


PAPER • OPEN ACCESS

Reviewing the Challenges in Maintaining the Reliability and Accuracy of IOT Systems for Remaining Useful Life Prediction

To cite this article: Kalaiarasan Sekar *et al* 2021 *IOP Conf. Ser.: Mater. Sci. Eng.* **1128** 012010

View the [article online](#) for updates and enhancements.




The Electrochemical Society
Advancing solid state & electrochemical science & technology

The ECS is seeking candidates to serve as the
Founding Editor-in-Chief (EIC) of ECS Sensors Plus,
a journal in the process of being launched in 2021

The goal of ECS Sensors Plus, as a one-stop shop journal for sensors, is to advance the fundamental science and understanding of sensors and detection technologies for efficient monitoring and control of industrial processes and the environment, and improving quality of life and human health.

Nomination submission begins: May 18, 2021



Nominate now!

REVIEWING THE CHALLENGES IN MAINTAINING THE RELIABILITY AND ACCURACY OF IOT SYSTEMS FOR REMAINING USEFUL LIFE PREDICTION

Kalaiarasan Sekar^{1,2}, Shahani Aman Shah², A Antony Athithan¹

¹Faculty of Engineering, Lincoln University College, Kuala Lumpur, Malaysia.

²UniKL MIAT, Universiti Kuala Lumpur, Kuala Lumpur, Malaysia

*Shahani@unikl.edu.my

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 on predicting Remaining useful life.

1. Introduction

Internet of things and Artificial intelligence plays a vital role in Aircraft predictive maintenance. 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 improve the component design. The Internet of things has heterogeneous applications in the aviation industry. Hence, ensuring the reliable outcome and performance of the IoT systems when synchronizing with complex computational devices in the aircraft components is necessary to reduce the prediction challenges due to false negatives and false positives data sets. Hence the same can impact the accuracy in prediction of the remaining useful life of an aircraft component. The Remaining useful life prediction for aircraft systems and subsystems can be measured using the data-driven and model-driven approaches. The theoretical methods and prognosis algorithms can be developed for predicting the remaining useful life of an aircraft component, but which has a major challenge of validation to ensure the accuracy of the predictions [1]. Similarly, structural health monitoring with IoT platforms can be used to predict the endurance of the damage and damage evaluation. The structural monitoring can be developed by obtaining real-time data which could be achieved through reliable high-speed internet and wireless sensor networks. Although, the huge challenge lies in providing a low-cost computational system amid growing maturity in IoT systems [2, 3]. The complexity also being faced



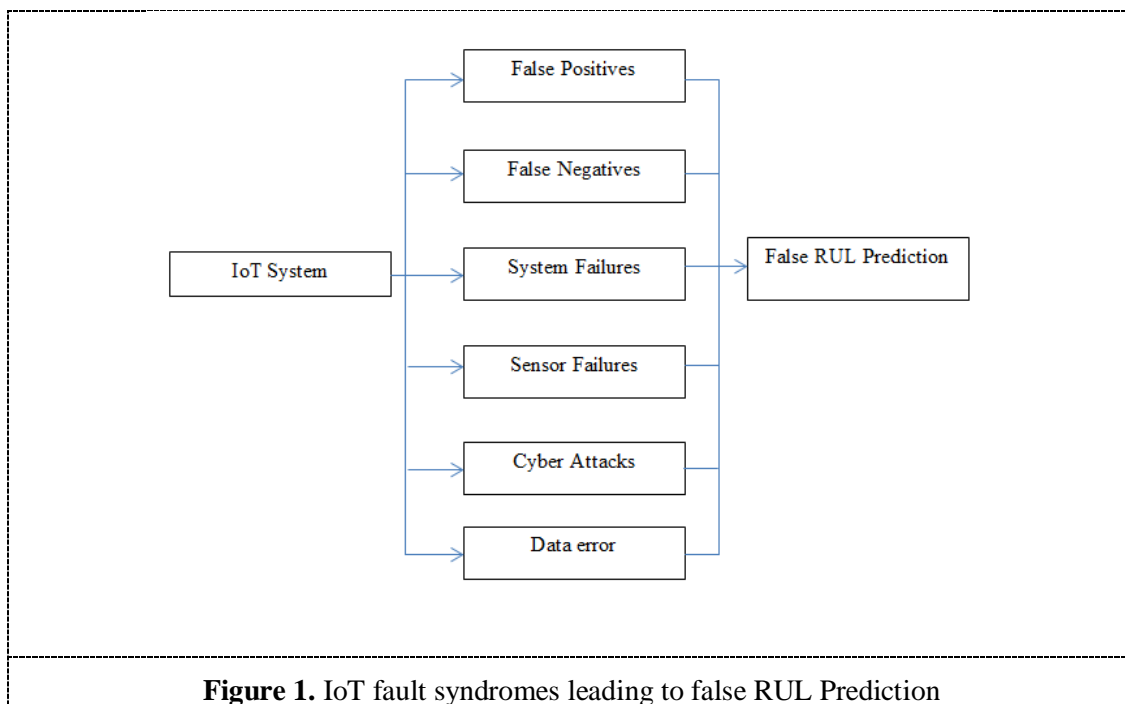
while measuring the QoS (Quality of service) of heterogeneous IoT systems, through Model-driven approach verification.[4].The quality of data is vital in predicting the remaining useful life of a system and structure since the proposed system will have to predict less or no false negatives with a critical operating environment[5]. The limitations in the IoT system include security challenges, quality of service, constraints in obtaining the real-time data, and also difficulty in collecting remaining useful life data from a particular machine type [6]. This section reveals the complexity faced by the researchers on various techniques proposed with the IoT platform for remaining useful life prediction with high-quality reliable data.

