Neutrosophic-based machine learning context for the trustworthiness of devices in the internet of things

Abdullah Ali Salamai
Department of Management, Applied College, JazanUniversity, Jazan, Kingdom of Saudi Arabia
Email: abSalamai@jazanu.edu.sa

Abstract

The industrial sector is among the most suited sectors that may considerably advantage from the implementation of the ideas and technology of the Industrial Internet of Things (IIoT), and it is one of the most competitive industries in the world. The increased use of automated processes in manufacturing sectors results in a wide variety of applications based on IIoT. These applications call for the efficient integration of a wide variety of different systems and the execution of smooth operations across all machines. The issue of integration and smooth operation presents IIoT as a new subject of study in smart manufacturing. This carries with it several problems, including those on security, accountability, confidence, and dependability. As part of the Industrial Internet of Things (IIoT), many devices will be linked to one another and interact with one another through wireless and internet infrastructure. When this kind of situation plays out, the reliability of the IIoT devices becomes a key component in the process of preventing injection by hostile machines. As a result, an intelligent computer model is required to effectively cluster and categorize the level of trustworthiness possessed by the IIoT devices. In this article, we describe a trust model for the Internet of Things (IIoT) that is based on the neutrosophic TOPSIS and is utilized by IIoT apps to determine the trust score of IIoT devices. The reliability of devices is evaluated by the model that was constructed using the historical knowledge, chronological knowledge, and network behavior information that is received from IIoT devices. In addition to that, the model suggests KNN, and a Decision tree to categorize the attributes that were collected.

Keywords: Machine Learning; Neutrosophic Sets; IoT; IIoT; Smart manufacturing

1. Introduction

Integration of advanced computer technology into many business sectors is taking place with the purpose of achieving better levels of efficiency and capability. The Internet of Things (IoT), which supports a future of linked gadgets that may connect and interact with one other for automated purposes, is one example of a tech that has been extensively embraced in recent years and is continuing to do so. The Internet of Things (IoT) is becoming an increasingly industry-wide phrase, which has resulted in the development of specialized services in this field that place a greater emphasis on precision and effectiveness. One example of a deployment of the Internet of Things that are more narrowly focused is the Industrial Internet of Things (IIoT). The Industrial Internet of Things (IIoT) is an implementation of the Internet of Things (IoT) that is used in industrial settings. In this kind of IoT deployment, a large number of pieces of hardware and software are linked to a network by using a wide variety of software and hardware tools. In spite of these numerous advantages, the primary goal of Industry-standard 5.0 is still to make various industries safer, more intelligent, and more sophisticated[1]–[3]. In the context of Industry 5.0, the fundamental idea behind smart manufacturing is to construct a robust intelligent network structure across the entirety of the supply chain. This is accomplished by providing connections among diverse manufacturing units, like manufacturing, storage facilities, construction machinery, facility centers, and delivery networks. In other words, the

goal is to digitize the entire supply chain[4], [5]. The names "Industry 5.0 norm," "industrial IoT," and "smart factory" are not interchangeable; rather, the following is an explanation of how these distinct but related areas of research are organized:

Industry 5.0: The construction of steam power was the primary emphasis of Industry 1.0, while the introduction of mass manufacturing in the 1870s was the primary focus of Business 2.0. Industry 5.0: The year 1970 marked the beginning of the age of digital electronic equipment, which is when Industry 3.0 emerged. The concept of computerizing industrial sectors may be traced back to the German government, which dubbed the initiative "industry 4.0." The term "4.0" alludes to the fourth technological revolution, which focuses on integrating artificial intelligence into manufacturing equipment. In the fourth industrial revolution, known as Industry 4.0, malware systems (CPS) like the Internet of Things, configuration management, cloud services, and other innovations are incorporated into the production processes. The term "Industry 4.0" refers to the industry's complete digital transition, whereas "Industry 5.0" is predicated on mass personalization, cognitive processing systems, and other similar concepts. Both Industry 4.0 and Industry 5.0 have been proposed by separate organizations, but they share many of the same guiding principles, methodologies, and technological advancements. The human-centricity, sustainability, and resilience of businesses are the three pillars on which Industry 5.0 is built. An increased level of individualization is one of the factors that will be considered by Industry 5.0. The transition from Industry 4.0 to Business world 5.0 paves the way for the development of senior positions and relieves product managers of the responsibility of producing their designs[6], [7].

