Received: 23 April 2024 | Revised: 18 June 2024 | Accepted: 22 July 2024 | Published online: 7 August 2024

Journal of Computational and Cognitive Engineering
2024, Vol. 00(00) 1–18
DOI: 10.47852/bonviewJCCE42023198
BON VIEW PUBLISHING

RESEARCH ARTICLE

Dempster Combination Rule-Aided Multi-Sensor Decision-Level-Based Data Fusion in Industrial Internet of Things (IIoT) over Zero-Trust Security

Anamika Singh[1], **Rajesh Kumar Dhanaraj**[2,*] and **Anupam Kumar Sharma**[1,*]

[1] *School of Computing Science and Engineering, Galgotias University, India*

[2] *Symbiosis Institute of Computer Studies and Research (SICSR), Symbiosis International (Deemed University), India*

Abstract: Data fusion is a process of accommodating data from discrete sources to generate more relevant information with enhanced accuracy and compatibility rather than the data gathered and information produced by the identical or particular source. To achieve better accuracy in the information inferred by the Industrial Internet of Things (IIoT) system, data fusion is an emerging technology that takes data from different involved devices as input and generates more consistent and accurate information. To safeguard the IIoT data involved in communication foremost is to ensure the authenticity of the devices to block unauthorized access and thus enhance the data confidentiality and data integrity as well. Zero-trust security is thus employed in the IIoT infrastructure to meet the security requirements in question. The proposed approach, Dempster combination rule-aided multi-sensor decision-level-based data fusion (MS-DLDF) in Industrial Internet of Things (IIoT) over zero-trust security, breaks down the whole concept into phases – initially, the device authenticity is ensured before entering and accessing the network, next, the device data is then encoded to avoid data theft or breach from any unauthorized device, and lastly, the data fusion algorithm is executed to gather data from multiple sources as input and reach to more appropriate and relevant information as compared to the information inferred from a single source. The proposed MS-DLDF concludes with the outstanding results of the Dempster combination rule with the increased number of sensors in complex networks as compared to the single-source data fusion and Bayesian estimation data fusion with enhanced accuracy by 6%, minimal computation time by 15%, increased precision rate 6%, reduced false positive rate by 31%, and the amplified data confidentiality rate by 2%, respectively.

Keywords: data fusion, multi-sensor, zero-trust security, Dempster combination rule, single-source data fusion (SSDF), Bayesian estimation data fusion (BEDF)

1. Introduction

Smart and effective data retrieving and gathering are the tasks the Industrial Internet of Things (IIoT) infrastructure performs. IIoT is an archetype that establishes communication and makes connections among multiple discrete devices with the aid of the Internet. Thus, with the involvement of many devices, immense coarse data is produced via the smart sensors associated with the device. With the application of digitization, the IIoT infrastructure gained much popularity by employing smart devices in the network to execute and manage operations on and by devices to provide better functioning. The diverse devices in the network collaborate with each other to initiate communication. Everything in the IIoT network operates around the devices without human intervention. The smart IIoT infrastructure comprises different intelligent sensors around the network to establish seamless communication among the devices. With the involvement of numerous smart sensors in the IIoT, the raw data is collected from multiple datasets held by different devices in the network to analyze and obtain more accurate, compatible, and relevant information that infers better quality than that of information acquired from data retrieved from individual device datasets, resulting in more effective decision-making to any state with standard and enhanced services.

Single-source data fusion (SSDF) [1] is a data fusion technique in which the source data or the evidence is collected from a single-source device or single sensor as an input. Therefore, with the availability of single sensor data, the accuracy and decisiveness of information produced as output is compromised. In Alfrhan et al. [2], the Bayesian estimation method is taken forward for clustering and combining the data for generalization.

With the emergence of IIoT, the network thus formed becomes more prone to cyberattacks and data theft by malicious devices in the network. The data held by the devices are the credentials that the industry uses for its functioning over the network.

***Corresponding author:** Rajesh Kumar Dhanaraj, Symbiosis Institute of Computer Studies and Research (SICSR), Symbiosis International (Deemed University), India. Email: rajesh.dhanaraj@sicsr.ac.in and Anupam Kumar Sharma, School of Computing Science and Engineering, Galgotias University, India. Email: anupam.sharma@galgotiasuniversity.edu.in

The traditional security solutions are now not enough to meet the current security requirements of the system or the network. Thus, zero-trust security is the improved and uplifting technology that fulfills the security requirements in question. Zero-trust security came into existence years back in 1994 by Stephen Paul Marsh in his presented thesis on computer security at the University of Stirling [3]. The concept of zero-trust security is based on the foundation of "never trust; always verify". The system with zero-trust security assumes that the nodes or devices in the network are not trustworthy, either being members of the network or extraneous nodes seeking permission to access the network [4]. Therefore, zero trust performs continuous monitoring and authentication of the devices before granting permission to enter the network to establish communication with the authorized device and the associated resources. Based on different characteristics, zero-trust security with the aid of artificial intelligence and other machine learning techniques creates a device profile to recognize the authentic device depending on its usual behavior and communication patterns and blocks the devices from showing unusual behavior. Zero-trust security in the proposed approach has significant importance in safeguarding the device's data because data fusion in IIoT involves an immense number of private datasets that need to be protected from malicious devices.

Data fusion operates on the phenomenon of a "gathering and summarizing" approach. There are different data fusion techniques involved that, with the aid of smart sensors associated with the devices in the network, extract the relevant data as an input dataset and after analyzing and examining all the datasets obtain better and more consistent information [5]. The selection of data from multiple datasets yields better, and more relevant information than the information produced from a single dataset infers. The resultant information obtained is from the fused data that is produced by multiple dataset inputs from distinct sources [6]. The sensors employed provide the data with advantages and loopholes, which are considered in decision-making to choose the more accurate dataset by combining multiple datasets. The IIoT infrastructure involves sensors, data analysis, decision-making, and communication techniques to enhance the production of IIoT infrastructure, resulting in more conclusive, relevant, and prudent information with reduced power consumption as low-power hunger sensors can also be employed [7].

One of the challenges addressed in the data fusion method is that the devices in the IIoT environment held both trivial and nontrivial raw data required for the IIoT infrastructure's sound performance. The identification and labeling of the devices with the quality of data they possess are key considerations to provide sensible and more decisive information. The identification of the device's data could be performed by calculating the quality of the device data to provide more relevant information with the aid of fuzzy values. The fuzzy values thus calculated recognize the device with higher quality data desired or the productivity of the IIoT system or the device with the least relevant data that need not be considered in the acquiring of information from the raw data. The data fusion-based generated information is directly proportional to the level at which the raw data is monitored and observed under situations. All the devices are monitored, and the dataset is then extracted to generate information that is more accurate as compared to the information generated from the individual dataset from the single-source device.

The Dempster rule of combination is a method that facilitates the amalgamation of different sources of proof to achieve trust. In the combination rule, the trust achieved with the combination of discrete sources is authorized only for the source data that are labeled as uncertain and held as arbitrary values, provided they are scientifically justified [8]. The Dempster rule generally follows the method of generalization. Every source is treated as an independent evidence having some uncertainty and distinct belief; the combination rule is then applied to generalize a trust function via continual pooling of evidences. The use of the Dempster combination rule empowers the system with a generalized configuration to quantify, represent, and manage variability in the source evidences.

Deep Q-learning is a category of reinforcement learning that utilizes deep neural networks to produce more optimized and accurate results of the Q-learning [9]. Deep Q-learning is a feasible approach in dealing with large problems with increased state action and exponentially the Q-table. With the aid of deep Q-learning (DQL), the approximation of each state-action pair can be achieved efficiently. DQL uses neural networks in place of Q-table for a state-action pair; instead of mapping the state-action values on a Q-table, DQL creates a pair of action, Q-value pair. In DQL, the effective handling of large spaces is possible so is the need for an IIoT network [10].

The proposed paper implements multi-sensor-based decision-level data fusion (MS-DLDF) because the undertaken category of data fusion cross-verifies the accuracy of the dataset involved in the information generation by providing an intermediate data fusion result as the preprocessed state before concluding the final information. The cross-verification phase ensures the quality of the information before the final decision of the data fusion process. The proposed paper adopts the multi-sensor data fusion technique for the IIoT infrastructure to gather and combine the raw data extracted from discrete sensors. The overall methodology of the adopted approach works on different phases – (1) device authentication and identification, (2) identifying the quality of the dataset, and (3) MS-DLDF. The first step is achieved by examining the communication pattern and building a profile of the device based on the features it possesses. For building a profile, the considered feature or the parameter used is the "smart sensors" associated with every device in the IIoT network and the communication pattern noted by the policy administrator during the communication process. After ensuring the authenticity of the device using the DQL algorithm, the next is to label the individual device with the quality of the dataset the particular device contains, and it is performed with the aid of the fuzzy logic sets delineating the low-quality and less adopted dataset or the dataset with high quality and acceptance. The fuzzy sets are built on a five-level scale that implies the quality of the data ranging from low to high with labels (AS, GS, M, GW, AW), respectively. Based on the quality of the data desired by the system, the model then activates the corresponding sensors of the devices needed to extract the required dataset and then examines and analyzes the dataset to obtain more sensible and relevant information with the aid of Decision-Level Data Fusion (DLDF). Multi-sensor data fusion is employed in this approach with the aim of sensing and collecting data from the IIoT environment where thousands of devices are interconnected to establish the communication responsible for the functioning and growth of the IIoT framework.

Despite several modifications in the field of IIoT framework, the device's security has always been a major consideration to meet the enhanced security requirements in more complex networks. The IIoT infrastructure faces some challenges that are highlighted and focused in the adopted approach. Multi-sensor data fusion motivates more accurate, robust, and decisive information rather than the data acquired from a single source. By collecting, sensing, and fusing the data from multiple sensors and then acquiring a generalized information, the system produces more convenient, relevant, and sensible information when the smart sensors extract information from discrete devices rather than from an individual device. Moreover, the IIoT infrastructure with thousands of devices contains both trivial and nontrivial data that need to be classified for the generation of more sensible information. The adopted approach employed fuzzy logic sets that evaluate the quality of the data held by the devices to ensure that the information thus obtained is more decisive and meaningful. The traditional security solutions are now not sufficient to meet the enhanced security needs in the complex network in the IIoT framework. To ensure the high-security desires of the IIoT infrastructure, the proposed paper outlines the use of zero-trust security combined with deep learning-based device authentication.

The major contributions of the paper are as follows:

1) Deep learning-based zero-trust security network safeguards the IIoT devices from the reach of unauthorized access by verifying the authenticity of the device at the initial stage based on the device profile.
2) MS-DLDF in the IIoT framework provides more decisive, sensible, and compatible information that is cross-verified at the intermediate stage with accuracy and relevance depending on the datasets extracted.
3) Fuzzy sets identify and label the quality of the data an individual device holds.
4) Quality check of the data classifies the trivial and nontrivial data, thus improving the quality of the obtained information by ignoring the nontrivial dataset.

The paper is structured with Section 2 providing the literature review that summarizes the related works based on the underlying approach with the contribution and the solution to the research gap in question. Section 3 explains the methods and materials referred to in the proposed paper. Next, section 4 elaborates on the overall adopted approach with all the associated graphs and algorithms. Section 5 provides insight into the experimental setup and the analysis of the results obtained after evaluating the performance of the underlying approach on certain parameters. The paper concludes with Section 6, disclosing the conclusion and the future scope of the overall study.

2. Literature Review

Digitization or the industrial fourth revolution led to the IIoT where information is produced from multiple source data extracted from various devices involved in the network. IIoT infrastructure intends to develop a system where coordination and association are enabled between the devices in the network to balance the real-world scenarios and the networked space. Data fusion performs a collective analysis of the different data from different sources for a specific scenario or state. The more monitored and observed raw data is adopted, the more decisive and sensible information the system infers [3]. Data fusion has been experienced widely in IoT frameworks because of the involvement of an immense number of discrete devices. IIoT infrastructure constitutes of an immense number of interconnected devices to establish communication via the Internet. The individual devices have smart sensors to sense and extract the required data for relevant information. Nowadays, the traditional educational system has switched to digitized and smart educational systems [4]. To facilitate the modernized learning system, network-oriented and circumstances-attentive smart devices have significant importance. In a smart learning environment, the records of a huge number of students are fetched, combined, and then analyzed to generate more accurate information. In Khan and Anwar [5], the approach for data fusion technique in digital learning and educational data mining is introduced in smart education to establish communication with the authorized device on a hybrid infrastructure with the blended paradigm of traditional and digital paradigms.

