Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Anomaly Classification and Recovery in Industrial Machinery and Academic Applications: A Systematic Mapping based on Artificial Intelligence and Machine Learning Approaches

Muhammad Yousaf (Corresponding Author)
Faculty of Computer Science & IT, Superior University Lahore, 54000, Pakistan
Email: su92-mscsw-f24-005@superior.edu.pk
Talib Nadeem Usmani
Advance Cybersecurity Engineer at Honeywell, USA
Email: talib@securitypentester.ninja
Nasir Ayub
Deputy Head of Engineering Calrom Limited, M16EG, United Kingdom
Email: nasir.ayyub@hotmail.com
Umair Ghafoor
Deputy Head of Engineering Calrom Limited, M16EG, United Kingdom
Email: umairghafoor@hotmail.com
Asfar Ali
Information Technology Department LHC, Department of Information Technology, Superior University Lahore, 54000, Pakistan, Email: asfarali761@gmail.com
Syed Muhammad Rizwan
Department of Computer Engineering, University of Engineering and Technology Lahore, Pakistan Email: rizwan.naqvi@ieee.org
Hamayun Khan
Department of Computer Science, Faculty of Computer Science & IT, Superior University Lahore, 54000, Pakistan Email: hamayun.khan@superior.edu.pk
Muhammad Zunnurain Hussain
Bahria University Lahore Campus, Email: zunnurain.bulc@bahria.edu.pk
Majid Ali
Tec Joints, Block G3 Phase, 2 Johar Town, Lahore, Pakistan
Email: majidq67@gmail.com

ABSTRACT

The problem of unscheduled shutdowns in the industry and Academic sectors has been of great concern and has led to serious losses in the economy, as well as the security of various sectors being compromised. Recovery of anomalies is now a major research topic of contemporary data-driven systems, even though anomaly detection is a well-researched topic, recovery mechanisms are relatively under-researched. This paper is a review paper on statistical, machine learning, deep learning, and hybrid techniques of anomaly recovery in both academic and industry environments. The paper compares the existing

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

approaches, pinpoints the gaps in the studies and describes the trends in the future. The findings also indicate the importance of integrated detection and recovery systems in improving the performance of the systems and the reliability of the data. The increasing use of data-oriented technologies within the educational and industrial context has resulted in the development of vast amounts of data on digital platforms, sensors, and automated surveillance systems. However, these datasets are often affected by anomalies caused by sensor malfunctions, communication problems, system malfunctions, or human mistakes. These anomalies may have a major influence on the reliability of data and lower the quality of analytical models applied to make decisions. Despite detailed studies on the methods of anomaly detection, relatively less emphasis has been placed on anomaly recovery, which aims at re-creating corrupted or missing data values. This paper entails a detailed examination of anomaly detection and anomaly recovery methods based on machine learning methods. The paper discusses the classical statistical techniques for Anomaly Classification and Recovery in Industrial Machinery and Academic Applications and present a systematic mapping based on Artificial Intelligence, Machine Learning algorithms and deep learning models that can be applied to find abnormal patterns in data sets used for Industrial and Academic Applications. In addition, we discuss reconstruction-based recovery models, such as Autoencoders, Variational Autoencoders, and Generative Adversarial Networks to fix corrupted data. The article recognizes the gaps in the existing literature on integrated frameworks of anomaly management and the necessity to integrate detection and recovery processes in one framework. The results show that machine learning models have a significant positive effect on the accuracy of anomaly detection, whereas deep learning and generative models provide opportunities to use them to recover anomalies. A combination of these may be applied to enhance the reliability of data and the functionality of the system, both in the academic and industrial contexts. Finally, the paper offers future research directions on how to develop scalable and intelligent anomaly management systems that would operate in large data environments.

Keywords: Anomaly Recovery, Machine Learning, Deep Learning, Data Quality, Industrial Systems, Anomaly Detection, Anomaly Recovery, Machine Learning, Deep Learning, Industrial Monitoring, Academic Data Analysis, Data Reconstruction

Introduction

Unplanned downtime, or unscheduled production stoppage due to equipment failure, is a chronic and expensive problem in contemporary production. It is always found that downtime wastes between 5-20% of the total production time per sector in different industries [1], and a survey that was conducted globally revealed that 82 percent of the companies reported at least one major downtime in the last three years [2]. The economic costs are substantial; according to the estimates by Deloitte, unplanned downtime costs industrial manufacturers around USD 50 billion every year on a global scale [3]. In the case of large-scale automotive manufacturing plants, unplanned downtime may lead to very high losses, hourly costs of downtime can be as high as USD 2 million, equal to lost production, overtime, and logistical fines [4]. In addition to the direct financial losses, the downtime may result in the wastage of raw materials, default on timelines, and disruption of the supply chains, especially in the just-in-time (JIT) systems [5]. Moreover, industrial accidents are usually preceded

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

by equipment failure, which is evidenced by the Deepwater Horizon disaster, where maintenance failures led to an explosion that caused the death of 11 people [6]. The conventional maintenance approaches are ineffective when it comes to these complex issues. Reactive maintenance that entails fixing machines after a breakdown is an easy process, but results in unpredictable downtime, and is excessively costly in the long-run [7].

$$p\left(C_k\right) p\left(x|C_k\right) = p\left(C_k\right) \prod_{i=1}^{n} p\left(x_i|C_k\right) \quad \text{Eq (1)}$$

Preventive maintenance, which is performed at a fixed rate, helps to reduce the risks but may also lead to unnecessary replacement of parts or missed failures between inspections [8] a better method, condition-based maintenance (CBM), continues to rely heavily on advanced sensors and monitoring infrastructure, implying that maintenance responses are still commonly only prompted when monitored indicators exceed predefined thresholds, which makes the method rather reactive by nature [9]. Such restrictions have generated a strong desire to have a smarter, more proactive strategy.

Predictive Maintenance (PDM)

The answer is the shift in paradigm to predictive maintenance (PdM), which is a concept that can be facilitated by the fourth industrial revolution (Industry 4.0). PdM is a data-based approach to maintenance that relies on technologies, such as the Internet of Things (IoT) [10], artificial intelligence (AI) [11], and analytics of big data [12]. Real-time measurements are taken on the crucial parameters, which include vibration, temperature, and pressure, using the sensors. This data is then fed through advanced machine learning (ML) algorithms to identify these subtle signs of machine degradation, estimate the remaining useful life (RUL) of a machine and can be serviced where and when it is most needed to produce the minimal amount of disturbance [13]. This would be very helpful and a study conducted by the U.S. Department of Energy suggests that a switch to PdM would, at best, cut down on maintenance time by up to 35 per cent and would be capable of saving 8-12 per cent on maintenance costs compared to preventive measures [14, 15]. Another business model effect of PdM is that it facilitates maintenance-as-a-service that can assist the manufacturing industry to minimize downtime, enhance customer relationships and competitiveness in industries like energy and transport [16, 17].

$$p_\lambda\left(C_k\right) = \frac{\sum_{i=1}^{N} I\left(y_i = C_k\right) + \lambda}{N + K\lambda} \quad \text{Eq (2)}$$

The advent of digital technologies has contributed to the transformation of the systems of education and industry towards an environment saturated with data. Enterprise applications and sensor networks produce and document large volumes of various types of information in learning management systems [18, 19]. Hardware failure, cyber-attacks, human errors and interference by the environment compromise the quality of information or disrupt the analysis process. Conventional explanations are not effective in dealing with the intricacy and divergence of the datasets [20, 21].

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Fault Detection and Diagnosis (FDD)

Fault detection and diagnosis (FDD) is a fundamental technological element of PdM, and it aims at determining and categorizing familiar fault conditions. Model-based FDD is based on deep knowledge of the processes, whereas data-driven FDD progressively applies machine learning to analyze sensor data [22-24]. Nevertheless, there are also new or poorly labeled faults in industrial systems that the traditional FDD cannot identify. This is where anomaly detection techniques are necessary since they establish abnormal behavior without prior definition of faults [25, 26]. This is facilitated by online and unsupervised learning, which adapts to ever-changing industrial streams of data. One of the biggest problems in the two fields is interpretability. Most deep learning models are black boxes and the engineer may not know why an anomaly or a fault has been detected. Consequently, Explainable AI (XAI) is becoming a central part of the PdM research to generate human-explainable knowledge to be utilized in root-cause analysis [27, 28]. Machine learning/deep learning, on the other hand, are flexible in identifying and correcting the aberrant data. This paper provides a useful description of current abnormality recovery methods. Reason for Industry Shift to Industry 4.0 [29, 30].

$$p_\lambda\left(x_1 = a_j | y = C_k\right) = \frac{\sum_{i=1}^{N} I\left(x_1 = a_j, y_i = C_k\right) + \lambda}{\sum_{i=1}^{N} I\left(y_i = C_k\right) + A\lambda} \quad \text{Eq (3)}$$

We see Industrial Technologies get integrated with IoT and CPS. The connection of smart devices, sensors and machines to cloud computing platforms enables efficient monitoring, automation, data collection and control operations [31, 32]. The transition is being aided by technologies like AI and ML. Modern systems generate large volumes of data through digital platforms, smart devices, sensors, and automated monitoring systems. In industrial settings, technologies such as the Internet of Things (IoT), Cyber-Physical Systems (CPS), and smart manufacturing infrastructures continuously collect operational data from machines and production processes. Academic institutions increasingly rely on digital learning management systems, student information systems, and online assessment platforms to manage educational data [33].

Table 1: Types of Anomalies and Their Characteristics [34]

Types of Anomalies and Their Characteristics			
Type of Anomaly	**Description**	**(Academic)**	**(Industrial)**
Point Anomaly	A single data value that deviates sharply from normal	Sudden zero marks in an exam	Sudden spike in temperature sensor

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Contextual Anomaly	Normal in one context but abnormal in another	Low marks during exam week	High temperatures in the winter season
Collective Anomaly	A group of data points showing abnormal behavior together	Sudden drop in attendance for 7 days	Multiple sensors drifting together
Pattern Anomaly	Abnormal sequence or trend in data behavior	Irregular LMS login pattern	Abnormal vibration pattern
Missing-Data Anomaly	Missing or partially missing data values	Missing attendance records	Sensor signal dropout

Machine Learning in Anomaly Recovery and Detection

In the recent past, approaches to machine learning have been deemed to be successful as far as the recovery of anomalies is concerned. Models based on reconstruction, such as autoencoders, can be trained to learn compact representations of normal data and be capable of generating missing or corrupted values. Generative models can be used to generate realistic synthetic data to replace anomalous observations, and include Variational Autoencoders (VAEs) and Generative Adversarial Networks (GANs). These methods enable smart systems to ensure continuity of data and minimise the effects of anomalous measurements. Though various studies have suggested models of anomaly detection, there are relatively few studies on the integrated models of anomaly detection and anomaly recovery in a single framework. A number of approaches are currently in use, and they largely treat detection and reconstruction as separate processes, which limits their use to real-world scenarios [37, 38]. Also, a lot of models are created concerning a particular domain and do not have cross-domain applicability between educational and industrial settings. Due to the increased demand to use smart monitoring systems, there is an increased need to have effective structures that can not only detect anomalies but also automatically recover the corrupted information. Machine learning has the potential to provide a powerful toolkit of solutions to these problems through permitting adaptive, scalable and data-driven anomaly management solutions [39, 40].

$$y_j = f\left(\sum_{i=1}^{n} w_{ji} x_i - \theta_j\right) \quad \text{Eq (4)}$$

Therefore, this review paper aims to analyze the existing literature on anomaly detection and anomaly recovery algorithms and particularly their application in academia and industry. The article talks about machine learning algorithms, statistical algorithms, and deep learning algorithms to identify and reconstruct abnormal data. Additionally, it indicates the gaps that exist in the existing studies and how the future of the integrated anomaly recovery models that may increase the dependability of data and performance of a system may appear [41, 42]. The usage of Artificial Intelligence and Machine Learning is facilitating the effective utilization of data produced by IoT [43]. A digital twin is a virtual model that creates a digital replica of a physical entity, system, etc., which runs in parallel. The digital twin is built on quality sensor data that provides reliable communication protocols. These handheld replicas of physical assets are models, processes, and systems of the ship. They would use real-time data to monitor

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

the performance and condition of machinery [44, 45]. A good digital twin provides improvements in system transparency and helps simulate, model and predict the performance of challenging systems in dynamic scenarios. The task of executing real-time digital twin architecture faces some significant challenges [46]. Scholars have discussed IoT, ML and digital twin technologies separately as well as together in the literature. Although very rare to see, a unified implementation of these is desirable for a real industrial system. Many systems, particularly in food processing, small-scale industries, and education, continue utilizing traditional control systems with a low degree of automation [47, 48]. The implementation of ML-based digital twins in the food processing industry and small industries. The task of executing real-time digital twin architecture faces some significant challenges. Although very rare to see, a unified implementation of these is desirable for a real industrial system [49, 50]. Many systems, particularly in food processing, small-scale industries, and education, continue utilizing traditional control systems with a low degree of automation. The use of ML-based digital twins in food processing. In recent years, the rapid growth of data-driven technologies has significantly transformed both academic and industrial environments [51, 52].

