Chapter 8
Deep Learning Based Security Preservation of IoT: An Industrial Machine Health Monitoring Scenario

Aneesh G. Nath and Sanjay Kumar Singh

8.1 Introduction

The internet of things (IoT) is the collection of devices or objects connected to each other and to the internet, which can automatically transfer or receive data through different communication systems like Wi-Fi, RFID, Bluetooth, cellular, satellite, Ethernet, etc. Studies reveal that 127 new IoT devices are connecting to the internet every second. According to Statista [1], approximately 75.44 billion devices will be connected to the internet, and the connected devices generate 79 zettabytes of data by 2025. This creates real-time big data processing issues and security vulnerabilities to the connected devices [2, 3]. Moreover, there is another dimension in viewing the data sensing issues, which can be better described by 'risks' rather than security. Some of such risks are sensor failures, irregular triggering of sensors, noisy or abnormal data issues, etc.

Among the IoT applications in various fields, like health, traffic monitoring, agriculture, smart grid, and energy-saving, the IoT application in industry is of greater importance. As a slight increase in industrial productivity will improve the worldwide GDP on the scale of trillions of dollars, the application of IoT in industry invites a lot of research attention. At the same time, the primary moto of Industrial IoT (IIoT) lies in increasing efficiency and improving health/safety of industrial production while IoT tries to provide one more objective, i.e., the 'better experience' to the end-user. Other than that, IIoT takes favor of IoT technology to enhance the intelligence of the network and its security options for the automation of industrial

A. G. Nath · S. K. Singh (✉)
Department of Computer Science and Engineering, Indian Institute of Technology (BHU), Varanasi, Uttar Pradesh 221005, India
e-mail: sks.cse@itbhu.ac.in

A. G. Nath
e-mail: aneeshgnath.rs.cse18@itbhu.ac.in

A. Makkar and N. Kumar, *Deep Learning for Security and Privacy Preservation in IoT*, Signals and Communication Technology,
https://doi.org/10.1007/978-981-16-6186-0_9

processes and its optimization. The physical processes are managed and controlled by the programmable logic controller. They collect the sensed data and send commands to the actuators as the sensor-actuator direct communication is not possible. Finally, the overall network is configured with servers, computers, and other devices with internet services on top of it.

8.1.1 Deep Learning and IIoT

The ideology of 'right information and data at the right time for decision making' is the driving force of data-driven failure detection and predictive maintenance and manufacturing, through which organizations are transforming into the revolutionary Industry 4.0. Failure detection and predictive maintenance play a vital role in automation in the manufacturing industry. It ensures optimum cost, safety, availability, and reliability by monitoring different machinery components employing various sensors and other equipment. The availability of low-cost sensors and big data made data-driven approaches more popular as opposed to model-driven techniques nowadays. Since 2006, deep learning (DL) started to refine all the state-of-the-art models and has ever since becoming a rapidly growing research covering a wide range of areas. DL becomes popular in a short span of time of its automatic feature engineering, unsupervised pre-training, and high abstraction capabilities. Even in resource-constrained networks, DL becomes more employable well with these features.

Furthermore, DL has been implemented extensively potential to provide more accurate results and faster processing time. The internet-connected low-cost sensors have given popularity to modern manufacturing systems, which generate big data of machinery. Big data demands deep learning processing and analyzing capabilities, and hence DL plays a vital role in decision making [4, 5] of big machinery data. Compared to the traditional physics-based models [6], data-driven machine health monitoring systems offers a bottom-up paradigm for solutions. The detection of faults after the occurrence of certain failures are called diagnosis, and the predictions of the future working conditions and the remaining useful life is called prognosis.

8.1.2 Security and Risks

The security in terms of an IoT requires to satisfy integrity, confidentiality, authentication, availability, and access control. Among these, integrity and availability are the most critical features that an IIoT system required. The security service providers most often develop refined IoT systems that prevent IoT-based attacks, confidentiality, authentication, etc. These security requirements have been considered by big data technologies, and DL algorithms excel in security attack detection. In this context, this study investigates deep learning and big data technologies in the security of IIoT in view of SRF diagnosis.

IoT has been proven to be vulnerable to security breaches. IIoT devices tend to generate large volumes of data, with a large variety and veracity. This forces it to incorporating big data technologies to get better data handling and enhanced performance. Similarly, environmental factors, noise, and missing data issues are prevalent with IIoT data acquisition. They are categorized into the risk category rather than security in this study. When data is uploaded to the cloud to decision making, the security challenges become more complicated. The significant cybersecurity challenges and opportunities for cybersecurity with IoT and artificial intelligence (AI) has been discussed by Pan et al. [7].

