI, especially deep learning, has recently altered computer vision in various industries and made a machine capable of detecting, classifying, and processing complex visual information with high accuracy. Convolutional Neural Networks (CNNs) and the variations of the concept, such as You Only Look Once (YOLO), Single Shot MultiBox Detector (SSD), and Faster R-CNN, have become the current standards of real-time object detection [22; 23]. Their implementation in thermal imaging scenarios is especially disruptive, since adaptive feature extraction and transfer learning is able to reduce the noise and low contrast inherent to infrared threshold data, which is usually produced by thermal sensors. As an example, a deep CNN model that was trained with warm-up data about thermographic data on electrical installations obtained an accuracy of 99.98 stressing that deep learning can be highly discriminative when applied to IRT [24].

A thermal imaging model by the UAV with the help of YOLOv8 models has proven to have over 96 percent (mean Average Precision, mAP) in the localization of faults and object detection in power infrastructure monitoring [25]. These findings confirm the suitability of the implementation of state-of-the-art detection algorithms to dynamic setting, thermally-heterogeneous environments. Nevertheless, there is still a major weakness in the form of a critical constraint because the current models are mainly focused on structural defects not on human presence or intrusion. In addition, most of them depend on offline processing and so, cannot be useful in real-time applications. The suggested study will be unique because it will utilize CNN and YOLOv8 networks specifically trained on multi-spectrum (thermal and visible) data to identify human intrusion around power infrastructure. This approach agrees with the state of the art of AI studies, which is concerned with data fusion and efficiency of real-time inference on the edge devices [26].

More importantly, although CNNs are very effective in extraction of spatial features; their computationally complexity may be a barrier to implementation in energy-constrained systems like transmission corridors. To optimize the models, it is required to perform quantization and pruning and attain the lightweight architecture integration and deployment [27]. Thus, the design of the proposed system where the focus lies on the trade-off between detection performance and computational efficiency is a needed step towards the introduction of deployable AI-based remote critical infrastructure surveillance systems.

Intrusion Detection, Threat Classification, and Real-Time Systems

Although AI-based object detection is a highly studied field, there is added complexity in the case of intrusion detection of power infrastructure because of uncertainties in the environment, as well as, contextual ambiguity. The traditional intrusion detection systems (IDS) are usually simple threshold-based intrusion detection systems that do not differentiate between authorized personnel, wildlife, and actual intruders [28]. Therefore, system inefficiency and low operator trust are caused

by false alarms and ineffective situational interpretation. Further studies have therefore shifted to multimodal fusion and intelligent reasoning schemes which combines contextual information of time of detection, distance to protected assets and thermal intensity so as to enhance accuracy. Specifically, fuzzy logic has shown good prospects of threat-level analysis due to its capability to manage uncertainties and approximate reasoning human-like [29].

According to the latest studies, fuzzy inference and AI detection have proven useful in making smart choices in any security or industrial system [30]. Nonetheless, the integration of this type is not developed in the particular environment of the security of power transmission. The proposed study addresses this gap by coming up with a rule-based fuzzy logic system to determine the extent of intrusion dynamically depending on the geospatial and thermal parameters. Not only does this improve situational awareness but it also solves one of the most enduring problems in the field; that of minimizing false alarms without impairing detection sensitivity. Embedded AI and fuzzy reasoning have been considered to be essential in the frontier of managing intelligent infrastructure through real-time decision support [31]. This, therefore, makes this study fit in the body of knowledge as it advances the gap in the detection accuracy and the contextual intelligence which has not been often synthesized among the available intrusion detection literature.

Edge Processing, Geolocation, and System Integration

The emergence of edge computing technology in a short period has changed the design of remote systems of infrastructure surveillance and monitoring. The centralized processing of clouds is not viable in situations like in high-voltage transmission corridors where the bandwidth, connectivity, and latency are limited by factors that make centralization impractical [32]. The edge devices, which can do the inference in real time and at the local level, offer an efficient alternative by reducing the amount of data sent and allowing an immediate response. It is especially applicable in the case of AI-based surveillance, when huge sets of images have to be processed in real time [33]. Taking advantage of such edge systems with the help of infrared cameras and GPS modules, it is possible to accurately determine the intrusion events with the minimum power and bandwidth consumption.

The latter is further reinforced by recent reviews of UAV based inspection systems which note the need to have onboard processing and constant communication on real-time monitoring [34]. Equally, according to [35], the success of any system integration, such as metadata tagging, tower identification, and synchronous alerting, is one of the most important determinants of scalability and successful operation. The architecture of the proposed system, consisting of a combination of edge AI calculation, geolocation using GPS positioning, and wireless notification functions, is in line with these concepts. It provides prompt context-driven alerts in support of fast field response. Furthermore, the system, via incorporating AI and geospatial analytics in edge devices, reduces latencies, improves reliability and still operates autonomously during coverage-restricted areas.