The Industrial Internet of Things (IIoT) is a subset of the Internet of Things that is designed specifically for use in commercial settings, such as those found in manufacturing, energy, transportation, and agriculture. The Industrial Internet of Things (IIoT) is a term that refers to intelligent sensors, machine connections, and industrial automation that are utilized to enhance the productivity and dependability of industrial operations. The term "IIoT" refers to the M2M devices that are integrated into various industrial control systems and automation systems[8].

Absent options that are trustworthy and secure, the IIoT will never realize its full potential. The implications of safety breaches may be severe, particularly when working with actuators that have the potential to inflict physical harm on their targets. Applications of the Internet of Things that are not mission-critical often make advantage of the trust mechanism. When first developed, the mechanisms of trust and reputation were used in huge systems to facilitate communications between many corporate organizations. Following that, both trust and notoriety have been implemented into applications related to information technology and online commerce. In addition, if the power to handle data is restricted, different forms of trust must be used. Because of all of these aspects, trust emerges as a potentially useful option for enhancing and bolstering the safety of IoT networks[9].

The following are some of the contributions that this work has made:

I. To begin, we have presented the trust measures for the spatial knowledge (SK), the temporal experience (TE), and the behavior pattern (BP) based on a large number of trust attributes in order to reflect the qualities and events that are associated with the IIoT device.

II. As a second step, we have suggested the neutrosophic TOPSIS for the applications of the Internet of Things (IIoT) determine the trust score of the IIoT devices.

III. In addition, we have developed a neutrosophic decision tree and KNN to categorize the extracted features to build the final trust score, which can then be used for further decision-making.

2. Internet of Things

The phrase "Internet of Things" refers to a collection of "things" that have been outfitted with programming, computers, actuators, and detectors, and have been connected to the internet so that they may share and gather information with one another (IoT). The Internet of Things nodes is composed of wearable sensors and processing energy, both of which are intended to be present and common in a variety of business sectors. Household automation based on the Internet of Things refers to the possibility of managing home appliances using electronically managed and Internet-connected technologies. In addition, the Internet of Things offers cities innovative opportunities to make use of information in order to manage transportation, cut pollution, improve the efficiency with which infrastructure is used, and keep inhabitants safe and clean[10]. After that, the Smart Grid is a component of an Internet of Things system that can remotely monitor and manage everything, including lights, road markings, heavy traffic, parking, and the forecast of things comparable to power influxes as the result of catastrophic events and disasters. IoT devices that are outfitted with sensors are employed in order to monitor the location of medical equipment in real-time. Examples of such equipment include scooters, oxygen pumps, cardioverters, and other surveillance gear. Forecast management is one of the most promising aspects of the Internet of Things in the car industry. The technology is able to gather data from chips and sensors installed all over a connected vehicle, which can then be analyzed in the cloud and used to predict when the vehicle will need repair. The Internet of Things (IoT) in the industry might connect machines, equipment, and sensors to an outlet, which would provide much-needed insight into production for process engineers and management. Using sensors such as brake beams and RFID, for instance, businesses could be able to carry out impromptu spot checks of certain regions as workers go through the assembly[11].

Several Internet of Things nodes is deployed in areas of the natural environment that are inaccessible to electrical power sources. The nodes only have a limited amount of power that is sufficient to carry out the function for which they were designed and the critical safety orders that, in most cases, deplete the battery power. Three different approaches are practical that may be used to solve the issue with battery life. The most essential approach is to use the fewest safety requirements on the node, which is not encouraged, especially when handling sensitive information. However, this is the way that should be used since it is the most necessary. The second strategy involves increasing the capacity of the battery. Because the majority of Internet of Things nodes are planned and intended to be of compact volume and weight, there is less room for a bigger battery. The ultimate approach generates sufficient electricity using just renewable resources. However, these improvements to nodes would need the use of more complex components, which would increase the monetary cost of nodes[12], [13].