8.1.3 Security and Integrity Issues of Rotating Machinery: A Background

Approximately 40% of all machinery in the daily production process is constituted by Rotating machinery, and it is prevalent in any industry [8]. Almost all manufacturing processes involve correlated rotating machines. All these machines have its limits, and when it goes beyond its particular limits, faults may occur, which affects the machine component's structural integrity. It leads to a detrimental impact on product quality and the performance of the equipment. Unfortunately, in most cases, these faults may also aggregate secondary faults. In one of such claims, high vibrations and wear of the bearings resulted from misaligned machines, leading to leaking shaft seals or hot couplings. Similar to misalignment, unbalance and looseness also creates several such impacts. These are called 'structural faults' [8], which is very common in rotating machinery. This study focus on the IIoT security issues and DL in view of rotating machinery fault diagnosis. In this, the primarily used IoT device is the sensor, which is used for data acquisition. In the rotor faults diagnosis scenario, the integrity and data sensing issues can be primarily reflected with vibration data, and a giant portion of works use vibration as the data source; our discussion mainly focuses on vibration based fault categorization and analysis. The unbalance, misalignment, and looseness are the primary causes of vibration in rotating machinery [9].

Around 40% of rotor related problems are due to unbalance, 30% by misalignment, 20% by resonance, and the remaining 10% are due to other reasons [10]. According to the fault categorization that we are considering, SRF is followed by the faults affecting the shaft, which are the secondary cause of vibration. Also, the broken rotor bar (BRB) fault has also been included in the fault category list. The most common. Bent shaft (BS), shaft crack (SC), rub impact fault (RIF), and corrosion and wear (Cr&Wr) are the faults that affect the shafts. They are frequently associated with SRF and are considered to fall within the shaft fault category. This categorization is shown in Fig. 8.1. Shaft faults are the crucial rotor faults considered a secondary phenomenon resulting from structural rotor faults. Usually, the vibration that affects the rotor is highly non-linear and complicated vibration motion such as periodic, quasi-periodic, and chaotic vibrations. The rotor-bearing system is a multi fault system that can have

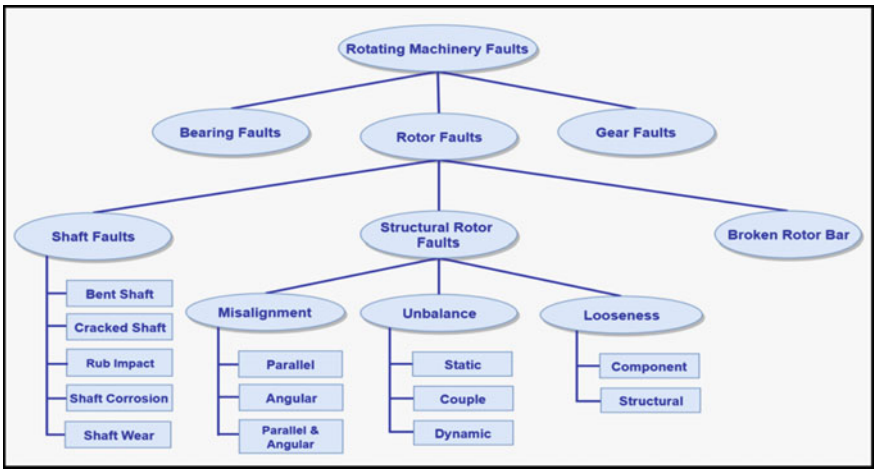

Fig. 8.1 Structural rotor faults categorization

a varying degree of nonlinearity. But the remaining discussion uses the assumption of a single fault rotor system, which often an idealistic situation.

8.1.4 Structural Rotor Faults for Case Analysis

When the distribution of mass in the rotor is not even then, it results in rotor unbalance, and it causes the inertia axis of the rotor misaligned with the geometric axis. The causes of misalignment are improper aligned couplings and bearings, thermal distortion, asymmetrical load, etc., which induce vibration in the rotor. The effect of misalignment is that the bearings have to bear a higher load than they are particularly designed for. Long-term running of machinery or improper assembly causes looseness of machinery; it is of two types, structural looseness and component looseness. The looseness effect is similar to unbalance, while component looseness causes detachments and secondary damage. The rub fault is caused by the contact between stationary parts and the rotor under tighter clearances. Thermal and mechanical stresses create cracks, which makes the shaft non-withstandable for normal operating forces. A broken rotor bar fault is typical induction motor rotors due to uneven current flow that create thermal and bending issues. The environmental factors intensify the electrochemical reaction, which causes corrosion-based faults on the shaft's surface.

8.2 Framework Description

Figure 8.2 shows an ideal framework which deals with an industrial system with IIoT based fault diagnosis and prognosis. The industrial manufacturing system uses equipment and production processes to create products, which is being controlled by the manufacturing and operating control module. This manufacturing process has to be monitored for the prediction of faults and so that it can be protected from unexpected shutdowns. Hence a module called a data acquisition module is connected to it. There are six main modules in the framework: (1) Data (3) Decision-Making Module, (4) Performance Checking module, and (5) Maintenance planning and corrective decision module.