Engineering-wise, these forms of integration represent a concept of a so-called smart cyber-physical system (CPS), in which sensing, computation, and communication are all coordinated to create situational intelligence [36]. It addresses design issues of self-adaptive resilient surveillance infrastructures that are capable of real-time responsiveness through the concentration on modularity and real-time responsiveness. A combination of AI, thermal sensing, fuzzy reasoning, and geospatial intelligence, therefore, is a large step toward the next-generation protection of power infrastructure.

Primary Contributions and Novelty.
In accordance with the review provided above and the thesis proposal, the following contributions are outstanding:
Transmission-line tower intrusion detection, as opposed to fault/hot-spot detection, domain specific.

IR thermal imaging - apply AI object detect- fuzzy logic threat classification - geolocation + real-time alerting built-in pipeline. Open literature rarely involves the end-to-end integration.
Context-based classification of threats through the use of fuzzy logic (not only detection) which takes into consideration time, proximity and thermal intensity - improves decision-making and minimizes false positives.
Edge-ready/realtime simulation with latency of less than 100ms/frame target and remote/highvoltage deployability.

Scalability and multi-domain adaptability - although concerned with power-lines, the framework can be adapted to other vital infrastructure (oil pipelines, substations) - expanding the consequences.These contributions put the work in a good position to be published as a high-impact article and used in the security of infrastructure.

Critical Evaluation of Methodology
The suggested research design is a simulation-based approach (with no physical hardware implementation yet), which is suitable during the research phase and the limitation of the cost/ethical factors. The application of synthetic metadata (GPS, tower ID, timestamps) is valid. Such tools as Python, PyTorch, OpenCV, scikit-fuzzy are selected and popular.

Still, certain considerations and possible limitations are to be mentioned:

- **Dataset realism**: It is okay to rely on publicly available thermal IR imagery (e.g., FLIR) and artificial frames, refer to the actual thermal data of transmission towers (in the presence of occlusions, long ranges, weather conditions vary) that can differ greatly. There has to be the disconnect between simulation and deployment.
- **Edge hardware constraints:** Achieving a latency of less than 100 ms per frame is ambitious. Factors like model size, hardware, and thermal image resolution play a role. Performance may also be affected by power supply, connectivity, durability, and real-world conditions.

- **False alarms and environmental variability:** While fuzzy logic helps provide context, outdoor power-line corridors face specific challenges. Factors like foliage, wildlife, and weather effects—such as fog, rain, and heatwaves—can lead to false positives or reduce detection. Putting more emphasis on these environmental factors and their solutions would make the method better.
- **Explainability and operator trust:** Fuzzy logic provides clarity, but deep-learning components can still act as black boxes. In critical infrastructure security, trust, responsibility, and clarity are crucial.
- **Full-scale deployment and long-term monitoring:** The scope does not cover full-scale field deployment or long-term monitoring. While this makes sense, moving to the real world is a future step that should be clearly planned.

  Overall, the methodology is solid and meets the objectives. However, achieving real-world deployment needs more focus on data realism, hardware durability, system scalability, and operational limits.

Gaps, Challenges and Future Research Directions.
Based on the literature review and the thesis proposal, several gaps and directions to be followed in the future are identified:

Access to annotated thermal information to detect intrusion: Numerous investigations are devoted to fault detection (hot spots, overhead line defects) and not unauthorized human presence. There are no custom datasets in this direction.

Adaptation to new environmental situations: The outdoor situation (fog, heat haze, vegetation growth, animal movement) lowers the thermal difference and could affect the detection/classification. The models should have domain-adaptation, lifelong learning, and powerful pre-processing.
Hardware, connection in remote corridors: In remote corridors, energy supply (solar), network connectivity (LoRa, GSM), device durability, thermal camera calibration and maintenance can be practiced.
Connection to bigger grid-security systems: Surveillance is not the only component - should be linked to dispatch, maintenance process, geospatial displays, incident reporting and operator interfaces.
Explainability and operation of human in the loop: Autonomous systems users still should be able to understand, validate and respond to alerts. There will be significance to human-machine teaming and accountability.
Cyber-security and privacy: Infrared surveillance systems that are installed in the open or semi-opened areas bring up privacy and data security issues. The two types of threats (physical intrusion and cyber intrusion) overlap.
Field tests and validation: Lab/simulation-controlled results are promising--but field tests (at the limited number of tower spans of interest) at the long times will be a test of maturity of the system, rates of false alarms, maintenance overhead and values of real response.