3. Industrial Internet of Things

In today's world, new company operations face many obstacles, including the necessity to move products on time, the presence of competitive pressure, new standards, and creative trade techniques. Because of this, many businesses rely on the Industrial Internet of Things (IIoT), which refers to all or any achievements carried out by companies to prototype, monitor, and improve their business procedures during the gathering of insights from multitudes of allows us to connect, things, and computer systems to support them in attaining economic profit. As a result, many companies rely on the Industrial Internet of Things (IIoT). As its name suggests, the Industrial Internet of Things (IIoT) is a concept that utilizes the Internet to connect and manage different computers, gadgets, and machinery used in industrial settings[14], [15].

The term "Industry 4.0" refers to the convergence of the Internet of Things (IoT) with the traditional industrial value chain. The Industrial Internet of Things is the most appropriate engine for creativity that can be used to reduce operating costs (OPEX) and capital spending (CAPEX), monitor, and improve business procedures regardless of how challenging they are, and enable creative business model development. The IIoT has reaped the benefits of growing attention from both academia and industry, which has resulted in exponential developments in the field's use of modern approaches. For instance, utilizing big data methods, a large amount of sensor information is collected and uploaded to the cloud in order to make an intelligent decision. The additive manufacturing process, often known as 3D printing, may be used in production to generate changed items of numerous shapes at cheaper costs and within shorter periods [16], [17].

The Internet of Things (IoT) in the industrial sector has seen an explosive expansion in recent years because of several developments in both industry and technology. The invention of steam engines in the 18th century laid the groundwork for one of the most significant advances in industrial progress. Because of the mechanization that was made possible by steam engines, factory output was able to go from the period of clean manual labor to the era of automation which led to a significant rise in overall output. During the 1870s, machines that were previously driven by steam were gradually replaced by machines that were propelled by electrical energy. Concurrently, the specialization of specialized industries led to another industrial breakthrough in the form of an explosion in output. The 1960s saw the beginning of what is now known as the "digitalization" revolution, which was the third industrial revolution. During this period of change, the use of programmable controllers and advanced electronics to increase production efficiency resulted in the development of new industrial automation[18], [19].

The methods of communication and information quickly changed from the beginning of the 20th century through the start of the 21st century, resulting in the development of newer technical spectrums. These methods significantly improved industrial productivity by enhancing the levels of intelligence present in the sensing, communication, decision-making, and production spheres. The IIoT has lately become mainstream in both the industrial and educational sectors. This may be attributed to the concept of integration as well as enhanced data collection strategies inside traditional companies. In 2011, the Hanover Fair was the primary venue at which Industry 4.0 was used to launch the 4th industrial transformation and generate a great deal of awareness in Europe[20], [21].

Within the framework of the Industrial Internet of Things (IIoT), machines collaborate to perform tasks without the need for human intervention. These machines are intelligent enough to adapt to a variety of application scenarios relating to healthcare, production, supply chain, and remote monitoring. Contact between machines, also known as machine-to-machine (M2M), enables the nodes that make up the Internet of Things to independently share data. The effective use of the 'Big data' technology developed by machines has the advantage of using the obtained information to enhance the scheme implementation by producing important domain-specific knowledge. With its omnipotent and omniscient sense, information connectivity, information gathering, and information investigation capabilities, the Industrial Internet of Things (IIoT) is being hailed as a potentially fruitful solution to the problem of how to bring successful applications into the 21st century. This is accomplished by connecting physical objects and enabling the combined mechanization of things and industrial processes[22], [23].

The Industrial Internet of Objects (IIoT) ensures the connectivity of disparate things by using a wide variety of software platforms, actuators, and sensors that are designed to detect and collect data from their immediate environments and, as a result, cause devices to perform certain activities. Because of recent developments in information and communication technology, some of the inherent constraints of IIoT have been eliminated (ICT). For instance, ambient backscatter may help IIoT devices attain higher power by assisting in interactions. In addition, information technology on mobile devices may extend the capabilities of an IIoT device by outsourcing process-intensive chores to edge servers. This frees up the mobile device to focus on other tasks. In addition, the current state of blockchain technology creates difficulties that are analogous to weaknesses in compatibility, safety, and secrecy[24].