2. Challenges in IoT System reliability

2.1. The IoT System Reliability

The major challenge lies with the heterogeneous devices from small low power to high range systems is implementing a multilayer security. Since, these heterogeneous networks are more vulnerable security attacks and providing with the fault data. So, any IoT system would contain a standard mechanism within itself to indicate the redundancy during the malfunction and security attack [7]

The IoT system with the heterogeneous multilayered infrastructure has a greater challenge in obtaining a reliable data which eventually leads to false Remaining useful life predictions. The vulnerability in the system leads to anomalous data being generated and sent which in most severe cases affect human lives [8]



2.2. Challenges in Anomaly detection

IoT systems working on heterogeneous Platform are in need to generate huge amount of data which the large computation is necessary to be adopted. When it comes to handling of huge data with large computational systems, anomaly detection is largely needed for identifying the misbehaving data with normal data sets [9].The Key issues restricting the anomaly detection and the possible causes for those issues are shown in Table 1.

Table 1. Key Issues and Possible Causes in Anomaly Detection

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

2.3. *Equipment Reliability Challenges*

The Reliability of the equipment makes possible to meet the requirements expected by the manufacturers and Maintenance personals [10, 11]. Optimization of the IoT devices and equipment’s during management of large data becomes a challenge [12].The computational and Mathematical models developed with generated data rely highly on equipment efficiency. The Quality of the data will be compromised upon reliability affected on those equipment’s which in turn leads to False Prediction of Remaining Useful life of a components [13].

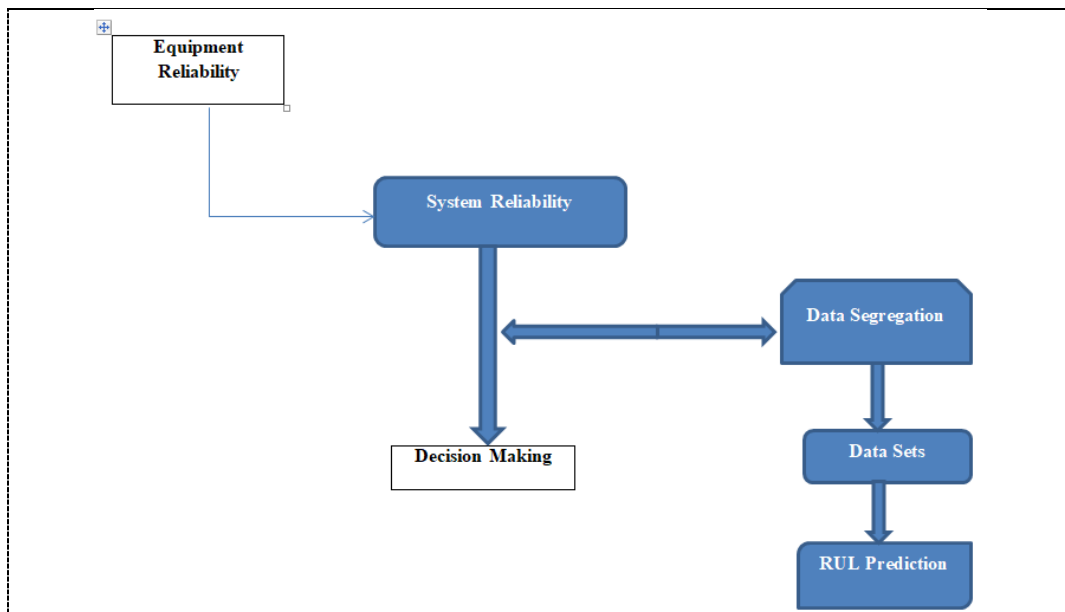


Figure 2. Scope of Equipment Reliability where coloured boxes focus mainly on this review

2.4. Challenges in IoT Architecture

Due to multilayered architecture of IoT system, it is imperative that the system produces reliable output throughout its mission cycle[14-16].In Terms of architectural challenges for IoT system itself, four major layers are considered to prove its reliability for providing the output.[17,18].In Other words, the common multilayered IoT architecture contains Service layer, support, communication and Perception layers .Each layers on the architecture poses different failure conditions on functioning which questions the reliability and leads to false Prediction.[19,20].The service layer in the multilayered architecture on aircraft engine components will use smart sensors to measure engine parameters like Exhaust gas temperature(EGT),N1 compressor speed, whereas the support layer intended to work on FDEP(Functional dependency),service switches, trigger switches , and in the modes of MTBF and MTTR, through where the availability of the system is measured[21,22,23].