8.2.1 Data Acquisition Module

This is step gathers the data for machinery diagnostics and prognostics. The sensor module selection and sensor strategy developments are the two primary functions associated with this module. The communication technology, especially wireless communication, helps in transferring the data to other modules. The data acquisition process transforms the raw data into different formats convert it into proper representations suitable for further processing.

The main parameters of data acquisition systems are sampling rate, number of channels, and resolution, etc. The wireless transmission of data is done by means of a Wireless Sensor Network (WSN), which comprises other wireless sensing

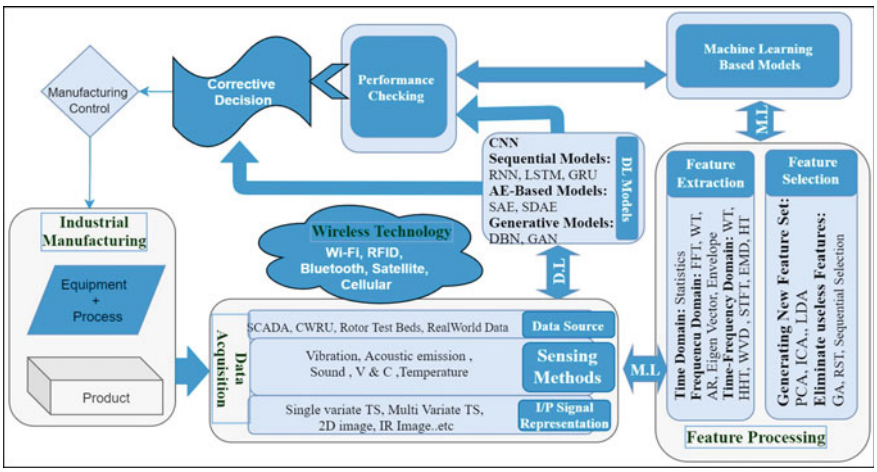

Fig. 8.2 IIoT framework

units. WSN is composed of different stages such as data acquisition communication, processing, and fusion. The mainly used transmission protocols are Modbus, BACnet, DNP3, MQTT etc. These have their security vulnerabilities as follows:

Modbus fails to provide authentication, integrity or confidentiality. As Modbus communicate without encryption, it lacks confidentiality. Authentication not provided since it does not have public/private key management. Lack of security check leads to compromise on the integrity of the data. Availability can be limited by flooding attacks.

BACnet contains no proper mechanisms for maintaining the confidentiality of data, resulting in a reconnaissance attack. Data Encryption Standard (DES) and Advanced Encryption Standard (AES) encryption mechanisms are used, but no procedure for providing authentication. It is prone to denial of service (DoS) attacks.

DNP3 is comparatively reliable but lacks sufficient security mechanisms, so that it fails to provide authentication, encryption, and access control. The non-availability of message authentication causes data integrity issues, and lack of encryptions results in eavesdropping and spoofing. DoS attacks are also common. The public key infrastructure (PKI) in IIoT devices is not feasible also.

MQTT has no encryption method implemented. By accessing the identity of a single client, all the client information is exposed to the intruder. Data integrity is provided by message authentication code like hash-based message authentication code (HMAC), which uses a lightweight cryptographic hash function. The commonly used sensors in IIoT are:

- Accelerometers
- Velocity transducers
- Displacement or Distance transducers: (Infrared sensors, LVDT or Hall-effect sensors, etc.)
- Piezo-electric sensors.

As described before, vibration sensors are most commonly used. From the data availability point of view, it has got certain drawbacks. The effectiveness of the reading affects the sensor mount position. Moreover, its contacting nature creates a number of disturbances to the sensor readings. There are three kinds of vibration signals are collected: displacement, velocity, and acceleration. The other sensing methods are acoustic emission [11], sound [12], voltage and current [13], and temperature [14] are more and more applied in condition classification. The statistics of sensing methods in rotor fault diagnosis is shown in Fig. 8.3.

