The Pharma Innovation Journal 2023; 12(3): 2775-2780

www.ThePharmaJournal.com

The Pharma Innovation

ISSN (E): 2277-7695
ISSN (P): 2349-8242
NAAS Rating: 5.23
TPI 2023; 12(3): 2775-2780

www.thepharmajournal.com
Received: 09-12-2022
Accepted: 14-01-2023

Khushwant Singh
University Institute of Engineering and Technology, MDU, Rohtak, Haryana, India

Dheerdhwaj Barak
Vaish College of Engineering, Rohtak, Haryana, India

Yudhvir Singh
University Institute of Engineering and Technology, MDU, Rohtak, Haryana, India

Corresponding Author:
Khushwant Singh
University Institute of Engineering and Technology, MDU, Rohtak, Haryana, India

Reviewing the IOT systems reliability and accuracy

Khushwant Singh, Dheerdhwaj Barak and Yudhvir Singh

Abstract
Internet of things (IoT) has been implemented in aviation predictive maintenance in recent years for the enhancement of better maintenance prediction, to reduce downtime, unnecessary maintenance actions, increase safety, increase system readiness, and refine the management process and to improve component design. The IoT system in predictive maintenance is very optimistic in gathering and analysing, predicting the component failures and to determine the remaining useful life of a systems. Since Remaining useful life of an system is defines as the length from the current time to the end of its useful life. Due to its futuristic increasing demand of IoT in aviation maintenance, the biggest challenge is to ensuring the reliability and accuracy of any specific IoT system allotted for monitoring aircraft components in the near future. Hence, this review paper clearly explains the challenges associated with IoT systems.

Keywords: IOT systems reliability, accuracy, reliability

Introduction
Predictive maintenance for aircraft is greatly aided by the Internet of Things "and artificial intelligence. In recent years, internet of things (IoT) has been used in aviation predictive maintenance for the improvement for better maintenance prediction, to decrease downtime and unnecessary maintenance operations, to promote safety, raise system readiness, and to improve component design. The aviation sector provides a variety of uses for the Internet of things. Thus it is essential to guarantee the IoT systems' accurate results and performance when synchronising with sophisticated computational devices in aeroplane components in order to lessen the obstacles associated with making predictions based on false negative and false positive data sets. As a result, the same may affect how accurately a component of an aircraft's remaining useful life is predicted. Using data-driven and model-driven methodologies, the remaining useful life prediction for aircraft systems and subsystems may be calculated. An aircraft component's remaining usable life can be predicted using theoretical approaches and prognostic algorithms, but validating the forecasts to assure their accuracy presents a significant difficulty [1]. Similar to this, damage evaluation and endurance predictions can be made using structural health monitoring with IoT systems. Real-time data can be acquired for the structural monitoring by using wireless sensor networks and dependable high-speed internet. Yet, offering a low-cost computing system in the midst of IoT systems developing maturity is a big difficulty [2, 3]. The intricacy that is encountered. By model-driven method verification, heterogeneous IoT systems QoS (Quality of service) is measured [4].
Since the proposed system will need to anticipate fewer or no false negatives in a demanding operating environment, data quality is essential when estimating a system or structure's remaining usable life [5]. The IoT system has a number of restrictions, including issues with security, service quality, receiving real-time data, and gathering data on a machine type's remaining useful life [6]. This section highlights the challenges faced by researchers using the various IoT platform-based methodologies for life prediction with high-quality, dependable data.

Challenges in IoT System reliability
The IoT System Reliability
Implementing a multilayer security system is the main challenge with heterogeneous devices, ranging from small low power to high range systems. Due to these heterogeneous networks' increased susceptibility to security threats and the transmission of fault information. So, any IoT system would come equipped with a standard mechanism to signal redundancy in the event of a failure or security breach [7].