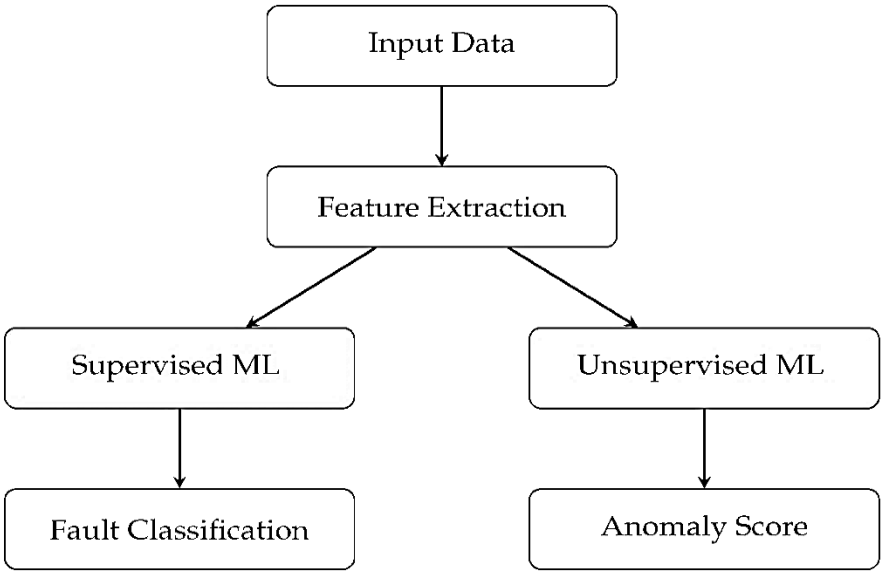

Figure 1: Machine learning approaches: Supervised models classify faults, while unsupervised models detect anomalies [53].

One of the major issues affecting modern data-driven systems is the presence of anomalies within collected datasets. Anomalies are data points or patterns that deviate significantly from expected behavior [54, 55]. These deviations may be due to sensor malfunctions, system malfunctions, human error, disruption in communication, or malicious cyber attack. The deviations in the academic systems can be reflected in the form of the lack of attendance files, peculiar test results, or irregular tendencies in the online learning processes [56]. The anomalies in the industrial environment may be due to faulty sensors, unexpected machine behavior, abnormal temperature changes, or network connectivity issues. In cases where these anomalies are not identified or corrected, they

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

can have a negative effect on the data analysis, decision-making processes and system reliability [57, 58]. Traditionally, research on anomaly detection, i.e., detecting abnormal data points within datasets, has been viewed as the traditional approach to anomaly management. To identify anomalies in structured and unstructured data, different statistical and machine learning methods have been devised [59, 60].

$$g^t(x) = \sum_{i=1}^{t} y_i \prod_{j=1, j \neq i}^{t} \frac{(x - x_j)}{(x_i - x_j)}$$

Eq (5)

The first ones were the methods that operated on the statistical numbers, such as Z-score analysis, SD levels, and interquartile range analysis. Despite the simplicity and computational efficiency of these methods, they are not often able to capture the complicated nonlinear relationships of high-dimensional data [61, 62]. As a result, increasingly, systems of anomaly detection are based on machine learning algorithms capable of learning patterns based on historic data, and alerting about aberrant behavior. The machine learning techniques useful in the context of this task of detecting anomalies have demonstrated promising results with Support Vector Machines (SVM), Decision Trees, Random Forest, and Isolation Forest [63]. In more recent times, deep learning models, such as Autoencoders, Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) networks, have been extensively used to analyze large-scale and time-series data. Complex data structures and time dependency can be modeled by such models, which improves the precision of anomaly detection in dynamic environments [64, 65]. Although the research on anomaly detection has made considerable advances, the issue of anomaly recovery has not been thoroughly investigated yet. It is not always necessary to detect an anomaly and especially in systems that require continuous and correct data feeds [66, 67]. In the event of abnormal or missing values, it may be necessary to reconstruct or recreate the proper data to have the systems functioning and the data intact. This is known as the anomaly recovery, which includes reconstruction of the corrupted data using predictive or generative models with reliable values. Recovery of anomalies is particularly crucial in academic and industrial use, where the quality of data is very critical in decision-making.

$$fd_k(x) = \frac{1}{n} \sum_{i}^{n_m} l(p_i, q_i; x)$$

Eq (6)

The absence or wrong information in the education systems can result in the wrong evaluation of the student's performance and academic development. Similarly, in industry, faulty sensor readings may result in failure to diagnose the system correctly or failure to monitor production effectively [68, 69]. Therefore, it requires good anomaly recovery procedures to ensure that there is appropriate analytics and that the system functions properly [70]. The review provides a methodical literature review of anomaly detection, data reconstruction and machine learning. This was done through the identification of a limited number of keywords that can be found in the related research

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

publications as identified by a host of online databases, including IEEE Xplore, Scopus, Web of Science, and Google Scholar. The relevance was used to select the inclusion studies so as to determine the quality of publication and rigor of the methods. In the article, brief descriptions of the eighteen chosen papers of the special issue of the journal about improved methods around soft computing are given. The results of these studies were compared and analyzed by researchers.

Literature Review

Initial investigations on the handling of anomalies were concerned with statistical methods like Z-score, control charts, and threshold-based methods. These techniques are computationally efficient, but do not work well in complex and non-linear environments. One-Class Support Vector Machines, Isolation Forests, and clustering-based methods are all machine learning methods that enhance adaptability and generalization. Robustness was also improved by ensemble learning as a result of integrating several classifiers [71, 72]. Deep learning models (Autoencoders, LSTM networks, Transformers) have been demonstrated to be more effective in time-series and high-dimensional data analysis [73]. Recently, the study of generative models of realistic data reconstruction has also been investigated. It has been observed that major improvements in anomaly detection have been achieved, in particular, by using deep learning and time series forecasting models. The principal techniques that enhance performance in detection in a complex environment are LSTM-based prediction, dynamic thresholding and reconstruction-based autoencoders. Nevertheless, the anomaly recovery domain is a poorly researched area with no comprehensive frameworks that can bring together detection, reconstruction, and validation processes [74, 75]. The review emphasizes the significance of domain-free, interpretable and scalable systems of managing anomalies using advanced machine learning and generative models. Filling these gaps is crucial to enhancing the quality of data, system reliability, and decision-making both in academia and industry [76]. The original study of anomaly management embraced the use of mainly statistical tools such as threshold analysis, control charts, and Z-score tools. Although computationally effective and easy to operate, they have problems with the modeling of non-linear trends [77, 78]. The below figure shows the anomaly Management Process in Intelligent Systems. The process of anomaly management presented in the diagram includes anomaly detection, identification, recovery and corrective measures, and is represented by repair or replacement processes. The intelligent systems anomaly management entails a structured workflow, which is significant in maintaining the integrity and performance of the system.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851
Online ISSN 3007-3197
Print ISSN 3007-3189

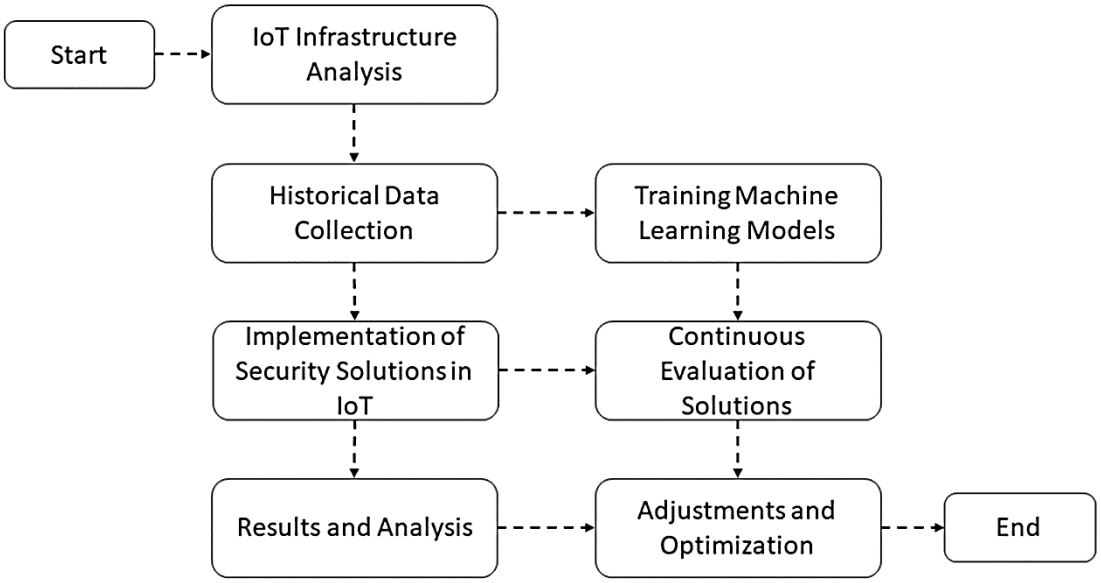

Figure 2: Generic Anomaly Management Flowchart illustrating a smart manufacturing system [79].

This process involves four major processes that are detection, identification, recovery and corrective action [80]. To begin with, anomalies will be detected and procedures to discover their nature and cause will be launched. After identification, a recovery process is undertaken on the system, which may involve repairing or replacing the system in order to restore the system to functionality and reduce the consequences of the anomaly. To gain a more accurate view of this workflow, the image that is included in the text is a visual representation of this workflow, indicating the most important steps that can be considered essential in an efficient management of anomalies. The accuracy of detection and flexibility turned out to be a breakthrough with the introduction of machine learning-based approaches, such as One-Class Support Vector Machines, Isolation Forests, and many others, clustering algorithms [81, 82].

Hybrid Anomaly Management Frameworks

The deviant patterns could be due to aircraft failures, environmental interferences, cyber attacks, or there could be no ability to access data. These anomalies should be detected to avoid system failure, waste in operation and quality of information. The main methods applied to the detection of anomalies in the early years of research were mainly based on statistical methods. The analysis of Z-score, thresholding according to standard deviation, and interquartile range (IQR), was also widely used in common statistical methodologies as an easy way to abbreviate abnormal data [83, 84]. According to these methods, the normal data must also be of a specific distribution, and deviations of the mean values will also show that there are abnormalities present in the data. Even though statistical methods are easy, and computationally efficient, they do not usually observe complicated patterns that exist in high-dimensional data [85]. As modern industrial systems generate huge amounts of heterogeneous information, there must be more advanced means to expose nonlinear ties and time dependencies [86]. To overcome these limitations, machine learning-based anomaly detection algorithm concepts have been depicted. Machine

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851

Online ISSN 3007-3197
Print ISSN 3007-3189

learning algorithms can also learn patterns over past data and identify anomaly observations without explicitly requiring a set of statistical assumptions. Support Vector Machines (SVM), k-Nearest Neighbor (k-NN), Decision Trees and the Random Forest algorithms are the most common of these methods [87, 88]. These algorithms derive the differentials in their classification of data by learning normality and abnormality. In particular, random forest types of models in detecting anomalies in industry have shown a high degree of performance on data of high dimensions and noise [89]. The other machine learning model that can be useful in identifying anomalies is the Isolation Forest, which identifies anomalies by isolating abnormal observations through random partition of the data space. In contrast to distance-based models, Isolation Forest is based on the isolation properties of anomalies, instead of density estimation [90]. The approach has been widely used regarding large datasets as it is computationally effective and scalable. In recent years, the topic of deep learning approaches to the field of anomaly detection has become of huge interest. DNNs can learn more complex data structures and emulate latent correlations in a large dataset. The Autoencoder is one of the most popular deep learning methods that is utilized in detecting anomalies. Autoencoders are neural networks designed to come up with condensed forms of input data [91, 92].

$$minimum f d_k(x) = \sum_{m=1}^{C*M} \frac{1}{n} f d_m(x)$$

Eq (7)

In the reconstruction, the model attempts to reconstruct the original input. When the reconstruction error is big, then it is approached as an anomaly, or the input data is treated as a big error. Autoencoders have been successfully used in sensor monitoring, network protection and evaluation of industrial machinery. Another well-known deep learning architecture is the Long Short-Term Memory (LSTM) network, which is used to recognize anomalies in time-series data and is particularly suitable for processing time-series data [93, 94]. LSTM networks can learn long-term relationships and temporal patterns of sequential data. LMST-based anomaly detection models can be highly applicable in the industrial environment where sensor data are observed over time, in which case, the deviation of a system can be detected [95, 96]. Very sophisticated techniques accumulate reconstruction and prediction mechanisms to augment the functionality of anomaly detectors. An example is the LSTM Autoencoders, which are a combination of preserved features of autoencoders and the time learning of LSTM networks [97, 98]. The encouraging results of these hybrid architectures towards the detection of more complicated anomalies in sequential data have been shown. Besides the research process of detection, another important research area has been established in the area of anxiety recovery. Though anomaly detection aids in identifying the abnormal data values, data recovery or reconstruction of the lost corrupted data is also relevant in the reliability of systems [99, 100]. A large number of industrial systems are based on continuous data streams in making decisions. Lack or inaccurate data may have a profound impact on predictive models and control systems. Recovery techniques that utilize reconstruction are widely used in addressing this problem [101]. Autoencoder

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

models are not only restrictive to the use of anomaly detection, but also for the reconstruction of missing or corrupted data values. Likewise, Variational Autoencoders (VAEs) can be used to produce probabilistic restructions of input data through the learning of latent distributions. This application is possible in models of this type, particularly in the case of partial or noisy data.

