Quest Journals
Journal of Software Engineering and Simulation
Volume 9 ~ Issue 2 (2023) pp: 01-08
ISSN(Online) :2321-3795 ISSN (Print):2321-3809
www.questjournals.org

Research Paper

Prevention of False Data Injection in Dataset Using Ml and Dl

A. Prakash[#1], Gokuladharshani.R[*2], Lakshmibharathi.S[*3], Nandhini Bagavane.N[*4]

[#1]*Assistant Professor (Department of CSE)*
[*2,3,4]*Students (Department of CSE)*
Department Of Computer Science and Engineering
Sri Manakula Vinayagar Engineering College

Abstract—IoT is an interconnected and allotted network of embedded systems communicating through wired and wireless communication technology. It is defined as network of physical objects or things empowered with limited computation storage and conversation capabilities as well as embedded with electronics (sensors and actuators). Nowadays there are literally masses of hundreds of Internet of things (IoT) gadgets easily available to the customers. those consist of security cameras, smart home and smart speaker systems, smart toys and infant monitors, drones, domestic appliances, routers and internet gateways, and basically some other hardware products which can transmit information and be controlled over the net. FDIA is an attack this will result in a catastrophic outcomes. False information injection attack can be executed in each dynamic and static datasets, as a present device we easily discover and prevent in a static environment. in which with the present machine even the dynamic records is made static after which detects FDIA's. FDIA in a static environment is the existing machine, in which we seek to have few solutions for the FDIA in a dynamic environment or for time collection information. So, to enhance protection in dynamic environment is our proposed challenge towards FDIA and we create a brand-new version known as "PdD" model – Predictive Dynamic version. Proposed framework performs crucial role in live streaming records in terms of heterogeneous environment (dynamic nature). So, we use GRU set of rules because it offers better RMSE value than different AI algorithms. This detects every time there may be a few FDI attack.

Keywords— *Internet Of Things; False Data Injection Attack; Gated Recurrent Unit; Predictive Dynamic Model; Root Mean Square Error*

Received 05 Feb., 2023; Revised 13 Feb., 2023; Accepted 15 Feb., 2023 © The author(s) 2023. Published with open access at www.questjournals.org

I. INTRODUCTION

The recent development in communication technology, including the internet of things (IoT), has remarkably transcended the conventional sensing of surrounding environments. IoT technology can enable modernisations that enhance life high-quality and feature the capability to gather, quantify and recognize the surrounding environments. This case simplifies the new communication forms among things and human beings and thus enables the realisation of clever cities. IoT is one of the quickest rising fields within the history of computingwith a predicted 50 billion devices via the quit of 2020. On the one hand, IoT technology play a critical role in improving actual-existence smart applications, including smart healthcare, smart homes, smart transportation and smart education. Alternatively, the crosscutting and huge-scale nature of IoT systems with various components involved in the deployment of such structures have introduced new safety challenges. IoT structures are complicated and contain integrative arrangements. Therefore, retaining the safety requirement in a huge-scale attack surface of the IoT device is challenging. Solutions have to include holistic considerations to meet the safety requirement. but, IoT devices usually work in unattended surroundings. Therefore, an intruder may also physically access these gadgets. IoT gadgets are related commonly over wireless networks where an outsider may also get entry to personal facts from a communication channel through eavesdropping. IoT devices cannot support complex security systems given their restricted computation and energy sources. Smart structures are pushed through a combination of three things:

- Sensors and Actuators
- Connectivity
- People and Process

complex security systems of the IoT are due to not simplest limited computation, conversation and power sources but also sincere interaction with a physical area, especially the behaviour of a physical environment in unanticipated and unpredictable modes, because the IoT device is likewise part of a cyber-physical device; autonomously, IoT systems must constantly adapt and continue to exist in a particular and predictable manner with protection as a key priority, especially in settings in which threatening situations, such as in fitness systems, might occur. Furthermore, new attack surfaces are introduced by using the IoT surroundings. Such attack surfaces are caused by the interdependent and interconnected environments of the IoT. therefore, the security is at higher hazard in IoT systems than in other computing systems, and the traditional answer may be ineffective for such systems applying present security protection mechanisms, as an example encryption, authentication, access control, network safety and application security, is hard and insufficient for big systems with several related devices, with each a part of the device having inherent vulnerabilities. For instance, 'Mirai' is a high-quality type of botnets that has lately caused massive-scale DDoS attacks by using exploiting IoT gadgets. Current security mechanisms need to be enhanced to match the IoT ecosystem. Machine studying and deep studying (ML/DL) are powerful methods of information exploration to research about 'ordinary' and 'unusual' behaviour according to how IoT components and devices interact with each other within the IoT environment. This classifies the solution for the injection of false data into the dataset and Butterfly effect of ML and DL.