The shifting of the traditional paradigm of architectural, engineering, and manufacturing sectors to the digital platform experiences the availability of data from discrete sources for extracting and gathering relevant data [6]. In Tsanousa et al. [7], a systematic review was made to interrogate the integration of IoT and building information modeling (BIM) to empower data-guided architectural, engineering, and manufacturing (AEM) management. A two-tier framework is enabled to examine and delineate the data flow and categorize the absorption level of data with data clarification and the objective of employing the data fusion technique. The concatenation of BIM and IoT, along with the creation of the digital twins, provides the solution to the challenges of data fusion in BIM and IoT, which point out the procedure of retrieving and assembling the BIM and IoT data, respectively [8]. A four-tier data process framework is enabled to restrict the source of data from BIM and IoT-data retrieval, combined presentation, gathered examination, and employment [9]. The key feature of DLDF that makes it different from other methods of data fusion is that it produces intermediate results or intermediate information from the extracted dataset and thus cross-verifies the relevance and the quality of the information obtained; after getting assured with the information generated, the final decision is then made with the final information that is revealed as the outturn of the overall process [10].

Based on Fawzy et al. [11], the considerable loopholes in the data fusion technique were addressed, such as the depiction of events with minimal or no certainty, the integration of noncomparable knowledge, and the criteria for combining and describing the discrete source findings. A review was performed to address the employment of deep learning in IoT security in Meng et al. [12]. Moreover, considering the security aspect of IoT infrastructure, the examination of the relevance of deep learning in enhancing security is performed. With the emergence of the fourth industrial revolution or Industry 4.0, the peer techniques of device authentication are not enough to meet the increased security requirements of complex networks. Deep reinforcement learning provides an ambient solution to efficiently recognize the device when considering complex networks with thousands of devices [13]. In any network, there is always a possibility of attack either from intruders or insiders. To inhibit the attacks, zero-trust security model is a well-formulated design that doesn't simply trust the devices based on their locality but rather asks the devices to authenticate their identity every time they access the network. IIoT devices comprise of smart sensors to fetch and combine datasets from discrete sources. Multi-sensor data fusion has a significant importance in the IIoT networks in facilitating sound decision-making [14]. In Azam et al. [15], the benefits of multi-sensor data fusion over single-source data fusion are addressed. The decision-level data fusion in multi-sensor-oriented systems provides cross-verification and ensures the relevance and quality of the information produced by generating the intermediate results from the fetched dataset, and then depending on the intermediate results, the effective decision-making is achieved to fuse the data from multiple discrete sources [16]. The shifting of traditional paradigms to the digital platform has witnessed the incremented involvement of sensors, which need interactive algorithms that facilitate the efficient fetching and fusion of datasets. Based on Kong et al. [17], the comparative analysis is made to examine the behavior and characteristics of the decision confusion produced by the testimonial-oriented categorization and the single categorization framework. Unlike supervised and unsupervised learning algorithms, Q-learning is an intelligent learning algorithm that is performed from the selection of action by the agent for the state entered the environment to assigning rewards to the agent based on its performance [18]. In the work of Al-Hamadani et al. [19], the applications and algorithms of reinforcement learning in health care and robotics are summarized. For robotics, the review is performed on the manipulation of the object and grabbing in industries as well as in health care. The improved Q-learning for planning the path of mobile robots is explained in Zhou et al. [20], with performance on three different complexity levels.

Deep learning is a widely accepted technology and is experienced in almost every corner of the world. According to Hamda et al. [21], a deep-quality learning network-driven e-learning or the distance learning to configure a robust system in order to approximate the Q-values obtained is explained. An improved Q-learning algorithm based on approximate state matching in an agricultural plant protection environment to learn the most optimized policy for the Unmanned Aerial Vehicle (UAV) in agriculture plant protection is suggested in El Faouzi and Klein [22]. In Qi et al. [23], deep learning-based speed profiling for the users of mobile in the 5G networks is demonstrated with 94.5% of detection in terms of f1 score. The applications and the challenges of reinforcement learning in the blockchain technology are summarized in the work of Lee et al. [24].

According to Logananthara et al. [25], various problem-solving strategies are discussed based on the knowledge-based systems in various domains with controlled environments. A systematic review is made by Ding et al. [26] delineating the challenges, applications, and future trends of secure data fusion in IIoT. In the work of Chango et al. [27], a review of the employment and application of data fusion in learning analytics is discussed, covering the challenges and current state of the art. In Qin et al. [28], the issues in data fusion are addressed along with the approach to overcome the gap in the data fusion technique. The study explains that the use of ensemble learning in the data fusion technique has outstanding performance in dealing with the challenges addressed in peer approaches. In digitized-driven architecture, engineering and construction (AEC), how the fusion of data from the Internet of Things and information systems can achieve data-driven AEC is delineated, and a two-level conceptual framework interconnecting BIM and IoT is proposed by Huang et al. [29]. Based on Yue et al. [30], a review is made on the deep learning application in empowering the IoT. The review is made on two broad areas- the architecture and methodology aspect and the other are the security and privacy provided by deep learning in IoT. The applications, architecture, and foundation implementation of zero-trust security are reviewed in He et al. [31]. The core technologies in zero-trust security including the authentication of identity, evaluation of trust, and controlling the access of devices in the network are also summarized. From Tong et al. [32], research is performed on the techniques that facilitate the fusion of data using multiple sensors addressing the validity and relevancy of data gathered from different sources. The algorithms for merging the information are also introduced.

A multi-sensor fusion of information and the algorithms reacted to the intelligent optimization in the field of mobile robots are explained by Guo et al. [33]. Based on Gao et al. [34], the applications and the security measures provided by the zero-trust security network in empowering power Internet of Things are explained. A systematic review of the zero-trust security-based security in cloud computing is performed by Sarkar et al. [35], discussing about the challenges in cloud computing and the requirements for the zero-trust network. In the study of Peres et al. [36], a holistic approach to the view of industrial artificial intelligence in Industry 4.0 is reviewed. The summary of the research on the techniques used for identifying and assessing functional and nonfunctional requirements, and all other factors for examining smart manufacturing systems is made by Sharma and Villanyi [37]. According to Singh [38], the issues of unemployment due to the lack of technological unawareness in Industry 4.0 are summarized and explained. The indexing and discussion of the research made on the various deep learning and machine learning techniques in providing or empowering cybersecurity along with the underlying challenges are provided by Xin et al. [39]. Based on Sharma et al. [40], the applications, issues, and future trends of deep learning and machine learning in various domains are compiled and discussed.

In the work of Buck et al. [41], the current adoption, applications, and associated challenges in the zero-trust security-based prevention and security measure are reviewed. An ensemble learning-based analysis and prediction of anomalies with the aid of log processing is proposed by Wang et al. [42]. The adopted approach outstands in improving the recall, accuracy, and F1 values in detecting anomalies. According to Pang et al. [43], a review is conducted to delve into the applications and use of deep learning in anomaly detection. The survey bifurcates 3 high-level categories and 11 fine-grained categories of deep learning. A fusion of binary normal/attach classifier and multi-attacks classifier is performed to develop a model for anomaly detection is conceptualized in AlDahoul et al. [44]. Based on Hu et al. [45], a review on hyperspectral anomaly detection driven by deep learning approach is portrayed to highlight the advantages offered by the underlying approach. The profiling of nodes in the social media platform using the PageRank algorithm is brought up by Elbaghazaoui et al. [46]. From the research of Safi et al. [47], a distributive profiling approach is adopted to classify IoT and non-IoT devices and the network they belong to; moreover, the regular updating of profiles thus formed. A smart navigation technique for blind people facilitating smart homes integrating fuzzy logic in IoT devices is discussed by Tayyaba et al. [48] to navigate and avoid obstacles. In the study of Hosney et al. [49], artificial intelligence-based zero-trust security architecture is proposed. An enhanced Q-learning algorithm is discussed by Sun et al. [50], to approximate the matching of state in agricultural plant protection on the datasets uniformly distributed in UAV parameter and real farm. Based on Ramezanpour et al. [51], the empowering of 5G/6G network with intelligent zero-trust security architecture, with the assumptions, complexities, and significance of machine learning referring to O-RAN is delineated. The profiling technique with the aid of deep learning for the mobile users levering 5G cellular networks is suggested by Saffar et al. [52]. The involvement of deep learning automatically generates mobile speed profiling.

The adopted approach focused on MS-DLDF to retrieve the information with enhanced compatibility and is more decisive. The existing single-source data fusion involves the participation of single dataset from an individual source that infers less consistent and decisive information as compared to multi-source data fusion that involves the dataset from multiple sources. The existing approaches lacked to focus on the intermediate layer in fusing the results of the multi-sensor of the participating devices. The adopted approach fills the gap by implementing the MS-DLDF that analyzes the intermediate results to provide more compatible and decisive information. The peer approaches involve the dataset from single source only that infers restricted and less decisive information as compared to the information inferred from the proposed MS-DLDF. The proposed method amplifies the IIoT environment performance in the context of accuracy, computation time, precision, false positive rate, and data confidentiality rate, which the existing approaches despite the several improvements failed to highlight.

3. Materials and Methods

3.1. Materials

The experimental evaluation of the proposed method is derived from the public dataset available in IIoT_data of 59.06 MB in CSV format having 405,184 records. The supplementary dataset under consideration is X-IIoTID dataset of 106.71 MB containing 820,835 records.

3.2. Methods

The proposed methodology Dempster combination rule-aided multi-sensor decision-level-based data fusion (MS-DLDF) outperforms the existing SSDF [1] and Bayesian estimation data fusion (BEDF) [2] involved in the simulation. In El Gourari et al. [1], the single-source data fusion technique is delineated reflecting the lack of decisiveness of the information generated with the single-source dataset. BEDF [2] incorporates the data fusion technique that lacks focus on the security of the data being used for the fusion process. Therefore, the proposed approach provides an ambient solution for enhancing the decisiveness and consistency of information with the aid of MS-DLDF. The MS-DLDF facilitates the generation of intermediate results that provide the insight into the final information the adopted datasets will produce. To ensure the authenticity of the device and ignore all the malicious devices to enter the IIoT network, deep Q-learning-based device verification and authentication are empowered. The adopted approach stands strong by categorizing the devices with trivial and nontrivial data via transfer fuzzy learning.

4. Proposed Methodology

MS-DLDF is an uplifting concept that gathers and combines datasets from discrete independent sources for obtaining information that comparatively infers more reliable and adequate information with improved quality than that obtained from individual datasets. The appropriate analysis is made on all the extracted datasets from multiple smart sensors associated with each device. The overall adopted approach MS-DLDF comprises three core concepts – initially, the trustworthiness of the device entering the network needs to be assured to guarantee the security of the device data, and hence, transparent communication between the authentic devices is established. To ensure the authenticity of the devices in the network, deep Q-learning-driven identification and recognition of the devices are performed based on the actions performed by the agent. Following this, in order to achieve the information with assured decisiveness and accuracy, the dataset from different devices should be relevant, complete, and correct. To fix the concern of source data validity and correctness, the fuzzy set is created to identify the data quality as per its relevance in effective decision-making for achieving accurate and consistent information. The last phase performs sensing of the dataset from multiple sensors and initiates the data fusion applying decision-level data fusion from multiple sensors for cross-verification of the information before the final outcome. The overall system model delineating the proposed approach is illustrated in Figure 1.