The diverse multilayered infrastructure of the IoT system makes it more difficult to collect trustworthy data, which ultimately results in inaccurate remaining usable life projections. Anomaly data are generated and communicated as a result of the system's vulnerability, and in the worst circumstances they endanger human life [8]"

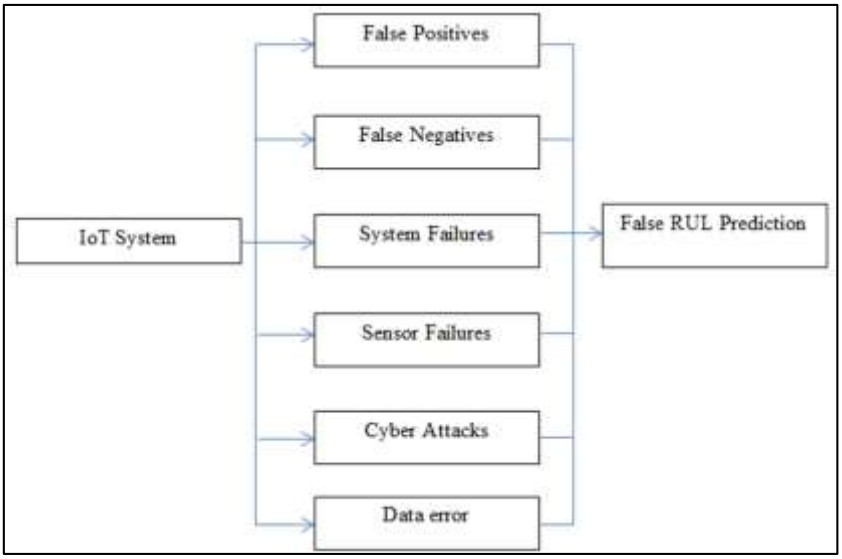

Fig 1: IoT fault syndromes leading to incorrect RUL

Challenges in Anomaly detection

"IoT systems operating on heterogeneous platforms must produce enormous amounts of data, necessitating the need of big compute. Anomaly detection is crucial for locating the problematic data in regular data sets when handling enormous amounts of data with powerful computational systems [9]. The primary challenges limiting anomaly identification and their potential sources are displayed in Table 1."

Table 1: Key Issues and Possible Causes in Anomaly Detection

Key Issues	Possible Causes
Incomplete	Incomplete
Data Points	External data from Environment
Encrypted Data	Protected Data
Sensor Error	Multilayered Sensors
Data Noise	Transmission system failure
Data Surge	Overload of Data

Equipment Reliability Challenges

"It is possible to meet the expectations of the equipment's creators and maintenance staff because of the equipment's dependability [10, 11]. By managing large amounts of data, IoT equipment and devices become challenging to optimise [12]. The efficiency of the hardware is crucial for the mathematical and computerized models built from the generated data. The dependability of such devices will be impaired, which will lower the data's quality and lead to inaccurate estimates of a component's remaining useful life [13]."

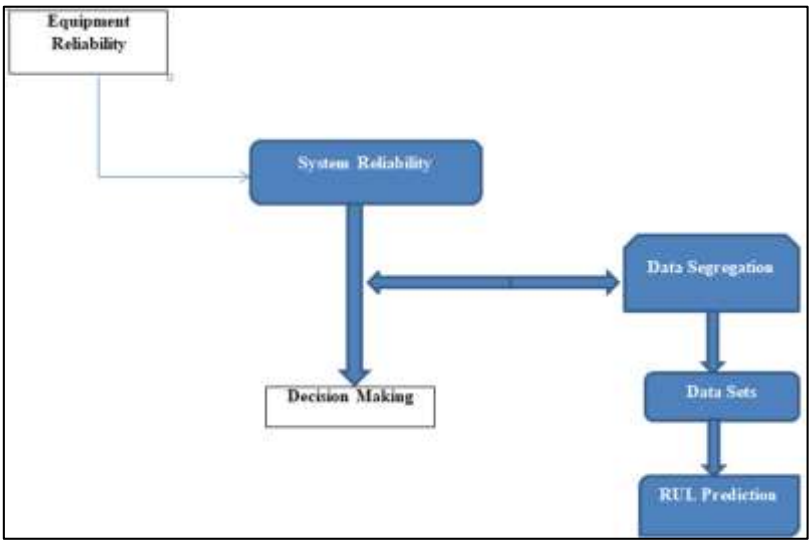

Fig 2: Scope of quipment Reliability where coloured boxes focus mainly on this review

Challenges in IoT Architecture

"The IoT system must deliver dependable output throughout its mission cycle due to its multilayered architecture [14–16]. Four primary levels are taken into account while discussing the architectural issues for the IoT system itself to demonstrate its dependability for producing the output [17, 18]. In other words, the Service layer, Support layer, Communication layer, and Perception layer are all parts of the same multilayered IoT architecture. Each layer of the design offers a unique set of functional failure circumstances, casting doubt on its dependability and producing misleading predictions [19, 20]. The support layer intended to work on FDEP (Functional Dependency), service switches, trigger switches, and in the modes of MTBF and MTTR, through which the availability of the system is measured [21, 22, 23], while the service layer intended to work on smart sensors to measure engine parameters like Exhaust gas temperature (EGT) and N1 compressor speed.