II. LITERATURE SURVEY

[1] A comprehensive review of the uses of ML & DL and an extensive list of issues, challenges related to securing
IOT systems.

[2]An extensive list of features and challenges to use ML & DL in effectively securing IOT systems and a novel attack detection approach is defined.

[3] A review of different framework models (network model and danger model) that are related to 5G connected IOT space.

[4] A novel training algorithm for better tuning the parameters of the DCNN to accurately detect intrusion in IOT networks

[5] A preliminary exploration of IPSec man-inthe-middle attack detection

[6] The three algorithms are experimented and it is derived that based on the results, the GRU algorithm is found to be the most efficient algorithm among the three

[7] An alternative domestic network hierarchy where IOT devices are isolated in a separate VLAN which shows a WireGuard VPN-based remote access solution to control IOT device from outside the home

[8] The study makes use of keys and timestamps to confirm hubs and messages exchanged.
Authentication and
Identification of IOT devices is also provided

[9] A review of the most critical aspects of IOT with specific focus on the security issues and challenges involved with IOT devices

[10] An approach to provide confidential communication between sender and receiver. The method also includes revocation of keys if misused is also detected

III.SYSTEM STUDY

A. FDIA

FDIA is false data injection attack where hackers or attackers delete or modify data within the dataset, therefore it may lead to some catastrophic results. In false data injection attack(FDIA) an attackerstealthilycompromises measurements from IoT sensors (by using a completely small margin), such that the manipulated sensor measurements bypass the sensor's fundamental 'faulty data' detection mechanism and propagates to the sensor

output undetected. FDI attacks have already triggered many recognized disastrous incidents, along with the Northeast blackout of 2003 in the America and the Ukrainian energy grid attack affecting over 230,000 people, leaving them without electricity for several hours delay of timely maintenance and lead to mid-air engine failures which are catastrophic.

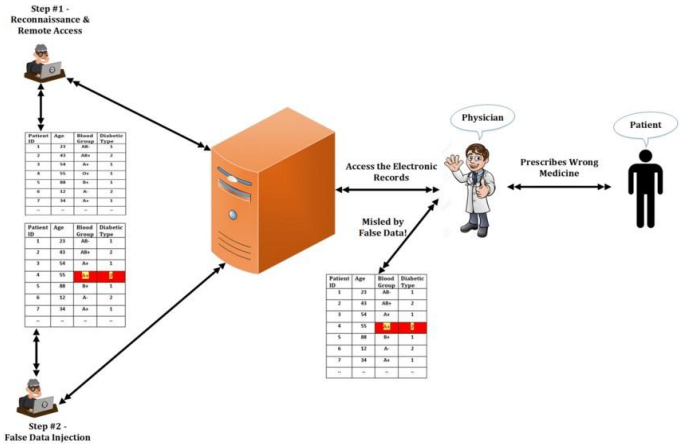

Figure 1. FDIA

We have two types of FDI Attacks:

- Continuous FDIA
- Interim FDIA

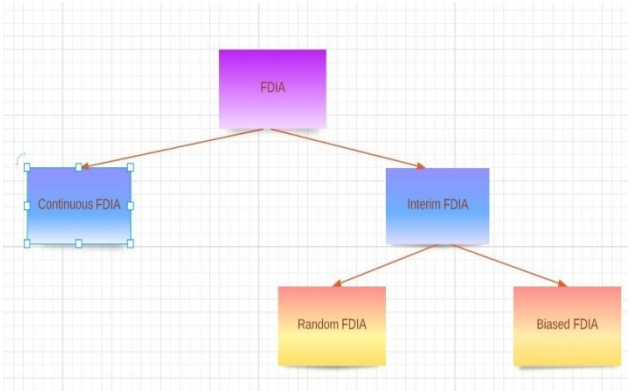

Figure 2. Types of false datainjection attacks

In the case of continuous FDIA, the attack is continuous, which means, once the attack begins, from that factor onward all the sensor readings are compromised. in the case of meantime FDIA, the duration of attack is a short time interval. In evaluation, hacking the sensor information communication hyperlinks and data processing applications is an easier option for an attacker.