4. Neutrosophic-based Machine Learning Approach

Building trust takes time and requires consideration of a wide range of factors, both internal and external to the relationship being considered. The trust ratings are regularly updated whenever there is a new interaction that takes place. Beginning with a fresh encounter, the trust computation cycle then moves through steps of evaluation, computation, and experience. The level of trust between two IIoT devices affects the consumption habits of a particular service that is provided by the other device. This, in turn, influences the choice of whether an IIoT device will engage in a transaction with some other IIoT device. Building trust in a biological body is relatively simple; nevertheless, it is impossible to develop trust in a machine system since computers do not have senses. In addition, the optimal trustworthiness score that can be assigned to an object with a high degree of accuracy is difficult to measure. If everything is understood and viewed differently, then this is a much more challenging task. Therefore, various programs that operate on the IIoT devices may give a given device a varied trust score depending on how they interact with it. These trust scores may include trustworthy, extremely trustworthy, and non-trustworthy. These variances add another layer of complexity to the

process of deciding whether an IoT device can be trusted. As a result, it is essential to develop a mathematical model that specifies the traits or properties that are common to all forms of trust. Because the IIoT creates such a huge quantity of data, it is difficult to determine how much of it can be employed directly to determine the trust score. As a result, it seems to become important to define the trust specifically for a certain application, a time range, and a context. Figure 1 shows the methodology.