The perception layer presents difficulties in reliable monitoring in terms of sensor node failures to determine measurements like temperatures and humidity, which all provide False output or no output condition. The communication layers also pose problems with wireless communication, noisy data, attenuation of signals, and failures in the perception layer. The IoT architecture layers and potential failure mechanisms that might result in incorrect RuL Prediction are shown in Figure 3."

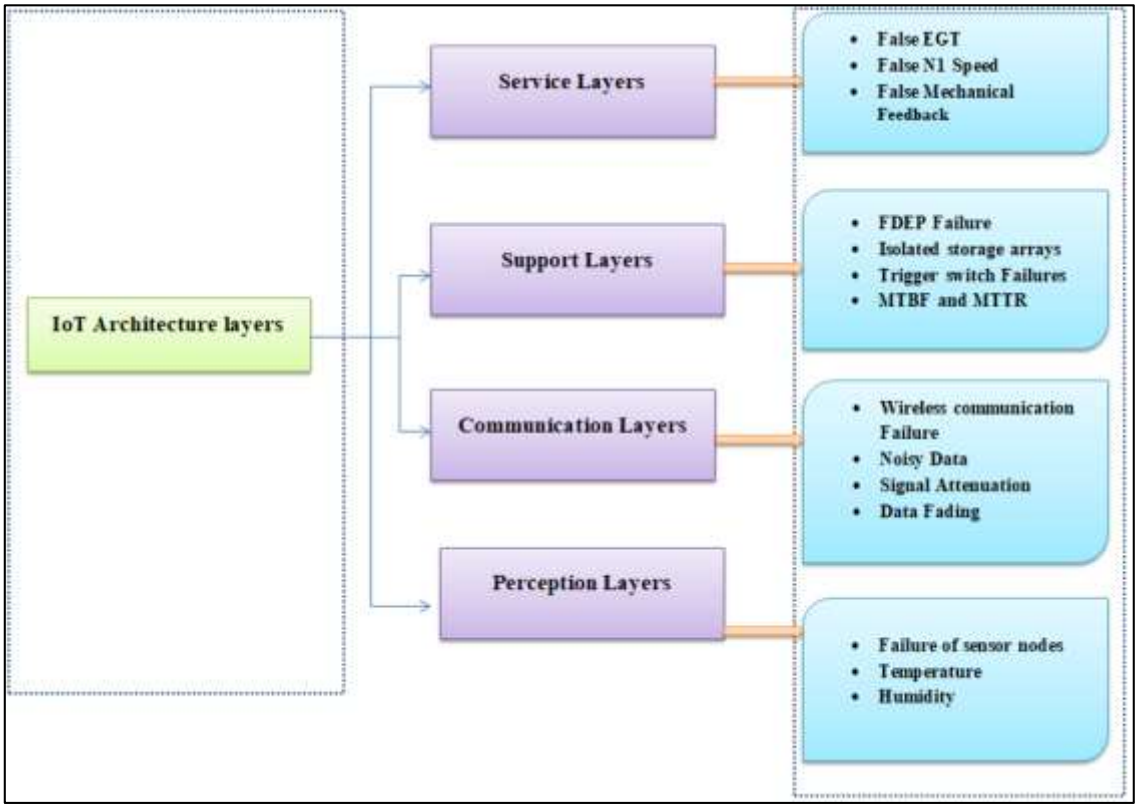

Fig 3: IoT Architecture and Possible failures

Performance Challenges

"The Heterogeneity of an IoT system will have the complexity and constraints on hardware and software which requires massive computational system which leads to noticeable degradation on the performance parameters in terms of High throughout, latency of the system, and accuracy of the data [24]. Specifically, the high accuracy requirement in the IoT system may affect the control aspects in case of unmanned air vehicle which affects the Ultra, Low and End to End latencies. Also the entire system would liable to provide unique complex challenges in terms of sensors [25, 26]. Table 2 Shows the specific possible causes which affects the performance efficiency of any Multilayered IoT Systems."