8.2.2 Feature Processing

Feature processing extracts the information buried in a raw signal and suppresses the noise, and identify the most specific features of a particular fault, and presents

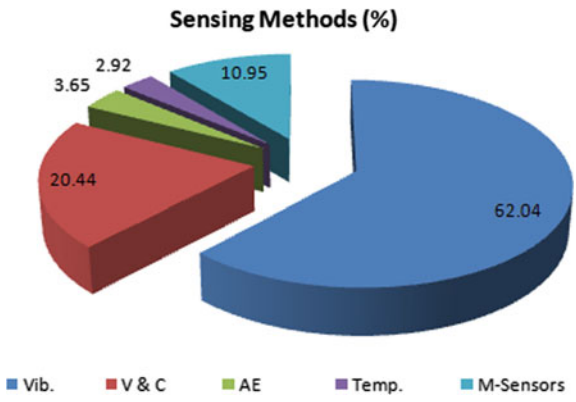

Fig. 8.3 Sensing methods in RFD

the essential features of an incipient failure or fault for decision making. It uses a variety of signal processing techniques in two phases, known as feature extraction and feature selection. The signal processing techniques such as filtering, data compression, amplification, data validation, and de-noising are the most commonly used in feature processing. In feature selection, meant for selecting prominent features with techniques, eliminates unwanted and non-sensitive features using specific criteria. [15].

The signal processing technique uses various algorithms to preprocess the raw data and extract specific characteristic features of different faults. The significant methods under this are categorized into three domains: frequency domain, time domain, and time–frequency domain. Time–frequency distributions, wavelet and wavelet packet methods, empirical mode decomposition (EMD), spectral kurtosis (SK), envelope analysis, and minimum entropy deconvolution are some subcategories of these three rotating machinery fault diagnosis methods. These methods include Fourier transform, statistical moments, autoregressive, Walsh transform, power spectral density, and entropy. The popular dimensionality reduction techniques like principal component analysis (PCA), linear discriminant analysis (LDA), independent component analysis (ICA), etc. come under the first category, and people use Rough Set Theory (RST), genetic algorithm (GA) and sequential selection in second category methods [15].

8.2.3 Decision-Making Module

The decision-making module can be divided into four categories, that are (i) physical model, (ii) statistical model, (iii) data-driven model, and (iv) hybrid model. Data-driven and hybrid models are the most common models in today's fault diagnostics system. As the large amount of data generated from sensors and the historical data is available at any time, data-driven methods have proven to be ideal in identifying the

fault and evaluate the machine health condition. Hybrid models are used when there is no sufficient data available for data-driven models. Semi-supervised techniques are also used in such scenarios. Diagnostics and prognostics are the two strategies in maintenance decision-making. Fault diagnostics take actions such as fault detection, isolation, and identification only when the fault has been occurred, while prognostics predict the fault before they occur.

The data-driven models are nowadays classified mainly into shallow learning (or simple machine learning) and deep learning. Based on architecture, design philosophy, underlying principle, and type of input, these models are further divided into subcategories. The ML models work with the features that are extracted from the feature processing phase, while DL-based models process the raw data directly. This feature processing demands extensive domain expertise and time. The most widely used ML classifiers for SRF are support vector machines (SVM) and artificial neural networks (ANN). SVMs are tried with different kernels, while various learning algorithms and activations are used with ANN. Under the instance-based category of algorithms, the k-Nearest Neighbor (k-NN) is popular, and the probability-based Bayesian methods are also demonstrated in RFD. Then the decision tree (DT), random forest (RF) algorithms are also used at large in RFD. Along with these models, simple classifiers like linear discriminant analysis (LDA), logistic regression (LR), etc., can also be found in the literature. The ensemble classification algorithms AdaBoost (AB) are experimented with by some researchers by combining the hypothesis of well-known models.

The deep learning algorithms are not constrained with the limitation of learning the non-linear relation of features. It learns higher levels of abstraction of input data with deeper layers, limits the time needed for feature processing, and avoids the need for specialized expertise in the domain. By multiple-layer deep architectures enables DL to find multiple complex features on their own. CNN's are the most accepted model compared to any other DL models in RFD. CNN's are influential with temporal data adequate solution for images, where the user has to provide appropriate input representation. Stacked autoencoder (SAE), stacked denoise autoencoder (SDAE), etc., are the autoencoder-based models commonly IIoT based RFD framework. From the generative hybrid graphical model category, multiple RBMs or AEs are stacked together to generate deep belief networks (DBN) has been widely used in this context. To deal with the temporal data, sequential DL models such as a recurrent neural network (RNN), long short-term memory (LSTM), gated recurrent unit (GRU), etc., have been explored [16]. Generative adversarial network (GAN) is widely used from the deep generative model category.

8.2.4 Performance Checking Module

This module visualizes and analyses the performance of the manufacturing process with the help of some key performance indicators. The primary tools used in this

module are diagrams, charts, graphs, alarms, etc. It can either directly make visualizations from raw data collected through sensors or processed data which is delivered by the previous steps. These indicators help the operators to evaluate the performance and take decisions by visual inspection of the performance indicators.

