Hindawi
Mathematical Problems in Engineering
Volume 2022, Article ID 3048038, 10 pages
https://doi.org/10.1155/2022/3048038

Research Article

Examining the Effect of Cyber Twin and Blockchain Technologies for Industrial Applications Using AI

Hariprasath Manoharan,[1] **Yuvaraja Teekaraman**,[2] **Ramya Kuppusamy**,[3] **Naveenkumar Kaliyan**,[4] **and Amruth Ramesh Thelkar**[5]

[1]*Department of Electronics and Communication Engineering, Panimalar Institute of Technology, Chennai 600 123, India*
[2]*Department of Electronic and Electrical Engineering, The University of Sheffield, F127a Sir Frederick Mappin Building, Mappin Street, Sheffield S1 3JD, UK*
[3]*Department of Electrical and Electronics Engineering, Sri Sairam College of Engineering, Bangalore City 562 106, India*
[4]*Department of Instrumentation and Control Engineering, Sri Manakula Vinayagar Engineering College, Puducherry 605107, India*
[5]*Faculty of Electrical & Computer Engineering, Jimma Institute of Technology, Jimma University, Jimma, Ethiopia*

Correspondence should be addressed to Yuvaraja Teekaraman; yuvarajastr@ieee.org and Amruth Ramesh Thelkar; amruth.rt@gmail.com

Received 28 October 2021; Revised 20 January 2022; Accepted 7 February 2022; Published 2 March 2022

Academic Editor: Vijay Kumar

In current generation the concept of cyber twin technology has been emerging as an improved platform for different applications. This paper emphasize on examining the effect of cyber twin technology for manufacturing equipment in Industry 4.0 applications by solving three different elementary objectives. For the proposed conception a new system model is identified for integrating triobjective cases with artificial intelligence algorithm. In addition, high security measures are also incorporated using blockchain technology which is one basic requirement for industrial applications for creating real twins. Both system model and algorithm have been combined for providing effective performance in real time using a physical entity. The effectiveness of the proposed model is tested with sensor prototype and simulated with four scenarios where the projected model provides better performance for more than 72% when compared with existing methodologies.

1. Introduction

In current system where the domain is moving towards sixth generation, most of the wireless transmission schemes are implemented under cyber twin technology and their performance has been greatly improved in different applications like healthcare, Industry 4.0, transportation, etc. The process of cyber twin technology provides reproduction of digital platform for both living and nonliving entities. By using this technology it is easy to optimize the functionalities of different physical quantities by integrating sensors and in this process high quality of communication can be provided using both machine learning and artificial intelligence techniques. But primary challenge that is present in cyber twin technology is about security when creating a twin because it is easy for users to enter inside different systems by creating large amount of dark shadows. Therefore, to provide high security for digital twin process blockchain technology can be integrated with all applications. This blockchain technology provides high amount of security to all communication platforms by following proper Internet standard. The process of blockchain technology emerges by providing unique identification to each twin that are created and original twin will be identified using supercomputers shown in Figure 1.

The process of creating cyber twins is mainly applicable for manufacturing industry where the strength of a device will be tested by experts in real time using three-dimensional technologies. These technologies will be enabled with augmented