[11] LIMITATIONS OF EXISTING SYSTEM

IV.PROCEDURE FOR PAPER SUBMISSION

Major problem in this existing system is that data inside the dataset are homogeneous in natures this is the information collected which are static in nature; they are no longer that flexible to locate FDIA in heterogeneous environment.

B. PROPOSED SYSTEM

We use a version called “PdD” version in which this version will resolve the issue faced by using the existing system. right here we have an algorithm called “GRU “set of rules (GRU – gated recurrent unit). GRU primarily based version predicts the final useful life (RUL)2 maximum appropriately. those IoT sensors display unique parameters and send out alerts to the respective server operator if the RUL is approaching its quit of lifestyles. device employs PdD systems to predict the RUL using the facts collected from the IoT sensors. these sensors send time-collection data (cycles) each hour to the neighborhood storage like database. After every information are captured, the data is transmitted to the ground station / server. on the floor station / server, the

incoming stay facts is saved inside the database and sent to the PdD system to predict RUL of the engine. The PdD system sends out indicators if the expected RUL is much less than the permissible secure operation RUL. assume that education records have N device of the identical make and type that provide failure data, and every device offers set multivariate time-series facts from the sensors of the device. Additionally, assume that there are r sensors of the identical type on each device. Then statistics collected from each system may be represented in a matrix. The GRU is an improved model of well-known recurrent neural networks. Similar to the LSTM unit, the GRU has gating devices that modulate the flow of information, but without having a separate memory mobile. GRUs was shown to exhibit even better performance on certain smaller datasets. The memory block of GRU is easier than that of LSTM. The neglect, input and output gates are replaced with an update and a reset gate.

$zt = \sigma(Wz \cdot [ht-1, xt] + bz)$,---------- (1)
$rt = \sigma(Wr \cdot [ht-1, xt] + br)$,----------(2)
$eht = act(W \cdot [rt * ht-1, xt] + bh)$,---- (3)
$ht = (1 - zt) * ht-1 + zt * eht$,----------(4)

where zt and rt are the update gate and reset gate at time t, respectively.eht is a temporary value to make new hidden state at time t.