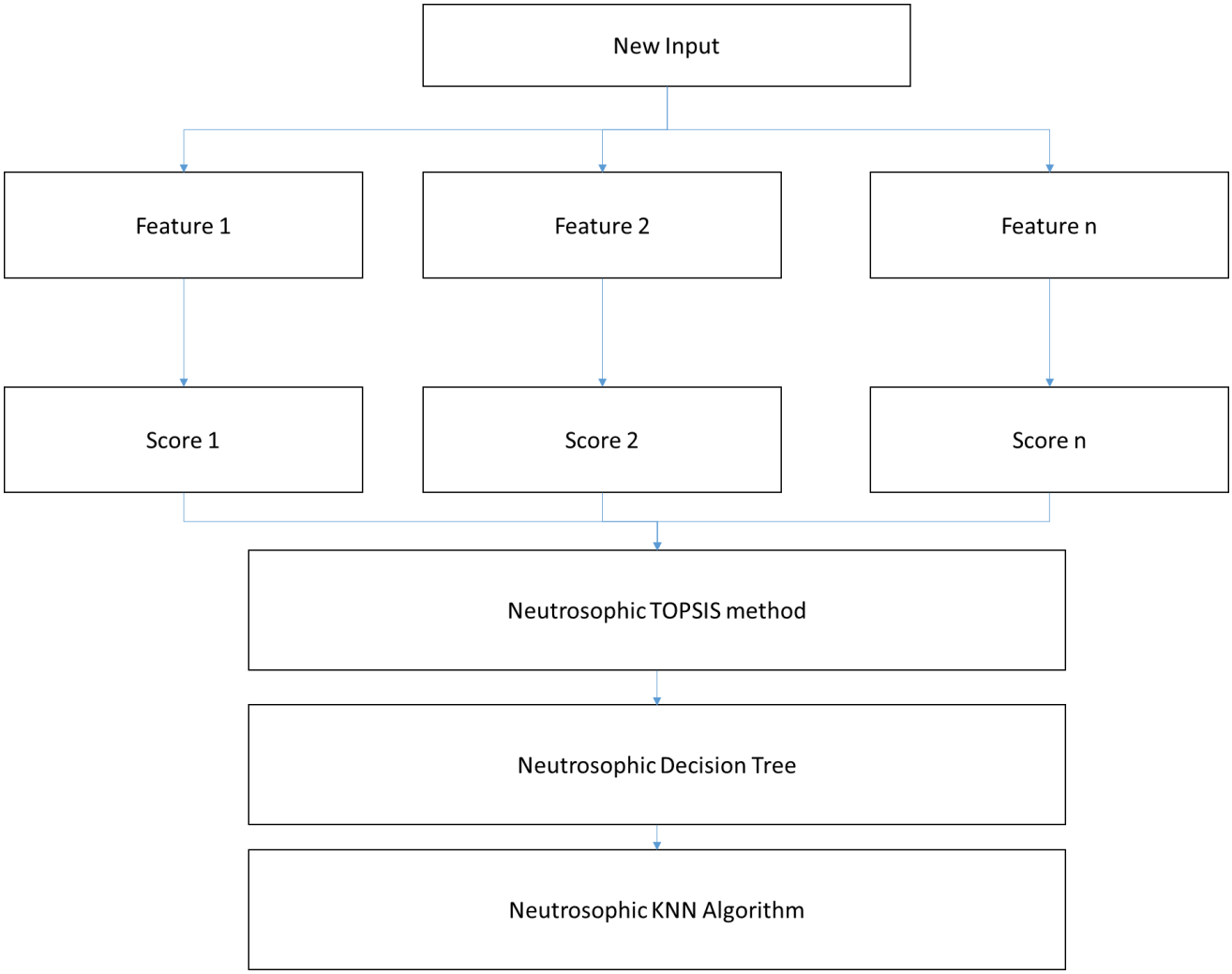

Figure 1: The neutrosophic-based machine learning

Neutrosophic TOPSIS Method

The trust computer simulation that has been developed for the industrial IoT can accommodate a wide variety of devices, including actuators, sensors, and controllers. The suggested mathematical model is not reliant on the underlying architecture or protocols in any way. The IIoT device may have many distinct traits, like its location, classification, identity, its technology, its MAC address, its IP address, its signal-to-noise ratio, its utilization (activity), its age, and other device attributes. The trust calculation will be affected in a variety of ways by the properties of the device. As part of this body of work, we have suggested a computational model for the calculation of trust that is based on machine learning. The machine learning model includes the calculation of a trust score by utilizing TOPSIS, neutrosophic K-NN grouping, and a neutrosophic Decision Tree for categorizing the extracted attributes to provide a final trust score that can be used for decision-making[25], [26].
Developed by Yoon and Hwang, the outranking method known as the Technique for Order Preferences by Similarity to Ideal Solution (TOPSIS) ranks preferences in descending order. It is predicated on the premise that the optimal option should have the smallest distance possible between itself and the positive ideal solution, and the greatest distance possible between itself and the negative ideal solution. The positive ideal solution is the optimal answer because it satisfies all of the criteria

with the highest possible value, while the negative ideal solution satisfies all of the criteria with the lowest possible value. It is a well-known strategy to outranking that is used for selection in a variety of areas, including the choice of suppliers and websites, amongst other applications.

Perform the calculations for the weighted matrix. Find out what the good and bad aspects of the perfect solution are. Determine the amount of space that separates each potential outcome and the positive and negative ideal solutions. Calculate the relative proximity coefficient.

Decision Tree

Decision Trees are supervised machine learning algorithms that can predict a variable that represents a goal. This is accomplished by assessing a collection of supplied input variables using a tree-like structure of rules that regulate the connection between the input and output variables. The training process for this tree-based supermodel begins with the assignment of a root node, which is supposed to represent all of the data. Afterward when, this original root node is even further subdivided and partitioned into decision nodes, each of which is constructed based on the values of characteristics that are used for the goals of prediction. These decision nodes are often shown by a collection of branches, with the top branch illustrating the observations count signifying instances that are to be allocated to a lower subsidiary. This procedure of branching out is performed many times until a point is reached when all of the observations included inside a decision point carry a categorization that is comparable to one another. A leaf node is a point in a decision tree at which the process of branching and dividing decision nodes comes to an end[27], [28].

The process of branching begins with picking the variable that is most suited to operate as a splitting variable from the set of parameters that have been provided. This decision is made after a comparison of the relative splitting quality of each of the variables. In the event of a predictor variable that is based on continuous data, each variable may be employed as an element of the established process. On the other hand, when using a model with a categorical predictor variable, the values of the target variables that are represented in each category are what are used to separate the branches[29]–[31].

The procedure for dividing the data is carried out based on the value that is produced from the equation below, which represents the statistical Pearson Chi-Squared (2) test of the predictor variables.

$$x^2 = \sum_{i=1}^{k} \frac{(o_i - E_i)^2}{E\_i} \quad (1)$$

The procedure for splitting that was described before is carried out recursively until all the provided opportunities have been exceeded by one of the logs' worth values.

The greater the size of a decision tree, the greater the overall complexity of the tree, which in turn might increase the risk of the model overfitting, which in turn decreases the tree's resilience. As a result, pruning may be used on the established model in a way that simplifies it without losing the overall accuracy. This is accomplished by eliminating leaves from trees that aren't essential to maintain a high degree of accuracy.