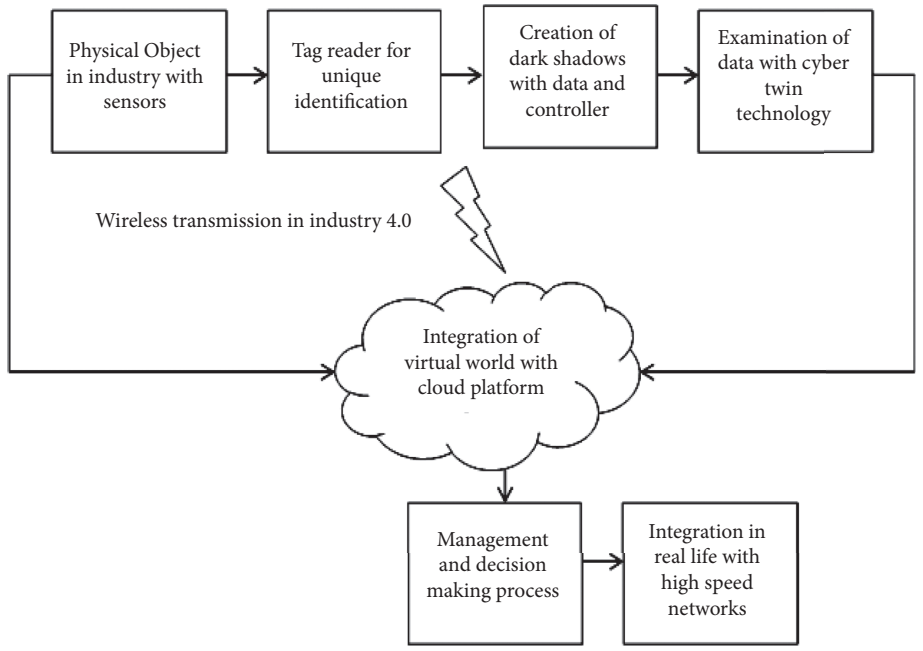

Figure 1: Systematic procedure of integration in Industry 4.0 using cyber twin.

reality gears which allow the entities to communicate with other individuals even if they are located at different countries. The process of cyber twin with blockchain technologies will provide great advantage for converting traditional system to control oriented system, where authorities can be able to control the machines in real time without staying in the meadow. The aforementioned process is also highly scalable because the entire data will be stored in cloud using encrypted and authentication keys where only authorized users are allowed to use the data for creating dark shadows. In addition the process of cyber twin can be treated as an extension of sensor integration process where if large amount of data is being collected then it will work more effectively for serving the real twin. Further, if extension process is continued then more applications can be integrated under the same technologies for avoiding all detrimental situations because cyber twin technology provides prediagnosis of a physical module before implementation. Even investment cost of cyber twin technology is much lesser and high sustainability of manufacturing products will be provided with high secured networks. The major advantage of cyber twin technology is that lifetime of all industrial components can be greatly increased by reducing the factor of reliability. This in turn can be applied to all appliances; thus real time product sustainability can be implemented in an effective manner. Moreover with integration of cyber twin technologies all components can effectually utilize resources that are allocated to them in a conditional mode. This makes the cyber twin technology to be distinctive as compared to digital twin procedures where each consumer can gain more advantage on imminent performance of distinct products. The novelty and contributions of the proposed work on cyber twin technology are explicated as follows:

(i) The cyber twin for industrial applications decreases the menace of traffic that is present in the network as autonomous manufacturing products are generated

(ii) Primary resource allocation constraint problems are solved using cyber twin technology in the designed mathematical model, thus increasing the scalable routes

(iii) Integration of physical entity is done which is represented in form of sensing devices where all relevant information is transacted in form of blocks

(iv) Implementation of SVM for future growth of interaction in all business activities is done, thus enhancing computer aided design with human interactions

1.1. Existing Methodologies. There are many existing methodologies that deliberate the integration of cyber twin and blockchain technologies in many applications. In this section some existing methodologies have been discussed where one major issue of blockchain technology termed as scalability has been discussed [1]. In order to describe scalability, probability of failure in terms of hypergeometric and binomial distributions has been used for describing the effectiveness using different inequalities. But the same methods have not been applied for Internet of Everything (IoT) which indicates it cannot be applied to some real time situations [1]. Subsequently, a decentralized storage system has been recognized for providing standard solutions that modify the necessary content that is present in industry [2]. This method implements a smart indenture code that provides high security to all appliances in industry. However, registering to this decentralized process is essential which is much monotonous and the entire data for this is stored in open source platform which indicates that there is a possibility in duplication of packets.

Even though many authors have successfully integrated both cyber twin and blockchain technologies, examining the sustainability of network after integration is one important case study that is provided in [3]. A turbo machinery appliance which is present in the industry will be integrated with cyber twin technology and after integration it has been proved that life cycle of the machine can be greatly improved. But cost of implementation is much higher because more number of phases needs to be maintained. The same method has been protracted to oil and gas companies [4] with a new reference model that contains four different layers. A large number of protractile devices should be taken into account for this big industrial case for ensuring the safety of all workers in the industry. Even though a virtual model has been developed conservation and preclusion cost is much higher.