CONCLUSION

The paper outlines a strong and timely and academically sound method of power-transmission infrastructure security through the use of an AI-powered thermal surveillance system. It shows its sound compatibility with the state-of-the-art research (IR thermal imaging, AI object detection, edge computing) and offers its novel contribution, namely, a combination of fuzzy-logic threats classification and the deployment of metadata-enabled alerting within a power-line security setting.

Although simulation-based at present, the study provides the foundational base to implementation in the field in the future, and in case of success, which would immensely increase utility-grid stability and security- especially in remote or under-observed areas. By filling the mentioned gaps (data realism, environmental robustness, hardware constraints), this work will be taken to the next level and ready to be published and operated effectively.

References

1. Tsehay Admassu Assegie, An optimized KNN model for signature-based malware detection, Int. J. Comput. Eng. Res. Trends 8 (2021) 46–49.
2. S.A. M, P. G, A survey on various intrusion detection system tools and methods in cloud computing, in: 6th International Conference on Computing for Sustainable Global Development (INDIACom), 2019, pp. 439–445.
3. Govindraj Chittapur, S. Murali, Basavaraj S. Anami, Copy create video forgery detection techniques using frame correlation difference by referring SVM classifier, Int. J. Comput. Eng. Res. Trends 6 (2019) 4–8.
4. Adel Binbusayyis, Haya Alaskar, Thavavel Vaiyapuri, M. Dinesh, An investigation and comparison of ML approaches for intrusion detection in IoMT network, J. Supercomput. 78 (2022) 17403–17422.
5. Mesut Ugurlu, ˘ Alper Dogru ˘ ˙ Ibrahim, A survey on DL based intrusion detection system, in: 2019 4th International Conference on Computer Science and Engineering (UBMK), 2019, pp. 223–228, https://doi.org/10.1109/ UBMK.2019.8907206.
6. Arwa Aldweesh, Abdelouahid Derhab, Ahmed Z. Emam, DL approaches for anomaly-based intrusion detection systems: a survey, taxonomy, and open issues, Knowl. Base Syst. 189 (2020), 105124.
7. Ferrag, Mohamed Amine, Leandros Maglaras, Sotiris Moschoyiannis, Helge Janicke, DL for cyber security intrusion detection: approaches, datasets, and comparative study, J. Inf. Secur. Appl. 50 (2020), 102419.
8. Al Garadi, Mohammed Ali, Amr Mohamed, Abdulla Khalid Al-Ali, Xiaojiang Du, Ihsan Ali, Mohsen Guizani, A survey of machine and DL methods for internet of things (IoT) security, IEEE Commun. Surv. & Tutor. 22 (2020) 1646–1685.

9. Zeeshan Ahmad, Adnan Shahid Khan, Wai Shiang Cheah, Johari Abdullah, Farhan Ahmad, Network intrusion detection system: a systematic study of ML and DL approaches, Transactions on Emerging Telecommunications Technologies 32 (2021), e4150.
10. Michael W. Berry, Supervised and Unsupervised Learning for Data Science, Springer International Publishing USA, 2019.
11. Huaglory Tianfield, Data mining based cyber-attack detection, Syst. simul. technol. 13 (2017).
12. A. Ponmalar, V. Dhanakoti, An intrusion detection approach using ensemble support vector machine-based chaos game optimization algorithm in big data platform, Appl. Soft Comput. 116 (2022), 108295.
13. Monika Vishwakarma, Nishtha Kesswani, A new two-phase intrusion detection system with Naïve Bayes ML for data classification and elliptic envelop method for anomaly detection, Decision Analytics Journal 7 (2023), 100233, https://doi.org/ 10.1016/j.dajour.2023.100233.
14. Wenchao Li, Ping Yi, Yue Wu, Li Pan, Jianhua Li, New intrusion detection system based on KNN classification algorithm in wireless sensor network, Journal of Electrical and Computer Engineering 1752 (2021) 1–8.
15. B.S. Sharmila, Nagapadma Rohini, Intrusion detection system using naive bayes algorithm, in: 2019 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE), IEEE, 2019, pp. 1–4.
16. Subhash Waskle, Lokesh Parashar, Upendra Singh, Intrusion detection system using PCA with random forest approach, Int. Conf. Electron. Sustain. Commun. Syst. (ICESC) (2020) 803–808.
17. Razan Abdulhammed, Miad Faezipour, Abdelshakour Abuzneid, Alessa Ali, Effective features selection and ML classifiers for improved wireless intrusion detection, in: 2018 International Symposium on Networks, Computers and Communications (ISNCC), IEEE, 2018, pp. 1–6. T. Sowmya and E.A. Mary Anita Measurement: Sensors 28 (2023) 100827 13
18. S. Ganapathy, K. Kulothungan, P. Yogesh, A. Kannan, A novel weighted fuzzy C–means clustering based on immune genetic algorithm for intrusion detection, Procedia Eng. 38 (2012) 1750–1757.
19. Partha Sarathi Bhattacharjee, Md Fujail Abul Kashim, Shahin Ara Begum, A comparison of intrusion detection by K-means and fuzzy C-means clustering algorithm over the NSL-KDD dataset, in: 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), IEEE, 2017, pp. 1–6.
20. K. Samunnisa, G. Sunil Vijaya Kumar, K. Madhavi, Intrusion detection system in distributed cloud computing: hybrid clustering and classification methods, Measurement: Sensors 25 (2023), 100612.
21. Md Moin Uddin Chowdhury, Frederick Hammond, Glenn Konowicz, Chunsheng Xin, Hongyi Wu, Li Jiang, A few-shot DL approach for improved intrusion detection, in: 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), 2017, pp. 456–462.