8.2.5 Maintenance Planning and Corrective Decision Module

Based on the output of the performance indicators, maintenance planning and corrective decision are taken by scheduling optimization and other algorithm-based techniques [17] by this module. Certain optimization algorithms such as Genetic Algorithm (GA), Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), and Bee Colony Algorithm (BCA) are utilized in this module. The maintenance scheduling or other corrective measures are are the outcome of this module. Finally, the corrective measure is performed through the manufacturing control module, which gives necessary instructions to the manufacturing unit and sensors through IIoT protocols. The feedback control based on the decision from the maintenance decision-making module and other previous modules is the triggering source of this module.

8.3 IIoT Security Issues and Attacks

The data that IIoT deal with possessing different characteristics compared to the general big data. To better understand the demands for IIoT data analytics and security issues, it is needed to explore the properties of IIoT data. It is essential to address the fact that IIoT data is streaming data of large-scale. The IIoT sensors are distributed widely among the different applications, and they stream data continuously. This leads to generating data with temporal relation and at a huge volume. In connection to this, the property of heterogeneity of data due to the veracity of data acquisition devices has to be considered. Then in order to correlate with time and location information, timestamps must be included with IIoT data. The sensing frequency and other resolution information are also important. The data gathered from the industry is highly noisy. Irregular triggering of sensors and hard-working environments results in generating irregular and noisy data. All these issues will affect the security-related operations performed on data as discussed in Table 8.1.

Table 8.1 Attacks and security issues

Layer affected	Attack category	Description	Effect
Perception layer	Botnets	A malware that infects the misconfigured device or attacks the server	Attack the physical objects and affect the infrastructure
	Sleep deprivation attack	Disturb the sleep routine of battery-powered devices, and extend the wakeup period	Battery drains and shutdowns
	Node tampering and jamming	The node is wholly or partially undergoes physical replacement or wireless sensor nodes' radio frequencies being interfered with	It jams the node, and the service is denied
	Eavesdropping	The attacker overhears information that is passed via a private communication channel	Affects the confidentiality of the message. RFID is most affected
Network layer attacks	Man-in-the-middle (MIM.)	The attacker captures the total control of the communication channel	Attacker reads, changes, erases and inserts the message
	ARP cache poisoning	counterfeiting ARP packets of another host on the network	Enables impersonation for the attacker
	DNS Spoofing	Malicious mapping information forges the response of a recursive DNS query	Malicious mapping information has been stored in DNS resolver
	Session Hijacking	Attacker secure the user's session identifier	Attacker's session transferred instead of user's
	Denial of Service (DoS)/DDoS: U.D.P. Flood, SYN Flood, ICMP Flood, Ping of Death, Slowloris, N.T.P. Amplification	Malicious attack that aims in consuming resources or bandwidth of genuine users. Multiple UDP datagrams, continuous ICMP Echo-Request packets, TCP SYN Packets, large ping packets, TCP) SYN Packets, multiple HTTP requests are used by the attacker	Genuine users will not get service at the right time

(continued)

Table 8.1 (continued)

Layer affected	Attack category	Description	Effect
	Routing Attacks: Sybil Attack, Selective Forwarding Attack, Sinkhole Attack, Hello Flood, Wormhole Attack	Disrupt routing operation. Nodes are selected to break the network, absorb the traffic, selectively forward, tunnel the messages, etc	Wrong routing and message delivery
	Middleware Attacks: Cloud-Based- Cloud Malware Injection, Cloud Flooding Authentication Attacks- Brute Force, Dictionary Attack, Replay Attack Signature Wrapping Attack-	Information theft, flooding attack, etc., happens over the middleware components like a cloud by malicious activities. A malicious copy of the victim's service instance will be uploaded. Authentication attacks exploit the authentication process by finding the login credentials by a number of methods	Use users information to masquerade as that person
Application layer attacks	Malware	The devices are disrupted through firmware flaws using executable codes by the attackers	Disrupting the entire IoT architecture
	Phishing Attack: Spear Phishing, Clone phishing, Whaling,	Appearing to be a trustworthy entity, attackers extract critical information such as username and password from individual users, organizations, important officials, etc	Security breaches of IoT applications
	Code Injection Attack: SQL Injection, Script Injection, Shell Injection	Malicious executable codes are deployed into the address space of the victim's process. It injects SQL database statements, scripts, and commands	IoT application failure

8.3.1 The Way DL Deal with IIoT Security

DL effectively finds the security issues by a mechanism such as rule-based, signature-based, flow-based, and traffic-based. Traditional data flow and working conditions are predefined; it can successfully detect abnormal activities. But the frequent network updates and topological changes and to encounter intelligently planned attacks, the detection system should also be smart. Sensor network traffic flow is one of the main indications of the DL methods to identify security issues. From the anomaly detection perspective, DL considers the anomalies in a system as patterns that are different from a standard pattern. Any security issues mentioned in the previous section, as well as the fault conditions, creates abnormal patterns. For instance, the intruder's intervention in the connections of the victim creates abnormal traffic with the unusual data flow. These anomalies are categorized into three, namely, point anomalies, contextual anomalies, and collective anomalies.