An inspection method for preventing the cyber threat in Industry 4.0 has been deliberated [5] where it has been proved that data should be kept confidential and high amount of integrity should be provided for preserving the data which is much important in all industrial applications. Since it is difficult for startup industry to incorporate cyber twin and blockchain technology the authors [6] have provided valuable information about the structure of implementation which can be applied for providing security and privacy in IoE networks. But computational transaction cost is much higher that needs to be solved by using some new technologies.

Additionally, mathematical model has been developed by using underlying model of computer networks [7] where seven different layers and their functionality have been defined with equilibrium conditions. Appropriate threshold conditions have been defined after examining the characteristics of computer virus but definition of propagation model is not necessary for IoE networks as the propagation speed is already much higher. After proper investigation architecture of cyber defense and its mathematical model has been developed to overcome the research gap of propagation models [8]. The major difference in abovementioned methods [7, 8] is in terms of numerical and analytical constructions which are well defined with models, examples, and parameters. It is necessary to define some basic mathematical models for mechanists before describing all parametric values [9]. In the first step all necessities have to be identified and after deep understanding a submodel framework which includes biological, reactor, and physicochemical items has to be created.

It is well known that if digital twin process is introduced then dark shadow part for all energy objects should be created in advance and it should be shared with scientific prototypes among public. By using the same concept authors [10] have developed an intelligent technology by combining sensor technology for high complexity problems. These types of perceptions will provide real object behavior which in turn creates more advantage in industrial applications. In detail all the applications have to be converged as they are having their own pros and cons [11]; this leads to construction of high data collection and processing techniques. When examining about cyber twin dimensions eight different application oriented analyses like extensiveness integration, types of mode connectivity, frequency updating, etc. have to be simulated for all technical services and systems [12]. Thus an advanced two-dimensional support model is introduced with logical layout of different layers in asynchronous mode.

In current generation smart manufacturing industries with high correlation which is not duplicated from any physical loop process have been conferred [13]. This is done in order to realize the prerequisite of all industrial applications which includes operation of cranes for a separate management process [14]. Similarly, addictive manufacturing technologies by using blockchain technology have been considered for development in aircraft industry [15]. The process describes the way of securing the data using end-to-end encryption by considering aircraft infrastructure. As a part of cyber twin technology the bandwidth needs to be shared by several users by restructuring different voltage estimated in order to show effectual performance of cyber-physical systems [16]. Further developments are made in the field of cyber twin technologies which extends support for sixth-generation networks [17]. The experimental results in these updated networks provide a great support to strong communication part which builds up the network data with centric arrangements. In recent periodical the authors [18] have integrated the artificial intelligence technique in cyber-physical systems which deliver high advantage for industrial applications, thereby making human interaction process to be self-effacing. Apart from cyber twin in industry process it can even be applied in construction sites for building effective progress in home and safety measures [19] which can be termed as a new development in personnel competency. However high safety measures are not implemented with modernised procedures in all aforementioned recent techniques [17–19] even with the presence of physical entities.

1.2. Research Gap and Motivation. Many research gaps have been observed from existing literature [1–16] where there is less security for all geometric models which are integrated with efficient algorithms. Although much literature has examined the concept of cyber twin for various applications, the majority of literature has neglected the convention of real time twin technologies for manufacturing applications. Also there is no efficient system model for proper designing of physical entities.

Therefore, the proposed system aims to overcome the research gaps by introducing a new system model that can be applied in real time for Industry 4.0 applications. The proposed model uses sensor as a physical entity for creating real time twins and also enables blockchain transactions with high accuracy rate. In addition the system model has been integrated with efficient artificial intelligence algorithm termed as Support Vector Machine (SVM) to enhance efficiency of various parameters which serves as a backbone for functioning of physical entity.

1.3. Objectives. The projected perception of cyber twin with blockchain technology using SVM for Industry 4.0

applications predominantly focuses on the following objectives such as reduction of node failure probability, minimization of wastage by distributing accurate loads to physical entities, and decreasing the time period for creation of dark shadows by using a newfangled system model. In addition, a triobjective case is also introduced by examining the cost of implementing proposed model with all physical entities.