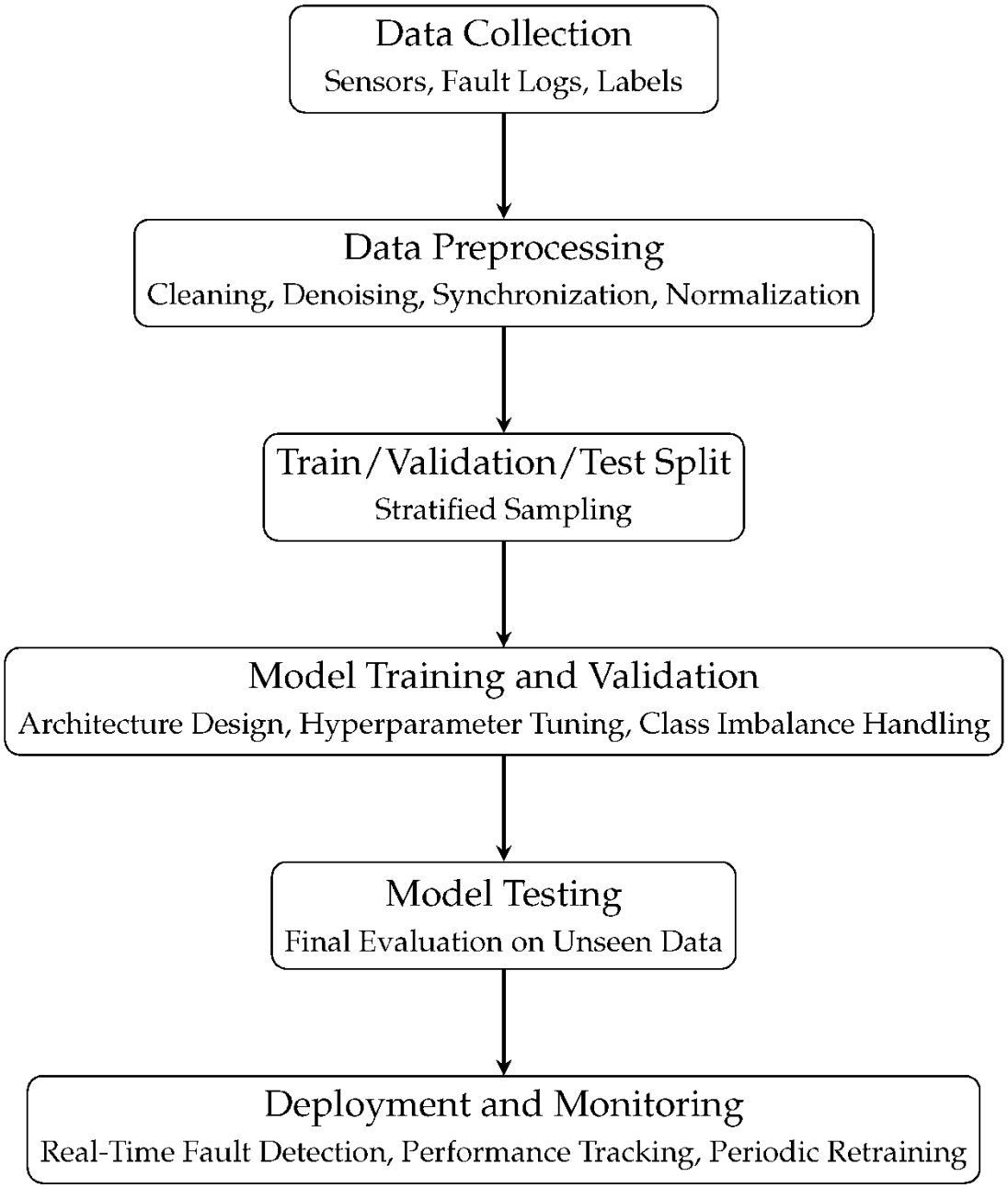

Figure 3: Current Anomaly Management for industrial faults detection [102].

Another new technique of anomaly recovery is Generative Adversarial Networks (GANs). In GANs, there are two neural networks and they are two (a generator and a

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

discriminator) that are trained simultaneously. The generator attempts to reduce the actual data samples, whereas the discriminator attempts to learn how genuine the data generated sample is. This adversarial training can be performed on GANs that can generate high-quality synthetic data, which may be budgeted as substitutes for anomalous or missing observations [103].

Data-driven Technologies in Academic and Industrial Environments

Hybrid anomaly management systems that possess both the detection and recovery mechanisms have been tested in other new research. The collective resiliency of the system and data integrity of smart monitoring systems is improved with such a combination of solutions [104]. Though the study on anomaly detection and recovery has advanced, there are still some challenges that are yet to be addressed. Most of the application fields have a lot of models and they may not be able to generalize to other datasets. Moreover, deep learning models can require large datasets to be trained, and they can require high computational power. Other challenges involve interpretability as complex neural network architectures may behave like a black box, in the sense that users of the system are unable to understand how they are the drivers behind decisions being made for anomaly predictions. Moreover, it is challenging to detect and fix irregularities in extensive systems of IoT and cyber-physics in any real-time [104, 105]. These environments produce streams of data that need quick data processing and decision-making. Thus, a research area of focus is coming up with scalable and efficient anomaly management frameworks. Overall, it can be concluded that research indicates that machine learning and deep learning approaches have significantly increased the capability of detecting anomalies. These methods assume that the data that takes place normally is distributed tightly and anomalies in these cases are in the form of an excess variance in the expected statistical inclination. Despite the ease of statistical methods that is easy to use and easy to calculate, it is ineffective in capturing complexities in high-dimensional and non-linear data [110].

$$G_B = \sum_{i=1}^{N} W_i \,.\, G_{L_i}$$

Eq (8)

In a bid to overcome these weaknesses, researchers came up with machine learning-driven anomaly detection techniques. Machine learning algorithms can be trained to learn patterns along historical data and identify abnormal observations, without a hard and fast commitment to any statistical assumption. Among the most famous algorithms, there are Support Vector Machines (SVM), Decision Trees, Random Forests and k-Nearest Neighbor (k-NN) algorithms [111]. These models classify information in lines of learning between normal and abnormal patterns. Random Forest models have been particularly successful as regards both industrial monitoring systems, not only can they withstand noise, but also they can handle extremely large feature spaces. Another popular machine learning anomaly detection algorithm is the Isolation Forest algorithm. Isolation Forest is capable of identifying anomalies, whereas distance-based algorithms cannot identify them. Abnormal observations are identified by isolating abnormal observations with random partitions of the dataset

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

[112]. The anomalies are not common and are unlike usual data and can be divided with fewer partitions. This algorithm is computationally inexpensive and appropriate for large-scale data and is used in industrial monitoring studies. Over the last several years, deep learning techniques have had a continuously increasing impact on research in the context of anomaly detection. Hierarchical data representations and capture of complex data relationships in large data collections can be learned with deep neural networks [113]. An Autoencoder is considered to be one of the most popular deep learning models in anomaly detection. Autoencoders are neural networks that are trained in such a way that they learn to create small-sized data out of the large-sized input data, and then restore the size of the data to its original size. In case the reconstruction error is huge, then the input data is considered to be anomalous. This has been effectively used in sensor monitoring, network intrusion detection, and industrial fault detection [114]. Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks have been discovered to perform excellently when it comes to time-series data. These models are able to handle the time dependencies and sequential trends of dynamic datasets [115].

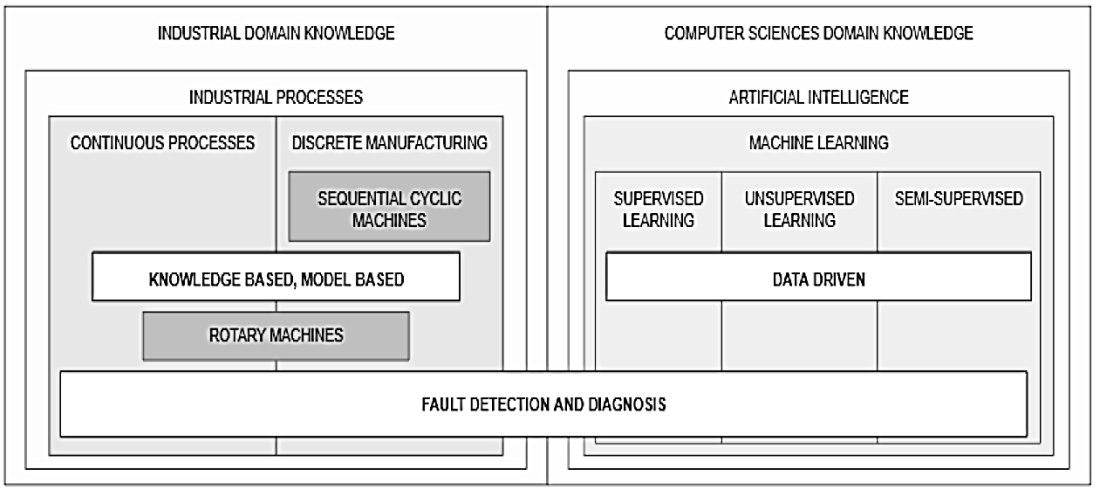

Figure 4: Classical and data-driven detection in Anomaly Management [116].

In the industry, based on sensor data that is continuously measured over a period, LSTM-based anomaly detection models can detect deviant patterns and inconsistent behavior of the system. Despite the significant focus put on the application of anomaly detection techniques, only a small part has been carried out regarding anomaly recovery [117]. The detection methods will only identify values that are anomalous, but not able to deal with the corruption of the data values by the corruptors. Practically, it suffices not only to identify the aberrations, as one must receive complete and accurate datasets to effectively utilize analytical models and automated decision systems in real-world systems. To curb the same, researchers have proposed methods of recovery using reconstruction means. Besides applying to the detection of anomalies, autoencoders enable the re-creation of the missing/corrupted values [118, 119]. Similarly, Variational Autoencoders (VAEs) can be trained to

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

make probabilistic representations of input data and can be used to simulate missing observations in cases of uncertainty. Another possible way forward in the future that promises to recover anomalies is through the use of Generative Adversarial Networks (GANs) [120]. GANs incorporate two neural networks (called the discriminator and the generator), which are simultaneously trained. The non-real sample generator tries to generate life-like synthetic data, whereas the discriminator tries to decide whether it is real or artificial data [121]. With such adversarial training, GANs will be able to generate high-quality data, which can be used to replace anomalous or missing data. However, recent studies have delved into the hybrid anomaly management models that combine both mechanisms of detection and recovery [122].

$$o_t = \sigma(W_o x_t + W_o h_{t-1} + b_o) \quad \text{Eq (9)}$$

They are statistical (or machine learning) based systems that detect anomalies first, and then use forecasting or generative models to recreate corrupted datapoints. The combined methods enhance the resilience of the systems and continuity of data in intelligent monitoring systems [123]. Although the novelty of the topic of anomaly detection and recovery has been developed significantly over the years, there are still several problems. Existing models are numerous and specialized in some areas of application and may not be effective with different data sets. In addition, models based on deep learning have high information demands and are computationally costly [124]. The second weakness is that complicated machine learning models are hard to interpret and therefore, the task of the system operators would be difficult to understand the logic behind how the abnormalities are predicted. Besides, the massive IoT and cyber-physical systems to date seem to have issues in terms of detecting anomalies and recovering them in real-time. These spaces generate streams of data, which need to be processed in real-time and make decisions immediately [125]. The development of scalable and efficient tools to deal with the anomalies, therefore, is a focal point of research. In sum, literature has demonstrated that machine learning and deep learning has highly advanced the features of detecting anomalies. Still, they should come up with more consolidated structures that can capture both the proper anomaly detection and effective anomaly recovery procedures, particularly when the quality of data is paramount in decision-making [126].