A point anomaly is indicated by a data instance different from a normal pattern in the dataset, but the anomalous behavior of a data instance in a particular context is called a contextual anomaly. The anomalous behavior of a group of similar data instances compared with the entire dataset is called a collective anomaly. The abnormal activities of a host in a network are monitored with the Host Intrusion Detection System (HIDS) [18]. In remote devices also, these monitoring systems are deployed. Similarly, different network layers are analyzed to detect any possible security threats by Intrusion Detection System (NIDS) [19]. DL can analyze or detect Malware either statically or dynamically. In static, it is done in binary form, and in dynamic, the activities are monitored by executing binary files. DL can identify ransomware attacks where Malware encrypts the victim's computer for demanding a ransom for decryption. Similarly, the three types of intruders are detected by DL, named Masquerader, Misfeasor, and Clandestine user. A masquerader is a person who tries to get unauthorized access while the misfeasor tries to access privileged features that a user was not supposed to access. Clandestine user tries to achieve supervisory control of a system to avoid auditing and access control. IoT Botnet Attack Detection [20] is done by DL to avoid remotely controlling a device connected to a common protocol infrastructure by the attacker. By turning the device into a bot, a variety of attacks, including DDoS, is possible.

The situation becomes difficult to detect when there is no direct contact of the intruder with the elements of the network. As DL is capable of detecting small anomalies, it can identify the anomaly patterns that are difficult for humans to discover. In the case of Integrity, DL is a very effective tool to detect data integrity issues. A DL based system is trained using normal working conditions and sensor data flow. In the case of faults or attacks like command injection, the pattern difference is identified by DL models. The node that is compromising the integrity of the data is identified by the DL algorithm and can block it to maintain trustworthiness. So for the attacks targeting the security elements, DL is a very effective tool. The denial of service attack is very critical in sensor networks, which affects the availability of data to a great extent. DL methods are instrumental in detecting the broadcasting nodes,

sources with unfamiliar addresses, an unreasonable amount of traffic making nodes, etc., which are easily found out by DL algorithms. It can perform the operation of a simple network analyzer to detect the DoS attacks, as well as analyzing the network logs as a human operator do.

In the case of attacks affecting the confidentiality of data, it can be used to find the intruder. If the intruder merely eavesdrops on the network traffic, it is very hard to detect using DL. The attacker has to change the network flow to detect his presence by the DL algorithm. But once the intruder engages with an activity that changes the network flow, DL will be able to recognize the abnormal behavior. Normally the malicious activities severe than eavesdrop attacks and are classified under other attack categories. When the security elements are targeted, authentication of the network will be challenged. The is a security control technique more essential when the attacks are targeting the security element. The 'prevention is better than cure' policy is most appropriate for these kinds of attacks. Encryption, good password management, frequently changing passwords, key management, etc., are important in this scenario. Even though these techniques have their weaknesses, they improve the system's robustness against unauthenticated access. Authorization issues are indicated by the change in the normal pattern of traffic from the verified user can be one of the indications of authorization issues. Such activities include executing abnormal commands, manipulating the sensors and actuators, or sending random traffic on the network. The intruder attacks will eventually be exposed by a DL if the sensitivity of the learning technique is high. The normal conditions of the system learned to find the abusive commands, unauthorized users, or intruders. There are chances of identifying normal traffics as attacks if the DL method is not trained carefully. But IIoT security matters demands this overcautious because an undetected attack could results in a higher cost than false positives.

8.3.2 Challenges of IIoT Security Implementation

(1) Data safety and privacy

Safety of data that comes from a large number of IIoT devices of different types that are being passed from device to device is very challenging. So the security rules should be in compliance with these components. Avoiding unnecessary and irrelevant data is also crucial in IIoT. When the data has to deal with mobile and cloud platforms, the data must be in compliance with its regulatory structures.

(2) IoT software related issues

There are chances that IoT software disrupts access to the computer system. As the number of IIoT devices is increasing day by day, this kind of threat is also increasing at the same pace. So, we have to reduce such issues and deal with the challenges created by IoT ransomware.

(3) Lack of upgradation

The IoT devices and software are not updated from time to time to deal with the newly araising security threats. The enormous number of IIoT devices are being manufactured every day to meet the demands of the market without concern over security. But even after the implementation also, the devices are not checked or updated for security attacks that are faced by IIoT devices.

(4) Network issues

A properly configured networking system is essential for the smooth functioning of IoT devices. A number of factors in networking affect IIoT security. Hence the organizations must plan security policies to protect IIoT devices too. The attackers are able to achieve access to the network through open ports, buffer overflows, and DoS attacks. Moreover, proper care must be given to configure the gadgets to protect them from the attackers.