2. System Model

This section describes the mathematical formulations that are necessary for integrating both cyber twin and blockchain technologies with prearranged sensors. Since cyber twin is emerging as a new model in industrial field it is required to replace binomial distribution model by defining a set of nodes using sampled data. In addition, if malevolent nodes are present then it should be identified by using a set of random variables as given in the following:

$$M_i = \sum_{i=1}^{n} t_i \frac{s_i}{w_i}. \tag{1}$$

Equation (1) represents the mean value of a particular node with hyposymmetrical distribution of networks. Therefore, the corresponding variance can be established as given in the following:

$$V_i = \sum_{i=1}^{n} \frac{t_i(1-c_i)(w_i - t_i)}{w_i - 1}. \tag{2}$$

Equation (2) denotes that difference between both replaceable and nonreplaceable nodes in duplication with failure of cells that are totally distributed by less number of wicked nodes will provide accurate likelihood distribution. If probability of failure is increased with resiliency then it can be expressed in matrix form as shown in the following:

$$P(i) = \sum_{i=1}^{n} \frac{\begin{pmatrix} A_i & T_i - C_i \\ a_i & t_i - c_i \end{pmatrix}}{\begin{pmatrix} T_i \\ C_i \end{pmatrix}}. \tag{3}$$

Equations (1)–(3) indicate the basic equations that are necessary for integrating sensors with minimum number of nodes using cyber twin and blockchain technologies. But in the proposed method cyber twin and blockchain technologies are applied for industrial applications and the capacity which is defined in terms of load should be minimized because if many users attempt cyber twin technology at same time then delay will be much higher due to network operations. Therefore, one main objective in the proposed work is to minimize the load for all menace functions which can be given as

$$ER_i = min \frac{1}{r_i} \sum_{i=1}^{n} l_i. \tag{4}$$

Equation (4) denotes that minimum number of simulations must be performed and total value of load should be allocated in accordance with duplicated nodes which forms the expected value of total risk functionalities in a given network. Since minimum number of simulations needs to be performed the delay in each network should be minimized as given in the following:

$$d_i = min \sum_{i=1}^{n} \rho_i \tau_i \mu_i. \tag{5}$$

Equation (5) indicates that if all the corresponding time which includes accessing a particular network and avoiding failures during connection and packet arrival rate are minimized then total delay in a network will be lesser and it will be within defined standard rate. Also, observation of packet to be received at correct time should be monitored by using the formula as given in the following:

$$NP_i = \sum_{i=1}^{n} OP_i \times \frac{nT_i}{Target\ time}. \tag{6}$$

Equation (6) is also used when new blocks are much closer to the target. Therefore, the target time should be much lesser in order to handle more number of industry processes. In the proposed method two different process are integrated; hence cost of implanting sensors according to given arrangement should be lesser and it can be calculated as

$$TC_i = \sum_{i=1}^{n} (S_0 + S_1 + \ldots + S_n) w_{in}. \tag{7}$$

In (7) there is necessity to extend sensors during cost calculation because there will be many sensors that work during physical insertion of objects. In industrial applications there will be many sensors for ensuing cyber twin process and in addition weight of each sensor should also be monitored for calculating accurate cost. Even though more number of sensors is integrated in industrial applications the proposed method inspects to minimize the cost of installation which is added as another objective. Therefore, the objective function can be given as

$$\mathrm{OB}_i = \min \sum_{i=1}^{n} \mathrm{ER}_i, d_i, \mathrm{TC}_i. \tag{8}$$

Equation (8) can be stated as triobjective function which integrates three different formulations as given in (4), (5), and (7). This type of model formulations is necessary when sensors are integrated and these formulations can also be implemented in real time simulations.

Equations (1)–(7) represent the following terms. t_i and w_i denote the total number of malicious nodes that can be processed with and without replacement. s_i represents exact size of each cell where sensors are integrated. c_i denotes the probability of failure inside a cell where sensors are connected. A_i and a_i denote the accumulative matrix with replaceable and nonreplaceable nodes. C_i and c_i represent the resiliency that is present at both replaceable and nonreplaceable nodes. r_i denotes the number of duplicated nodes. l_i represents total number of loads that are observed

in risk function. ρ_i denotes the time taken for connecting cloud storage with network access point. τ_i represents the time taken for requesting the corresponding action to be taken in case of failure in technologies. μ_i denotes request arrival rate for connecting different nodes. OP_i denotes the reference for old packets. nT_i represents the time allocated for n^{th} block. $S_0 + S_1 + \ldots + S_n$ denotes total cost of all installed sensors inside industry. w_{in} represents weight of each sensor to be installed.