Figure 1
The overview of the proposed architecture MS-DLDF

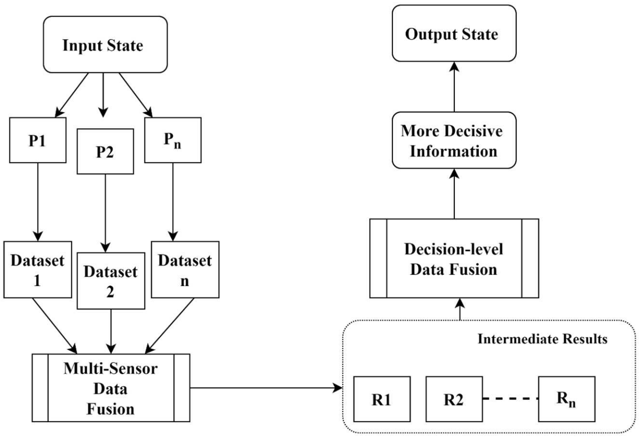
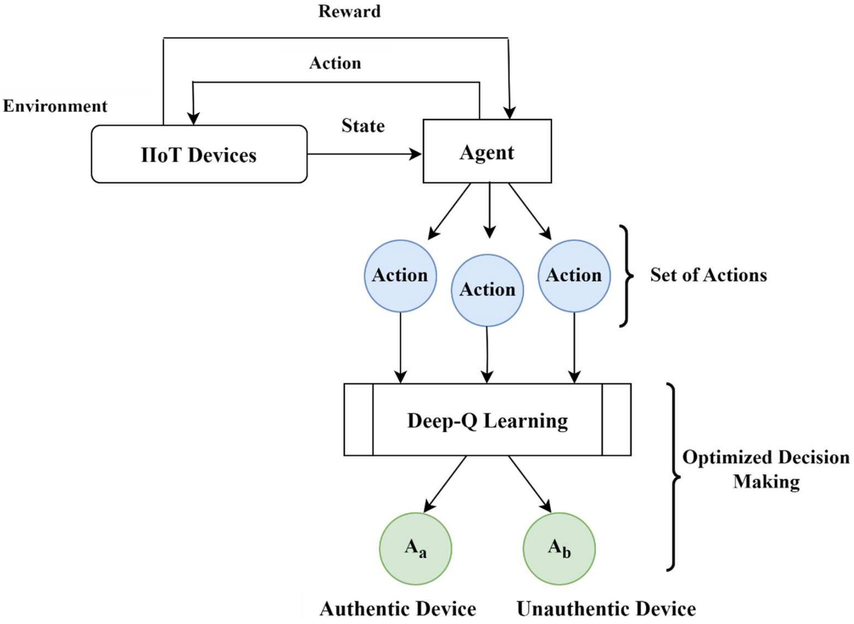


Figure 1 above demonstrates the summarized architecture of the proposed model explaining the workflow of the methodology. The initial stage in the adopted approach SDP-MS-DLDF is to verify the authenticity of the device by employing deep learning for intelligent authentication of the devices based on the sensor-oriented device profile. The deep Q-learning is employed to verify the device before allowing access. The agent chooses the most accurate action from the set of actions to refrain the legitimate and malicious devices. After verifying the authenticity of the device, the data held with the device is categorized based on its quality for the trivial and nontrivial raw data with the aid of transfer fuzzy learning. The quality of the source data is categorized via fuzzy logic into five categories: complete strong, prevalent strong, moderate, prevalent weak, and complete weak denoted as CS, PS, M, PW, and CW, respectively. Based on the quality of the data obtained from the preprocessing stage, the adopted datasets are then exposed to the explainable MS-DLDF model to analyze and combine the most relevant datasets obtained via multiple sensors and then perform decision-level data fusion to combine the datasets from discrete sources and acquire the most relevant, compatible, sensible, and decisive information as compared to the information obtained from the individual source dataset. The intermediate results are obtained from the multiple source data to assess the quality and decisiveness of the information being produced. The solution to the security requirements in the complex networks under question is provided in the proposed approach by enabling zero-trust security in IIoT networks integrating with a deep learning algorithm to intelligently recognize and verify the authenticity of the device in practice.

4.1. Deep Q-learning-based device recognition and authentication (DQL-DA)

Q-learning is an emerging technology that effectively generates sound decisions with an intelligent agent's aid. The agent is employed in the operating environment, and for every required state, it enters the environment and performs a set of actions to reach an appropriate and most relevant action for the current state in the process. Q-learning is integrated with the deep learning algorithm in order to support optimized decision-making in selecting the most accurate and appropriate action for the considered state in the environment. The zero-trust security involves continuous monitoring and verification of the devices entering the IIoT network. The continual verification of all the devices entering the network makes the devices dry up and adversely affects the production and efficiency of the IIoT framework. Also, the devices need to be verified to ensure the authenticity of the device to safeguard the network from any

Figure 2
The DQL-DA enabled IIoT framework in zero-trust network



unauthorized access and protect the devices from being targeted by a malicious device that results in disrupted data confidentiality and originality.

The first phase DQL-DA of the overall proposed system, that is, the device authentication, is represented in Figure 2 below.

The above Figure 2 explains the blueprint of the device authentication phase of the proposed approach. The state or event enters the environment, which is then passed to the agent, which is activated on receiving the state for which action is needed. Reinforcement learning works on three dimensions: state, action, and reward. RL is a type of learning that autonomously learns its action from the previous action and thus improves its learning and exponentially the results being produced. In reinforcement learning-aided decision-making, the state here is represented as the device that enters the network to access the services provided, while the environment is the IIoT network. After receiving the device to be authenticated, the agent gets initialized to perform certain actions to reach the most appropriate and optimized action. The agent then performs the set of actions to achieve the final action A_a and A_b, which implies allowing access to the device or blocking the device, respectively. The final action the agent takes is then transferred to the environment to generate a reward for the performance of the action of the agent for its accuracy and pertinence. The integration of deep learning enables optimized decision-making in choosing the action by the agent for a particular state. When the action taken by the agent falls in the A_a category, the authenticity of the device is verified at the initial stage, and the device is allowed to access the network. On the other hand, when the decision of the agent is A_b, then the device authenticity is not verified, and the device access is blocked. The delineated process comes with a solution to safeguard the IIoT network from any unauthorized access with enhanced data confidentiality and integrity. The Q-learning algorithm is mathematically stated by the Bellman equation that manifests the most appropriate and accessible actions by the agent aiming to achieve the maximum reward. Equation (1) below explains the Bellman optimality equation:

$$Q_{value}(S, A) = Rwd\ (S, A) + \ \delta \max_{A} Q_{value}(S', A) \tag{1}$$

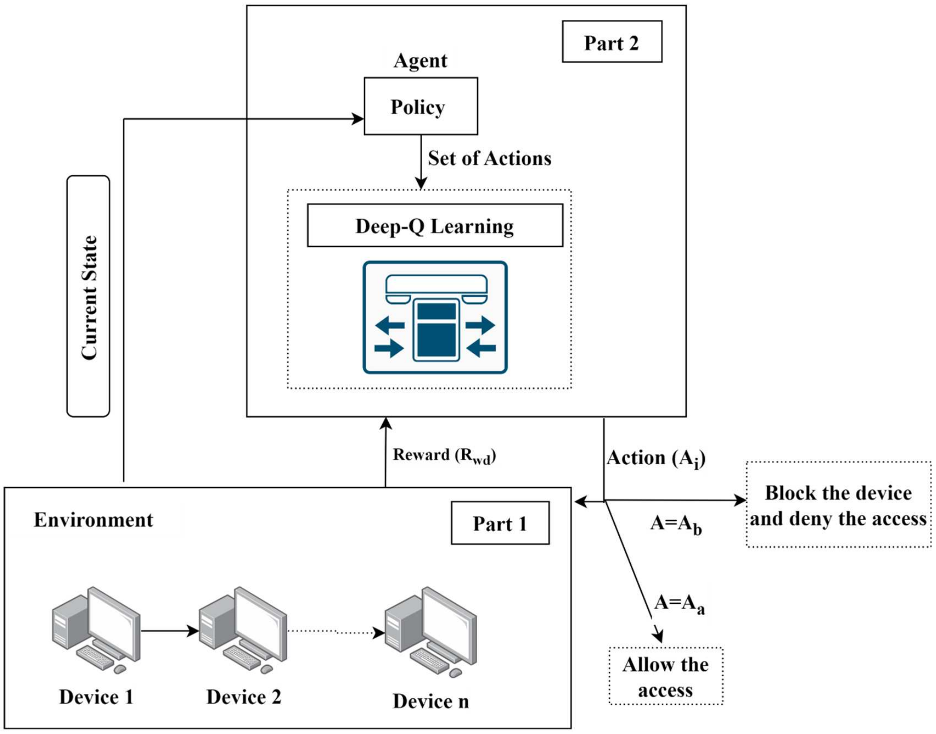
Equation (1) delineates that the generated Q_{value} is based on the state S from the environment, the most optimized action A an agent performs, and in turn, the environment passes the reward Rwd depending on the agent's performance concatenated with the maximum Q_{value} that is attainable from the succeeding state (S'). Moreover, a discount factor, δ, commands the benefaction or the role of rewards eventually. The Q_{value} generation is an iterative process, and every current Q_{value} again depends on the new Q_{value} of the next state. The architectural overview of the deep Q-learning-based device authentication scheme is represented in Figure 3 below.

The above-illustrated Figure 3 demonstrates the conceptual framework of the adopted DQL-DA. The overall architecture comprises two parts: 'Part 1' represents the 'Environment,' which includes all IIoT devices with smart sensors. The environment receives the state, enabling the agent to prompt the devices to perform specific actions. The state in the environment is transferred to "Part 2", which activates the agent to perform a set of actions based on the policies, and then the set of all the actions is exposed to the deep Q-learning framework to achieve a more optimized action that facilitates efficient decision-making in allowing or denying the access to the devices entering the environment of the IIoT infrastructure. As a result, the agent generates the action A_a or A_b, which denotes the acceptance of the device for accessing the network and blocking the device by denying access to the device, respectively. The action taken is then passed to the environment again, and then the environment based on the accuracy and optimality of the action taken by the agent assigns a reward to the agent. The rewards assigned to the agent are shown in Equation (2):

$$Rwd_t = \begin{cases} 1\ if\ A = \ A_a \\ 0\ if\ A = \ A_b \\ -1\ elseways \end{cases} \tag{2}$$

Equation (2) explains the scenario of reward assignment based on the actions performed by the agent. If the agent accepts the device, the agent is assigned by reward of "1", if denies access to the device, the reward assigned is "0", and in the state where

Figure 3
The architectural overview of the deep Q-learning-based device authentication scheme



the exact decision-making is in doubt, the reward assigned to the agent is “-1”. The overall concept hence provides the most optimal action to the required state for verifying the authenticity of the device to safeguard the IIoT infrastructure from malicious activities. The algorithm below explains the step-by-step working of the above-demonstrated DQL-DA:

Algorithm 1: Deep-Q-learning-based device recognition and authentication

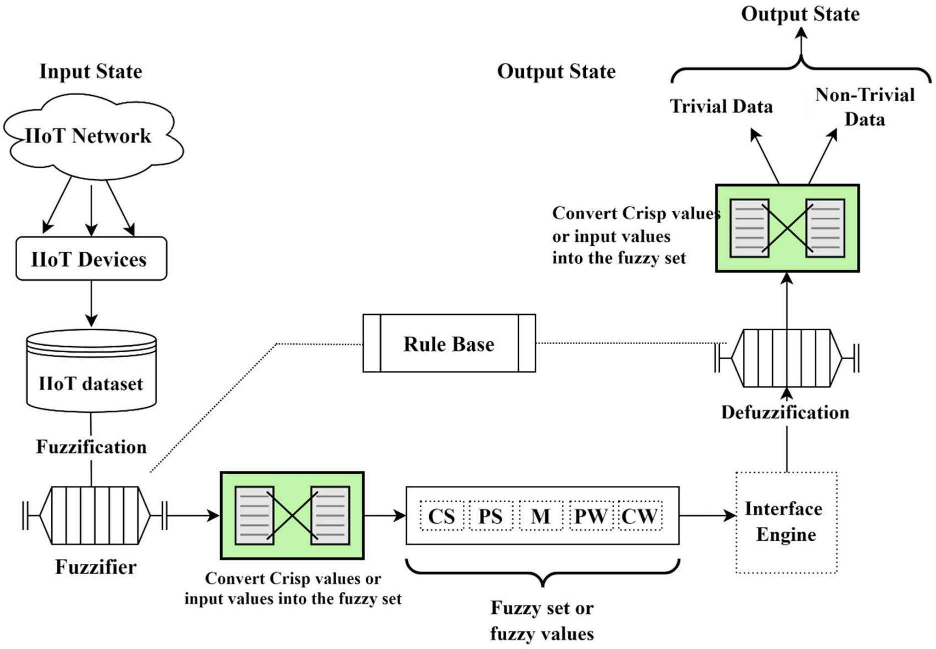
Input: Device $D = \{D_1, D_2, D_3 \ldots\ldots D_x\}$, Raw device data $= RD = \{RD_1, RD_2, RD_3 \ldots\ldots\ldots RD_y\}$, state S, set of actions A, agent Ag, environment E, time t, policy administrator module PA_m, reward Rwd_t