The Communication layers poses failures on wireless communication ,noisy data ,attenuation of signals and perception layer provides challenges in reliable monitoring in terms of sensor nodes failures to determine measurements like temperatures and Humidity, which all provides False output or no output condition. Figure 3 shows the IoT architectural layers and possible failure modes leading to false RuL Prediction.

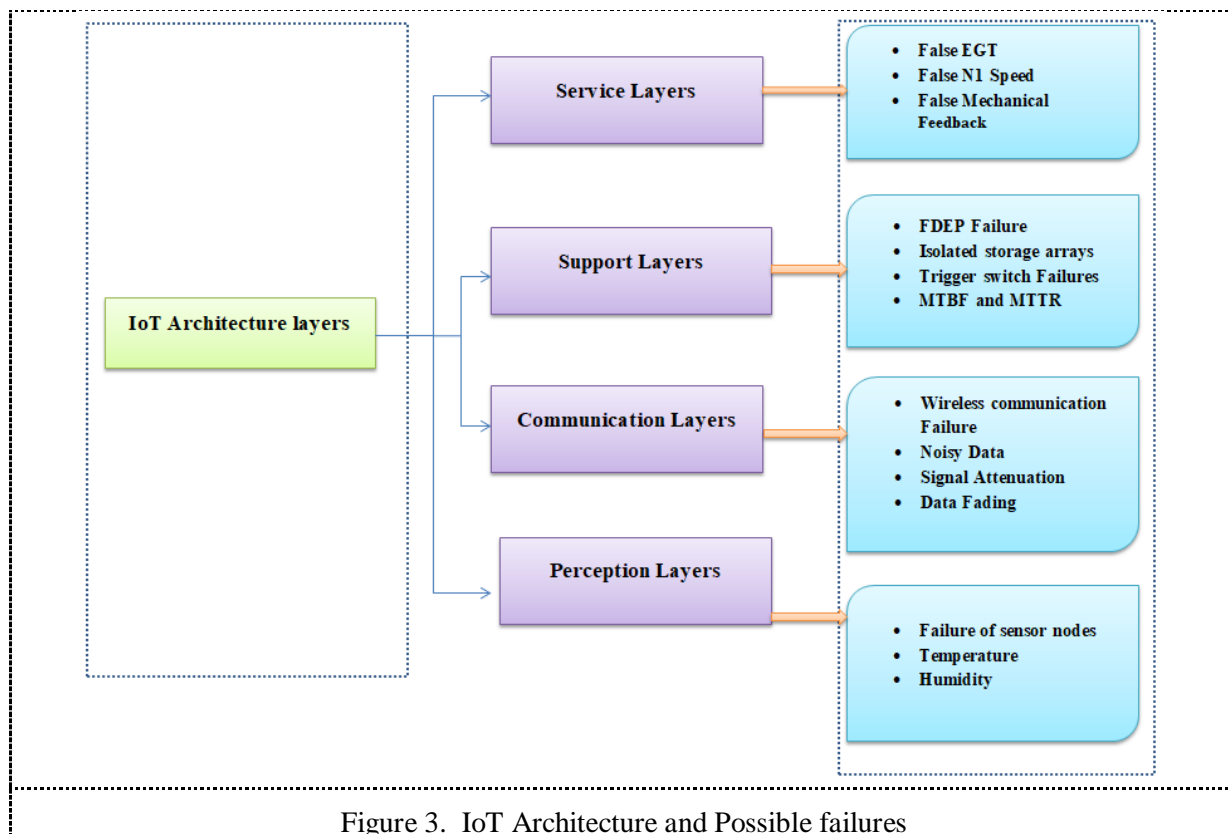


Figure 3. IoT Architecture and Possible failures

2.5. 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 throughput, 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