3. SVM for Cyber Twin and Blockchain

This section describes the implementation of precise algorithm for integrating corresponding sensors with industrial objects. After cautious simulation experimentation it is observed that only artificial intelligence paves the way for accurate processing of cyber twin and blockchain technologies in all industrial applications. To be accurate one type of artificial intelligence technique termed as SVM will be implemented for handling the issues inside the industry. The major advantage of implanting SVM is as follows: 1. To reduce weighted loss function. 2. To use in high dimensional space. 3. To provide exact separation between different sensors.

In addition to the aforementioned advantages the problem formulated using SVM is a linear one because complexity will be much lesser when linear algorithms are used. Therefore, this classification problem can be framed using (9) as

$$CF_i(x) = \sum_{i=1}^{n} w_{in} x_{in} + k_{in}, \tag{9}$$

where w_{in} represents the weight of hyperplane space. x_{in} represents the input data in hyperplane space. k_{in} represents the multiplicative products inside the hyperplane.

Once the classifications have been completed then in SVM, loss function should be framed in order to minimize the expected error. This error minimization should carried out within less number of simulations; therefore, in industrial applications if any error has occurred it will be retrieved within short span of time by connecting with cyber twin technology. The error minimization problem in SVM can be framed as

$$\delta_i = \sum_{i=1}^{n} \frac{1}{l_i} \left(Actual_i - Predicted_i\right), \tag{10}$$

where l_i denotes the length of simulation that is processed in each sensor.

Equation (10) indicates that difference between original and prophesied values of sensors should be detracted to find the value of original error. Also, the original values are reserved from previous data which is stored in cloud. The abovementioned (9) and (10) are applicable only for cyber twin integration but in proposed method blockchain technology is also present; hence the optimization problem for blockchain technology should also be framed which is given in (11).where DS_i represents degree of gratification for i^{th} sensors. TF_i denotes transaction fees of each block that is linked with sensors.

Equation (11) indicates that difference between satisfaction degree and fees of transacting each block should be minimized and the values in terms of difference should be maximized as transaction rate of blocks that should satisfy the following constraint:

$$\sum_{i=1}^{n} \vartheta_i \leq \omega_i, \tag{12}$$

where ϑ_i denotes considerable rate of transaction. ω_i represents total transaction rate.

If constraint indicated in (12) is not satisfied then optimization problem of blockchain technology will not be maximized; hence no security will be provided for appliances in industry and as a final point it leads to duplication of many packets in cyber twin technology. Therefore, careful experimentation of (11) and (12) has to be made while integrating two different technologies under the same platform. Flowchart of integrating blockchain and cyber twin technology with system model is given in Figure 2. If the steps shown in Figure 2 are implemented then a symmetry solution will be obtained within less number of iterations. The same method can be applied in both presence and absence of access points.

$$\beta_i = \max \sum_{i=1}^{n} \mathrm{DS}_i - \mathrm{TF}_i, \tag{11}$$

4. Results and Discussion

In order to prove the efficiency of proposed system model with SVM, a real time simulation model has been designed using cloud desk bench and all the data has been collected from previous history that is stored in Github. By using the collected data different type of sensors has been integrated and their basic parameters are checked under four different scenarios as given below.

Scenario 1: detection of node failure

Scenario 2: minimization of load in conformity with node tasks

Scenario 3: analysis on formation of dark shadow with respective delays

Scenario 4: operation cost of different sensors

All aforementioned scenarios are first implemented with their corresponding prototypes in Node Red MCU; then their ensued values that are provided by all sensor units are stored in cloud. The corresponding programming model has been transcribed in Node Red and the values that are stored in cloud have been implemented using a simulation model since the effect of sensor nodes will be understood better when a simulation setup is used. Also, past data and other existing methodology results have also been compared with proposed model.