Output: Optimized device authentication

```
1) Assign and initialize the value of x, y, and t, where x = y
2) Initialize the policy administrator module of zero-trust security network
3) Begin
4) For every $S_t$ $ariving\ in\ time\ t\ and\ RD_i \in D$, do
5) Activate agent $Ag$ for $S_t$
6) Read the communication pattern of $D_i$ and store in $C_i$
   // Matching and decision-making for device authentication via DQL-DA
7) For every $C_i \in D_i$, do
8) Calculate $A_t$
9) If $C_i = PA_m$
10) Then $A_t = A_a$, authenticity is confirmed, and the device is allowed to access the network
11) Transfer $A_t \rightarrow E$ to calculate $Rwd_t$ and $Q_{value}(S_t, A_t)$ using Equation (1):
    $Q_{value}(S_t, A_t) = Rwd(S_t, A_t) + \delta \max_A Q_{value}(S'_t, A_t)$
12) End if
13) Else
14) If $C_i \neq PA_m$
15) Then $A_t = A_b$, authenticity is not confirmed, and the device is blocked with denied access
16) Transfer $A_t \rightarrow E$ to calculate $Rwd_t$ and $Q_{value}(S_t, A_t)$ using Equation (1):
    $Q_{value}(S_t, A_t) = Rwd(S_t, A_t) + \delta \max_A Q_{value}(S'_t, A_t)$
17) End if
18) End for
19) End for
20) End
```

The algorithm (1) delineates the working scenario of the deep Q-learning-based device authentication based on the communication pattern of individual devices, and the policy administrator module that controls the access criteria a device should follow based on the policy to access the zero-rust security enables IIoT framework. The foremost step is to initialize the values of the devices in the network denoted by $D = \{D_1, D_2, D_3 \ldots\ldots D_x$ and the set of actions A and time t. The zero-trust security network comprises of three modules: the policy engine module, policy administrator module, and policy enforcement area module. The policy administrator is the one who sets policy and provides it to the policy engine

Figure 4
The conceptual framework of DC-FL-based classification of trivial and nontrivial raw data



module to ensure the security of the undertaken infrastructure. The policy administrator here reads the communication pattern of the devices and forms a policy based on that to recognize the unusual behavior of the device. For every device D_i, the state S and agent Ag are activated at a particular time. The communication pattern C_i of the device is viewed by the policy administrator and based on that, an authentication policy is created PA_m. Next, for every recorded communication pattern belonging to a device, the action is performed from the action set, and the cross-verification of communication pattern and policy is made. If communication pattern and policy are matched, the action being calculated results in A_a, and then the action is passed to environment E to calculate and assign reward Rwd_t to the agent. And the device is permitted to access the network. Contrary, if the comparison is not equal, the action value is calculated as A_b, and the device access is denied. Lastly, the Q_{value} is calculated using Equation (1).

4.2. Device data categorization via fuzzy learning (DC-FL)

Fuzzy logic is the learning algorithm that is applied to improve the learning and knowledge of the system based on the decision values that may not lie between only the true and false. The decisive nature of the system is hence enhanced to depict the results that are not bounded between just two values but have different values on the measuring scale. In the proposed methodology, the state of the art is to refine the raw data and categorize it based on the quality it possesses to produce more accurate, compatible, and relevant information. The adopted fuzzy learning approach gives the intermediate results in between that denote fragmentary true and false values for the problem in question rather than that produced by the Boolean system that generates only pure true and pure false values as a solution. The overall fuzzy learning-based system comprises four components, namely, rule base, fuzzification, inference engine, and defuzzification. The conceptual framework of DC-FL-based classification of trivial and nontrivial raw data is represented in Figure 4.

Figure 4 illustrated above explains the functioning of fuzzy logic learning in obtaining the fuzzy sets or fuzzy values in order to categorize the device's raw data as trivial or nontrivial. The IIoT infrastructure with thousands of devices but not devices in the network contains relevant efficient data to generate sensible and decisive information. The proposed paper provided the solution to the aforementioned loophole by enabling fuzzy learning that based on the quality of the data possessed by the individual device, which calculates the fuzzy set. The values are marked on a five-number scale measuring the strongest quality to the weakest quality denoting the crisp values 1 to 5, and the fuzzy values are represented as CS, PS, M, PW, and CW that infer "Complete Strong", "Prevalent Strong", "Moderate", "Prevalent Weak", and "Complete Weak", respectively. The foremost step in fuzzy learning is the initialization of the "rule base" that comprises the protocols and the If-Then statement that commands the decision-making based on the provided criteria. Next, in the input stage, the device data is exposed to a fuzzifier that converts the classical set of numbers into fuzzy set values based on the degree of quality represented by the classical value set. This process of converting the classical value set into the fuzzy set is known as "fuzzification". The fuzzy set generated is exposed to the intermediate stage, that is, the "inference engine", which assigns the corresponding degree of quality based on the present fuzzy set value depending on the rules set by the "rule base". The matching is performed in a way that the classical value set represents the degree {CS, PS, M, PW, CW}. The fuzzy set is mathematically represented as follows in Equation (3):

$$F_{set} = \{\text{CS, PS, M, PW, CW}\} \tag{3}$$

The last stage is "defuzzification", where the fuzzy set values attained by the inference engine are employed to the defuzzifier into the classical value set. The output stage comes with a classification of trivial and nontrivial raw data not only with two-edge degree representing true and false but comes with many shades of gray in between. The proposed DC-FL-based classification facilitates more accurate and relevant information obtained from the best-suited dataset ignoring all the irrelevant and weak datasets. The quality of the data in the proposed paper is based on the accuracy of the raw data a particular device holds. The accuracy of the data is mathematically stated as in Equation (4):

$$Accuracy\ (A) = \frac{T_{positive} + T_{negative}}{T_{positive} + T_{negative} + F_{positive} + F_{negative}} \tag{4}$$

Equation (4) measures the accuracy of the data based on which the quality of the data held by an individual device. The accuracy of data is calculated by adding all the truly positive events and the truly negative events and then dividing the value from the sum obtained by adding truly positive, truly negative, falsely positive, and falsely negative events.

Algorithm 2: Device data categorization via fuzzy learning

Input: Device $D = \{D_1, D_2, D_3 \ldots\ldots D_x\}$, Raw device data = $RD = \{RD_1, RD_2, RD_3 \ldots\ldots\ldots RD_y\}, Rl_{base}$, classical value set Cl_{set}

Output: Robust device raw data classification

```
1) Initialize $Rl_{base}$
2) Begin
3) For every $RD_i \in D$, do
// Perform fuzzification
4) Convert $Cl_{set} = F_{set}$
5) Activate $Cl_{set}$
6) For every $Cl_{set_n} \forall n \in Cl_{set}$, do
7) Formulate fuzzy value set $F_{set}$
8) Calculate the quality of data based on the accuracy using Equation (2):
   $Accuracy\ (A) = \frac{T_{positive} + T_{negative}}{T_{positive} + T_{negative} + F_{positive} + F_{negative}}$
9) Activate $Rl_{base}$ to initiate if-then decision-making
10) If $2 > A \geq 1$,
11) Then, the fuzzy value is {CS}, that is, "Complete Strong"
12) If $1 > A > 0$,
13) Then, the fuzzy value is {PS}, that is, "Prevalent Strong"
14) If $A = 0$,
15) Then, the fuzzy value is {M}, that is, "Moderate"
16) If $0 > A \geq -1$,
17) Then, the fuzzy value is {PW}, that is, "Prevalent Weak"
18) If $-1 > A \geq -2$,
19) Then, the fuzzy value is {CW}, that is, "Complete Weak"
20) End if
// Interface Engine
21) Transfer the fuzzy set to assign the corresponding degree to the values.
// Perform defuzzification
22) Convert $F_{set} = Cl_{set}$
23) End for
24) End for
25) End
```

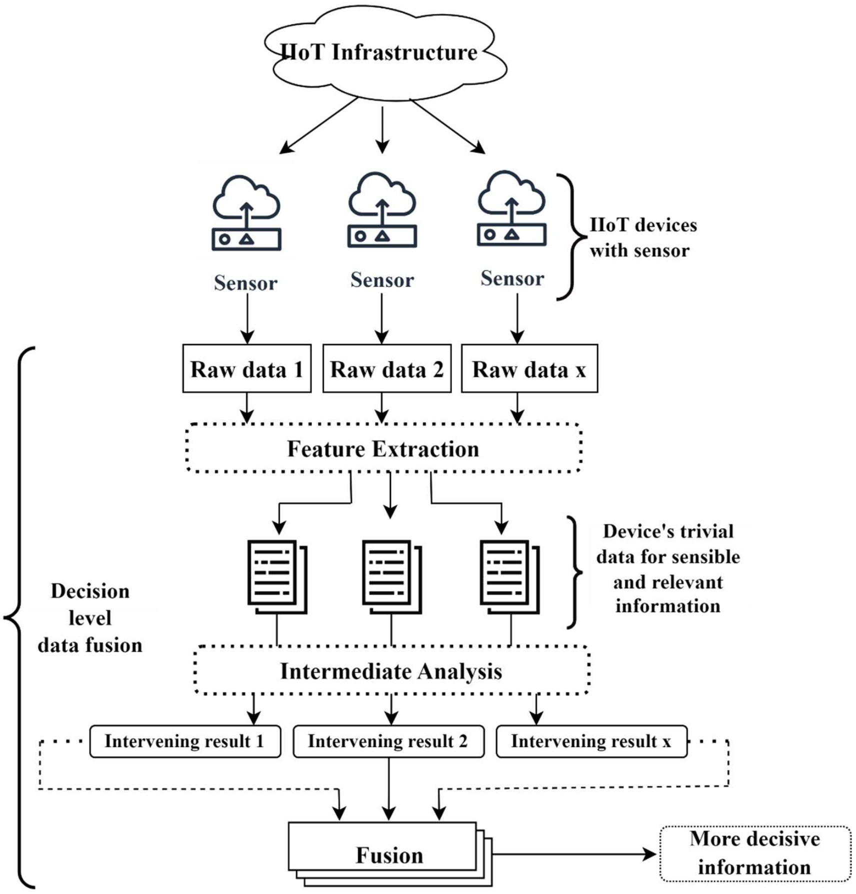
The formulated algorithm (2) delineates the step-by-step working of the DC-FL with the aim of categorizing the raw data based on its accuracy so as to identify the trivial and nontrivial dataset. The accuracy of the device's raw data is calculated, and then it is checked across a set of rules formulated by the rule base module. If the range of accuracy lies between $2 > A \geq 1$, then the strongest quality of data is claimed, and for the lowest or the most nontrivial dataset, the accuracy range should lie between $-1 > A \geq -2$. Employing fuzzy logic facilitates not only the corner values or the Boolean system values as true and false but also determines the degree of the quality considering multiple values in between, thus providing an ambient solution to the efficient and relevant data selection for obtaining sensible and compatible information.