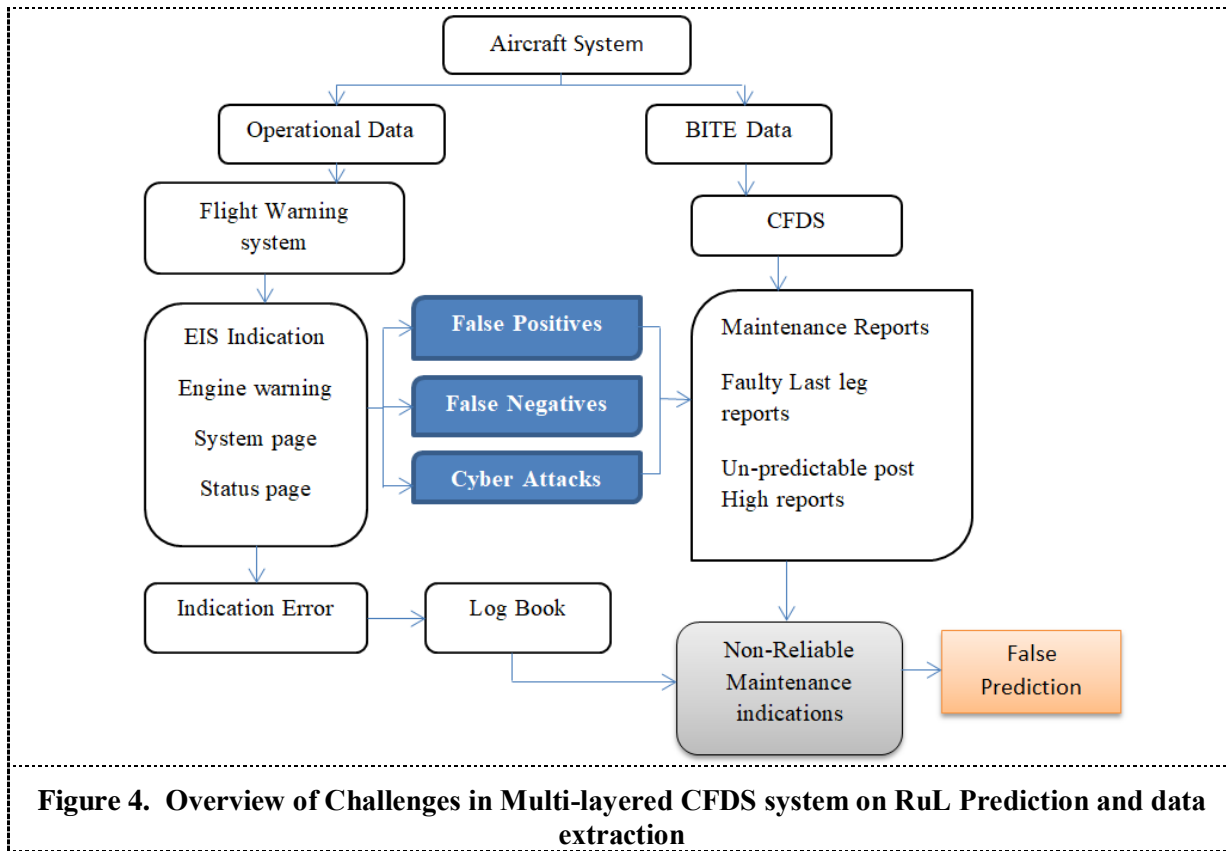
Possible Causes	Performance affecting Parameters
Infeasible Raw Data	High Throughputs and frames
Communication Delay	Low Latencies
High accuracy Requirement	Control failure

2.6. Challenges on Data Registration

The Future challenges on Data registration and Data generation need to incorporate rich sensors like LiDAR [26] and high computational systems for maximum reliability. The complexity is defined in data segregation, data extraction and categorisation of data in timely manner [27]

Considering the aircraft systems, the connected IoT systems may use both Operational data and BITE Data for Flight warning systems(FWS) and Central fault display unit(CFDS) for indication and creating a maintenance reports using cloud platforms. Since the fault syndromes developed in the sensors would eventually leads to Non-Reliable maintenance indications to the crew and leads to false prediction. The review points out the possible challenges from data registration to remaining useful life prediction.

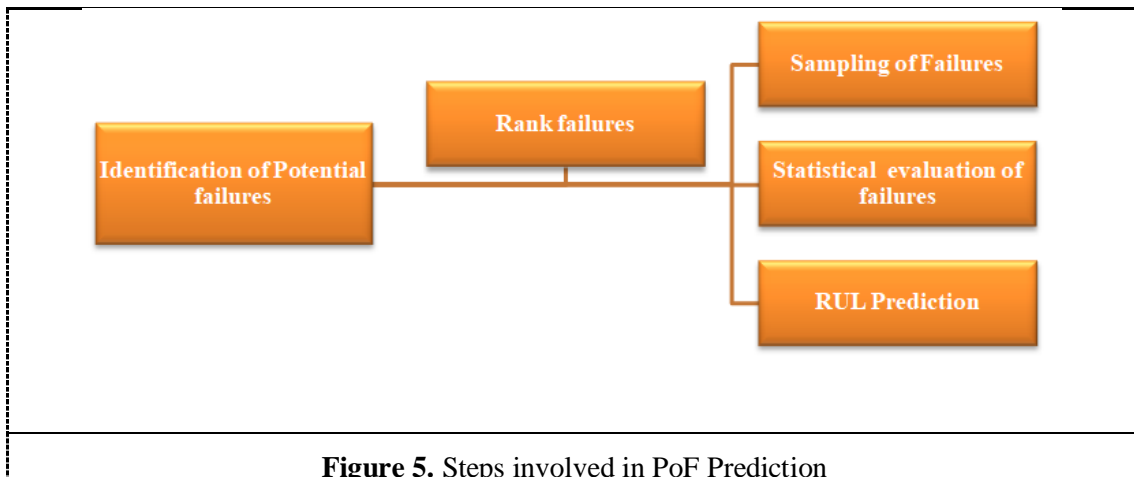
Especially on the studies conducted for data registration over years, major precise fault happens due to sensor overlapping at the close proximity regions [28, 29]. This is highly susceptible in heterogeneous systems. Figure 4 Shows the Overview of Challenges in Multi-layered CFDS system on RuL Prediction and data extraction