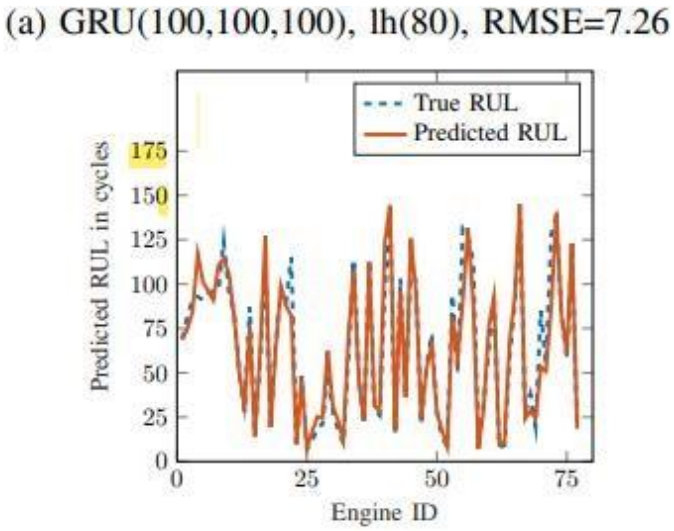

Figure 3. GRU Algorithm Prediction

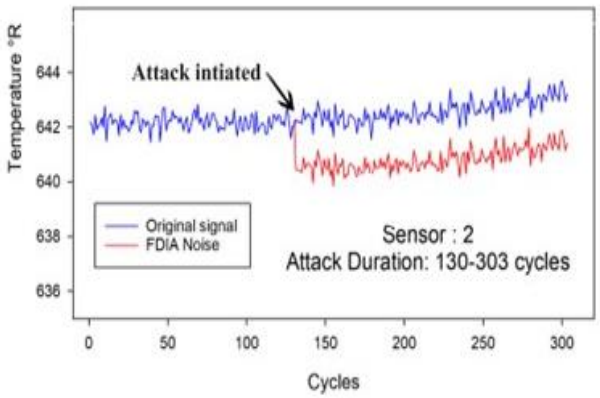

Figure 4. Continuous FDIA Signature

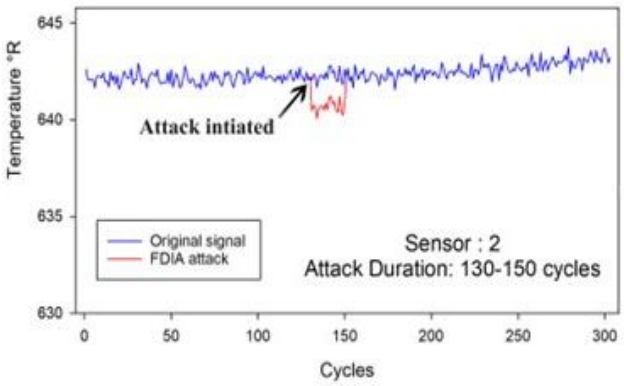

Figure 5. Interim FDIA Signature

Data Analysts might not be able to distinguish between fake and valid readings. This alert explores the opportunity of injecting false data into IoT sensor readings which are transmitted to evaluate the overall performance of the predictors, we utilize the root mean square error (RMSE) metric that is widely used as an assessment metric in version evaluation research. From the figure 3, we can recognize how is the prediction of GRU coincides with the real actual value of RUL.

C. PROPOSED ARCHITECTURE

At the beginning the raw information is collected by using the respective sensors located inside the environment. The sensors used to detect the minute modifications inside the physical environment, this collected data in a dataset, where data cleaning and analysis is completed, and then the collected records receives into the PdD version where it detects the FDI attack within the collected information. when we use this false data that's injected or modified or deleted data may also cause various issues in a larger scale. Therefore, before training the bots or machines blindly, we use this model PdD version to detect the opportunity of false facts injection within the collected information, that's we validate the data collected before using it. right here the Gated Recurrent Unit (GRU) set of rules has three segments or three layers where every contains a few 100s of nodes present, after the data is checked three times the results are decided via the "PdD model".

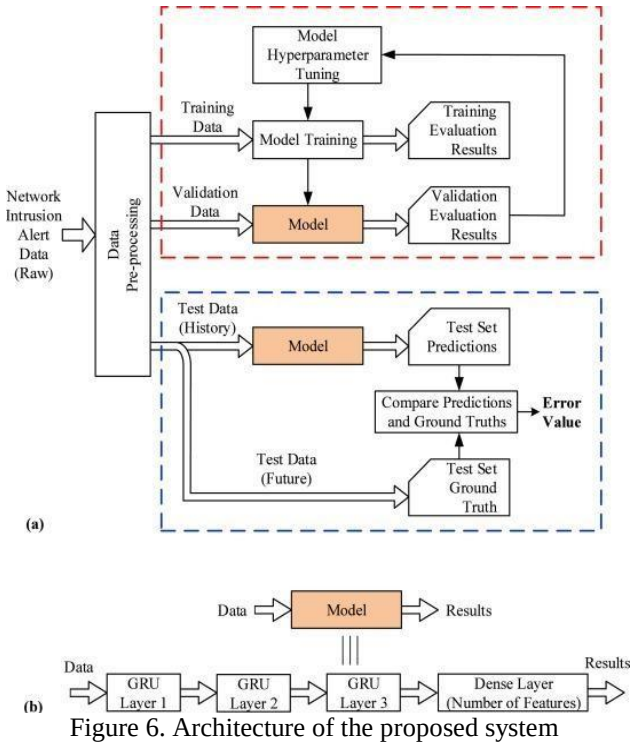

Figure 6. Architecture of the proposed system

V.HARDWARE REQUIREMENTS

1. Raspberry pi 4
2. Bread board
3. Jumper wires
4. Sensors
5. Buzzers
6. Radio transceiver
7. Connectivity

VI.SOFTWARE REQUIREMENTS

PROGRAMMING LANGUAGE

Python3: Python is a high-level, general-reason programming language. Its design philosophy emphasizes code readability with the use of considerable indentation. Python is dynamically-typed and rubbish-gathered. It supports multiple programming paradigms, including established, item-orientated and functional programming.