4.3. Multi-sensor-based decision-level data fusion (MS-DLDF) in IIoT over zero-trust security network

The IIoT infrastructure is built around thousands of devices, and the individual device contains a smart sensor that senses and ensures the availability of the desired dataset from the device. Smart sensor plays a pivotal role in fetching the requested dataset from the desired device. Data fusion as delineated above merges the raw data from multiple sources to produce a more meaningful and consistent information obtained from multiple sensors rather than the information inferred from the individual source. In the IIoT framework, by the adopted approach, the data should be gathered from various participating devices to the best of the knowledge. Multi-sensor data fusion is a framework configurated to acquire source data from multiple discrete sources to analyze and generalize the multi-source data. A multi-sensor data fusion model constructs a complicated environment that acquires data from multiple sensors to produce mode-appropriate and decisive information. With multi-sensor data fusion, the information or the results that can't be inferred from a single sensor is accurately achieved. In multi-sensor systems, the examination of positioning, tracking of source data, and identification are performed to fuse data from multiple discrete sources. The classification of the multi-sensor data fusion is based on the data fusion methods, level of abstraction in data fusion, and spatiotemporal vector of data fusion. Data fusion has three levels, namely, observation level, feature level, and decision level. Decision-level data fusion performs intermediate analysis of the dataset extracted and double-checks the quality of data by producing intermediate results before reaching the resultant fusion. The architectural model for MS-DLDF is demonstrated below in Figure 5.

The above-represented Figure 5 delineates the conceptual workflow of the adopted MS-DLDF in IIoT over zero-trust security network. The IIoT devices have an immense of devices, and every individual device contains smart sensors that sense and fetch data required for information generation, and further communication in the network hence is called multi-sensor. Every individual device contains the raw data that are extracted with the aid of sensors. The raw data is then employed for the classification of the trivial and nontrivial dataset via DC-FL-based classification of trivial and nontrivial raw data. After the selection of the relevant raw data, the intermediate data analysis is made on the dataset to produce intermediate results to cross-verify the relevance of the dataset in practice. The workflow produces the result as the fusion of the datasets from the intermediate results, producing more sensible and decisive information. The overall mathematical formulation of MS-DLDF is explained in the following equations via Dempster data fusion

Figure 5
The architecture of multi-sensor-based decision-level data fusion (MS-DLDF) in IIoT over zero-trust security network



algorithm. The foremost is to formulate the set of exclusionary entities stated in Equation (5):

$$E = \ '\Omega = \{\omega_1,\ \omega_2,\ \ldots..\omega_x\} \tag{5}$$

Equation (5) depicts the entire set of events or the device dataset involved in decision-making. E is the entire set of participating devices represented by $'\Omega$ and constitutes of multiple values $\{\omega_1,\ \omega_2,\ \ldots..\omega_x\}$, where x is the number of devices involved. After formulating the set, the next is to obtain a power set of the Dempster combination concept as stated in Equation (6):

$$2^{'\Omega} = \{\varnothing,\ \{\omega_1\},\ \{\omega_2\},\ \ldots\ldots\ \{\omega_1, \omega_x\}\ldots,\ '\Omega \tag{6}$$

The above-illustrated Equation (6) explains the power set, where ∅ denotes the empty set. The set created goes to the limit x, which represents the number of total events and devices involved in the simulation. Here, in the proposed approach, the number of devices in the network, say, three, then $'\Omega\ =\ \{p, q, r\}$. The power set thus formed is $2^{'\Omega}\ =\ 2^3 = \{\varnothing,\ p, q, r,\ \{p, q\},\ \{p, r\},\ \{q, r\}, '\Omega\}$

The values in the set have an equal proportion to that of $'\Omega$ and are represented as $2^{'\Omega}\ =\ 2^x$. The basic probability assignment is a function that usually follows two values as represented in Equation (7):

$$M : 2^{'\Omega} \rightarrow [0, 1] \tag{7}$$

In Equation (7), the mass function is explained as the assigning of a power set with the binary values 0 and 1. The dataset retrieved from the devices' multiple sensors involved in the process of generating information and the conditions of mapping 0 and 1 to mass function are mathematically stated in Equations (8) and (9):

$$M(\varnothing) = 0 \tag{8}$$

$$\sum M(\omega) = 1\ \forall\omega \in 2^{'\Omega} \tag{9}$$

In Equations (8) and (9), M is known as the "Basic Probability Assignment". $'\Omega$ represents the set of number of events or entities. If mass function M > 0, then the belief and plausibility functions are calculated.

After acquiring the dataset, the next is to combine the dataset for the information generation. The combination rule of Dempster data fusion for combining, say, two devices' raw data, is as stated below in Equations (10) and (11):

$$M_{12}(P) = \frac{\sum_{Q\cap R=P}\{M_1(Q).M_2(R)\}}{1-k} \tag{10}$$

when A≠ ∅ *and* $M(\varnothing\ ) = 0$

$$k = \sum_{Q\cap R=\varnothing}\{M_1(Q).M_2(R)\} \tag{11}$$

Equations (10) and (11) demonstrate the combining rule for the two datasets involved in decision-making. "k" represents the degree of collision between the adopted source dataset. The divisor $1-k$ performs as a regularization factor that supports assemblage by entirely disregarding the disputing raw data. The combination rule of Dempster follows commutative and associative law as stated in Equations (12) and (13), respectively:

$$M_1 \oplus M_2 = M_2 \oplus M_1 \tag{12}$$

Equation (12) explains the association between the basic probability assignment values of the devices from which the data is to be retrieved. The symbol ⊕ (addition) used describes the cumulative law of the combination rule of Dempster, which means that the information obtained from the fusion of two distinct sources remains the same when the datasets are swapped or their input sequence is changed. The information obtained from combining M_1 and M_2, likewise, the information acquired when the input sequence of dataset from multiple sensors is changed, say, M_2 and M_1. The results show both the cumulative and associative properties. Next is to calculate the "Trust" to ensure that the device belongs to the generated power set of the involved events. The mathematical statement of the trust value evaluated is shown in Equation (13):

$$T(P) = \sum_{Q \subseteq P} \{M(Q)\} \tag{13}$$

In Equation (13), $T(P)$ evaluates the faith that the device is a participant of the power set of the constituting devices in the network such that $P \subset {}'\Omega$.

Algorithm 3: MS-DLDF in IIoT over zero-trust security network

Input: Devices $D = \{D_1, D_2, D_3 \ldots\ldots\ldots D_x\}$, entire set $'\Omega = \{\omega_1, \omega_2, \ldots\ldots\omega_x\}$

Output: More sensible and decisive information

```
1) Begin
2) For all the incorporating devices, do
3) Formulate an "Entire set (E)" using Equation (5)
       $E = {}'\Omega = \{\omega_1, \omega_2, \ldots\ldots\omega_x\}$
4) For the formulated set $E = {}'\Omega$, do
5) Generate a "power set ($2^{'\Omega}$) using Equation (6)
       $2^{'\Omega} = \{\emptyset, \{\omega_1\}, \{\omega_2\}, \ldots\ldots \{\omega_1, \omega_x\} \ldots, {}'\Omega$
6) Calculate "Basic Probability Assignment" using Equations (6), (7), and (8)
       $M : 2^{'\Omega} \to [0, 1]$
       $M(\emptyset) = 0$
       $\sum M(\omega) \forall \omega \in 2^{'\Omega}$
7) For every device in set $E = {}'\Omega$, do
8) Evaluate the Dempster combination value (suppose for two devices from which the dataset is to be retrieved) using Equation (10):
       $M_{12}(P) = \frac{\sum_{Q \cap R = P} \{M_1(Q) . M_2(R)\}}{1 - k}$
9) For every $M_{x_i x_j}(D_{name})$, do
10) Calculate the "Trust function (T)" using Equation (13)
       $T(D_{name_i}) = \sum_{D_{name_j} \subseteq D_{name_i}} \{M(D_{name_j})\}$
    [where $D_{name_i}$ is the first device and $D_{name_j}$ is the second device from the entire set of participating devices]
11) If $T(D_{name_i}) \to [0, 1]$,
12) Then $D_{name_i} \in {}'\Omega$, hence belief is confirmed and fusion is processed
13) Else, the device is not from the participating set or the participant of the network
14) End if
15) End for
16) End for
17) End for
18) End for
19) End
```

The delineated algorithm (3) explains the step-by-step execution of the Dempster combination rule. The foremost step is to formulate the entire set E, which constitutes of all the participating devices in the IIoT network. Based on the entire set, power set $2^{'\Omega}$ is produced with all the combinations of involved devices. After forming the power set, the mass function (M), also called out as "Basic Probability Assignment", is calculated for the empty set and the values or devices representing the entire set with the surety that all the devices belong to the power set generated. Probability assignment has two conditions depending on which the values 0 and 1 are mapped. For every device that belongs to the entire set, the Dempster combination rule is applied for the selected devices. Say, for two discrete source datasets, the mass function is calculated. The last step is to ensure the faith that the selected device is a member of the entire set from which the dataset is to be extracted and is achieved by calculating the trust function for each participating device. If the trust value calculated lies between the range [0,1], then the device is a member of the network or the set formed, and then only the data fusion is initiated; otherwise, the device is refrained, and the process is to be restarted. By calculating trust value, the security is also ensured by ignoring all the devices that are not a member of the source set or the entire set.

Algorithm 4: MS-DLDF via Dempster combination rule for enhanced data security and information decisiveness

Input: Device $D = \{D_1, D_2, D_3 \ldots\ldots\ldots D_x\}$, raw device data $= RD = \{RD_1, RD_2, RD_3 \ldots\ldots\ldots RD_y\}$, state S, set of actions A, agent Ag, environment E, time t, policy administrator module PA_m, reward Rwd_t, Rl_{base}, classical value set Cl_{set}, entire set $'\Omega = \{\omega_1, \omega_2, \ldots\ldots\omega_x\}$

Output: MS-DLDF for more relevant and consistent information ignoring all nonrelevant dataset

```
1) Assign and initialize the value of x, y, and t, where x = y
2) Initialize the policy administrator module of zero-trust security network
3) Begin
4) For every $S_t$ arriving in time t and $RD_i \in D$, do
5) Activate agent $Ag$ for $S_t$
6) Read the communication pattern of $D_i$ and store in $C_i$
// Matching and decision-making for device authentication via DQL-DA
7) For every $C_i \in D_i$, do
```

```
8) Calculate $A_t$
9) If $C_i = PA_m$
10) Then $A_t = A_a$, authenticity is confirmed and the device is allowed to access the network
11) Transfer $A_t \rightarrow E$ to calculate $Rwd_t$ and $Q_{value}(S_t, A_t)$ using Equation (1):

    $Q_{value}(S_t, A_t) = Rwd\ (S_t, A_t) + \delta \max_A Q_{value}(S'_t, A_t)$

12) End if and go to step 17
13) Else
14) If $C_i \neq PA_m$
15) Then $A_t = A_b$, authenticity is not confirmed, and the device is blocked with denied access
16) Transfer $A_t \rightarrow E$ to calculate $Rwd_t$ and $Q_{value}(S_t, A_t)$ using Equation (1):

    $Q_{value}(S_t, A_t) = Rwd\ (S_t, A_t) + \delta \max_A Q_{value}(S'_t, A_t)$

17) For every $A_t$, do
18) Initialize $Rl_{base}$
19) For every $RD_i \in D$, do
// Perform fuzzification
20) Convert $Cl_{set} = F_{set}$
21) Activate $Cl_{set}$
22) For every $Cl_{set_n} \forall n \in Cl_{set}$, do
23) Formulate fuzzy value set $F_{set}$
24) Calculate quality of data based on the accuracy using Equation (2):

    $Accuracy\ (A) = \frac{T_{positive} + T_{negative}}{T_{positive} + T_{negative} + F_{positive} + F_{negative}}$

25) Activate $Rl_{base}$ to initiate if-then decision-making
26) If $2 > A \geq 1$, then, the fuzzy value is {CS}, that is, "Complete Strong"
27) If $1 > A > 0$, then, the fuzzy value is {PS}, that is, "Prevalent Strong"
28) If $A = 0$, then, the fuzzy value is {M}, that is, "Moderate"
29) If $0 > A \geq -1$, then, the fuzzy value is {PW}, that is, "Prevalent Weak"
30) If $-1 > A \geq -2$, then, the fuzzy value is {CW}, that is, "Complete Weak"
31) End if
// Interface Engine
32) Transfer the fuzzy set to assign the corresponding degree to the values.
// Perform defuzzification
33) Convert $F_{set} = Cl_{set}$
34) For all the incorporating devices, do
35) Formulate an "Entire set (E)" using Equation (5)

    $E = {'}\Omega = \{\omega_1, \omega_2, \ldots .\omega_x\}$

36) For the formulated set $E = {'}\Omega$, do
37) Generate a "power set ($2^{\Omega}$)" using Equation (6)

    $2^{'\Omega} = \{\varnothing, \{\omega_1\}, \{\omega_2\}, \ldots\ldots \{\omega_1, \omega_x\} \ldots, {'}\Omega$

38) Calculate "Basic Probability Assignment" using Equations (7) and (8)

    $M(\varnothing) = 0$

    $\sum M(\omega) \forall \omega \in 2^{'\Omega}$

39) For every device in set $E = {'}\Omega$, do
40) Evaluate the Dempster combination value (suppose for two devices from which the dataset is to be retrieved) using Equation (9), and calculate the "Trust function (T)" using Equation (10):

    $M_{12}(P) = \frac{\sum_{Q \cap R = P} \{M_1(Q) . M_2(R)\}}{1 - k}$

    $T\left(D_{name_i}\right) = \sum_{D_{name_j} \subseteq D_{name_i}} \left\{M\left(D_{name_j}\right)\right\}$

    [where $D_{name_i}$ is the first device and $D_{name_j}$ is the second device from the entire set of participating devices]

41) If $T\left(D_{name_i}\right) \rightarrow [0, 1]$,
42) Then $D_{name_i} \in {'}\Omega$, hence belief is confirmed, and fusion is processed
43) Else, the device is not from the participating set or the participant of the network
44) End if
45) End for
46) End for
47) End for
48) End for
49) End for
50) End for
51) End for
52) End
```