(5) Data consolidation and conversion

Data consolidation and transportation must consider security concerns. In IIoT, the privacy of data involves a variety of processes such as data segregation, avoiding tactful information. Also, in order to avoid unauthorized access to the device, the data is encoded. But there is a chance of Malware if a large number of smart IoT devices are unable to encrypt the user data. Proper encryption of data that does not lead to any threat by hackers. Weak encryptions are not recommended as it causes the intruders to gain access to data during data exchange.

(6) Strong password usage

Password security can be effective only if it uses strong passwords and keep it changing frequently. The IIoT must not use the default password and other credentials to enhance its security. Smart gadgets with weak passwords are most prone to hacker attacks. When the default passwords are inadequate, issues related to session management and lockout are present, and chances are there for the exposure of credentials, then the user interface with IIoT devices will become a failure.

(7) IoT hardware

IIoT hardware has to be undergone critical examination of the chip manufacturers to make it up to date with the security issues. The battery backup issue is a connection problem that the manufacturers must take care of for a long-running backup.

8.3.3 Industrial IoT Security Solutions

It is observed that more than 40% of security issues are due to brute force attacks or Malware, even though a number of intrusions have been there. There are four tiers assumed for security called device, communication, cloud, and lifecycle management. But the speed of growth of the industry makes it difficult for the security solutions to cope up so that no end-to-end security solution is available. Segmenting

the network is one solution in which those things that control the devices and equipment are kept as a separate network. A second method is to ensure basic structure, i.e., the credentials should be locked out after a few wrong tries and a change of default credentials upon activation. Imposing strong rules for multi-level password authentication can also control unauthorized access. It must make sure that buffer overflow doesn't affect the services, and it should not keep the ports open when it is used. Such practices will limit the chances for the intrusion of attackers. The firmware development and upgradation in a well-disciplined manner will help to solve the security issues to a great extent. Keeping up with industry standards and protocols, involvement, and collaboration in their development, etc., will help the industry to come out from a number of small security issues. Keeping a base architecture that addresses these issues, its standardization and inclusion will make the service providers be free from certain simple issues and concentrate on intensive security issues. This basic architecture provides a base security surety so that both purchasers and service providers have to least bother about the deploying platform security. So the services must include security as a part of the platform can only survive in the future.

8.3.4 SRF Case Study for IIoT Security with DL

We have done a literature review on SRF diagnosis works that have dealt with security issues of IIoT. But a very few researchers have attempted to address the data related issue that can handle the data security of IIoT with DL. One of such works was done by Yao et al. [21]. The raw data converted to color and polar images so that a number of security issues on data were overcome. Similar way, the raw input data converted to a symmetrized dot pattern (SDP) by Zhu et al. [22]. The signal's power spectral function was converted to a 2-D image form and was applied to a batch regularized CNN with VGG16 architecture by Yu et al. [23]. To handle multi-sensor data, a multi-stream CNN was proposed by Yuan et al. [24]. Some works attempted data fusion and/or future fusion methods. There were several attempts to make CNN suitable for multi-sensor data through data fusion or feature fusion methods along with structure alteration. Similarly, we can find 1-D convolution, multi-channel CNN, etc. Likewise, analyzing the DL works in SRF in terms of IIoT security perspective [25], there were no papers that strictly deal with IIoT security issues.

8.4 Conclusion

Rather than providing a general scenario of IoT security challenges and the role of deep learning in it, we have discussed the IIoT related security challenges in view of rotor fault diagnosis. A general description of the rotating machinery fault categorization, security and integrity issues, risks, etc., are given. Most importantly, an IIoT

framework which deals with the different phases of rotor faults with deep learning security provision is explained. The layer-wise categorization of the security attacks and their effects is also demonstrated to understand the types of security attacks better. Further, the DL approach in IIoT security issues has been discussed, and the challenges were analyzed. The market situation of IIoT security solutions is described briefly. Finally, we have investigated the literature of IIoT security challenges in RFD scenario, which revealed the fact that, so far, there have been no serious studies that happened in this regard. Hence, we suggest more works in IIoT security research to provide a more reliable fault diagnosis environment.