Table 2: Performance Affecting Parameter and Causes

Possible Causes	Performance affecting Parameters
Infeasible Raw Data	High Throughputs and frames
Communication Delay	Low Latencies
High accuracy Requirement	Control failure

Hardware Reliability Challenges

The Hardware non-reliability on the IoT system is highly susceptible due to non-quantification and evaluation of physical materials in the connected system. So the whole challenges create the necessity for prediction methodologies for assessing the hardware reliability. The Common methods are Physics of Failure (PoF) Prediction [30].

The Physics of Failure method is commonly used method which provides potential results for accurate prediction of RuL and mode of failure. Figure 5 Shows the steps involved in Physics of Failure (PoF)."

Fig 5: Steps involved in PoF Prediction

Challenges in Network Reliability

"The Major challenge in maintaining network reliability in the IoT Systems is very crucial where importantly Assessing QoS (Quality of Service) and Continuous Quantification should be considered. So always the user-friendly assessment and prediction technique should be assigned to evaluate the network efficiency of the system [30, 31]. Quantification of delay throughputs for QoS metric analysis is carried out to provide sufficient information on reliability of end to end IoT systems [32]. The QoS Profile generation which is linked with various components in the multi-layered system has been proposed for determination of latency and bandwidth [33]. The Statistical Modelling approach is carried out to calculate the QoS metrics like time consuming, time of response, and Repair times [34]. The Redundancy models were studied the infrastructure of Gateway and ISP redundancy [35]. The Various findings have been carried out by past researchers on assessing network reliability on the IoT systems. The Previous works carried out on Network reliability assessment will make a pathway for future researchers for selecting suitable and appropriate method for multi-layered systems.

System Security Challenges

The heterogeneous Multilayered IoT System will have more vulnerability for security attacks. To address this issues the IoT system design must be optimized to have important factors which includes Perfect Physical coupling, Communication, security, Scalability and Privacy requirements [36]. Especially various types of threats have been identified by previous researchers. Table 3 Shows the Summarized Literature review showing contribution of each works related to security attacks on the IoT System."

Table 3: Summarized Literature review showing contribution of Each Works related to Security Attacks on the IoT System

Contribution	Work	Findings
"Cyber-attacks	P. McDaniel *et al*. (2009) [37] A.O. Otuoze *et al*. (2018) [38] S. Goel *et al*. (2015) [39] V. Delgado-Gomes *et al*. [40]	Several Potential Cyber-attacks have been discussed through this works where Active and Passive attacks poses significant threats based on spy, eavesdrop and DoS
Spoofing Attacks	P. Pradhan *et al*. (2016) [41]	The Major Challenge in the IoT system is that susceptibility to the Spoofing attacks where GPS spoofing is due to high strength incorrect signals and ARP Spoofing is due to false messages linkage to MAC address of the hackers. The control protocol is affected which may mislead the network operating systems.
	P. Risbud *et al*. (2018) [42]	
Replay Attacks	J. Zhao *et al*. (2016) [43]	The Authenticity of the Information is highly intercepted due to replay attacks in the IoT systems. Those Incorrect information may lead to False RuL Prediction.
	T. Tran *et al*. (2013) [44]	
Smart Meter DoS Attacks	P. Yi *et al*. (2014) [45] C. Bekara *et al*. (2014) [46] Y. Guo *et al*. (2015) [47]	The Denial of Service attacks will large amount of replies and request packets which may leads to total system failure. The corrective action is achieved through integration of IoT devices in to Smart Grid.
Malware Attacks	E. Modiri Dovom *et al*. (2017) [48] P. Eder-Neuhauser *et al*. [49]	The malicious software is injected to the system which may cause interruptions or No service. The Communication layer of the IoT system is more prone to these attacks which may have to be Integrated for prevention."