KNN Algorithm

KNN is an algorithm for supervised machine learning that is applied for the objectives of both regression and classification. The KNN is an algorithm that, in general, has a low level of complexity and a high level of application. This is due to its capacity to provide a highly accurate prediction with just a little amount of training being required and a small number of parameters that need to be tuned.

The following are the stages that are often included in a KNN classification procedure. They are used to identify the class of an instance being tested by first acquiring the class of its nearby peer instances[32], [33].

Setting a K value, which is used to calculate distances between a testing instance and all of the accessible input training datasets, is the first stage in performing a KNN classification. Once this step is complete, the classification may continue. To place the testing instance in the category that

corresponds to the one that is most often shown by its K nearby points, these distances are used to generate the K training examples that display the minimum number of distance computations. In addition, the allocation of a class to the checking instance is accomplished by first determining the proportion of the various classes that are accessible within the K nearby instances, and then the testing instance selects the class that received the largest number of votes. As a further point of interest, the Minkowski Distance is often used in the process of calculating distances in a standard KNN scenario[34], [35].

$$D = \left(\sum_{i=1}^{n} |x_i - y_i|^f\right)^{\frac{1}{f}} \quad (2)$$

In addition, the classification of the value of K can be driven by the data, in which case a cross-validation strategy can lead to the selection of the number of K that is the most effective and indicative of the data, and where higher values can reduce the effect of noise while also leading to less distinguishable boundaries within classes. Experimenting with the behavior of the model using a variety of various K values and choosing the value that achieves the maximum level of performance is a more flexible method.

5. Numerical Illustration

To produce the datasets, we undertake simulations of the various properties of the IoT nodes that are represented by five associated sensors. The dataset for the 100 IoT nodes was prepared with a little deviation in the pattern. This was done. The impacts of distance among sensors have indeed been simulated by adding a minor offset and some small variations to each sensor's output. This was done so that the data would be comparable. There are three criteria such as spatial knowledge, the experience of temporal, and pattern of behavior. Table 1 shows the opinions of decision-makers. The spatial has the highest weight followed by pattern and temporal. Table 2 shows the normalization matrix. Device 7 is the best deception and device 2 is the worst device.

Table 1: The expert's survey.

	C1	C2	C3
Device 1	0.8	0.65	0.49
Device 2	0.63	0.47	0.55
Device 3	0.72	0.72	0.43
Device 4	0.48	0.43	0.73
Device 5	0.88	0.46	0.88
Device 6	0.66	0.59	0.6
Device 7	0.66	0.9	0.7

Table 2: The normalization matrix.

	C1	C2	C3
Device 1	0.431878	0.394381	0.288495
Device 2	0.340104	0.285168	0.323821
Device 3	0.38869	0.436853	0.253169
Device 4	0.259127	0.260899	0.429799
Device 5	0.475065	0.279101	0.518113
Device 6	0.356299	0.357977	0.353259
Device 7	0.356299	0.546067	0.412136

After doing an analysis of the interactions that took place in the reliable region, we marked the dataset using the details. The cluster centroid points that are located inside the untrustworthy region have been labeled as untrustworthy, whilst those that are located outside of the area have been labeled as trustworthy. These data are tagged in a way that allows them to be taught to recognize interactions. In order to avoid the issue of overfitting, we tested the model with a very small number of training examples. The confusion matrix form will be used to calculate how well the suggested classification would work, displaying both the current and expected adding intelligence on trustworthiness (T) and untrustworthiness (U). The suggested machine learning model has a lower false positive rate (FPR) and a higher true negative rate (TNR) in comparison to previous approaches, which demonstrates the superiority of the model that we have presented.

The results that were obtained from the confusion matrix contain a variety of performance analyses, including precision, NPV, accuracy, specificity, and sensitivity. These performance parameters are computed depending on the true positive (TP), the true negative (TN), the false positive (FP), and the false negative (FN) (FN). Following the learning of the sample, 115 of the 117 encounters that were determined to be untrustworthy were accurately categorized as having untrustworthiness, while two were incorrectly labeled. Figure 2 shows the accuracy of the KNN and the decision tree algorithm.