LIBRARY

Tensorflow: TensorFlow can teach and run the deep neural networks for image recognition, handwritten digit classification, recurrent neural network, phrase embedding, natural language processing, video detection, and many more. TensorFlow is run on more than one CPUs or GPUs and also cellular running systems.

VII.CONCLUSION

IoT safety and privacy are of paramount significance andplay a pivotal function in the commercialization of the IoTtechnology. Traditional security and privacy solutions sufferfrom a number of problems which might be related to thedynamic natureof the IoT networks. ML and more specially DL techniquesmay be used to allow the IoT devices to adapt to their dynamicsurroundings. The PdD model can help self-organizingoperation and also optimize the overall device performanceby using learning and processing statistical data from theenvironment (e.g., human users and IoT devices). Therefore, todiscover the fake data injection attack (FDIA) in aheterogeneous environment, using this "PdD model "withthe GRU set of rules is plenty efficient. As we've betterRMSE score than other AI algorithms.

REFERENCES

[1] O. Novo, N. Beijar, and M. Ocak, "Capillary Networks - Bridging the Cellular and loT Worlds," IEEE World Forum on Internet of Things (WF-IoT), vol. 1, pp. 571–578, December 2015.

[2] F. Hussain, Internet of Things; Building Blocks and Business Modles. . Springer, 2017.

[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys Tutorials, vol. 17, pp. 2347–2376, Fourthquarter 2015.

[4] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the internet of things: A survey of existing protocols and open research issues," IEEE Communications Surveys Tutorials, vol. 17, pp. 1294–1312, thirdquarter 2015.

[5] A. Mosenia and N. K. Jha, "A comprehensive study of security of internet-of-things," IEEETransactions on Emerging Topics in Computing, vol. 5, pp. 586–602, Oct 2017.

[6] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," IEEE Internet of Things Journal, vol. 4, pp. 1125–1142, Oct 2017.

[7] M. Ammar, G. Russello, and B. Crispo, "Internet of things: A survey on the security of iot frameworks," Journal of Information Security and Applications, vol. 38, pp. 8 – 27, 2018.

[8] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," IEEE Communications Surveys Tutorials, vol. 20, pp. 3453–3495, Fourthquarter 2018.

[9] F. Restuccia, S. DOro, and T. Melodia, "Securing the internet of things in the age of machine learning and software-defined networking," IEEE Internet of Things Journal, vol. 5, pp. 4829–4842, Dec 2018.

[10] K. A. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of things: A survey on machine learningbased intrusion detection approaches," Computer Networks, vol. 151, pp. 147 – 157, 2019.

[11] J. Hou, L. Qu, and W. Shi, "A survey on internet of things security from data perspectives," Computer Networks, vol. 148, pp. 295 – 306, 2019.

[12] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," Computer Networks, vol. 141, pp. 199 – 221, 2018.

[13] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: A survey," Journal of Network and Computer Applications, vol. 88, pp. 10 – 28, 2017.

[14] B. B. Zarpelo, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in internet of things," Journal of Network and Computer Applications, vol. 84, pp. 25 – 37, 2017.

[15] M. binti Mohamad Noor and W. H. Hassan, "Current research on internet of things (iot) security: A survey," Computer Networks, vol. 148, pp. 283 – 294, 2019.

[16] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the internet of things," Ad Hoc Networks, vol. 32, pp. 17 – 31, 2015. Internet of Things security and privacy: design methods and optimization.

[17] K. Sha, W. Wei, T. A. Yang, Z. Wang, and W. Shi, "On security challenges and open issues in internet of things," Future Generation Computer Systems, vol. 83, pp. 326 – 337, 2018.

[18] M. Tao, K. Ota, M. Dong, and Z. Qian, "Accessauth: Capacity-aware security access authentication in federated-iot-enabled v2g networks," Journal of Parallel and Distributed Computing, vol. 118, pp. 107 – 117, 2018.

[19] I. Farris, T. Taleb, Y. Khettab, and J. Song, "A survey on emerging sdn and nfv security mechanisms for iot systems," IEEE Communications Surveys Tutorials, vol. 21, pp. 812– 837, Firstquarter 2019.

[20] M. at. el, "Machine Learning for Internet of Things Data Analysis:A Survey ," Journal of Digital Communications and Networks, Elsevier, vol. 1, pp. 1–56, Feburary 2018.