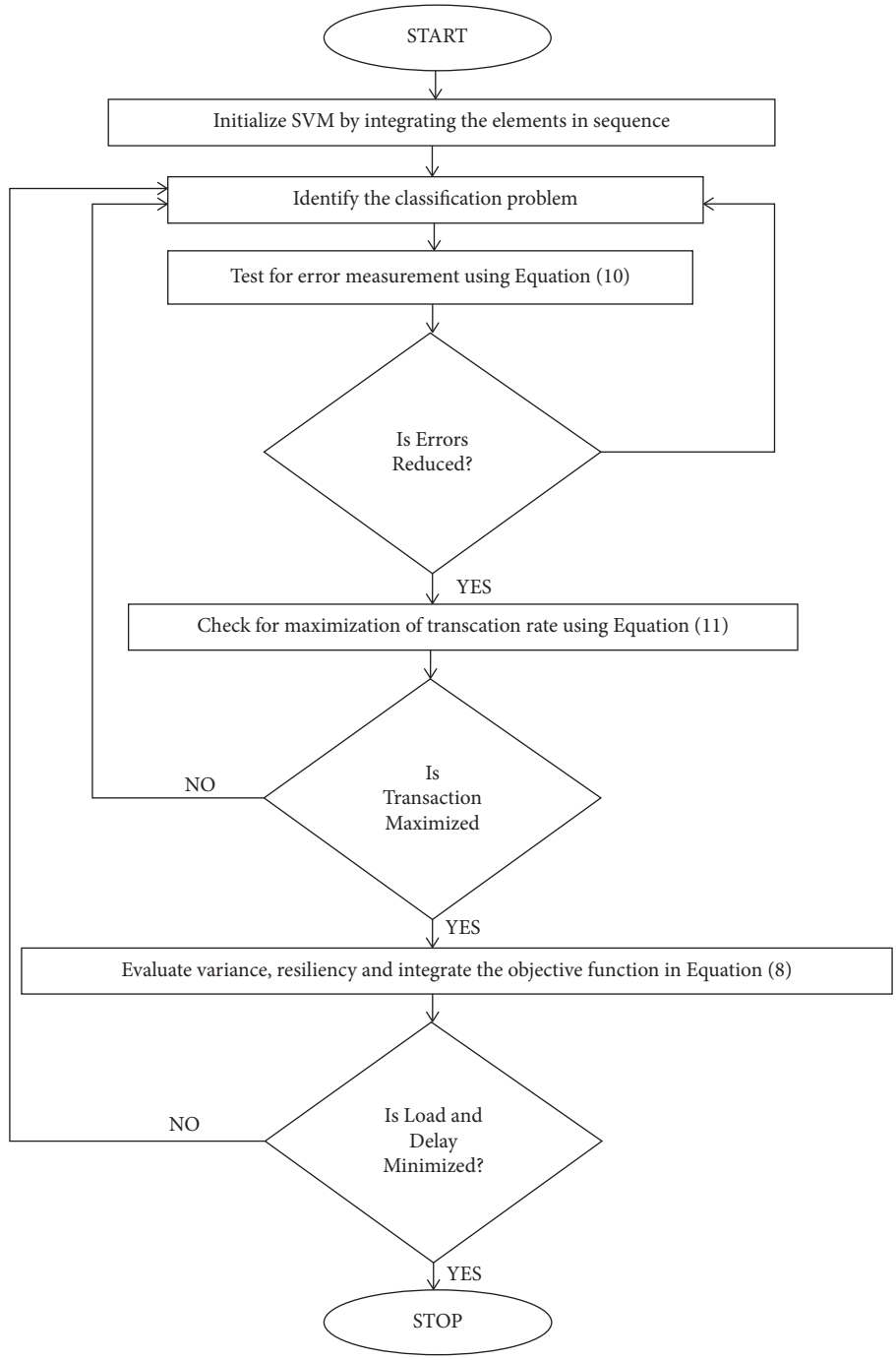

Figure 2: Flowchart of the proposed SVM and system model.

4.1. Scenario 1. In this scenario probability of failure of single sensor node and its effect on corresponding industrial applications have been deliberated. When a sensor has been integrated in a manufacturing machine all corresponding nodes must work in a proper manner; therefore the information will reach the destination end at corresponding time period. If failure of nodes in a particular process is higher, then it is difficult to monitor the exact status of a machine which leads to complete failure of entire process. Therefore in the first step, probability in failure of nodes should be checked and those failure nodes should be interchanged with high quality node setup. In addition, even if it not replaced the percentage of failure should be reduced which is decisive objective of proposed model. For preliminary exertion in this detection process both means and variance with hyposymmetrical distribution should be calculated using (1) and (2). If mean and variance are within the limits then failure of nodes can be simulated. The simulated model has been shown in Figure 3.