References

1. https://www.statista.com/statistics/1101442/iot-number-of-connecteddevicesworldwide/#:~:text=Internet%20of%20Things%20%2D%20active%20connections%20worldwide%202015%2D2025&text=The%20total%20installed%20base%20of,billion%20units%20worldwide%20by%202025
2. Mohan, N., Kangasharju, J.: Edge-fog cloud: a distributed cloud for internet of things computations. In: Proceedings of Cloudification of the Internet of Things (CIoT), 2016, pp. 1–6. https://doi.org/10.1109/CIOT.2016.7872914
3. Habeeb, R.A.A., Nasaruddin, F., Gani, A., Hashem, I.A.T., Ahmed, E., Imran, M.: Real-time big data processing for anomaly detection: a survey. Int. J. Inf. Manage. **45**, 289–307 (2019)
4. Yin, S., Li, X., Gao, H., Kaynak, O.: Data-based techniques focused on the modern industry: an overview. IEEE Trans. Industr. Electron. **62**(1), 657–667 (2015)
5. Jeschke, S., Brecher, C., Song, H., Rawat, D.B.: Industrial internet of things
6. Li, Y., Kurfess, T., Liang, S.: Stochastic prognostics for rolling element bearings. Mech. Syst. Signal Process. **14**(5), 747–762 (2000)
7. Pan, J., Yang, Z.: Cybersecurity challenges and opportunities in the new edge computing+ iot world. In: Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization, ACM, 2018, pp. 29–32
8. Chen, P.: Foundation and Application of Condition Diagnosis Technology for Rotating Machinery. Sankeisha Press, Japan (2009)
9. Patel, T., Darpe, A.: Vibration response in misaligned rotors. J. Sound Vib. **325**, 609–628 (2009)
10. Fahy, F., Thompson, D.: Fundamentals of sound and vibration. CRC Press, Boca Raton (2016). https://doi.org/10.1201/b1834 8
11. Caesarendra, W., Kosasih, B., Tieu, A.K., Zhu, H., Moodie, C.A., Zhu, Q.: Acoustic emission-based condition monitoring methods: review and application for low speed slew bearing. Mech. Syst. Signal Process. **72**, 134–159 (2016)
12. Lu, S., He, Q., Zhao, J.: Bearing fault diagnosis of a permanent magnet synchronous motor via a fast and online order analysis method in an embedded system. Mech. Syst. Signal Process. **113**, 36–49 (2018)
13. Oumaamar, M.E.K., Maouche, Y., Boucherma, M., Khezzar, A.: Static air-gap eccentricity fault diagnosis using rotor slot harmonics in line neutral voltage of three-phase squirrel cage induction motor. Mech. Syst. Signal Process. **84**, 584–597 (2017)
14. Lu, Y., Wang, F., Jia, M., Qi, Y.: Centrifugal compressor fault diagnosis based on qualitative simulation and thermal parameters. Mech. Syst. Signal Process. **81**, 259–273 (2016)
15. I. Guyon, A.E.: An introduction to variable and feature selection, J. Mach. Learn. Res. **3**, 1157–1182 (2003)
16. Nath, A.G., Sharma, A., Udmale, S.S., Singh, S.K.: An early classification approach for improving structural rotor fault diagnosis. IEEE Trans. Instrum. Meas. **70**, 1–13 (2020)

17. Konar, P., Sil, J., Chattopadhyay, P.: Knowledge extraction using data mining for multi-class fault diagnosis of induction motor. Neurocomputing **166**, 14–25 (2015). https://doi.org/10.1016/j.neucom.2015.04.040
18. Cox, K., Gerg, C.: Managing security with Snort and IDS tools. O'Reilly Series. O'Reilly Media, Inc. p. 3 (2004). ISBN 978-0-596-00661-7
19. Mazini, M., Shirazi, B., Mahdavi, I.: Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. J. King Saud Univ. Comput. Inf. Sci. **31**(4), 541–553 (2019)
20. Soe, Y.N., et al.: Machine learning-based IoT-Botnet attack detection with sequential architecture. Sensors **20**(16), 4372 (2020)
21. Yao, Y., Li, Y., Zhang, P., Xie, B., Xia, L.: Data fusion methods for convolutional neural network based on self-sensing motor drive system. In: Proceedings: IECON 2018—44th Annual Conference of the IEEE Industrial Electronics Society vol. 1, pp. 5371–5376 (2018)
22. Zhu, X., Hou, D., Zhou, P., Han, Z., Yuan, Y., Zhou, W., Yin, Q.: Rotor fault diagnosis using a convolutional neural network with symmetrized dot pattern images. Meas J Int Meas Conf **138**, 526–535 (2019)
23. Yu, W., Huang, S., Xiao, W.: Fault diagnosis based on an approach combining a spectrogram and a convolutional neural network with application to a wind turbine system. Energies (2018)
24. Yuan, Z., Zhang, L., Duan, L.: Multi-sourced monitoring fusion diagnosis for rotating machinery faults. In: Proceedings—Annual Reliability and Maintainability Symposium 2019, vol. 1, pp. 1–7 (2019). https://doi.org/10.1109/RAMS.2019.876901 8
25. Nath, A.G., Udmale, S.S., Kumar Singh, S. (2020) Role of artificial intelligence in rotor fault diagnosis: a comprehensive review. Artif. Intell. Rev. 2020. (Online). Available: https://doi.org/10.1007/s10462-020-09910-w