Anomaly Recovery

Anomaly recovery steps taken after anomaly occurrence have been identified. It also re-scales the levels of engagement of systems and operations in order to minimise the impoverishment of performance and collapse. Therefore, the entire procedures aimed at minimizing or correcting the non-standard conditions might comprise anomaly recovery. Remedy any faulty part, and disturbed data, and functioning parts [127]. This is achieved without end-of-life replacement of any defective component, but in reality, maintenance or calibration is put in place during the process. Replacement entails the removal of faulty or unwarranted parts and the replacement with new or working parts. The strategy is used in cases where repair is not worthwhile, inefficient, or not economical [128].

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851

Online ISSN 3007-3197
Print ISSN 3007-3189

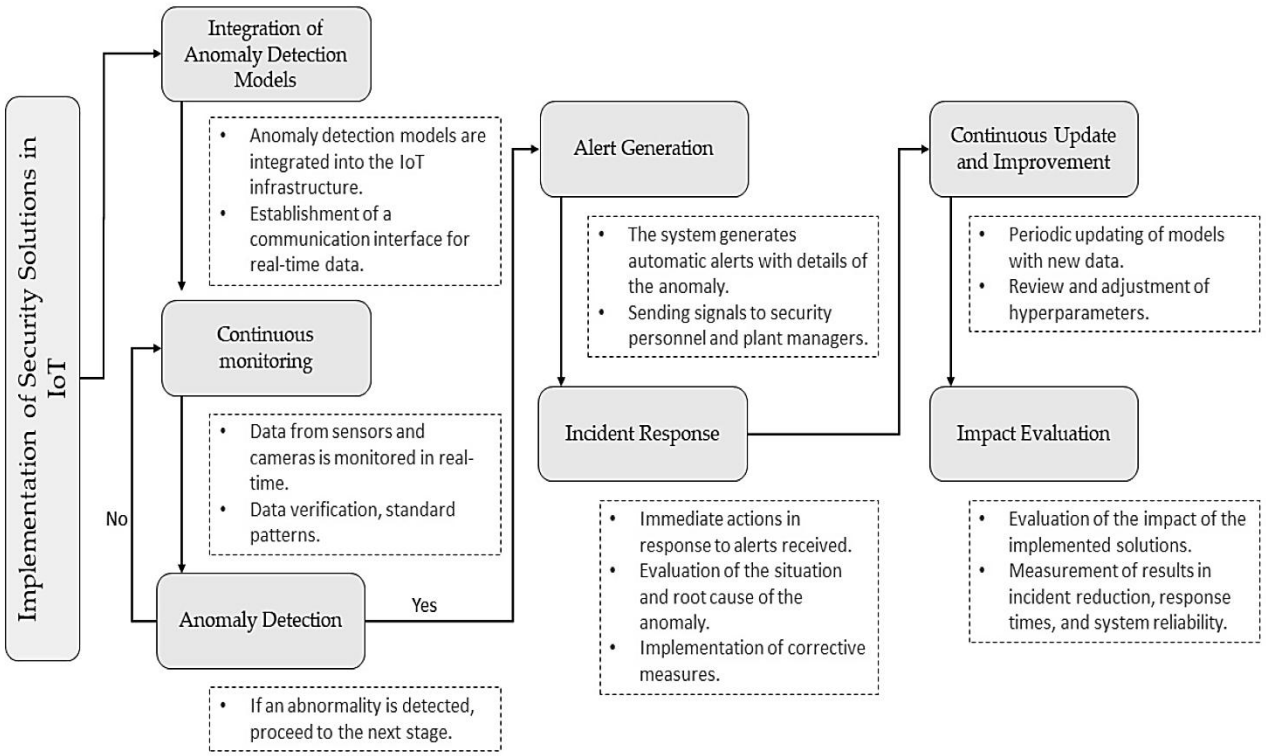

Figure 5: Generalized flow of ML-based security solutions in an IoT-enabled Anomaly detection and recovery model [132]. The above framework on anomaly detection and recovery offers a systematic method to the process in order to ensure that data is reliable and that the quality is improved. It starts with obtaining raw data, whether in academic or industrial sources, and preprocessing them to attenuate the noise, normalizing and handling the missing values. After preprocessing, the data is fed to the anomaly-detecting module, whereby the data will be subjected to statistical or machine learning to detect the abnormal patterns. When there are no anomalies, the data can be normal and this will proceed to the next stage [133]. However, the system goes to the stage of anomaly detection, where anomalies are identified using a detailed study of anomalies. Anomaly recovery techniques are then used to rectify, or substitute the damaged information, or even to reconstruct the damaged information so as to reduce its negative impact on system performance [134].

$$\tilde{c}_t = tanh(W_c x_t + W_c h_{t-1} + b_c) \quad \text{Eq (10)}$$

$$y = f\left(\sum_{k=1}^{K} h^k * w^k + c^k\right) \quad \text{Eq (11)}$$

Performance metrics and consistency checking are used to determine the data recovery and confirm it afterwards to provide a feeling of confidence. The outcome is a clean dataset may be generated, that can be thoroughly analyzed and utilized to make a choice. The following flowchart is therefore a systematic way to handle and

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

resolve anomalies in different applications efficiently, thereby increasing data integrity and reliability of the system. Despite many investigations of anomaly detection methods based on statistical, machine learning, and deep learning approaches, there are still some critical gaps in research [135]. The majority of current research works are devoted to identifying abnormal data patterns, whereas the relatively few studies are devoted to the issue of corruption or the loss of data recovery. The second limitation is that the majority of the models of anomaly detectors are designed to serve within one area of application, e.g., security in networks, industrial monitoring, or a healthcare system [136, 137]. The models are not usually generalizable and may not be generally applicable in other setups, like academic information systems and industry sensor networks. Also, the current recovery algorithms frequently employ models that are reconstruction-based and might have difficulty in recovering high-risk or complex anomalies. GAN and VAE generative models have shown promising results, and their use as connected anomaly management concepts is not so popular. Anomaly detection and anomaly recovery are also, in many cases, a separate action of most existing systems and, hence, require less system efficiency, but an increased amount of computational complexity. Therefore, generic designs of detection and recovery plans in one smart system are necessary [138, 139]. Moreover, real-time execution is still an issue, particularly in large-scale IoT and cyber-physical systems, where real-time streams of data need to be processed with minimum delay. They need to have efficient and scalable machine learning models to accommodate these dynamic environments [140]. Therefore, the current research effort ought to seek to develop a unified anomaly-detecting and recovery framework that may be informed by machine learning algorithms and may be successfully applied in academia and practice. It is important that such systems can identify anomalies, recreate corrupted data with reliability and ensure the integrity of the data to support intelligent decision making.

$$f_t = \sigma(W_f x_t + W_f h_{t-1} + b_f) \qquad \text{Eq (12)}$$

The study of anomaly detection shows that there is a critical lapse, where detection mechanisms are the way to go instead of integrated detection and recovery models. Even today, hardly any systems are read as one that goes beyond the efforts to incorporate both of the aspects, even though enhancement of detection systems has been found [141]. Inadequacies in evaluations across different domains also exist and methods of generating recovery are not fully employed, particularly in a data environment characterized by heterogeneous data. There are concerns on model interpretability and the feasibility of these systems, which are not yet sorted out. Mechanisms of recovery have not been mentioned in previous investigations, including those that have greatly developed the research approaches of anomaly detection. This is reflected in the literature of [142], and reflects a more general inability to actually formulate fully-integrated recovery approaches once machine learning has finally become a commodity in the business of managing anomalies.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Research Gaps in Anomaly Detection and Recovery

The sphere of discrepancy is getting increasingly bigger, as when the high-quality data usage is needed, the slightest failure or fault of the data that is possible can undergo tremendous influence on the work of the system [143]. The practice of anomaly in education and industry settings can bring negative implications to the decision-making processes, resulting in loss of money and ineffective work, which requires the need to identify and fix the corrupted data in addition to other methods of detecting it. LSTM autoencoders and other reconstruction schemes have been proposed to form low-dimensional representations of the data, but fail to scale to the more rare anomalies and tend to form junky detection outputs [144]. There are several different scoring schemes that are suggested to incorporate: point-wise differentiating and Dynamic Time Warping (DTW) as an intermediate towards increasing the detection accuracy, with median-based predictions being more efficient at the point anomaly detection. Even with these developments, the inaccuracy and false positives may still be realized in its intertwining with reconstruction errors like TadGAN [145]. The organizational information has spurred increased demands to employ a professional data analyst, but financial constraints do not allow full-time employment and leave an intellectual vacuum in data management [146, 147]. Several solutions, like smart machine intelligence, could serve as cost-effective solutions to counter such challenges so that 24-hour monitoring of key infrastructures could be provided, and anomalies could be detected and sent to human tests. These systems are capable of increasing efficiency as they detect small deviations that are usually overlooked in manual analysis. The current exploration is aimed at developing an elaboration of a high-quality anomaly identification model to apply during satellite telemetry system processing sensor information and notify the technical staff about an abnormal state. This structure will be brought down to the extent of false positives and false negatives to ensure that this performance is stable. To create and test an intricate solution combining machine learning and generative models to mitigate the liabilities of existing detection-only designs by introducing strong recovery algorithms [148].

$$i_t = \sigma(W_i x_t + W_i h_{t-1} + b_i) \quad \text{Eq (13)}$$

The framework improve the consistency and reliability of the data through preprocessing, validation and constant monitoring using standard forms and this minimizes the errors required to make effective decisions and keep operations effective. Moreover, to reduce system downtime because of data errors, the system will use automated validation, anomaly prediction and recovery methods, which will help identify and rectify errors early in the process. It will enhance consistency and persistent in the system through machine learning techniques. The framework will be applied both in academia and industry to facilitate better decision-making by presenting quality, reliable, and timely data to make organizations make the most out of resources and adapt to the changing environment. Lastly, the research helps in building self correcting intelligent systems, incorporating feedback loop and adaptive learning procedures, which allows the intelligent systems to learn through their errors and hence improve their performance as they go. The proposed holistic solution will bridge the gap between anomaly detection and recovery and, therefore, elevate the quality of data, reduce the risks of operation,

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

boost the power of the decision-making process, and create self-corrective mechanisms to achieve sustainable development of data-driven applications [149].

Table 2: Summary of Anomaly Detection Approaches in Literature (2020–2025)

Ref	Technique	Dataset / Domain	Key Contribution	Limitation
[150]	Distance-based Outlier Detection	Benchmarks	Defined challenges in high-dimensional detection	Poor recovery ability
[151]	Autoencoder Reconstruction	MNIST, Sensors	Good for nonlinear patterns	Needs large data
[152]	LSTM for Time-Series	Industrial Sensors	Captures temporal anomalies	Slow training
[153]	Isolation Forest	Mixed Datasets	Robust and simple	No recovery, only detection
[154]	GAN-based Recovery	Manufacturing	Realistic reconstruction	Expensive computation
[155]	Transformer Anomaly Detection	Server Logs	Long-range attention	Needs GPU
[156]	RPCA for Recovery	Videos	Low rank + sparse repair	Slow for big data
[157]	Hybrid ML + DL	IoT Data	High detection accuracy	Complex
[158]	VAE Reconstruction	Health Records	Low-dimensional latent modeling	Blurry output
[159]	Diffusion Models	Industrial Images	High-quality reconstruction	Very slow
[160]	Graph NN for Sensors	IoT	Good for spatial anomalies	Graph design required
[161]	Autoencoder + GMM	Tabular data	Multi-modal detection	Complex tuning
[162]	Ensemble ML	Academic Systems	Improved detection	Hard to scale
[163]	GAN + Attention	Manufacturing	Good recovery	Expensive

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

[164]	Multimodal Fusion	Smart Industry	Uses multi-sensors	Synchronization required

Research Gaps in Existing Literature

Summary of Anomaly Detection and Recovery Approaches (20202025) discusses various techniques between 2020 and 2025, with a significant shift in distance-based and statistical methods towards deep learning and hybrid methods. First works were devoted to distance-based outlier detection, that did not cope with large-dimensional data and was not able to recover anything. Improved autoencoder and LSTM model based anomaly detection, although had difficulty with huge datasets and expensive computations. These advances as Isolation Forest techniques improved the detection but not recovery. In the meantime, the recovery algorithms like GANs and Robust Principal Component Analysis (RPCA), investigated by [165]. Simulated versions but were expensive to compute and scale. Transformer models were introduced to enhance the detection of anomalies in complex sequences at the cost of a large amount of GPU resources. Middle-way solutions and hybrid-learning to enhance the precision at a cost of increasing the complexity of systems. Recent progress in generative and probabilistic models that incorporate Variational Autoencoders in the healthcare field with diffusion models to generate images, despite having such drawbacks as blurred pictures and slow inference. A significant shift towards more advanced frameworks, combining detection, recovery, and validation but in most cases being limited by complexity, interpretability, and scalability, is underscored in literature. This necessitates additional progression of effective and comprehensive machine learning systems to tackle the anomaly management effectively. In academia and industry, anomaly detection and recovery is a critical research area that aims at detecting outliers which do not conform to the anticipated data patterns. These anomalies can impact the stability of the system, reliability of the data, and the accuracy of the decision making and it is necessary to thoroughly identify them and restore them so that the systems can be reliable. Despite all that has been written about detection methods, less emphasis has been laid on anomaly recovery that entails recovery of corrupted data. This literature review evaluates the available literature and methods and their weaknesses and considers the possibility of machine learning methods to improve the detection and recovery.