2.7. 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).



2.8. *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.

2.9. *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] P. Risbud et al.(2018)[42]	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.
Replay Attacks	J. Zhao et al.(2016)[43] T. Tran el al.(2013)[44]	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.

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.

3. Validation and Prediction Challenges

3.1. Overview of Consideration and Challenges in IoT System Architecture design

This Section Provides the Summary of Literature review for various Modern Tool Validation Approaches in Providing Safety Aspect and Statistical prediction including Machine learning and Deep Learning Approaches. Especially, while concerning the importance of security in the IoT systems various challenges and Considerations have been put forth to design and Validate the system. The Consideration includes Better interaction of the IoT system with the Physical World [50], Constraints in the available resources [51], heterogeneity [52], Large Scale data registration [53] and segregation, Security breaches, Privacy settings [54] and trust management [55].

Table 4. Summarized Literature review showing contribution of Each Works related to Security Attacks on the IoT System

Consideration	Challenges
Physical World Integration	<ul style="list-style-type: none"> • OS Update • Compatibility • Coupling with Physical and Cyber world
Heterogeneity	<ul style="list-style-type: none"> • Continuous Monitoring needed • Reliable Detection Mechanism for Abnormal Behaviour • Reliability issues over Traditional Mechanisms • Reliable Security

	Algorithms
Constraints in the Resources	<ul style="list-style-type: none"> • Memory space allocation for large amounts of data • Availability of the system • Detection of Intrusion Points
Privacy	Firewall Reliability and Intrusion Detection
Large Scale Distribution	Scalable
Trust Management Administration	Reliable

3.2. RUL Prediction approaches and drawbacks

The section provides the summary of different modern prediction approaches which includes Deep learning and Machine learning models used for RUL Prediction using IoT Systems. RUL Prediction derived from the concept of Prognostics where future of the entire system is predicted using observations, statistical and mathematical models [55]. Any RUL Prediction is defined as observing the functional range of the entire system or component before it reaches the fatigue or failure range [56].

The RUL Prediction can be predicted and analysed through various approaches which includes traditional supervised and unsupervised machine learning, and deep learning models[57,58]. The Modern prognostic approaches contains various challenges in RUL Prediction process. Table 4 shows the summary of review of challenges and drawbacks considered on the various RUL Prediction approaches.

Table 5. Shows the summary of review of Challenges considered on Various RUL Prediction Approaches

RUL Prediction Approach	Work	Challenges
Physics Based Approach	A. Cubilo et al.(2016)[59] H.M Elattar et al.(2016)[60]	<ul style="list-style-type: none"> • Intense Computations Requirement • High fidelity • Complexity on modelling the defect • Reusable limits are less • Complex mechanical systems • Difficulty on identifying the fault

Hybrid based Approach	M. Schwabacher (2005)[61] Youdao Wang et al(2020)[58]	<ul style="list-style-type: none"> • Noisy data • Inaccuracy because of Noisy data • Both Model and Data Required
Data-Driven Approaches	X .S. Si et al(2011)[62] Youdao Wang et al(2020)[58]	<ul style="list-style-type: none"> • Intense and Large algorithms required • Short Prediction ranges • Inadequate and shortage of data for new systems
Supervised Machine learning	Brownlee et al(2016)[63] Kushal .R. D(2020)[57]	<ul style="list-style-type: none"> • Labelling of Data • Huge Labelling requires Intense training of the models • Identification of Inputs and Outputs
Unsupervised Machine Learning	Kushal .R. D(2020)[57] Shanthamallu et al.(2017)[64]	<ul style="list-style-type: none"> • Large Volume of Clustering • High Monitoring needed for Unlabelled Information