5. Experimentation, Results, and Analysis

5.1. Experimental setup

The experimentation of the proposed approach is delineated in this section on the parameter information consistency and overall precision of MS-DLDF as compared to SSDF. The performance evaluation is performed as the comparative analysis of the MS-DLDF via Dempster combination rule with zero-trust security in IIoT network with the single sensor inferred knowledge. The datasets involved in the simulation are evaluated using the python programming using IoTSim-Edge Simulator. The dataset involved in the experiments is from IIoT_data of 59.06 MB in CSV format having 405,184 records. The other dataset under consideration is the X-IIoTID dataset of 106.71 MB containing 820,835 records. The comparative analysis is performed on the parameters such as accuracy of information, resource utilization, and power consumption.

5.2. Result analysis

The underlying section of the paper delineates the results obtained from the experiments on the proposed MS-DLDF and the existing SSDF. The performance evaluation and result analysis are made on the following parameters:

1) Accuracy rate
2) Computation time
3) Precision
4) False positive rate
5) Data confidentiality rate

The tabular and graphical comparative analysis of the performance of MS-DLDF and existing SSDF is illustrated below.

5.2.1. Accuracy rate $(\boldsymbol{Acc_R})$

Accuracy is referred to as the quality of the information produced by the most relevant dataset with trivial raw data. The performance analysis of the accuracy of information produced by the proposed MS-DLDF and the existing SSDF is evaluated and compared using the mathematical statement given below in Equation (14):

$$Acc_R = \frac{T^{pt} + T^{nt}}{T^{pt} + T^{nt} + F^{pt} + F^{nt}} * 100 \tag{14}$$

In Equation (14), the accuracy rate (Acc_R) is measured as the ratio of all the truly positive events and all the events that are purely negative to the summation of all true positive, true negative, falsely positive, and falsely negative events. The table below represents the comparative analysis of the accuracy offered by the proposed MS-DLDF and the existing SSDF and BEDF.

Table 1 and Figure 6 above explain the comparison of the existing single-source or single sensor data fusion and BEDF to the proposed MS-DLDF. The samples involved in simulation ranges from 10,000 to 100,000. The x-axis denotes the samples, and the y-axis represents the accuracy rate in %. The proposed MS-DLDF approach achieves the highest accuracy when compared to the peer approaches SSDF [1] and BEDF [2]. The accuracy achieved by the adopted MS-DLDF is enhanced by 7% and 4% as compared to the existing SSDF and BEDF, respectively.

Table 1
Comparison results of accuracy rate

Sample	SSDF [1]	Bayesian estimation data fusion (BEDF) [2]	MS-DLDF (proposed)
10,000	90.68	90.99	91.68
20,000	89.78	91	92.78
30,000	86.89	88.78	92.89
40,000	83.77	87.66	93.77
50,000	84.89	89.12	94.89
60,000	85.4	90.56	95.49
70,000	86.01	92	96.01
80,000	92.32	93.43	95
90,000	90.12	91.71	94.12
100,000	92.88	93	93.88

5.2.2. Computation time

The next parameter under consideration is the time of information generation from the adopted MS-DLDF and the existing SSDF [1] and BEDF [2]. Computation time is referred to as the time taken by the network to generate a relevant information from the associated dataset. The computation time is mathematical stated as in Equation (15):

$$C_T = N * \left[RD_i^T\right] \tag{15}$$

The above-stated Equation (15) demonstrates the evaluation of the computational time C_T by computing the product of number of devices involved in the fusion process N to the individual time taken by the raw data of the associated device RD_i^T. Table 2 and Figure 7 below represent the comparison of the computation time taken by the existing two approaches SSDF [1] and BEDF [2] and the proposed MS-DLDF.

Figure 6
Sample devices versus accuracy rate

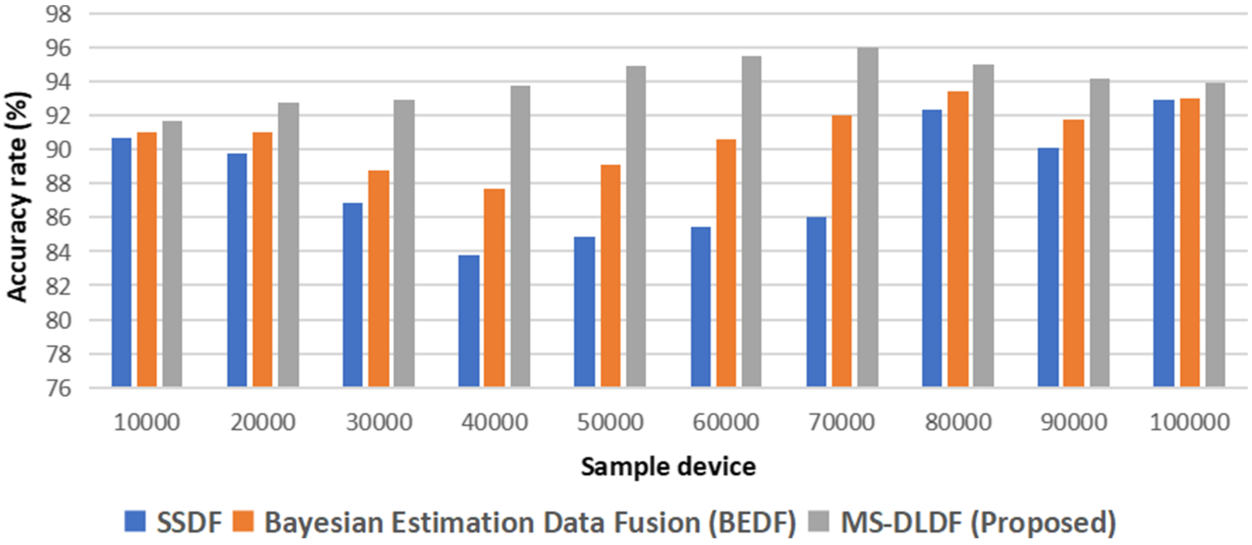


Figure 7
Sample devices vs computation time

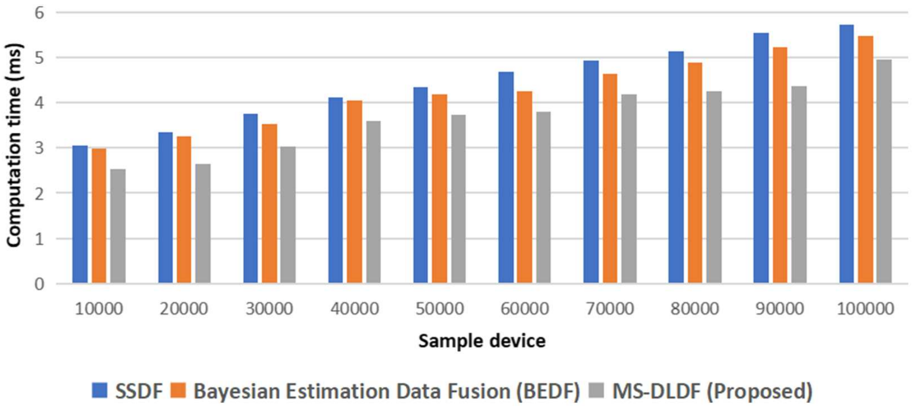


Table 2
Comparison results of computation time

Sample	SSDF [1]	Bayesian estimation data fusion (BEDF) [2]	MS-DLDF (proposed)
10,000	3.05	2.98	2.53
20,000	3.34	3.26	2.65
30,000	3.76	3.52	3.02
40,000	4.12	4.04	3.59
50,000	4.34	4.18	3.73
60,000	4.67	4.24	3.79
70,000	4.92	4.63	4.18
80,000	5.12	4.89	4.24
90,000	5.54	5.22	4.37
100,000	5.72	5.48	4.96

Table 3
Comparison results of precision

Sample	SSDF [1]	Bayesian estimation data fusion (BEDF) [2]	MS-DLDF (proposed)
10,000	92.71	94.44	95.27
20,000	91.81	94.45	96.37
30,000	88.92	92.23	96.48
40,000	85.8	91.11	97.36
50,000	86.92	92.57	98.48
60,000	87.43	94.01	99.08
70,000	88.04	95.45	99.6
80,000	94.35	96.88	98.59
90,000	92.15	95.16	97.71
100,000	94.91	96.45	97.47

Table 2 and Figure 7 above demonstrate the comparative analysis of the computation time on the sample with 10,000 to 100,000 devices for simulation. The x-axis of the graph represents the sample involved in the simulation, and the y-axis denotes the responses of the computational time in ms. From the simulation results, the proposed approach MS-DLDF has comparatively reduced computational time as compared to the peer approaches SSDF [1] and BEDF [2]. The MS-DLDF noted better computational time by 17% and 13%, respectively.

5.2.3. Precision

The precision is another parameter under consideration that is referred to as an attribute that concisely determines how much the assumed trivial datasets are actually trivial in making the information more decisive and relevant. The precision is mathematically stated as in Equation (16):

$$Pr = \frac{T^{pt}}{T^{pt} + F^{nt}} \tag{16}$$

Equation (16) above explains the calculation of the precision for the proposed MS-DLDF and existing SSDF [1] and BEDF [2]. The precision Pr is measured as the ratio of all the true positive events to the sum of the true positive and the false negative events in the simulation process. Table 3 and Figure 8 below demonstrate the comparative analysis of MS-DLDF, SSDF [1], and BEDF [2], respectively.

In the above-mentioned Table 3 and Figure 8, the precision rate for the proposed approach and the existing data fusion techniques are evaluated. In the graph, the x-axis represents the sample ranging from 10,000 to 100,000 used for simulation, and the y-axis demonstrates the results of the precision rate. The simulation results marked the effective and increased precision rate of the adopted MS-DLDF as compared to existing SSDF [1] and BEDF [2]. Moreover, the performance outcome of the MS-DLDF has enhanced precision rate by 8% and 4% as compared to SSDF [1] and BEDF [2], respectively.