Deep Learning Approaches for Time Series Anomaly Detection

Despite the fact that much research has been carried out on anomaly detection, very little systematic and domain independent research has been carried out in respect to anomaly recovery. Gaps Significant gaps are pointed out through emphasizing classification without taking into account the corrections of data and domain-specific solutions that make the generalizability difficult and the absence of generative model, as in the case of recovery studies, using GANs. Additionally, no unified structures that unify detection, reconstruction, and validation exist, and deployment problems due to model complexity and interpretability. Research done by Adnan, Li, Tinawi, Nicholson and others reveals that the detection power is enormous with little in recovery mechanisms and the researchers ought to keep on developing the anomaly recovery.

Reconstruction-Based Anomaly Detection Methods

According to recent literature, models based on the principle of deep learning are

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

becoming popular in time series anomaly detection and forecasting, with such approaches as Long Short-Term Memory (LSTM), stacked LSTMs, autoencoders, and recurrent neural networks (RNNs) being popular. The models are applicable in modelling time dependencies to predict future values, which will be used to identify abnormalities by comparing forecasts with real data. An important improvement is evidenced in a NASA study that used stacked LSTM models with nonparametric dynamic thresholding to process spacecraft telemetry data. This approach not only gives forecasts but calculates prediction errors using adaptive thresholds, which is a more flexible alternative to more traditional fixed-threshold approaches, such as x-sigma and distance-based approaches. Dynamic error thresholding is more adaptive to nonstationary data whose mean and variance change over time, and is more useful to detect anomalies in the changing time series scenario. Moreover, the dynamic thresholding techniques are more efficient in addressing both cyclic patterns, growth patterns and time variations and hence are more credible than the non stationary conditions that cannot be addressed by the static methods. By doing so, the sphere of anomaly detection with dynamic and unsupervised thresholding approaches will become an important breakthrough.

Reconstruction-based methods (also known as reconstruction-based algebraic anomaly detection or reconstruction-based abnormality detection) are methods of anomaly detection in which the autoencoders are recurrent networks (either LSTM or GRU). These models are coded to learn small encodings of common patterns in data and to infer by reconstructing sequences of inputs and identifying anomalies through large reconstructions errors indicating an occurrence of a deviation in a specific pattern. The approach is particularly useful with labeled data which is sparse in number, since it can capture long-term dependencies and nonlinearity, and hence it is effective at detecting subtle and complex anomalies that would otherwise have been overlooked by standard statistical tools. Research shows that autoencoders when combined with recurrent networks can be used to greatly enhance the accuracy of detection, particularly in high-dimensional and sequential data. The methods, however, are limited to some extent including bad representation of rare or extreme anomalies at training that may cause false positive or false negative identifications. Moreover, reconstruction-based models do not tend to possess strong recovery properties to restore corrupted information as they target finding deviation.

Method and Materials

The systematic review method has been employed in this research paper. To search the relevant articles, articles were collected on IEEE Xplore, Scopus, Web of Science, and Google Scholar databases. Keywords were anomaly recovery, data reconstruction, and machine learning. The selected articles were analyzed based on data sets, algorithms, measures of evaluation, and fields of application. A comparative analysis was conducted to find out strengths and weaknesses. The methodology of the systematic literature analysis that is applied in this review defines the exploration of the fields of anomaly recovery, data reconstruction and machine learning. A set of recent research articles was acquired in the most popular databases (IEEE Xplore, Scopus, Web of Science and Google Scholar) by the keywords related to the topic under consideration. The selection of the studies was done through a screening process; during the process, the relevancy of the studies, the quality of the publications of the studies, and the methodology rigor of the studies were looked at.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Each of the articles has been critically evaluated, based on a variety of parameters, such as the kind of data under study, the algorithms methods, the metrics that have been evaluated and the applications fields that have been addressed. On the basis of this profound analysis, a comparative evaluation of the results of the selected study was conducted, with references to differences and similarities in the methods and results. In order to overcome the shortcomings of the current anomaly detection and recovery methods, a single framework is needed that will combine the detection and recovery capabilities in one intelligent system. The proposed scheme will be used to identify the presence of anomalous data and recreate corrupted or missing values with the use of machine learning algorithms. This type of framework can be used in the academic data environment as well as in the industrial monitoring systems in which data reliability is an imperative. The proposed anomaly management system is a combination of the following steps: data collection, data preprocessing, anomaly detection, anomaly recovery and data validation. Each step is an important one to ensure that anomalies are detected appropriately, and data rebuilding is trustworthy.

Data Requirements and Practical Considerations

The model consists of preprocessing phase of data, anomaly detection, recovery mechanism and the performance evaluation phase. Preprocessing includes normalization and missing values. The reviewed system has four significant steps that involve data preprocessing. anomaly detection, recovery mechanism and performance evaluation. The preprocessing is normalization, noise removal and missing values. In order to overcome the shortcoming of the currently used anomaly detection and recovery methods, a single framework, which incorporates both the detection and recovery processes into a single intelligent system is needed. The designed framework is aimed at detecting the anomalous data and restoring the corrupted or lost values with the help of machine learning. This framework can be applied in the field of education information setting as well as industry monitoring systems where the validity of information is a major concern. The anomaly management framework suggested has multiple steps such as data collection, data preprocessing, anomaly detection, anomaly recovery and data validation. The steps are crucial in the process of determining the anomalies and estimating the data appropriately.

Data Collection and Data Preprocessing

The first phase of the framework is information collection basing on the various sources depending on the field of application. The data in the industrial context is usually received by sensors, monitoring devices, and Internet of Things (IoT) systems, which continuously assess the operating conditions, such as temperature, pressure, vibration, and machine performance indicators. Learning management systems (LMS), student information system, attendance records, online assessment system and so on can be regarded as academic sources of data. This data may be student grades, attendance records and log-ins and course interaction records. Such sources of information can be helpful in the detection of anomalies or inconsistencies. However, in the real-world data, missing data, noise, or corrupt values are typical. Thus, before using anomaly detection models, there is a need to preprocess the data. Preprocessing Data preprocessing is meant to enhance data quality and get the dataset ready to be

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

analyzed with machine learning. Some of the operations that are normally performed in this step are: deletion of duplicate records, missing values, normalization of feature values and conversion of categorical attributes into numerical value. Statistical approaches to missing data such as mean substitution or mean imputation can be used. Noise cutting can also be used to remove outliers that are not necessarily due to anomalies but are as a result of measurement errors. Some of the usual methods of standardizing the data are minimum and maximum scaling or z-score normalization. Standardization makes sure that the scales of all features are similar, and such enhances machine learning models. When the dataset is prepared and standardized it can be split into training and testing ones. The knowledge of normal behavior patterns is acquired using the training dataset and the testing dataset is used to quantify the performance of anomaly detection.

Detection and Recovery

The anomaly detection stage aims to identify abnormal patterns in the dataset. In the proposed framework, machine learning models are trained to learn normal system behavior and classify deviations as anomalies. Mathematically, the anomaly detection function can be represented as:

and xrep is the data vector that is to be inputted and the output is whether the observation is normal (0) or abnormal (1). Some of the machine learning algorithms that can be used to perform anomaly detection include Isolation Forest, Support Vector Machines, random forest and clustering-based. One of these techniques, Isolation Forest, is especially powerful since it seals off anomalous observations with random partitioning of the data space. The other benefit of applying RF models is that they are strong and can be used in high-dimensional data. Deep learning architectures such as Long Short-Term Memory (LSTM) networks can in the case of time-series data learn time-dependencies and detect sequential patterns of abnormality. These models have been particularly applied to industrial systems, whereby sensor data varies over time. After detection of anomalies, the framework goes through the recovery phase to rectify or rebuild abnormal values. The purpose of anomaly recovery is recovery of corrupted or missing values of data with the aim of guaranteeing that the data set is reliable. The recovery process can be mathematically given as:

$$f(x): R^m \rightarrow \{0,1\}$$

$$x_i' = \hat{x}_i$$

and xirepresents the anomalous value of data point, x i -represents the reconstruction value. Autoencoders are reconstruction-based methods that are popular in the recovery of anomalies. The models are trained with the compressed representations of normal data patterns, and used to interpolate missing or abnormal values. When a data point does not follow the pattern learned, the model tries to substitute the data point with a reconstructed value that is sensible according to the normal behavior of the system. Generative models such as Generative Adversarial Networks (GANs) can also be used to do anomaly recovery. GAN-based models produce artificial data samples, which are similar to the actual observations to a great extent. This helps

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

them to replace the abnormal values with realistic values. The other recovery approach is predictive models such as LSTM networks which provides the anticipated future values based on past data. The predicted value could be substituted in case the observed data is considerably different than the predicted value.

Once anomaly recovery is completed, the data that has been rebuilt should be validated to make sure that it reflects the normal system behavior. Some of the methods used in validation include statistical analysis, comparison with the past data trends, or model confidence analysis. Otherwise, it is possible to use other recovery methods, or the anomaly can be flagged to be checked manually. The resultant validated dataset can then be further analyzed, modelled or decision-making. The combination of detection and recovery systems makes the proposed framework guarantee a high quality of data and reliability of the system. Statistical methods have assumptions of probabilities and are prone to predetermined conclusions about data based on the assumptions. On the contrary, machine learning processes are aimed at determining normal behavioral patterns depending on historic data which could enable the systems to mature depending on the patterns that are observed. Deep learning is a sub-division of machine learning that goes an extra mile as far as creating more precise predictions and information, by identifying complex time and space associations of the information. In this context, generative models also play an important role since they generate realistic samples to reproduce data, thereby increasing the capacity to fill in the gaps in the data or generate new samples of data based on the learned patterns.

Data Validation and Correction

As the comparison reveals, the deep learning-based recovery models are more successful in terms of accuracy and robustness compared to the traditional models. Autoencoders performed better in reconstruction tasks in time series data. The comparative analysis shows that the constituted recovery models that are based on deep learning are always better than the traditional in terms of accuracy and robustness. Specifically, LSTM Autoencoders have been demonstrated to be very effective in reconstruction of information in time-series data. Furthermore, hybrid models which integrate statistical preprocessing and deep learning algorithms have moderate performance and are able to reduce the instances of false alarms. Despite these advantages, high computational costs still exist as a major drawback of application of these advanced recovery models.

Analysis and Discussion

The analysis of the anomaly detection and recovery techniques demonstrates that it is necessary to find appropriate machine learning models depending on the field of application and the data type. Datasets both in academia and industry tend to be noisy, contain gaps or oddities that can have an adverse effect on the performance of analysis. The machine learning algorithms are already capable of performing with increased performance in the activities of identifying anomalies. Isolation Forest, random forest and Support Vector Machines algorithms are used to detect abnormal patterns as they learn decision boundaries using past data. Among these techniques,

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

often effective are the models of the Random Forests, as they can handle noisy data and nonlinear associations. Deep learning has also increased the capability of detecting anomalies particularly with time-series data. Autoencoders and Long Short-Term Memory (LSTM) networks are models which can learn the hidden patterns in streams of sequence data. Autoencoders can identify abnormalities by reconstruction errors and LSTM networks by identifying time-dependencies.Besides the detection, the techniques of anomaly recovery are very important in ensuring the quality of data. The reconstruction-based techniques strive to fill in the corrupted or missing values of data with estimated normal values. Autoencoders are used in this application, as it can learn coded representations of normal system behaviour, and re-assemble input data according to that learning. Another promising avenue of application on the topic of anomaly recovery is generative models like Generative Adversarial Networks (GANs). These models generate simulated data values which are far more like the real observations. GAN-based models can be used to heal the continuity of datasets to be used in predictive analytics by replacing anomalous data with generated data. In spite of these developments, there are a number of challenges. The vast majority of anomaly detection models are also costly in terms of training and computing resources. In addition, deep learning models are not often interpretable, and the system operators cannot easily understand the reasoning of the prediction of anomalies. Moreover, real-time processing is also problematic in large-scale Internet of Things (IoT) settings where extremely large data streams need to be processed in real-time. In general, machine learning-based detection schemes and reconstruction-based recovery schemes synthesis could provide a possible solution to the problem of anomaly management. Combined systems, which include these methods, can provide remarkable enhancements in data credibility, and assist smart decision-making within educational and industrial structures.