[21] M. at. el, "Machine Learning for Internet of Things Data Analysis:A Survey ," Journal of Digital Communications and Networks, Elsevier, vol. 1, pp. 1–56, Feburary 2018.

[22] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," IEEE Internet of Things Journal, vol. 4, pp. 1250–1258, Oct 2017.

[23] A. Chowdhury and S. A. Raut, "A survey study on internet of things resource management," Journal of Network and Computer Applications, vol. 120, pp. 42 – 60, 2018. [23] P. Asghari, A. M. Rahmani, and H. H. S. Javadi, "Internet of things applications: A systematic review," Computer Networks, vol. 148, pp. 241 – 261, 2019. 27.

[24] D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for internet of things: A survey," Journal of Network and Computer Applications, vol. 66, pp. 198 – 213, 2016.

[25] J. Guo, I.-R. Chen, and J. J. Tsai, "A survey of trust computation models for service management in internet of things systems," Computer Communications, vol. 97, pp. 1 – 14, 2017.

[26] V. Gazis, "A survey of standards for machine-to-machine and the internet of things," IEEECommunications Surveys Tutorials, vol. 19, pp. 482–511, Firstquarter 2017.

[27] E. Ahmed, I. Yaqoob, A. Gani, M. Imran, and M. Guizani, "Internetof-things-based smart environments: state of the art, taxonomy, and open research challenges," IEEE Wireless Communications, vol. 23, pp. 10–16, October 2016.

[28] S. B. Baker, W. Xiang, and I. Atkinson, "Internet of things for smart healthcare: Technologies, challenges, and opportunities," IEEE Access, vol. 5, pp. 26521–26544, 2017.

[29] F. Javed, M. K. Afzal, M. Sharif, and B. Kim, "Internet of things (iot) operating systems support, networking technologies, applications, and challenges: A comparative review," IEEE Communications Surveys Tutorials, vol. 20, pp. 2062–2100, thirdquarter 2018.

[30] A. olakovi and M. Hadiali, "Internet of things (iot): A review of enabling technologies, challenges, and open research issues," Computer Networks, vol. 144, pp. 17 – 39, 2018.

[31] P. Bangalore and L. B. Tjernberg, "An approach for self evolving neural network based algorithm for fault prognosis in wind turbine," in 2013 IEEE Grenoble Conference. IEEE, 2013, pp. 1–6.

[32] S. Simani, S. Farsoni, and P. Castaldi, "Fault tolerant control of an offshore wind turbine model via identified fuzzy prototypes," in 2014 UKACC International Conference on Control (CONTROL). IEEE, 2014, pp. 486–491.

[33] M. Canizo, E. Onieva, A. Conde, S. Charramendieta, and S. Trujillo, "Real-time predictive maintenance for wind turbines using big data frameworks," in 2017 IEEE International Conference on Prognostics and Health Management (ICPHM). IEEE, 2017, pp. 70–77.

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

[35] K. Cho, B. Van Merrienboer, D. Bahdanau, and Y. Bengio, "On the ¨ properties of neural machine translation: Encoder-decoder approaches," arXiv preprint arXiv:1409.1259, 2014.

[36] R. Zhao, D. Wang, R. Yan, K. Mao, F. Shen, and J. Wang, "Machine health monitoring using local feature-based gated recurrent unit networks," IEEE Transactions on Industrial Electronics, vol. 65, no. 2, pp. 1539–1548, 2017.

[37] A. Bhandare, M. Bhide, P. Gokhale, and R. Chandavarkar, "Applications of convolutional neural networks," International Journal of Computer Science and Information Technologies, vol. 7, no. 5, pp. 2206–2215, 2016.

[38] R. R. Swain and P. M. Khilar, "A fuzzy mlp approach for fault diagnosis in wireless sensor networks," in 2016 IEEE region 10 conference (TENCON). IEEE, 2016, pp. 3183–3188.

[39] T. Ince, S. Kiranyaz, L. Eren, M. Askar, and M. Gabbouj, "Realtime motor fault detection by 1-d convolutional neural networks," IEEE Transactions on Industrial Electronics, vol. 63, no. 11, pp. 7067–7075, 2016.