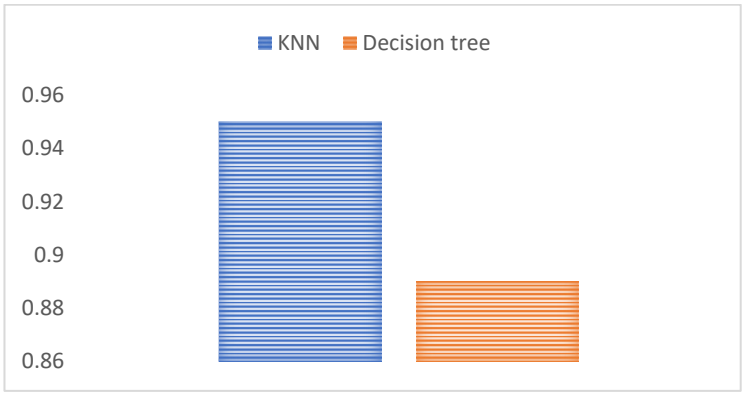

Figure 2: The comparison algorithm between KNN and decision tree.

6. Conclusion

As an alternative to the conventional weighted techniques, the work presented here suggests a unique way of calculating trust that makes use of an algorithm for machine learning to assess whether an interaction among IIoT devices can be trusted. We have developed a general-purpose computational framework that can be used for device interactions to facilitate, weight calculation, and classification. The reliability of the devices is evaluated using the model that was constructed using the geographical information, the temporal experience, and the behavioral pattern collected from the IIoT devices. To determine which kinds of experiences may be trusted, the first essential stage is putting into practice an unsupervised technique of labeling data in line with its trustworthiness. The neutrosophic TOPSIS, KNN, and decision tree approaches that were suggested are capable of accurately identifying the trust boundaries and producing the final trust score.

References

[1] X. Xu, M. Han, S. M. Nagarajan, and P. Anandhan, "Industrial Internet of Things for smart manufacturing applications using hierarchical trustful resource assignment," *Computer communications*, vol. 160, pp. 423–430, 2020.

[2] T. Wang, H. Luo, W. Jia, A. Liu, and M. Xie, "MTES: An intelligent trust evaluation scheme in sensor-cloud-enabled industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2054–2062, 2019.

[3] Y. Ren, F. Zhu, J. Qi, J. Wang, and A. K. Sangaiah, "Identity management and access control based on blockchain under edge computing for the industrial internet of things," *Applied Sciences*, vol. 9, no. 10, p. 2058, 2019.

[4] K. Huang *et al.*, "Building redactable consortium blockchain for industrial Internet-of-Things," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3670–3679, 2019.

[5] P. Nikander, J. Autiosalo, and S. Paavolainen, "Interledger for the industrial internet of things," in *2019 IEEE 17th International Conference on Industrial Informatics (INDIN)*, 2019, vol. 1, pp. 908–915.

[6] W. Z. Khan, M. H. Rehman, H. M. Zangoti, M. K. Afzal, N. Armi, and K. Salah, "Industrial internet of things: Recent advances, enabling technologies and open challenges," *Computers & Electrical Engineering*, vol. 81, p. 106522, 2020.

[7] S. Zhao, S. Li, and Y. Yao, "Blockchain enabled industrial Internet of Things technology," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 6, pp. 1442–1453, 2019.

[8] W. Sun, S. Lei, L. Wang, Z. Liu, and Y. Zhang, "Adaptive federated learning and digital twin for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5605–5614, 2020.

[9] T. Gebremichael *et al.*, "Security and privacy in the industrial internet of things: Current standards and future challenges," *IEEE Access*, vol. 8, pp. 152351–152366, 2020.

[10] S. He, W. Ren, T. Zhu, and K.-K. R. Choo, "BoSMoS: A blockchain-based status monitoring system for