Table 3: Comparison of Anomaly Recovery Techniques

Technique	Type	Advantages	Limitations
Z-Score	Statistical	Simple and fast	Limited for complex data
IQR Method	Statistical	Effective for outliers	Sensitive to data distribution
Isolation Forest	Machine Learning	Efficient for large datasets	Limited interpretability
Support Vector Machine	Machine Learning	High accuracy in classification	Computationally expensive
Autoencoder	Deep Learning	Effective for high-dimensional data	Requires large training data
LSTM Networks	Deep Learning	Suitable for time-series data	Complex training process
GAN-based Models	Generative Deep Learning	High-quality data reconstruction	Training instability

Table 4: Comparison of Anomaly Recovery Techniques

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Method	Model	Accuracy	Complexity	Limitations
Statistical	Z-Score	Low	Low	Non-adaptive
ML	Isolation Forest	Medium	Medium	No temporal modeling
DL	Autoencoder	High	High	Needs large dataset
DL	LSTM-AE	Very High	Very High	High computation
Generative	GAN	Very High	Very High	Training instability

Challenges and Future Research Directions

Availability of limited labeled data, privacy issues, and high computation requirements and lack of standard benchmarks are some of the major challenges. Uncommon and changing anomalies are hard to model precisely. The difficulty of intensive levels of calculation and absence of established benchmarks is a major setbacks in many aspects of the spheres of analysis. Furthermore, there are some rare and fluctuating anomalies, and it is hard to find the right model that could be difficult to analyze. The explainable models of recovery, edge-based processing, federated learning, and privacy preserving models should be the focus of future research in this work. A federated learning and privacy-preserving approaches need to be explored. It is also deemed necessary to create open benchmark data sets in order to allow research work in these directions and to make them standardized.

Conclusion

The present paper has reviewed the anomaly recovery methods in both academic and industrial systems in detail. The capabilities of deep learning and hybrid structures are huge in increasing the accuracy of data. Further investigation is needed to deal with scalability and deployment issues. The provided paper introduces comprehensive and novel research of the anomaly recovery techniques and demonstrates that deep learning and hybrid models have the possibility to enhance the trustworthiness of the information. It also highlights the need to conduct additional research that would help in improving scalability and ensuring that it can be effectively implemented in practice. The fast growth of data-driven technologies in the academic and industrial realms has only heightened the significance of effective anomaly management systems. Errors of the sensor system, communication issues or human error may cause data set anomalies. These anomalies can lead to severe outcomes on the confidence of the data, predictive analytics and the decision-making process, unless they are managed properly. This review paper has analyzed different methods applied in detecting anomalies and recovering anomalies with the help of machine learning methods. The traditional statistical tests such as Z-score and interquartile range analysis are simple to apply in revealing the basic anomalies, but in the complex data, it is limited. Machine learning algorithms like Isolation Forest, Support Vector Machines and Random Forest have been demonstrated to be more efficient in identifying the abnormal trends in large datasets. More advanced methods of anomaly

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

detection such as Autoencoders and Long Short-Term Memory networks can be used to detect anomalies by identifying more complicated patterns and time dependence of data. In addition to the detection of anomalies, recovery models are also important in data integrity such as reconstruction-based models and generative models. With these methods, we can be convinced that the corrupt/ missing data values can be replaced with the reconstructed observations that are credible. Although there have been major developments in the field of anomaly detection, the combination of detection and recovery systems in a single system is one of the critical areas of research. The many researches that have been carried out on the topic dwell on the aspects of detection yet have seldom recovery methods been thought of as standalone processes. Future studies ought to be done to come up with an integrated model of anomalies management that can identify and revert anomalies in real time. In short, machine learning-powered anomaly recovery systems are a promising avenue to enhance data reliability of intelligent systems. By integrating these two detection and reconstruction techniques, these structures could enhance the system and reduce data inconsistency and make correct decisions in academics and industrial settings.

Acknowledgement: We appreciate the generous support from all the contributor to the research and their different affiliations.
Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.
Availability of data and material: In the approach, the data sources for the variables are stated.
Authors' contributions: Each author participated equally in the creation of this work.
Conflicts of Interest: The authors declare no conflict of interest.
Consent to Participate: Yes
Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

References

Adnan, M., Islam, R., & Rahman, M. (2025). Machine learning-based anomaly detection for intelligent monitoring systems. Journal of Intelligent Systems, 34(2), 145–158.

Chevtchenko, S., Rocha, L., & Oliveira, P. (2023). Reconstruction-based anomaly detection using deep learning techniques for time-series data. Expert Systems with Applications, 213, 119184.

Kongkiatpaiboon, S., Laosuwan, T., & Chanklan, R. (2024). A deep learning approach for anomaly detection in industrial IoT systems. Sensors, 24(3), 1125.

Tancredi, U., Vignali, V., & Caviglione, L. (2022). Machine learning approaches for cyber-physical anomaly detection in industrial control systems. IEEE Access, 10, 67534–67547.

Tao, F., Gong, X., Qi, Q., & Zhang, M. (2022). Digital twin-driven smart manufacturing: Concepts and applications. Robotics and Computer-Integrated Manufacturing, 74, 102282.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Tinawi, R. (2019). Data anomaly detection in industrial control systems using machine learning models. International Journal of Computer Applications, 178(34), 1–8.

Zhang, Y., Cao, J., & Li, H. (2025). Generative adversarial networks for anomaly detection and recovery in IoT environments. Future Generation Computer Systems, 154, 202–214.

Ayub, N., Alghamdi, T., Din, I., Ali, A., Khan, H., Ganiyeva, O., & Makhmudov, S. (2025). An Enhanced Artificial Intelligence and Deep Learning Assisted Breast Cancer Classification and Diagnosis Based on the Internet of Medical Things (IOMTs). Engineering, Technology & Applied Science Research, 15(6), 30612-30616.

Abdullah, M. M., Khan, H., Farhan, M., & Khadim, F. (2024). An Advance Machine Learning (ML) Approaches for Anomaly Detection based on Network Traffic. Spectrum of engineering sciences, 2(3), 502-527.

Ahmed, A., Javed, M. A., Qureshi, J. N., Khan, H., & Yousaf, H. F. (2024). An insightful Machine Learning based Privacy-Preserving Technique for Federated Learning. The Asian Bulletin of Big Data Management, 4(4), 332-343.

Ayub, N., Alghamdi, T., Din, I., Ali, A., Khan, H., Ganiyeva, O., & Makhmudov, S. (2025). An Enhanced Artificial Intelligence and Deep Learning Assisted Breast Cancer Classification and Diagnosis Based on the Internet of Medical Things (IOMTs). Engineering, Technology & Applied Science Research, 15(6), 30612-30616.

A. Kiayias, A. Russell, B. David, and R. Oliynykov, “Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol,” in Proc. 37th Annual International Cryptology Conference (CRYPTO), Santa Barbara, CA, 2017, pp. 357–388.

A. Voit, D. Duenas-Cid, and R. Krimmer, “Blockchain for E-Voting: A Systematic Review,” IEEE Transactions on Engineering Management, vol. 68, no. 5, pp. 1470–1485, Oct. 2021.

Aqeel, N., Alam, A., Bhatti, Z., & Amir, A. (2024). A Survey on Tor’s Multi Layer Architecture and Web Implications in Dark Web. Spectrum of Engineering Sciences, 2(4), 212-231.

P. De Filippi and S. Loveluck, “The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure,” Internet Policy Review, vol. 5, no. 3, pp. 1–28, Sep. 2016.

J. Bonneau, “Why Buy When You Can Rent? Bribery and Vote Buying in Blockchain Voting,” in Proc. 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, UK, 2018, pp. 123–130.

K. Croman et al., “On Scaling Decentralized Blockchains,” in Proc. 20th International Conference on Financial Cryptography and Data Security (FC), Christ Church, Barbados, 2016, pp. 106–125.

Ali, G., Shahbaz, H., Hassan, M. A., Ahmad, M., & Waleed, M. (2024). An Enhanced Approach of Exploring Digital Economy Using Modern Computer Networks. Spectrum of Engineering Sciences, 2(4), 292-312.

Ahmad, I., Nasim, F., Khawaja, M. F., Naqvi, S. A. A., & Khan, H. (2025). Enhancing IoT Security and Services based on Generative Artificial

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Intelligence Techniques: A Systematic Analysis based on Emerging Threats, Challenges and future Directions. Spectrum of engineering sciences, 3(2), 1-25.

Ali, M., Cheema, S. M., Aslam, Z., Naz, A., & Ayub, N. (2023, March). CBAI: Cloud-Based Agile Infrastructure for Enhancing Distributed Agile Development. In 2023 4th International Conference on Computing, Mathematics and Engineering Technologies (iCoMET) (pp. 1-6). IEEE.

Ahmed, A., Rizwan, S. M., Ikram, F., Ahmed, N., Khan, H., & Hasan, M. Z. (2025). An Exploration of User-level Privacy-Preserving Federated Learning Technique: A Machine Learning Perspective on Classification, Threat Mitigations, and Exploring Federated Learning and Beyond. The Asian Bulletin of Big Data Management, 5(4), 292-318.

Akhtar, M. H., Ghafoor, U., Imran, O., Ayub, N., Abdullah, M. M., & Khan, H. (2026). An Efficient AI and Deep learning Assisted Self-Healing Network Approach: Analysis on Fault Detection Response and Recovery to Mitigate Threats in IoT-Security Ecosystem. The Asian Bulletin of Big Data Management, 6(1), 40-66.

Ahmed, A., Ahmed, N., Ghafoor, U., Rizwan, S. M., Qureshi, R., Khan, H., & Hussain, M. Z. (2025). An Enhanced Textual Review Classification and Sentiment Analysis Approach based on Machine Learning: A Comprehensive Analysis for Text Categorization Approaches. The Asian Bulletin of Big Data Management, 5(4), 259-291.

Ali, M., Cheema, S. M., Ayub, N., Naz, A., & Aslam, Z. (2022, December). Blockchain-based Privacy Preservation Framework for IoT-Based Information Systems. In 2022 3rd International Conference on Innovations in Computer Science & Software Engineering (ICONICS) (pp. 1-7). IEEE, 2022

Asghar, M. A., Aslam, A., Bakhet, S., Saleem, M. U., Ahmad, M., Gohar, A., & Khan, H. (2025). An Efficient Integration of Artificial Intelligence-based Mobile Robots in Critical Frames for the Internet of Medical Things (IoMTs) Using (ADP2S) and Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 160-183.

Ayub, N., Yaseen, A., Amin, M. N., Rizwan, S. M., Farooq, I., & Hussain, M. Z. (2025). Reliable Federated Learning (Rdl) Assisted Intrusion Detection And Classifications Approach Using (Ssl/Tls) For Network Security. Annual Methodological Archive Research Review, 3(7), 376-400.

Abdullah, M. M., Khan, H., Farhan, M., & Khadim, F. (2024). An Advance Machine Learning (ML) Approaches for Anomaly Detection based on Network Traffic. Spectrum of engineering sciences, 2(3), 502-527.

Ahmed, A., Javed, M. A., Qureshi, J. N., Khan, H., & Yousaf, H. F. (2024). An insightful Machine Learning based Privacy-Preserving Technique for Federated Learning. The Asian Bulletin of Big Data Management, 4(4), 332-343.

Ayub, N., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). Forecasting Multi-Level Deep Learning Autoencoder Architecture (MDLAA) for Parametric Prediction based on Convolutional Neural Networks. Engineering, Technology & Applied Science Research, 15(2),

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851
Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

21279-21283.

Mumtaz, J., Rehman, A. U., Khan, H., Din, I. U., & Tariq, I. Security and Performance Comparison of Window and Linux: A Systematic Literature Review. Securing the Digital Realm, 272-280.

Abbas, G., Basit, A., Ayub, N., Rafique, S., Ali, A., Khan, H., & Hussain, M. Z. (2026). An Enhanced Machine Learning & Deep Learning based Intrusion Detection System for Intelligent Network Security: A Comprehensive Analysis to Avoid Intrusions in Big Data-based IoT Ecosystem. The Asian Bulletin of Big Data Management, 6(1), 26-33.