5.2.4. False positive rate (FP_{rate})

The false positive rate is measured as the ratio of false entities or the malicious devices that are identified as the true entities or the authentic devices (true devices) to the total number of actual malicious devices. The mathematical statement for the false positive rate is given in Equation (17):

$$FP_{rate} = \frac{F_{positive}}{F_{positive} + T_{negative}} \tag{17}$$

In Equation (17), the false positive rate FP_{rate} is evaluated by taking the proportion of the malicious devices that are treated as the normal or authorized devices $F_{positive}$ to the total number of the actual devices that are infected or anomalous $T_{negative}$. The comparative

Figure 8
Sample devices versus precision

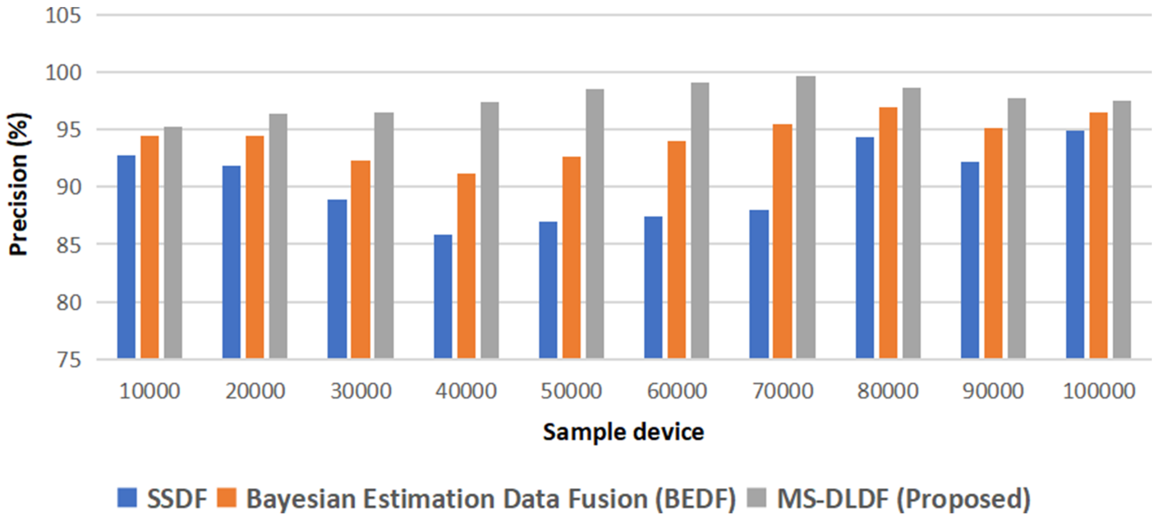


Table 4
Comparison results of false positive rate

Sample	SSDF [1]	Bayesian estimation data fusion (BEDF) [2]	MS-DLDF (proposed)
10,000	4.31	2.5	3.12
20,000	3.91	3.49	2.72
30,000	3.4	2.98	2.21
40,000	3.08	2.66	1.89
50,000	2.83	2.41	1.64
60,000	2.55	2.13	1.36
70,000	2.44	2.02	1.25
80,000	1.73	1.31	1.23
90,000	1.64	1.22	1.09
100,000	1.56	1.14	0.99

analysis of the FP_{rate} possessed by the proposed MS-DLDF and existing SSDF and BEDF is illustrated in Table 4 and Figure 9.

In Table 4 and Figure 9, the comparison is demonstrated in the context of a false positive rate between the proposed method and the existing two methods, SSDF [1] and BEDF [2], respectively. The x-axis of the graph represents the sample range involved in simulation from 1000 to 100,000 and the y-axis refers to the false positive rate of the three methods. As a result, the proposed MS-DLDF offers reduced false positive rates as compared to the peer SSDF [1] by 36% and BEDF [2] by 25%, respectively**.**

5.2.5. Data confidentiality rate $\boldsymbol{DC_{rate}}$

Data confidentiality refers to the privacy of the data; that is, the receptor receives the same data that is sent by the sender. The data confidentiality rate (DC_{rate}) is obtained as the amount of data received by the valid receiver in the network. The data confidentiality rate is mathematically stated in Equation (18):

$$DC_{rate} = \sum_{i=1}^{x} \frac{D_{id}}{D_i} \tag{18}$$

The data confidentiality rate DC_{rate} is calculated using Equation (18) as the proportion of data received by the valid receptor D_{id} to the total number of devices involved in simulation D_i. Data confidentiality rate is obtained in percentage. The comparison in performance of data confidentiality rate is delineated in Table 5 and Figure 10.

In Table 5 and Figure 10, the performance analysis of the data confidentiality rate possessed by the three undertaken approaches is evaluated and compared. The simulation involves devices rang-

Figure 9
Sample devices versus false positive rate

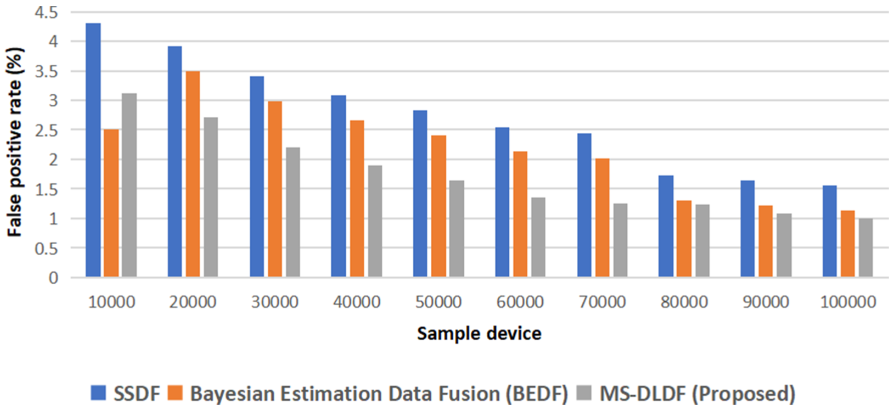


Figure 10
Sample devices versus data confidentiality rate

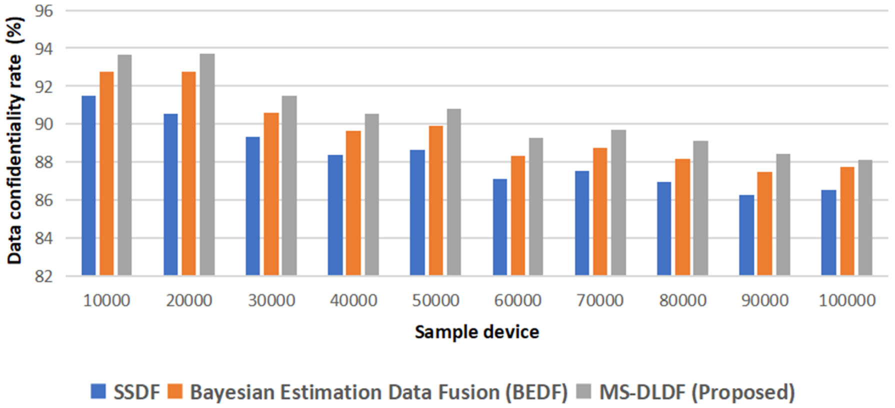


Table 5
Comparison results of data confidentiality rate

Sample	SSDF [1]	Bayesian estimation data fusion (BEDF) [2]	MS-DLDF (proposed)
10,000	91.51	92.74	93.68
20,000	90.53	92.76	93.7
30,000	89.34	90.57	91.51
40,000	88.39	89.62	90.56
50,000	88.66	89.89	90.83
60,000	87.09	88.32	89.26
70,000	87.54	88.77	89.71
80,000	86.96	88.19	89.13
90,000	86.26	87.49	88.43
100,000	86.53	87.76	88.09

ing from 10,000 to 100,000, with the x-axis representing the simulation devices and the y-axis denoting the data confidentiality rate in percentage. The analysis depicts that the proposed MS-DLDF has amplified data confidentiality rate as compared to existing approaches SSDF [1] and BEDF [2] by 3% and 1%, respectively.

The proposed novel approach, MS-DLDF, provides more decisive and consistent information when compared to the peer approaches, SSDF [1] and BEDF [2], respectively. MS-DLDF outperforms the existing approaches on the accuracy rate by 7% and 4% as compared to existing SSDF and BEDF, respectively, computation time by 17% and 13%, precision by 8% and 4%, false positive rate by 36% and 25%, and the data confidentiality rate by 3% and 1%, respectively.

6. Conclusion and Future Scope

Data fusion techniques have gained much popularity but are widely used in multisensory environments to combine and accommodate datasets or inputs from various sources. IIoT environment builds on devices and integrates different devices to function together. The information inferred by the multi-sensor data fusion is more decisive and relevant as compared to the single-source data fusion. The proposed approach implements the Dempster combination rule, and the comparative analysis is made by the peer approaches, SSDF [1] and Bayesian estimation [2], in terms of accuracy with the increased number of devices and sensors in the more complex network. The proposed methodology ensures the classification of the trivial and nontrivial data as well, while also enabling deep reinforcement learning for more optimal decision-making based on the fuzzy values evaluated. The objective of the paper is to effectively fetch the sensor data and to produce more consistent and sensible data. In the proposed paper, the parametric-based data fusion is compared to analyze the accuracy in terms of an increased number of multi-sensors in a complicated network. The proposed approach will be witnessed as a sound data fusion on multiple sensors irrespective of the domain with the increase in the more complicated networks comprising of huge number of devices and raw data with increment in the accuracy rate by 6%, reduced computation time by 15%, and enhanced precision rate by 6%, respectively, as compared to SSDF [1] and BEDF [2] to produce the most relevant, accurate, and sensible information as compared to the information inferred by the single-source data fusion. With the shifting paradigm of industries, businesses, education, etc., to the digital platform, the fetching, fusing, and facilitating of information are becoming more considerable. Therefore, the proposed MS-DLDF provides more consistent and appropriate information in any complicated network and environment in practice with assured data security. Nevertheless, of the contributions offered by the proposed approach, the limitations of the underlying method are when the source evidence data or the belief function possesses incomplete chunks of information. Moreover, the computational complexity of the Dempster combination rule in complicated environments needs to be addressed.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

The IIoT_data that support the findings of this study are openly available at https://data.world/gymprathap/iiot-data. The X-IIoTID datasets that support the findings of this study are openly available at https://data.world/muna-al-hawawreh/

industrial-internet-of-things-intrusion-dataset/workspace/file?filename=X-IIoTID-dataset-new.zip.

Author Contribution Statement

Anamika Singh: Methodology, Software, Writing – original draft, Visualization. **Rajesh Kumar Dhanaraj:** Conceptualization, Software, Formal analysis, Supervision**. Anupam Kumar Sharma:** Validation, Writing – review & editing.

References

[1] El Gourari, A., Raoufi, M., Skouri, M., & Ouatik, F. (2021). The implementation of deep reinforcement learning in e-learning and distance learning: Remote practical work. *Mobile Information Systems, 2021*(1), 9959954. https://doi.org/10.1155/2021/9959954

[2] Alfrhan, A., Moulahi, T., & Alabdulatif, A. (2021). Comparative study on hash functions for lightweight blockchain in Internet of Things (IoT). *Blockchain: Research and Applications, 2*(4), 100036. https://doi.org/10.1016/j.bcra.2021.100036

[3] Tevera-Ruiz, A., Garcia-Rodriguez, R., Parra-Vega, V., & Ramos-Velasco, L. E. (2023). Q-learning with the variable box method: A case study to land a solid rocket. *Machines, 11*(2), 214. https://doi.org/10.3390/machines11020214

[4] Baratloo, A., Hosseini, M., Negida, A., & El Ashal, G. (2015). Part 1: Simple definition and calculation of accuracy, sensitivity and specificity. *Archives of Academic Emergency Medicine (Emergency), 3*(2), 48–49.