Conclusion

To the greatest extent possible, this document will be able to illuminate the challenges associated with determining a part or system's remaining useful life utilising an IoT platform, "and it will also recommend the prerequisites and requirements that should be taken into account for any IoT infrastructure in the event of false data sets caused by sensor and system failure. The literature study also summarises the special difficulties brought on by the diverse IoT network. This covers issues with hardware dependability, problems with system reliability, issues with anomaly detection utilising IoT systems, issues with building the IoT architecture, issues with data registration and data segregation, issues with security, and more. Another significant problem is validating the chosen IoT model while taking various real-time elements into account, as addressed in chapter 3 of this work. The IoT model that is created for the forecast of remaining usable life primarily uses three ways: physics-based, hybrid, and data-driven approaches. The disadvantages that the researchers ran across while testing the model using these three distinct strategies are summarised in table 4 below. The difficulties are outlined in order to provide information on machine learning techniques that combine IoT systems for predicting remaining usable life.

We are certain that our evaluation will be able to provide academics the information they need to determine if IoT devices may be used for predictive maintenance in the aviation industry. The review's conclusion explains the difficulties multi-layered IoT systems face and encourages thinking about how those difficulties could have changed had they been there before the IoT Model was built. Hence, we firmly think that these considerations and information about

the design of the system and the performance of the specific model will ultimately minimise downtime and increase cost savings in aviation predictive maintenance".

References

1. Xiongzi C, Jinsong Y, Diyin T, Yingxun W. Remaining useful life prognostic estimation for aircraft subsystems or components: A review. In IEEE 2011 10th International Conference on Electronic Measurement & Instruments, 2011;2:94-98. IEEE.
2. Abdelgawad A, Yelamarthi K. Internet of things (IoT) platform for structure health monitoring. Wireless Communications and Mobile Computing; c2017.
3. Angadi A, Dias R, Bagali MU. An Aircraft Health Monitoring System using IOT. Indian Journal of Science and Technology. 2016;9(33):1-5.
4. Costa B, Pires PF, Delicato FC, Li W, Zomaya AY. Design and analysis of IoT applications: a model-driven approach. In 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), 2016, 392-399). IEEE.
5. The 5 step Roadmap to IoT-based Predictive Maintenance, how to leverage sensor data predictive analytics & Machine learning for more intelligent maintenance, Article Published by XM Pro, Inc. Agile Industrial IoT, Version 2.0.
6. Calabrese M, Cimmino M, Fiume F, Manfrin M, Romeo L, Ceccacci S, *et al.* SOPHIA: An event-based IoT and machine learning architecture for predictive maintenance in industry 4.0. Information. 2020;11(4):202.
7. Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems. 2018;82:395-411.
8. Moore SJ, Nugent CD, Zhang S, Cleland I. IoT reliability: a review leading to 5 key research directions. CCF Transactions on Pervasive Computing and Interaction; c2020. p. 1-17.
9. Sharma B, Sharma L, Lal C. Anomaly Detection Techniques using Deep Learning in IoT: A Survey. In 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE); c2019. p. 146-149. IEEE.
10. Bianchini A, Pellegrini M, Rossi J. Maintenance scheduling optimization for industrial centrifugal pumps. International Journal of System Assurance Engineering and Management. 2019;10(4):848-860.