4. Conclusion

To the best of our knowledge, this paper will be able to reveal the challenges associated with remaining useful life prediction of components or system using the IoT platform, and recommends the pre-requisites and requirements to be considered for any IoT infrastructure if in case of false data sets with sensor and system failure. Also, the literature review briefs the specific challenges obtained from the heterogeneous IoT network. This includes system reliability challenges, challenges in anomaly detection using IoT systems, challenges associated with constructing the IoT architecture, challenges in data registration and data segregation, challenges associated with hardware reliability, and security challenges. Also, one of the other major challenge lies with validation of the selected IoT model in consideration with different real time factors as discussed in chapter 3 from this paper. The IoT model which is constructed for Remaining useful life prediction basically perform on the three approaches which includes physics based , hybrid and data-driven approaches. The summary on table 4 describes the drawbacks encountered by the researchers on testing the model with these three different approaches. The challenges are summarised to provide the knowledge on the machine learning approaches which incorporates IoT system for remaining useful life prediction.

We believe this review will be able to provide the insights for researchers to identify the adoptability of IoT systems on aviation Predictive maintenance with reliable and cost-effective computational systems. The outcome of this review is to provide the understanding of the challenges associated with multi-layered IoT systems and leads to consider the consequences developed on the specific conditions in the system prior to construction of the IoT Model. So we strongly believe, these consideration and knowledge about the system construction and performance of the particular model would eventually reduce the downtime, enhance the cost saving in the aviation predictive maintenance.

References

- [1] Xiongzi, C., Jinsong, Y., Diyin, T. and Yingxun, W., 2011, August. Remaining useful life prognostic estimation for aircraft subsystems or components: A review. In *IEEE 2011 10th International Conference on Electronic Measurement & Instruments* (Vol. 2, pp. 94-98). IEEE.

- [2] Abdelgawad, A. and Yelamarthi, K., 2017. Internet of things (IoT) platform for structure health monitoring. *Wireless Communications and Mobile Computing*, 2017.
- [3] Angadi, A., Dias, R. and Bagali, M.U., 2016. An Aircraft Health Monitoring System using IOT. *Indian Journal of Science and Technology*, 9(33), pp.1-5.
- [4] Costa, B., Pires, P.F., Delicato, F.C., Li, W. and Zomaya, A.Y., 2016, August. 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)* (pp. 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., Paolanti, M., Toscano, G., Ciandrini, G., Carrotta, A. and Mengoni, M., 2020. SOPHIA: An event-based IoT and machine learning architecture for predictive maintenance in industry 4.0. *Information*, 11(4), p.202.
- [7] Khan, M.A. and Salah, K., 2018. IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82, pp.395-411..
- [8] Moore, S.J., Nugent, C.D., Zhang, S. and Cleland, I., 2020. IoT reliability: a review leading to 5 key research directions. *CCF Transactions on Pervasive Computing and Interaction*, pp.1-17.
- [9] Sharma, B., Sharma, L. and Lal, C., 2019, December. Anomaly Detection Techniques using Deep Learning in IoT: A Survey. In *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)* (pp. 146-149). IEEE.
- [10] Bianchini, A., Pellegrini, M. and Rossi, J., 2019. Maintenance scheduling optimization for industrial centrifugal pumps. *International Journal of System Assurance Engineering and Management*, 10(4), pp.848-860.
- [11] Ustundag, A. and Cevikcan, E., 2017. *Industry 4.0: managing the digital transformation*. Springer.
- [12] Lee, C.K.M., Zhang, S.Z. and Ng, K.K.H., 2017. Development of an industrial Internet of things suite for smart factory towards re-industrialization. *Advances in manufacturing*, 5(4), pp.335-343.
- [13] SCHEER, A.W., 2019. Enterprise 4.0-From disruptive business model to the automation of business processes.
- [14] Kempf, J., Arkko, J., Beheshti, N. and Yedavalli, K., 2011, March. Thoughts on reliability in the internet of things. In *Interconnecting smart objects with the Internet workshop* (Vol. 1, pp. 1-4).
- [15] Han, C., Jornet, J.M., Fadel, E. and Akyildiz, I.F., 2013. A cross-layer communication module for the Internet of Things. *Computer Networks*, 57(3), pp.622-633.
- [16] Palattella, M.R., Dohler, M., Grieco, A., Rizzo, G., Torsner, J., Engel, T. and Ladid, L., 2016. Internet of things in the 5G era: Enablers, architecture, and business models. *IEEE Journal on Selected Areas in Communications*, 34(3), pp.510-527.
- [17] Burhan, M., Rehman, R.A., Khan, B. and Kim, B.S., 2018. IoT elements, layered architectures and security issues: A comprehensive survey. *Sensors*, 18(9), p.2796.
- [18] Darwish, D., 2015. Improved layered architecture for Internet of Things. *Int. J. Comput. Acad. Res.(IJCAR)*, 4, pp.214-223.
- [19] Frustaci, M., Pace, P., Aloï, G. and Fortino, G., 2017. Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet of things journal*, 5(4), pp.2483-2495.
- [20] Xing, L., 2020. Reliability in Internet of Things: Current status and future perspectives. *IEEE Internet of Things Journal*, 7(8), pp.6704-6721.
- [21] Gopalakrishnan, M., Skoogh, A., Salonen, A. and Asp, M., 2019. Machine criticality assessment for productivity improvement. *International Journal of Productivity and*