Ali, R., Khan, H., Arif, M. W., Tariq, M. I., Din, I. U., Afzal, A., & Khan, M. A. Authentication of User Data for Enhancing Privacy in Cloud Computing Using Security Algorithms. In Securing the Digital Realm (pp. 187-200). CRC Press.

Ayub, N., Iqbal, M. W., Saleem, M. U., Amin, M. N., Imran, O., & Khan, H. (2025). Efficient ML Technique for Brain Tumor Segmentation, and Detection, based on MRI Scans Using Convolutional Neural Networks (CNNs). Spectrum of Engineering Sciences, 3(3), 186-213.

Anas, M., Imtiaz, M. A., Saad Khan, A. A., Naghman, N. F., Khan, H., & Albouq, S. AN ADVANCED MACHINE LEARNING (ML) ARCHITECTURE FOR HEART DISEASE DETECTION, PREDICTION AND CLASSIFICATION USING MACHINE LEARNING. Vol.-20, No.-3, March (2025) pp 54 – 72

Aziz, R., Mehmood, A., Tariq, A., Nasim, F., Farooq, U., Naqvi, S. A. A., & Khan, H. (2025). Critical Evaluation of Data Privacy and Security Threats: An Intelligent Federated Learning-based Intrusion Detection System Poisoning Attack and Defense for Cyber-Physical Systems its Issues and Challenges Related to Privacy and Security in IoT. The Asian Bulletin of Big Data Management, 5(1), 73-84.

Bacha, A., Sehar, H., Naseem, S., & Khan, M. I. (2024). FEDERATED LEARNING FOR THREAT INTELLIGENCE SHARING: A PRIVACY-PRESERVING COLLABORATIVE DEFENSE MODEL. Spectrum of Engineering Sciences, 656-664.

Khan, H. M. S., Hayat, C. M. A., Tayyab, H., & Ali, K. (2024). An Enhanced Cost Effective and Scalable Network Architecture for Data Centers. Spectrum of Engineering Sciences, 2(4), 1-32.

Rafay, A., Salman, W., Yahya, G., & Malik, U. (2024). SD Network based on Machine Learning: An Overview of Applications and Solutions. Spectrum of Engineering Sciences, 2(4), 150-165.

Javed, M. A., Ahmad, M., Ahmed, J., Rizwan, S. M., & Tariq, A. (2025). An Enhanced Machine Learning based Data Privacy and Security Mitigation Technique: An Intelligent Federated Learning (FL) Model for Intrusion Detection and Classification System for Cyber-Physical Systems in Internet of Things (IoTs). Spectrum of Engineering Sciences, 3(2), 377-401.

M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

Waleed, R., Ali, A., Tariq, S., Mustafa, G., Sarwar, H., Saif, S., ... & Uddin, I. (2024). An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications. Bulletin of Business and Economics (BBE), 13(2), 200-206.

U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023

Mumtaz, J., Bakhet, S., Javed, A., Naz, A., Rashail, M., & Khan, H. (2025). An Intelligent Diagnosis and Tumor Segmentation Method based on MRI Images Using Pre-trained Deep Convolutional Neural Networks (CNNs). The Asian Bulletin of Big Data Management, 5(1), 147-163

Zaheer, M., Azeem, M. H., Afzal, Z., & Karim, H. (2024). Critical Evaluation of Data Privacy and Security Threats in Federated Learning: Issues and Challenges Related to Privacy and Security in IoT. Spectrum of Engineering Sciences, 2(5), 458-479.

Noor, H., Khan, H., Din, I. U., Tariq, M. I., Amin, M. N., & Fatima, M. Virtual Memory Management Techniques. Securing the Digital Realm, 126-137.

Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

Ali, M., Khan, H., Rana, M. T. A., Ali, A., Baig, M. Z., Rehman, S. U., & Alsaawy, Y. (2024). A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices. Engineering, Technology & Applied Science Research, 14(5), 16751-16756.

Ali, M., Khan, H., & Rehman, S. U. (2023). Edge Computing for Low-Latency IoT Applications. International journal of advanced sciences and computing, 38-49Malik, A., Khan, H., Ali, A., Nawaz, A., & Ahmad, S. The Impact of Climatic Parameters on the Streamflows & Future Sustainable Hydro-Energy Generation Predicting Streamflows for the 21st Century Under Climate Change Scenarios.

Ali, M., Khan, H., Din, I. U., Tariq, M. I., & Javed, A. Design and Implementation Role of Middleware in Shared Network Environments: A Systematic Review. Securing the Digital Realm, 229-243.

Ahmed, A., Rizwan, S. M., Ikram, F., Ahmed, N., Khan, H., & Hasan, M. Z. (2025). An Exploration of User-level Privacy-Preserving Federated Learning Technique: A Machine Learning Perspective on Classification, Threat Mitigations, and Exploring Federated Learning and Beyond. The Asian Bulletin of Big Data Management, 5(4), 292-318.

Ahmed, A., Ahmed, N., Ghafoor, U., Rizwan, S. M., Qureshi, R., Khan, H., &

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Hussain, M. Z. (2025). An Enhanced Textual Review Classification and Sentiment Analysis Approach based on Machine Learning: A Comprehensive Analysis for Text Categorization Approaches. The Asian Bulletin of Big Data Management, 5(4), 259-291.

Abdullah, M. M., Ghafoor, U., Qadeer, Q. B., Khadim, F., Khan, H. S., Ahmad, A., & Khan, H. (2025). An Efficient of Artificial Intelligence based Brain Tumor Diagnosis and Classification: An Advance Medical Diagnosis Approach. The Asian Bulletin of Big Data Management, 5(2), 208-242.

Ayub, N., Uzair, M., Din, I., Ali, A., Khan, H., Yuldashev, F., & Makhmudov, S. (2025). An Efficient Human Activity Recognition (HAR) Model Based on Convolutional Neural Networks for Computing Devices Aiming to Reduce Latency and Tackle the Inactivity of Gadgets. Engineering, Technology & Applied Science Research, 15(6), 28885-28890.

Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (Al) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power loT Devices in 5G Networks. Spectrum of engineering sciences, 2(3), 528-586.

Ayub, N., Waheed, A., Ahmad, S., Akbar, M. H. A., Fuzail, M. Z., & Hashmi, A. H. (2025). Strengthening Network Security: An Efficient DL Enabled Data Protection and Privacy Framework for Threat Mitigation and Vulnerabilities Detection in IoT Network. Annual Methodological Archive Research Review, 3(6), 1-25.

Ali, I., Saleem, M. U., Khan, A. A., Naz, A., Nawaz, M., & Khan, H. (2025). An Enhanced Artificial Intelligence Generated Virtual Influencer Framework: Examining the Effects of Emotional Display on User Engagement based on Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 184-209.

Khan, A. Yasmeen, S. Jan, U. Hashmi, "Enhanced Resource Leveling Indynamic Power Management Techniqueof Improvement In Performance For Multi-Core Processors" ,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019

Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Oct. 2018

Imtiaz, M. A., Amir, A., Bakhet, S., Siddique, H., & Rizwan, S. M. (2025). An Optimal Diabetic Retinopathy Detection and Classification Approach based on integrated Hybrid Convolutional Neural Networks (CNNs). Spectrum of Engineering Sciences, 3(2).

H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018

Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synthesis of AgNPs from leaves extract of Saliva Sclarea, their characterization, antibacterial activity, and catalytic reduction ability. Zeitschrift für Physikalische Chemie, 238(5), 931-947.

S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020

Gordon, T. Diabetes, blood lipids, and the role of obesity in coronary heart disease risk for women. Ann. Intern. Med. 87, 393 (1977).

Rumelhart, D.E.; Hinton, G.E.; Williams, R.J. Learning representations by back-propagating errors. Nature 1986, 323, 533–536.

Criado, M.F.; Casado, F.E.; Iglesias, R.; Regueiro, C.V.; Barro, S. Non-iid data and continual learning processes in federated learning: A long road ahead. Inf. Fusion 2022, 88, 263–280.

Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor

Gularte, K.H.M.; Vargas, J.A.R.; Da Costa, J.P.J.; Da Silva, A.A.S.; Santos embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

Fatima, M., Ali, A., Ahmad, M., Nisa, F. U., Khan, H., & Raheem, M. A. U. Enhancing The Resilience Of Iot Networks: Strategies And Measures For Mitigating Ddos Attacks. Cont.& Math. Sci., Vol.-19, No.-10, 129-152, October 2024 https://jmcms.s3.amazonaws.com/wp-content/uploads/2024/10/10072102/jmcms-2410025-ENHANCING-THE-RESILIENCE-OF-IOT-NETWORKS-MF-HK.pdf

Javed, M. A., Anjum, M., Ahmed, H. A., Ali, A., Shahzad, H. M., Khan, H., & Alshahrani, A. M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets. Engineering, Technology & Applied Science Research, 14(6), 17894-17899.

Li, H.; Luo, L.; Wang, H. Federated learning on non-independent and identically distributed data. In Proceedings of the Third International Conference on Machine Learning and Computer Application (ICMLCA 2022), Shenyang, China, 16–18 December 2023; SPIE: Bellingham, WA, USA; pp. 154–162.

Vidal Filho, et al. Safeguarding the V2X Pathways: Exploring the Cybersecurity Landscape through Systematic Literature Review. IEEE Access 2024, 12, 72871–72895.

Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

Mustafa, M., Ali, M., Javed, M. A., Khan, H., Iqbal, M. W., & Ruk, S. A. (2024). Berries of Low-Cost Smart Irrigation Systems for Water Management an IoT Approach. Bulletin of Business and Economics (BBE), 13(3), 508-514.

Hassan, A., Khan, H., Ali, A., Sajid, A., Husain, M., Ali, M., ... & Fakhar, H. (2024).

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

An Enhanced Lung Cancer Identification and Classification Based on Advanced Deep Learning and Convolutional Neural Network. Bulletin of Business and Economics (BBE), 13(2), 136-141.

Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.

Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, "An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning", Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024

Saif, S., Hamayun Khan, A. A., Albouq, S., Hussain, M. Z., Hasan, M. Z., Uddin, I., ... & Husain, M. AN EFFICIENT MACHINE LEARNING-BASED DETECTION AND PREDICTION MECHANISM FOR CYBER THREATS USING INTELLIGENT FRAMEWORK IN IOTS. Vol.-15, No.-8, August (2024) pp 191-206

Noor, H., Khan, H., Din, I. U., Tarq, M. I., Amin, M. N., & Fatima, M. (2025). 12 Virtual Memory Management. Securing the Digital Realm: Advances in Hardware and Software Security, Communication, and Forensics, 126.

Yousaf, M., Khalid, F., Saleem, M. U., Din, M. U., Shahid, A. K., & Khan, H. (2025). A Deep Learning-Based Enhanced Sentiment Classification and Consistency Analysis of Queries and Results in Search Using Oracle Hybrid Feature Extraction. Spectrum of Engineering Sciences, 3(3), 99-121.

Khan, H., Usman, R., Ahmed, B., Hashimi, U., Najam, Z., & Ahmad, S. (2019). Thermal-aware real-time task schedulabilty test for energy and power system optimization using homogeneous cache hierarchy of multi-core systems. Journal of Mechanics of Continua and Mathematical Sciences, 14(4), 442-452.

Ali, M., Cheema, S. M., Ayub, N., Naz, A., & Aslam, Z. (2022, December). Impact of adopting robots as teachers: a review study. In 2022 International Conference on Emerging Technologies in Electronics, Computing and Communication (ICETECC) (pp. 1-9). IEEE.

Naveed, A., Khan, H., Imtiaz, Z., Hassan, W., & Fareed, U. (2024). Application and Ethical Aspects of Machine Learning Techniques in Networking: A Review. Spectrum of engineering sciences, 2(3), 455-501.

Ayub, N., Bakhet, S., Arshad, M. J., Saleem, M. U., Anam, R., & Fuzail, M. Z. (2025). AN ENHANCED MACHINE LEARNING AND BLOCKCHAIN-BASED FRAMEWORK FOR SECURE AND DECENTRALIZED ARTIFICIAL INTELLIGENCE APPLICATIONS IN 6G NETWORKS USING ARTIFICIAL NEURAL NETWORKS (ANNS). Spectrum of Engineering Sciences, 3(4), 348-364.

Ghafoor, U., Ayub, N., Yaseen, A., Anas, M., Farooq, I., Khan, S., & Naghman, N. F.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

(2025). AI Assisted Heart Disease Prediction and Classification and Segmentation based on PIMA and UCI Machine Learning Datasets. Annual Methodological Archive Research Review, 3(7), 248-276.

Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023

Jabeen, T., Mehmood, Y., Khan, H., Nasim, M. F., & Naqvi, S. A. A. (2025). Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1), 143-161.

Khan, A. K., Bakhet, S., Javed, A., Rizwan, S. M., & Khan, H. (2025). Framework for Predicting Customer Sentiment Aware Queries and Results in Search Using Oracle and Machine Learning. Spectrum of Engineering Sciences, 3(2), 588-617.

Hashmi, U., & ZeeshanNajam, S. A. (2023). Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems. Journal of Mechanics of Continua and Mathematical Sciences, 14(4), 442-452.

Saeed, N., Ayub, N., Haider, A., Ghafoor, U., Ali, A., Wahab, A., ... & Hussain, M. Z. Exploration of Behavior-Based Advanced Persistent Threat (APT) Detection: A Systematic Analysis based on Open CTI, MITRE ATT&CK, and Machine Learning.

Sultan, H., Rahman, S. U., Munir, F., Ali, A., Younas, S., & Khan, H. (2025). Institutional dynamics, innovation, and environmental outcomes: a panel NARDL analysis of BRICS nations. Environment, Development and Sustainability, 1-43.

Hussain, M., Ahmed, H. A., Babar, M. Z., Ali, A., Shahzad, H. M., Rehman, S. U., ... & Alshahrani, A. M. (2025). An Enhanced Convolutional Neural Network (CNN) based P-EDR Mechanism for Diagnosis of Diabetic Retinopathy (DR) using Machine Learning. Engineering, Technology and Applied Science Research, 15(1), 19062-19067.

Ramzan, M. S., Nasim, F., Ahmed, H. N., Farooq, U., Nawaz, M. S., Bukhari, S. K. H., & Khan, H. (2025). An Innovative Machine Learning based end-to-end Data Security Framework in Emerging Cloud Computing Databases and Integrated Paradigms: Analysis on Taxonomy, challenges, and Opportunities. Spectrum of engineering sciences, 3(2), 90-125.

Mujtaba, A., Zulfiqar, M., Azhar, M. U., Ali, S., Ali, A., & Khan, H. (2025). ML-based Fileless Malware Threats Analysis for the Detection of Cyber security Attack based on Memory Forensics: A Survey. The Asian Bulletin of Big Data Management, 5(1), 1-14.

Hussain, S., Sarwar, N., Ali, A., Khan, H., Din, I., Alqahtani, A. M., ... & Ali, A. (2025). An Enhanced Random Forest (ERF)-based Machine Learning Framework for Resampling, Prediction, and Classification of Mobile Applications using Textual Features. Engineering, Technology & Applied Science Research, 15(1), 19776-19781.

Khan, H., Imtiaz, M. A., Siddique, H., Rana, M. T. A., Ali, A., Baig, M. Z., ... & Alsaawy, Y. (2025). An Enhanced Task Migration Technique Based on

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Convolutional Neural Network in Machine Learning Framework.

Farooq, I., Ahmed, S. A., Ali, A., Warraich, M. A., Aqeel, M., & Khan, H. (2024). Enhanced Classification of Networks Encrypted Traffic: A Conceptual Analysis of Security Assessments, Implementation, Trends and Future Directions. The Asian Bulletin of Big Data Management, 4(4), 500-522.

Fawy, K. F., Rodriguez-Ortiz, G., Ali, A., Jadeja, Y., Khan, H., Pathak, P. K., ... & Rahman, J. U. (2025). Catalytic exploration metallic and nonmetallic nano-catalysts, properties, role in photoelectrochemistry for sustainable applications. Reviews in Inorganic Chemistry, (0).

Liaqat, M. S., Sharif, N., Ali, A., Khan, H., Ahmed, H. N., & Khan, H. (2024). An Optimal Analysis of Cloud-based Secure Web Applications: A Systematic Exploration based on Emerging Threats, Pitfalls and Countermeasures. Spectrum of engineering sciences, 2(5), 427-457.

Adil, M. U., Ali, S., Haider, A., Javed, M. A., & Khan, H. (2024). An Enhanced Analysis of Social Engineering in Cyber Security Research Challenges, Countermeasures: A Survey. The Asian Bulletin of Big Data Management, 4(4), 321-331.

Maqsood, M., Dar, M. M., Javed, M. A., & Khan, H. (2024). A Survey on the Internet of Medical Things (IOMT) Privacy and Security: Challenges Solutions and Future from a New Perspective. The Asian Bulletin of Big Data Management, 4(4), 355-368.

Khawar, M. W., Salman, W., Shaheen, S., Shakil, A., Iftikhar, F., & Faisal, K. M. I. (2024). Investigating the most effective AI/ML-based strategies for predictive network maintenance to minimize downtime and enhance service reliability. Spectrum of Engineering Sciences, 2(4), 115-132.

Ahmad, J., Salman, W., Amin, M., Ali, Z., & Shokat, S. (2024). A Survey on Enhanced Approaches for Cyber Security Challenges Based on Deep Fake Technology in Computing Networks. Spectrum of Engineering Sciences, 2(4), 133-149.

Ayub, N., Ejaz, A., Hassan, B., Hussain, M. Z., Nadeem, M., Sabir, L., & Fatima, S. (2025). An Efficient Machine Learning And Deep Learning Based Deep Packet Security Framework For Detection Of Computing Network Faults In The Iots. Spectrum of Engineering Sciences, 3(5), 659-674.

Ayub, N., Imtiaz, M. A., Ali, E., Alqahtani, A. M., Ali, A., Ashurov, M., ... & Law, F. L. (2025). A Decision Framework for Intra Task Fixed Priority INTEL PXA270 Distributed Architecture for Soft RT-Applications Based on Deep Learning. Engineering, Technology & Applied Science Research, 15(3), 23553-23558.

Ayub, N., Waheed, A., Ahmad, S., Akbar, M. H. A., Fuzail, M. Z., & Hashmi, A. H. (2025). Strengthening Network Security: An Efficient DL Enabled Data Protection and Privacy Framework for Threat Mitigation and Vulnerabilities Detection in IoT Network. Annual Methodological Archive Research Review, 3(6), 1-25.

Farooq, M., Younas, R. M. F., Qureshi, J. N., Haider, A., & Nasim, F. (2025). Cyber security risks in DBMS: Strategies to mitigate data security threats: A systematic review. Spectrum of engineering sciences, 3(1), 268-290.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Ayub, N., Habib, Z., Bakhet, S., Riaz, S., Rizwan, S. M., Abid, M., ... & Khan, H. (2025). An Optimal Ai & Deep Learning Mechanism For Mitigating Hacking Threat Identification Using Secure Network Infrastructure Based On Linux And Software-Defined Network (Sdn). Spectrum of Engineering Sciences, 3(5), 675-687.

Aslam, I., Tariq, W., Nasim, F., Khan, H., Khawaja, M. F., Ahmad, A., & Nawaz, M. S. (2025). A Robust Hybrid Machine Learning based Implications and Preventions of Social Media Blackmailing and Cyber bullying: A Systematic Approach.

Ayub, N., Anwer, M. A., Iqbal, A., Rizwan, S. M., Shahbaz, A., Abid, M. H., & Rafi, S. (2025). Enhanced ML Framework based on Artificial Neural Network for countermeasures of Data Protection and Network Vulnerabilities Detection in Industrial Internet of Things. Annual Methodological Archive Research Review, 3(5), 410-431.

Jabeen, T., Mehmood, Y., Khan, H., Nasim, M.F. and Naqvi, S.A.A., 2025. Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1), pp.143-161.

Ali, H., Ayub, N., Irfan, A., Fayyaz, S., Masood, H., Ahmad, A., ... & Khan, H. (2025). A Unified AI-powered Social Media Platform for Intelligent Scheduling and Data Driven Analytics Using Multi-Layered Artificial Neural Networks (ANNs): https://doi. org/10.5281/zenodo. 17572988. Annual Methodological Archive Research Review, 3(11), 94-134.

Khawar, M. W., Ayub, N., Shaheen, S., Iftikhar, B., Masood, H., Ahmad, A., & Khan, H. (2025). An Efficient system based on Artificial Intelligence for the Detection and Mitigation of network Intrusion using encrypted traffic protocols: A Systematic Approach. Annual Methodological Archive Research Review, 3(11), 32-71.

Musharraf, S. T., Masab, M. M., Ayub, N., Murtaza, S., Ullah, H., Ahmad, A., ... & Khan, H. (2025). An Efficient Artificial Intelligence-Based Early Prediction of Heart Attack Using Deep Learning CNN and SVM Models: https://doi. org/10.5281/zenodo. 17551611. Annual Methodological Archive Research Review, 3(10), 265-301.

Niaz, H. U., Qadeer, Q. B. Q., Niaz, H., Mansib, H., Awais, M., & Khan, H. (2025). Artificial Intelligence Assisted Autonomous Unmanned Aerial Vehicles (UAVs) and Aerial drones based on Machine Vision for Enhancing Remote Sensing of Precision crop Health Monitoring. The Asian Bulletin of Big Data Management, 5(4), 155-177.

Nawaz, S., Salman, W., Shahid, U., Khokhar, M. L., Iqbal, M. Z., & Hamid, A. (2024). A Survey on Latest Trends and Technologies of Computer Systems Network. Spectrum of Engineering Sciences, 2(4), 85-114.

Raza, A., Khan, H., & Rehman, S. U. (2023). Computational Analysis of Nanomaterials for Energy Storage. International Journal of Advanced Sciences and Computing, 143-154.

Zainab, Khan, H., Din, I. U., Tariq, M. I., Khalid, A., & Naz, A. (2023, May). An Efficient Implementation of an IoT-Based Smart Home Security System. In International Conference on Computing & Emerging Technologies (pp.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)
https://doi.org/10.5281/zenodo.20028851

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

249-259). Cham: Springer Nature Switzerland.

Muhammad Anas,Muhammad Atif Imtiaz,Saad Khan,Arshad Ali,Noor Fatima Naghman,Hamayun Khan,Sami Albouq, AN ADVANCED MACHINE LEARNING (ML) ARCHITECTURE FOR HEART DISEASE DETECTION, PREDICTION AND CLASSIFICATION USING MACHINE LEARNING, Cont.& Math. Sci, Vol.20, No.3 https://doi.org/10.26782/jmcms.2025.03.00005

Farooq, I., Ghafoor, U., Umer, S., Ali, A., Shahid, A. K., & Khan, H. (2025). An Efficient Big Data Security and Privacy in Healthcare for Enhancing Remote Sensing and Monitoring: A Technological Perspective based on ACL for Preserving Big Data Analytics in Cloud. The Asian Bulletin of Big Data Management, 5(4), 231-258.

Khan, A. K., Ghafoor, U., Ayub, N., Ali, A., Abdullah, M. M., & Khan, H. (2026). AI and Machine Learning Assisted Customer Aware Queries: A Comprehensive Analysis to improve User experience based on Natural Language Processing (NLP), Databricks, and Oracle APEX. The Asian Bulletin of Big Data Management, 6(1), 94-118.

Akhtar, M. H., Ghafoor, U., Imran, O., Ayub, N., Abdullah, M. M., & Khan, H. (2026). An Efficient AI and Deep learning Assisted Self-Healing Network Approach: Analysis on Fault Detection Response and Recovery to Mitigate Threats in IoT-Security Ecosystem. The Asian Bulletin of Big Data Management, 6(1), 40-66.

Arshad, S., Ayub, N., Basit, A., Ali, A., Rizwan, S. M., Abdullah, M. M., ... & Hussain, M. Z. An Efficient Deep Learning Enabled Multimodal Sentiment Analysis based on Neural Networks and Text Mining Architectures for Short-Form Social Media Data: A Comprehensive Analysis.

Mahmood, F., Shehroz, M., Ansari, Z., & Rauf, F. (2024). A Survey of Software-Defined Networks Based on Advance Machine Learning Based Techniques. Spectrum of Engineering Sciences, 2(4), 232-257.

Gul, W., Nawaz, A., Hamaz, M. T., & Khan, H. AN EFFICIENT MODEL FOR THE SELECTION OF LEADERSHIP COMPETENCIES AND PERFORMANCE IMPROVEMENT FOR THE SUCCESS OF TRANSPORTATION PROJECTS, JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES Vol.-16, No.-5, May (2021) pp 49-65 https://doi.org/10.26782/jmcms.2021.05.00005

Hamayun Khan,Sheeraz Ahmed,S. Farhan Haider Shah,Rehan Ali Khan,Zeeshan Najam,Hasnain Abbas,Asif Nawaz,Zubair Aslam Khan, JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES, Vol.-15, No.-8, August (2020) pp 628-646 https://doi.org/10.26782/jmcms.2020.08.00053