11. Ustundag A, Cevikcan E. Industry 4.0: managing the digital transformation. Springer; c2017.
12. Lee CKM, Zhang SZ, Ng KKH. Development of an industrial Internet of things suite for smart factory towards re-industrialization. Advances in manufacturing. 2017;5(4):335-343.
13. SCHEER AW. Enterprise 4.0-From disruptive business model to the automation of business processes; c2019.
14. Kempf J, Arkko J, Beheshti N, Yedavalli K. March. Thoughts on reliability in the internet of things. In Interconnecting smart objects with the Internet workshop, 2011;1:1-4.
15. Han C, Jornet JM, Fadel E, Akyildiz IF. A cross-layer communication module for the Internet of Things. Computer Networks. 2013;57(3):622-633.
16. Palattella MR, Dohler M, Grieco A, Rizzo G, Torsner J, Engel T, *et al.* Internet of things in the 5G era: Enablers, architecture, and business models. IEEE Journal on Selected Areas in Communications. 2016;34(3):510-527.
17. Burhan M, Rehman RA, Khan B, Kim BS. IoT elements, layered architectures and security issues: A comprehensive survey. Sensors. 2018;18(9):2796.
18. Darwish D. Improved layered architecture for Internet of Things. Int. J Comput. Acad. Res. (IJCAR), 2015;4:214-223.
19. Frustaci M, Pace P, Aloi G, Fortino G. Evaluating critical security issues of the IoT world: Present and future challenges. IEEE Internet of things journal. 2017;5(4):2483-2495.
20. Xing L. Reliability in Internet of Things: Current status and future perspectives. IEEE Internet of Things Journal. 2020;7(8):6704-6721.
21. Gopalakrishnan M, Skoogh A, Salonen A, Asp M. Machine criticality assessment for productivity improvement. International Journal of Productivity and Performance Management; c2019.
22. Quijada Fumero P, Salunkhe O. Demonstration of real-time criticality assessment using a test-bed (Master's thesis); c2017.
23. Souza MLH, da Costa CA, de Oliveira Ramos G, da Rosa Righi R. A survey on decision-making based on system reliability in the context of Industry 4.0. Journal of Manufacturing Systems. 2020;56:133-156.
24. Bagchi S, Abdelzaher TF, Govindan R, Shenoy P, Atrey A, Ghosh P, *et al.* New Frontiers in IoT: Networking, Systems, Reliability, and Security Challenges. IEEE Internet of Things Journal. 2020;7(12):11330-11346.
25. Yick J, Mukherjee B, Ghosal D. Wireless sensor network survey. Computer networks. 2008;52(12):2292-2330.
26. Wang Q, Zhu Y, Cheng L. Reprogramming wireless sensor networks: challenges and approaches. IEEE network. 2006;20(3):48-55.
27. Habib A, Ghanma M, Morgan M, Al-Ruzouq R. Photogrammetric and LiDAR data registration using linear features. Photogrammetric Engineering & Remote Sensing. 2005;71(6):699-707.
28. Bellekens B, Spruyt V, Berkvens R, Penne R, Weyn M. A benchmark survey of rigid 3D point cloud registration algorithms. Int. J Adv. Intell. Syst. 2015;8:118-127.
29. Liu S, Tong X, Chen J, Liu X, Sun W, Xie H, *et al.* A linear feature-based approach for the registration of unmanned aerial vehicle remotely-sensed images and airborne LiDAR data. Remote Sensing, 2016;8(2):82.
30. Ahmad M. November. Reliability models for the internet of things: A paradigm shift. In 2014 IEEE International Symposium on Software Reliability Engineering Workshops. IEEE; c2014. p. 52-59.
31. Maalel N, Natalizio E, Bouabdallah A, Roux P, Kellil M. Reliability for emergency applications in internet of things. In 2013 IEEE International Conference on Distributed Computing in Sensor Systems; c2013. p. 361-366. IEEE.
32. Kamyod C. End-to-end reliability analysis of an IoT based smart agriculture. In 2018 International Conference on Digital Arts, Media and Technology (ICDAMT); c2018. p. 258- 261. IEEE.