defending against unauthorized software updating in industrial Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 948–959, 2019.
[11] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *Proceedings of the 52nd annual design automation conference*, 2015, pp. 1–6.
[12] K. Rose, S. Eldridge, and L. Chapin, "The internet of things: An overview," *The internet society (ISOC)*, vol. 80, pp. 1–50, 2015.
[13] M. H. ur Rehman, I. Yaqoob, K. Salah, M. Imran, P. P. Jayaraman, and C. Perera, "The role of big data analytics in industrial Internet of Things," *Future Generation Computer Systems*, vol. 99, pp. 247–259, 2019.
[14] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial internet of things (IIoT): An analysis framework," *Computers in industry*, vol. 101, pp. 1–12, 2018.
[15] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial internet of things," *Journal of Software Engineering and Applications*, vol. 9, no. 10, pp. 533–546, 2016.
[16] W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Computer networks*, vol. 148, pp. 283–294, 2019.
[17] Y. He, J. Guo, and X. Zheng, "From surveillance to digital twin: Challenges and recent advances of signal processing for industrial internet of things," *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 120–129, 2018.
[18] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Business horizons*, vol. 58, no. 4, pp. 431–440, 2015.
[19] H. Wang, O. L. Osen, G. Li, W. Li, H.-N. Dai, and W. Zeng, "Big data and industrial internet of things for the maritime industry in northwestern norway," in *TENCON 2015-2015 IEEE Region 10 Conference*, 2015, pp. 1–5.
[20] F. Al-Turjman and S. Alturjman, "Context-sensitive access in industrial internet of things (IIoT) healthcare applications," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2736–2744, 2018.
[21] C. Qiu, F. R. Yu, H. Yao, C. Jiang, F. Xu, and C. Zhao, "Blockchain-based software-defined industrial Internet of Things: A dueling deep ${Q} $-learning approach," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4627–4639, 2018.
[22] H. Xu, W. Yu, D. Griffith, and N. Golmie, "A survey on industrial Internet of Things: A cyber-physical systems perspective," *Ieee access*, vol. 6, pp. 78238–78259, 2018.
[23] H. P. Breivold and K. Sandström, "Internet of things for industrial automation--challenges and technical solutions," in *2015 IEEE International Conference on Data Science and Data Intensive Systems*, 2015, pp. 532–539.
[24] O. Vermesan and P. Friess, *Internet of things applications-from research and innovation to market deployment*. Taylor & Francis, 2014.
[25] H. Sharma, A. Tandon, P. K. Kapur, and A. G. Aggarwal, "Ranking hotels using aspect ratings based sentiment classification and interval-valued neutrosophic TOPSIS," *International Journal of System Assurance Engineering and Management*, vol. 10, no. 5, pp. 973–983, 2019.
[26] P. Biswas, S. Pramanik, and B. C. Giri, "TOPSIS method for multi-attribute group decision-making under single-valued neutrosophic environment," *Neural computing and Applications*, vol. 27, no. 3, pp. 727–737, 2016.
[27] Y. Ben-Haim and E. Tom-Tov, "A Streaming Parallel Decision Tree Algorithm.," *Journal of Machine Learning Research*, vol. 11, no. 2, 2010.
[28] A. Priyam, G. R. Abhijeeta, A. Rathee, and S. Srivastava, "Comparative analysis of decision tree classification algorithms," *International Journal of current engineering and technology*, vol. 3, no. 2, pp. 334–337, 2013.
[29] H. Chauhan and A. Chauhan, "Implementation of decision tree algorithm c4. 5," *International Journal of Scientific and Research Publications*, vol. 3, no. 10, pp. 1–3, 2013.
[30] M. Pandey and V. K. Sharma, "A decision tree algorithm pertaining to the student performance analysis and prediction," *International Journal of Computer Applications*, vol. 61, no. 13, pp. 1–5, 2013.
[31] N. Bhargava, G. Sharma, R. Bhargava, and M. Mathuria, "Decision tree analysis on j48 algorithm for data mining," *Proceedings of international journal of advanced research in computer science and software engineering*, vol. 3, no. 6, 2013.
[32] W. Xing and Y. Bei, "Medical health big data classification based on KNN classification algorithm," *IEEE Access*, vol. 8, pp. 28808–28819, 2019.
[33] S. Zhang, X. Li, M. Zong, X. Zhu, and R. Wang, "Efficient kNN classification with different numbers of nearest neighbors," *IEEE transactions on neural networks and learning systems*, vol. 29, no. 5, pp. 1774–1785, 2017.
[34] S. Zhang, X. Li, M. Zong, X. Zhu, and D. Cheng, "Learning k for knn classification," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 8, no. 3, pp. 1–19, 2017.

[35] Z. Deng, X. Zhu, D. Cheng, M. Zong, and S. Zhang, "Efficient kNN classification algorithm for big data," *Neurocomputing*, vol. 195, pp. 143–148, 2016.