[40] E. Ramasso and A. Saxena, "Performance benchmarking and analysis of prognostic methods for cmapss datasets." International Journal of Prognostics and Health Management, vol. 5, no. 2, pp. 1–15, 2014.

[41] D. K. Frederick, J. A. DeCastro, and J. S. Litt, "User's guide for the commercial modular aero-propulsion system simulation (c-mapss)," 2007.

[42] N. O. Tippenhauer, C. Popper, K. B. Rasmussen, and S. Capkun, "On ¨ the requirements for successful gps spoofing attacks," in Proceedings of the 18th ACM conference on Computer and communications security. ACM, 2011, pp. 75–86.

[43] T. Giannetsos and T. Dimitriou, "Spy-sense: spyware tool for executing stealthy exploits against sensor networks," in Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy. ACM, 2013, pp. 7–12.

[44] B. Wang, Y. Lei, N. Li, and T. Yan, "Deep separable convolutional network for remaining useful life prediction of machinery," Mechanical Systems and Signal Processing, vol. 134, p. 106330, 2019.

[45] F. O. Heimes, "Recurrent neural networks for remaining useful life estimation," in 2008 international conference on prognostics and health management. IEEE, 2008, pp. 1–6.

[46] G. S. Babu, P. Zhao, and X.-L. Li, "Deep convolutional neural network based regression approach for estimation of remaining useful life," in International conference on database systems for advanced applications. Springer, 2016, pp. 214–228.

[47] S. Zheng, K. Ristovski, A. Farahat, and C. Gupta, "Long shortterm memory network for remaining useful life estimation," in 2017 IEEE International Conference on Prognostics and Health Management (ICPHM). IEEE, 2017, pp. 88–95.

[48] N. Gunnemann and J. Pfeffer, "Predicting defective engines using ¨ convolutional neural networks on temporal vibration signals," in First International Workshop on Learning with Imbalanced Domains: Theory and Applications, 2017, pp. 92–102.

[49] H. Bai, M. Atiquzzaman, and D. Lilja, "Wireless sensor network for aircraft health monitoring," in First International Conference on Broadband Networks. IEEE, 2004, pp. 748–750.

[50] X.-S. Si, W. Wang, C.-H. Hu, and D.-H. Zhou, "Remaining useful life estimation–a review on the statistical data driven approaches," European journal of operational research, vol. 213, no. 1, pp. 1–14, 2011.

[51] A. P. Verma, "Performance monitoring of wind turbines: a data-mining approach," 2012.

[52] Y. Guan and X. Ge, "Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks," IEEE Transactions on Signal and Information Processing over Networks, vol. 4, no. 1, pp. 48–59, 2017.

[53] S. Zheng, K. Ristovski, A. Farahat, and C. Gupta, "Long shortterm memory network for remaining useful life estimation," in 2017 IEEE International Conference on Prognostics and Health Management (ICPHM). IEEE, 2017, pp. 88–95.
[54] A. L. Ellefsen, E. Bjørlykhaug, V. Æsøy, S. Ushakov, and H. Zhang, "Remaining useful life predictions for turbofan engine degradation using semi-supervised deep architecture," Reliability Engineering & System Safety, vol. 183, pp. 240–251, 2019.
[55] R. Caponetto, F. Rizzo, L. Russotti, and M. Xibilia, "Deep learning algorithm for predictive maintenance of rotating machines through the analysis of the orbits shape of the rotor shaft," in International Conference on Smart Innovation, Ergonomics and Applied Human Factors. Springer, 2019, pp. 245–250.
[56] Y. Guan and X. Ge, "Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks," IEEE Transactions on Signal and Information Processing over Networks, vol. 4, no. 1, pp. 48–59, 2017.
[57] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," IEEE Transactions on Smart Grid, vol. 8, no. 4, pp. 1630–1638, 2016.
[58] A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, "A survey on sensor-based threats to internet-of-things (iot) devices and applications," arXiv preprint arXiv:1802.02041, 2018.
[59] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using kalman filter," IEEE transactions on control of network systems, vol. 1, no. 4, pp. 370–379, 2014.
[60] M. A. der Mauer, T. Behrens, M. Derakhshanmanesh, C. Hansen, and S. Muderack, "Applying sound-based analysis at porsche production: Towards predictive maintenance of production machines using deep learning and internet-of-things technology," in Digitalization Cases. Springer, 2019, pp. 79–97.