- Performance Management.*
- [22] Quijada Fumero, P. and Salunkhe, O., 2017. *Demonstration of real-time criticality assessment using a test-bed* (Master's thesis).
- [23] Souza, M.L.H., da Costa, C.A., de Oliveira Ramos, G. and da Rosa Righi, R., 2020. A survey on decision-making based on system reliability in the context of Industry 4.0. *Journal of Manufacturing Systems*, 56, pp.133-156.
- [24] Bagchi, S., Abdelzaher, T.F., Govindan, R., Shenoy, P., Atrey, A., Ghosh, P. and Xu, R., 2020. New Frontiers in IoT: Networking, Systems, Reliability, and Security Challenges. *IEEE Internet of Things Journal*, 7(12), pp.11330-11346.
- [25] Yick, J., Mukherjee, B. and Ghosal, D., 2008. Wireless sensor network survey. *Computer networks*, 52(12), pp.2292-2330.
- [26] Wang, Q., Zhu, Y. and Cheng, L., 2006. Reprogramming wireless sensor networks: challenges and approaches. *IEEE network*, 20(3), pp.48-55.
- [27] Habib, A., Ghanma, M., Morgan, M. and Al-Ruzouq, R., 2005. Photogrammetric and LiDAR data registration using linear features. *Photogrammetric Engineering & Remote Sensing*, 71(6), pp.699-707.
- [28] Bellekens, B., Spruyt, V., Berkvens, R., Penne, R. and Weyn, M., 2015. A benchmark survey of rigid 3D point cloud registration algorithms. *Int. J. Adv. Intell. Syst*, 8, pp.118-127.
- [29] Liu, S., Tong, X., Chen, J., Liu, X., Sun, W., Xie, H., Chen, P., Jin, Y. and Ye, Z., 2016. A linear feature-based approach for the registration of unmanned aerial vehicle remotely-sensed images and airborne LiDAR data. *Remote Sensing*, 8(2), p.82.
- [30] Ahmad, M., 2014, November. Reliability models for the internet of things: A paradigm shift. In *2014 IEEE International Symposium on Software Reliability Engineering Workshops* (pp. 52-59). IEEE.
- [31] Maalel, N., Natalizio, E., Bouabdallah, A., Roux, P. and Kellil, M., 2013, May. Reliability for emergency applications in internet of things. In *2013 IEEE International Conference on Distributed Computing in Sensor Systems* (pp. 361-366). IEEE.
- [32] Kamyod, C., 2018, February. End-to-end reliability analysis of an IoT based smart agriculture. In *2018 International Conference on Digital Arts, Media and Technology (ICDAMT)* (pp. 258-261). IEEE.
- [33] Brogi, A. and Forti, S., 2017. QoS-aware deployment of IoT applications through the fog. *IEEE Internet of Things Journal*, 4(5), pp.1185-1192.
- [34] Li, S. and Huang, J., 2017, June. GSPN-based reliability-aware performance evaluation of IoT services. In *2017 IEEE International Conference on Services Computing (SCC)* (pp. 483-486). IEEE.
- [35] Sinche, S., Polo, O., Raposo, D., Fernandes, M., Boavida, F., Rodrigues, A., Pereira, V. and Silva, J.S., 2018, June. Assessing redundancy models for IoT reliability. In *2018 IEEE 19th International Symposium on "A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)* (pp. 14-15). IEEE.
- [36] Sha, K., Wei, W., Yang, T.A., Wang, Z. and Shi, W., 2018. On security challenges and open issues in Internet of Things. *Future Generation Computer Systems*, 83, pp.326-337.
- [37] McDaniel, P. and McLaughlin, S., 2009. Security and privacy challenges in the smart grid. *IEEE Security & Privacy*, 7(3), pp.75-77
- [38] Ghansah, I., 2012. *Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks: Interim Project Report*. California Energy Commission.
- [39] Goel, S. and Hong, Y., 2015. Security challenges in smart grid implementation. In *Smart grid security* (pp. 1-39). Springer, London.
- [40] Brito, R., Carvalho, A. and Gericota, M., 2015, June. A new three-phase voltage sourced converter laplace model. In *2015 9th International Conference on Compatibility and Power Electronics (CPE)* (pp. 160-166). IEEE.
- [41] Pradhan, P., Nagananda, K., Venkitasubramaniam, P., Kishore, S. and Blum, R.S., 2016,