[5] Khan, M. N., & Anwar, S. (2019). Paradox elimination in Dempster–Shafer combination rule with novel entropy function: Application in decision-level multi-sensor fusion. *Sensors, 19*(21), 4810. https://doi.org/10.3390/s19214810

[6] Tang, Y., Zhou, Y., Ren, X., Sun, Y., Huang, Y., & Zhou, D. (2023). A new basic probability assignment generation and combination method for conflict data fusion in the evidence theory. *Scientific Reports, 13*(1), 8443. https://doi.org/10.1038/s41598-023-35195-4

[7] Tsanousa, A., Bektsis, E., Kyriakopoulos, C., González, A. G., Leturiondo, U., Gialampoukidis, I., ..., & Kompatsiaris, I. (2022). A review of multisensor data fusion solutions in smart manufacturing: Systems and trends. *Sensors, 22*(5), 1734. https://doi.org/10.3390/s22051734

[8] Jang, B., Kim, M., Harerimana, G., & Kim, J. W. (2019). Q-learning algorithms: A comprehensive classification and applications. *IEEE Access, 7*, 133653–133667. https://doi.org/10.1109/ACCESS.2019.2941229

[9] Castanedo, F. (2013). A review of data fusion techniques. *The Scientific World Journal, 2013*(1), 704504. https://doi.org/10.1155/2013/704504

[10] Chatzichristos, C., van Eyndhoven, S., Kofidis, E., & van Huffel, S. (2022). Coupled tensor decompositions for data fusion. In Y. Liu (Ed.), *Tensors for data processing* (pp. 341–370). Academic Press. https://doi.org/10.1016/B978-0-12-824447-0.00016-9

[11] Fawzy, D., Moussa, S. M., & Badr, N. L. (2023). An IoT-based resource utilization framework using data fusion for smart environments. *Internet of Things, 21*, 100645. https://doi.org/10.1016/j.iot.2022.100645

[12] Meng, F., Li, A., & Liu, Z. (2022). An evidence theory and data fusion-based classification method for decision making. *Procedia Computer Science, 199*, 892–899. https://doi.org/10.1016/j.procs.2022.01.112

[13] Chen, G., Liu, Z., Yu, G., & Liang, J. (2021). A new view of multisensor data fusion: Research on generalized fusion. *Mathematical Problems in Engineering, 2021*(1), 5471242. https://doi.org/10.1155/2021/5471242

[14] Gagolewski, M. (2022). Data fusion: Theory, methods, and applications. *arXiv Preprint:2208.01644*. https://doi.org/10.48550/arXiv.2208.01644

[15] Azam, K. S. F., Ryabchykov, O., & Bocklitz, T. (2022). A review on data fusion of multidimensional medical and biomedical data. *Molecules, 27*(21), 7448. https://doi.org/10.3390/molecules27217448

[16] Kumar, K. K., Ramaraj, E., & Indira, D. N. V. S. L. S. (2021). Data fusion method and Internet of Things (IoT) for smart city application. In *Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks,* 284–289. https://doi.org/10.1109/ICICV50876.2021.9388532

[17] Kong, L., Peng, X., Chen, Y., Wang, P., & Xu, M. (2020). Multi-sensor measurement and data fusion technology for manufacturing process monitoring: A literature review. *International Journal of Extreme Manufacturing, 2*(2), 022001. https://doi.org/10.1088/2631-7990/ab7ae6

[18] Kessler, L., Rempe, F., & Bogenberger, K. (2021). Multi-sensor data fusion for accurate traffic speed and travel time reconstruction. *Frontiers in Future Transportation, 2*, 766951. https://doi.org/10.3389/ffutr.2021.766951

[19] Al-Hamadani, M. N., Fadhel, M. A., Alzubaidi, L., & Harangi, B. (2024). Reinforcement learning algorithms and applications in healthcare and robotics: A comprehensive and systematic review. *Sensors, 24*(8), 2461. https://doi.org/10.3390/s24082461

[20] Zhou, Q., Lian, Y., Wu, J., Zhu, M., Wang, H., & Cao, J. (2024). An optimized Q-Learning algorithm for mobile robot local path planning. *Knowledge-Based Systems, 286*, 111400. https://doi.org/10.1016/j.knosys.2024.111400

[21] Hamda, N. E. I., Lagha, M., & Hadjali, A. (2022). Mathematical methods for data fusion in IOT: A survey. In *Advanced Intelligent Systems for Sustainable Development (AI2SD'2020), 2*, 1084–1101. https://doi.org/10.1007/978-3-030-90639-9_88

[22] El Faouzi, N. E., & Klein, L. A. (2016). Data fusion for ITS: Techniques and research needs. *Transportation Research Procedia, 15*, 495–512. https://doi.org/10.1016/j.trpro.2016.06.042

[23] Qi, J., Yang, P., Newcombe, L., Peng, X., Yang, Y., & Zhao, Z. (2020). An overview of data fusion techniques for internet of things enabled physical activity recognition and measure. *Information Fusion, 55*, 269–280. https://doi.org/10.1016/j.inffus.2019.09.002

[24] Lee, S. K., Hong, S. H., Jun, W. H., & Hong, Y. S. (2022). Multi-sensor data fusion with a reconfigurable module and its application to unmanned storage boxes. *Sensors, 22*(14), 5388. https://doi.org/10.3390/s22145388

[25] Logananthara, R., Palm, G., & Ali, M. (2003). Intelligent problem solving. Methodologies and approaches. In *13th International Conference on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems.* 19–22.

[26] Ding, W., Jing, X., Yan, Z., & Yang, L. T. (2019). A survey on data fusion in internet of things: Towards secure and privacy-preserving fusion. *Information Fusion, 51*, 129–144. https://doi.org/10.1016/j.inffus.2018.12.001

[27] Chango, W., Lara, J. A., Cerezo, R., & Romero, C. (2022). A review on data fusion in multimodal learning analytics and educational data mining. *WIREs: Data Mining and Knowledge Discovery, 12*(4), e1458. https://doi.org/10.1002/widm.1458

[28] Qin, X., & Gu, Y. (2011). Data fusion in the Internet of Things. *Procedia Engineering, 15*, 3023–3026. https://doi.org/10.1016/j.proeng.2011.08.567

[29] Huang, X., Liu, Y., Huang, L., Onstein, E., & Merschbrock, C. (2023). BIM and IoT data fusion: The data process model perspective. *Automation in Construction, 149*, 104792. https://doi.org/10.1016/j.autcon.2023.104792

[30] Yue, Y., Li, S., Legg, P., & Li, F. (2021). Deep learning-based security behaviour analysis in IoT environments: A survey. *Security and Communication Networks, 2021*(1), 8873195. https://doi.org/10.1155/2021/8873195

[31] He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A survey on zero trust architecture: Challenges and future trends. *Wireless Communications and Mobile Computing, 2022*(1), 6476274. https://doi.org/10.1155/2022/6476274

[32] Tong, Y., Bai, J., & Chen, X. (2020). Research on multi-sensor data fusion technology. *Journal of Physics: Conference Series, 1624*, 032046. https://doi.org/10.1088/1742-6596/1624/3/032046

[33] Guo, Y., Fang, X., Dong, Z., & Mi, H. (2021). Research on multi-sensor information fusion and intelligent optimization algorithm and related topics of mobile robots. *EURASIP Journal on Advances in Signal Processing, 2021*(1), 111. https://doi.org/10.1186/s13634-021-00817-4

[34] Gao, P., Yan, L., Chen, Z., Wei, X., Guo, L., & Shi, R. (2021). Research on zero-trust based network security protection for power internet of things. In *IEEE 4th International Conference on Automation, Electronics and Electrical Engineering,* 458–461. https://doi.org/10.1109/AUTEEE52864.2021.9668726

[35] Sarkar, S., Choudhary, G., Shandilya, S. K., Hussain, A., & Kim, H. (2022). Security of zero trust networks in cloud computing: A comparative review. *Sustainability, 14*(18), 11213. https://doi.org/10.3390/su141811213

[36] Peres, R. S., Jia, X., Lee, J., Sun, K., Colombo, A. W., & Barata, J. (2020). Industrial artificial intelligence in industry 4.0 – Systematic review, challenges and outlook. *IEEE Access, 8*, 220121–220139. https://doi.org/10.1109/ACCESS.2020.3042874

[37] Sharma, R., & Villányi, B. (2022). Evaluation of corporate requirements for smart manufacturing systems using predictive analytics. *Internet of Things, 19*, 100554. https://doi.org/10.1016/j.iot.2022.100554

[38] Singh, H. (2021). Big data, industry 4.0 and cyber-physical systems integration: A smart industry context. *Materials Today: Proceedings, 46*, 157–162. https://doi.org/10.1016/j.matpr.2020.07.170

[39] Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., ..., & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *IEEE Access, 6*, 35365–35381. https://doi.org/10.1109/ACCESS.2018.2836950

[40] Sharma, N., Sharma, R., & Jindal, N. (2021). Machine learning and deep learning applications – A vision. *Global Transitions Proceedings, 2*(1), 24–28. https://doi.org/10.1016/j.gltp.2021.01.004

[41] Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security, 110*, 102436. https://doi.org/10.1016/j.cose.2021.102436

[42] Wang, B., Hua, Q., Zhang, H., Tan, X., Nan, Y., Chen, R., & Shu, X. (2022). Research on anomaly detection and real-time reliability evaluation with the log of cloud platform. *Alexandria Engineering Journal, 61*(9), 7183–7193. https://doi.org/10.1016/j.aej.2021.12.061

[43] Pang, G., Shen, C., Cao, L., & Hengel, A. V. D. (2021). Deep learning for anomaly detection: A review. *ACM Computing Surveys, 54*(2), 38. https://doi.org/10.1145/3439950

[44] AlDahoul, N., Abdul Karim, H., & Ba Wazir, A. S. (2021). Model fusion of deep neural networks for anomaly detection. *Journal of Big Data, 8*(1), 106. https://doi.org/10.1186/s40537-021-00496-w

[45] Hu, X., Xie, C., Fan, Z., Duan, Q., Zhang, D., Jiang, L., ..., & Chanussot, J. (2022). Hyperspectral anomaly detection using deep learning: A review. *Remote Sensing, 14*(9), 1973. https://doi.org/10.3390/rs14091973

[46] Elbaghazaoui, B. E., Amnai, M., & Fakhri, Y. (2022). Data profiling and machine learning to identify influencers from social media platforms. *Journal of ICT Standardization, 10*(2), 201–218. https://doi.org/10.13052/jicts2245-800X.1026

[47] Safi, M., Kaur, B., Dadkhah, S., Shoeleh, F., Lashkari, A. H., Molyneaux, H., & Ghorbani, A. A. (2021). Behavioural monitoring and security profiling in the Internet of Things (IoT). In *IEEE 23rd International Conference on High Performance Computing & Communications; 7th International Conference on Data Science & Systems; 19th International Conference on Smart City; 7th International Conference on Dependability in Sensor, Cloud & Big Data Systems & Application (HPC-C/DSS/SmartCity/DependSys),* 1203–1210. https://doi.org/10.1109/HPCC-DSS-SmartCity-DependSys53884.2021.00185

[48] Tayyaba, S., Ashraf, M. W., Alquthami, T., Ahmad, Z., & Manzoor, S. (2020). Fuzzy-based approach using IoT devices for smart home to assist blind people for navigation. *Sensors, 20*(13), 3674. https://doi.org/10.3390/s20133674

[49] Hosney, E. S., Halim, I. T. A., & Yousef, A. H. (2022). An artificial intelligence approach for deploying zero trust architecture (ZTA). In *5th International Conference on Computing and Informatics,* 343–350. https://doi.org/10.1109/ICCI54321.2022.9756117

[50] Sun, F., Wang, X., & Zhang, R. (2021). Improved Q-learning algorithm based on approximate state matching in agricultural plant protection environment. *Entropy, 23*(6), 737. https://doi.org/10.3390/e23060737

[51] Ramezanpour, K., & Jagannath, J. (2022). Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN. *Computer Networks, 217*, 109358. https://doi.org/10.1016/j.comnet.2022.109358

[52] Saffar, I., Morel, M. L. A., Singh, K. D., & Viho, C. (2019). Deep learning based speed profiling for mobile users in 5G cellular networks. In *IEEE Global Communications Conference,* 1–7. https://doi.org/10.1109/GLOBECOM38437.2019.9013508

How to Cite: Singh, A., Dhanaraj, R. K., & Sharma, A. K. (2024). Dempster Combination Rule-Aided Multi-Sensor Decision-Level-Based Data Fusion in Industrial Internet of Things (IIoT) over Zero-Trust Security. *Journal of Computational and Cognitive Engineering*. https://doi.org/10.47852/bonviewJCCE42023198