33. Brogi A, Forti S. QoS-aware deployment of IoT applications through the fog. IEEE Internet of Things Journal. 2017;4(5):1185-1192.
34. Li S, Huang J. GSPN-based reliability-aware performance evaluation of IoT services. In *2017* IEEE International Conference on Services Computing (SCC)l; c2017. p. 483-486. IEEE.
35. Sinche S, Polo O, Raposo D, Femandes M, Boavida F, Rodrigues A, *et al*. Assessing redundancy models for IoT reliability. In 2018 IEEE 19th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM); c2018. p. 14-15. IEEE.
36. Sha K, Wei W, Yang TA, Wang Z, Shi W. On security challenges and open issues in Internet of Things. Future Generation Computer Systems. 2018;83:326-337.
37. McDaniel P, McLaughlin S. Security and privacy challenges in the smart grid. IEEE Security & Privacy. 2009;7(3):75-77
38. Ghansah I. Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks: Interim Project Report. California Energy Commission; c2012.
39. Goel S, Hong Y. Security challenges in smart grid implementation. In Smart grid security. Springer, London; c2015. p. 1-39.
40. Brito R, Carvalho A, Gericota M. A new three-phase voltage sourced converter laplace model. In 2015 9th International Conference on Compatibility and Power Electronics (CPE); c2015. p. 160-166. IEEE.
41. Pradhan P, Nagananda K, Venkitasubramaniam P, Kishore S, Blum RS. GPS spoofing attack characterization and detection in smart grids. In 2016 IEEE Conference on Communications and Network Security (CNS); c2016. p. 391-395. IEEE.
42. Risbud P, Gatsis N, Taha A. Vulnerability analysis of smart grids to GPS spoofing. IEEE Transactions on Smart Grid. 2018;10(4):3535-3548.
43. Gao YL, An XH, Liu JM. A particle swarm optimization algorithm with logarithm decreasing inertia weight and chaos mutation. In 2008 international conference on computational intelligence and security. 2008;1:61-65. IEEE.
44. Tran TT, Shin OS, Lee JH. Detection of replay attacks in smart grid systems. In 2013 International Conference on Computing, Management and Telecommunications (ComManTel); c2013. p. 298-302. IEEE.
45. Yi P, Zhu T, Zhang Q, Wu Y, Li J. A denial of service attack in advanced metering infrastructure network. In 2014 IEEE International Conference on Communications (ICC); c2014. p. 1029-1034. IEEE.
46. Bekara C. Security issues and challenges for the IoT-based smart grid. Procedia Computer Science. 2014;34:532-537.
47. Guo Y, Ten CW, Hu S, Weaver WW. Modeling distributed denial of service attack in advanced metering infrastructure. In 2015 IEEE power & energy society innovative smart grid technologies conference (ISGT); c2015. p. 1-5. IEEE.
48. Dovom EM, Azmoodeh A, Dehghantanha A, Newton DE, Parizi RM, Karimipour H. Fuzzy pattern tree for edge malware detection and categorization in IoT. Journal of Systems Architecture. 2019;97:1-7.
49. Eder-Neuhauser P, Zseby T, Fabini J. Malware propagation in smart grid monocultures. e & i Elektrotechnik und Informationstechnik. 2018;135(3):264-269.
50. Boyer SA. SCADA: supervisory control and data acquisition. Research Triangle Park: Isa, 1999, 3.
51. Sha K, Wei W, Yang TA, Wang Z, Shi W. On security challenges and open issues in Internet of Things. Future Generation Computer Systems. 2018;83:326-337.
52. Morrow B. BYOD security challenges: control and protect your most sensitive data. Network Security, 2012;(12):5-8.
53. Yu T, Sekar V, Seshan S, Agarwal Y, Xu C. November. Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things. In Proceedings of the 14th ACM Workshop on Hot Topics in Networks; c2015. p. 1-7.
54. Sha K, Alatrash N, Wang Z. A secure and efficient framework to read isolated smart grid devices. IEEE Transactions on Smart Grid. 2016;8(6):2519-2531.
55. Yan Z, Zhang P, Vasilakos AV. A survey on trust management for Internet of Things. Journal of network and computer applications. 2014;42:120-134.
56. Salunkhe T, Jamadar NI, Kivade SB. Prediction of Remaining Useful Life of mechanical components-a Review. International Journal of Engineering Science and Innovative Technology (IJESIT). 2014;3(6):125-135.
57. Dalal KR. Analysing the Role of Supervised and Unsupervised Machine Learning in IoT. In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC). IEEE; c2020. p. 75-79.
58. Wang Y, Zhao Y, Addepalli S. Remaining Useful Life Prediction using Deep Learning Approaches: A Review. Procedia Manufacturing. 2020;49:81-88.
59. Cubillo A, Perinpanayagam S, Esperon-Miguez M. A review of physics-based models in prognostics: Application to gears and bearings of rotating machinery. Advances in Mechanical Engineering. 2016;8(8):1687814016664660.
60. Elattar HM, Elminir HK, Riad AM. Prognostics: a literature review. Complex & Intelligent Systems. 2016;*2*(2):125-154.
61. Schwabacher M. A survey of data-driven prognostics. In Infotech@ Aerospace, 2005, 7002.
62. Si XS, Wang W, Hu CH, Zhou DH. Remaining useful life estimation–a review on the statistical data driven approaches. European journal of operational research, 2011;213(1):1-14.
63. Brownlee J. Master Machine Learning Algorithms: discover how they work and implement them from scratch. Machine Learning Mastery; c2016.
64. Shanthamallu US, Spanias A, Tepedelenlioglu C, Stanley M. A brief survey of machine learning methods and their sensor and IoT applications. In 2017 8th International Conference on Information, Intelligence, Systems & Applications (IISA); c2017. p. 1-8. IEEE