- October. GPS spoofing attack characterization and detection in smart grids. In *2016 IEEE Conference on Communications and Network Security (CNS)* (pp. 391-395). IEEE.
- [42] Risbud, P., Gatsis, N. and Taha, A., 2018. Vulnerability analysis of smart grids to GPS spoofing. *IEEE Transactions on Smart Grid*, 10(4), pp.3535-3548.
- [43] Gao, Y.L., An, X.H. and Liu, J.M., 2008, December. A particle swarm optimization algorithm with logarithm decreasing inertia weight and chaos mutation. In *2008 international conference on computational intelligence and security* (Vol. 1, pp. 61-65). IEEE.
- [44] Tran, T.T., Shin, O.S. and Lee, J.H., 2013, January. Detection of replay attacks in smart grid systems. In *2013 International Conference on Computing, Management and Telecommunications (ComManTel)* (pp. 298-302). IEEE.
- [45] Yi, P., Zhu, T., Zhang, Q., Wu, Y. and Li, J., 2014, June. A denial of service attack in advanced metering infrastructure network. In *2014 IEEE International Conference on Communications (ICC)* (pp. 1029-1034). IEEE.
- [46] Bekara, C., 2014. Security issues and challenges for the IoT-based smart grid. *Procedia Computer Science*, 34, pp.532-537.
- [47] Guo, Y., Ten, C.W., Hu, S. and Weaver, W.W., 2015, February. Modeling distributed denial of service attack in advanced metering infrastructure. In *2015 IEEE power & energy society innovative smart grid technologies conference (ISGT)* (pp. 1-5). IEEE.
- [48] Dovom, E.M., Azmoodeh, A., Dehghantanha, A., Newton, D.E., Parizi, R.M. and Karimipour, H., 2019. Fuzzy pattern tree for edge malware detection and categorization in IoT. *Journal of Systems Architecture*, 97, pp.1-7.
- [49] Eder-Neuhauser, P., Zseby, T. and Fabini, J., 2018. Malware propagation in smart grid monocultures. *e & i Elektrotechnik und Informationstechnik*, 135(3), pp.264-269.
- [50] Boyer, S.A., 1999. *SCADA: supervisory control and data acquisition* (Vol. 3). Research Triangle Park: Isa.
- [51] Sha, K., Wei, W., Yang, T.A., Wang, Z. and Shi, W., 2018. On security challenges and open issues in Internet of Things. *Future Generation Computer Systems*, 83, pp.326-337.
- [52] Morrow, B., 2012. BYOD security challenges: control and protect your most sensitive data. *Network Security*, 2012(12), pp.5-8.
- [53] Yu, T., Sekar, V., Seshan, S., Agarwal, Y. and Xu, C., 2015, 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* (pp. 1-7).
- [54] Sha, K., Alatrash, N. and Wang, Z., 2016. A secure and efficient framework to read isolated smart grid devices. *IEEE Transactions on Smart Grid*, 8(6), pp.2519-2531.
- [55] Yan, Z., Zhang, P. and Vasilakos, A.V., 2014. A survey on trust management for Internet of Things. *Journal of network and computer applications*, 42, pp.120-134.
- [56] Salunkhe, T., Jamadar, N.I. and Kivade, S.B., 2014. Prediction of Remaining Useful Life of mechanical components-a Review. *International Journal of Engineering Science and Innovative Technology (IJESIT)*, 3(6), pp.125-135.
- [57] Dalal, K.R., 2020, July. Analysing the Role of Supervised and Unsupervised Machine Learning in IoT. In *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)* (pp. 75-79). IEEE.
- [58] Wang, Y., Zhao, Y. and Addepalli, S., 2020. Remaining Useful Life Prediction using Deep Learning Approaches: A Review. *Procedia Manufacturing*, 49, pp.81-88.
- [59] Cubillo, A., Perinpanayagam, S. and Esperon-Miguez, M., 2016. A review of physics-based models in prognostics: Application to gears and bearings of rotating machinery. *Advances in Mechanical Engineering*, 8(8), p.1687814016664660.
- [60] Elattar, H.M., Elminir, H.K. and Riad, A.M., 2016. Prognostics: a literature review. *Complex & Intelligent Systems*, 2(2), pp.125-154.
- [61] Schwabacher, M., 2005. A survey of data-driven prognostics. In *Infotech@ Aerospace* (p. 7002).

- [62] Si, X.S., Wang, W., Hu, C.H. and Zhou, D.H., 2011. Remaining useful life estimation—a review on the statistical data driven approaches. *European journal of operational research*, 213(1), pp.1-14.
- [63] Brownlee, J., 2016. *Master Machine Learning Algorithms: discover how they work and implement them from scratch*. Machine Learning Mastery.
- [64] Shanthamallu, U.S., Spanias, A., Tepedelenlioglu, C. and Stanley, M., 2017, August. A brief survey of machine learning methods and their sensor and IoT applications. In *2017 8th International Conference on Information, Intelligence, Systems & Applications (IISA)* (pp. 1-8). IEEE.