22. Wen-Hui Lin, Hsiao-Chung Lin, Ping Wang, Bao-Hua Wu, Jeng-Ying Tsai, Using convolutional neural networks to network intrusion detection for cyber threats, in: 2018 IEEE International Conference on Applied System Invention (ICASI), IEEE, 2018, pp. 1107–1110.
23. Ishfaq Manzoor, Neeraj Kumar, A feature reduced intrusion detection system using ANN classifier, Expert Syst. Appl. 88 (2017) 249–257.
24. Wen-Hui Lin, Hsiao-Chung Lin, Ping Wang, Bao-Hua Wu, Jeng-Ying Tsai, Using convolutional neural networks to network intrusion detection for cyber threats, in: 2018 IEEE International Conference on Applied System Invention (ICASI), IEEE, 2018, pp. 1107–1110.
25. B. Riyaz, Sannasi Ganapathy, A DL approach for effective intrusion detection in wireless networks using CNN, Soft Comput. 24 (2020) 17265–17278.
26. Pengju Liu, An intrusion detection system based on convolutional neural network, in: Proceedings of the 2019 11th International Conference on Computer and Automation Engineering, 2019, pp. 62–67.
27. Sanchit Nayyar, Sneha Arora, Maninder Singh, Recurrent neural network based intrusion detection system, in: 2020 International Conference on Communication and Signal Processing (ICCSP), 2020, pp. 136–140, https://doi.org/10.1109/ICCSP48568.2020.9182099.
28. S. Sivamohan, S.S. Sridhar, S. Krishnaveni, An effective recurrent neural network (RNN) based intrusion detection via bi-directional long short-term memory, in: 2021 International Conference on Intelligent Technologies (CONIT), IEEE, 2021, pp. 1–5.
29. Chuanlong Yin, Yuefei Zhu, Jinlong Fei, Xinzheng He, A DL approach for intrusion detection using recurrent neural networks, IEEE Access 5 (2017) 21954–21961.
30. Soroush M. Sohi, Jean-Pierre Seifert, Ganji Fatemeh, RNNIDS: enhancing network intrusion detection systems through DL, Comput. Secur. 102 (2021), 102151.
31. M. Al-Zewairi, S. Almajali, A. Awajan, Experimental evaluation of a multi-layer feed-forward artificial neural network classifier for network intrusion detection system, in: 2017 International Conference on New Trends in Computing Sciences (ICTCS), 2017, pp. 167–172, https://doi.org/10.1109/ICTCS.2017.29.
32. Feng Jiang, Yunsheng Fu, Brij B. Gupta, Yongsheng Liang, Seungmin Rho, Fang Lou, Fanzhi Meng, and Zhihong Tian. DL based multi-channel intelligent attack detection for data security, IEEE trans. Sustain. Comput. 5 (2018) 204–212.
33. F. Farahnakian, J. Heikkonen, A Deep Auto-Encoder Based Approach for Intrusion Detection System, 2018 20th International Conference on Advanced Communication Technology (ICACT), 2018, pp. 178–183, https://doi.org/10.23919/ICACT.2018.8323688.
34. Pengzhou Cheng, Mu Han, Gongshen Liu, DESC-IDS: towards an efficient real-time automotive intrusion detection system based on deep evolving stream clustering, Future Generat. Comput. Syst. 140 (2023) 266–281.

35. Jielun Zhang, Fuhao Li, Feng Ye, An ensemble-based network intrusion detection scheme with bayesian DL, in: ICC 2020-2020 IEEE International Conference on Communications (ICC), 2020, pp. 1–6.
36. Xianwei Gao, Chun Shan, Changzhen Hu, Zequn Niu, Zhen Liu, An adaptive ensemble ML model for intrusion detection, IEEE Access 7 (2019) 82512–82521.