Figure 3 is plotted using system model in (3) and also by following the flow of proposed SVM model. It can be observed from Figure 3 that node length is varied in

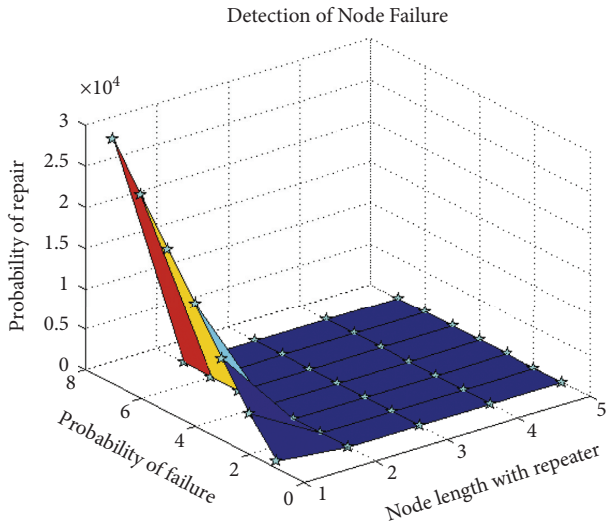

Figure 3: Discovery of node failure and repair.

presence of repeater from 1000 to 30000 Kms. For every node length probability of failure and repair is inspected and it is compared with existing method [1]. It is implicit that the proposed model produced only low probability of failure with high restoration percentage of the same nodes without any change in corresponding networks. For example, if node length of 15000 Kms is considered after extending with repeater then the existing model provides failure probability at a rate of 0.056 and corresponding recovery rate of the same node is 0.03. But for the same node length the proposed model provides only low failure rate of 0.015 and the recovery rate is much higher for the same node which is equal to 0.1. This scenario proves that the proposed model can be used for real time operation with small failure rate.

4.2. Scenario 2. In this scenario the major objective of load minimization is deliberated because after realizing the physical nature of implemented sensors surplus load should be obliterated. If high amount of load is provided then amount of wastage will be increased; therefore, in industrial process load should be minimized. The basic performance of sensor is that even with small amount of load transmitting sensors should be in a position to share the resources for receiving sensors. This objective is accomplished using the proposed model where the simulated values are shown in Figure 4.

Figure 4 provides the substantiation for load minimization which is measured in millijoules (mJ). For simulating the present scenario nodal tasks are assigned from 2 to 10 and corresponding loads are measured. For each node task the load that is allocated to sensors should be reduced where both existing and proposed model processed the same minimization problem. But the proposed model reduces the load in higher amount when compared to existing method. For example, if node task is 6 then corresponding load that is allocated to sensor is 2.8 mJ whereas for same nodal task the proposed method minimizes the load to 0.67 mJ which is much lesser and amount of wastage is reduced when proposed method is implemented in real-time applications.

4.3. Scenario 3. Once the failure rate and load are exactly observed from integrated sensors then in next step delay of sensors will be calculated because packets which are represented in the form of information should be processed without any delay. Since probability of failure is directly proportional to delay if any single packet is transmitted with delay then rate of failure will be amplified. Therefore, delay of sensors that are integrated with manufacturing appliances should be reduced. For the proposed model delay is simulated by considering all previous data from existing models and the simulated values are represented in Figure 5.

Figure 5 is plotted by observing the time of shadow creation because in the proposed model cyber twin is used. Whenever cyber twin is integrated then delay of creating dark shadow should be observed. Therefore, time period is considered by using different time periods from 60 to 360 per cycle. For each time period delay in creating dark shadows and process of transmitting information is observed. The contour figure indicates that dark shadows are created with less amount of time when proposed model is used. For example, if time period is 180 per cycle then existing method [2] delivers the packet and it created shadow at a delay of 769 seconds whereas for the same time period the proposed method produces less delay which is observed as 368 seconds. Therefore, the proposed method proves to be much efficient in creating dark shadows within less amount of time where all necessary communications transpire at the correct time period inside the industry for different manufacturing utensils.

4.4. Scenario 4. In the proposed method there is inevitability to examine cost of implementing different sensors and for integrating cyber twin with blockchain technologies. The process of cost calculation should be inspected using all contraptions that are present with sensors. Therefore, total cost is calculated using (7) by considering weights of different sensors. In the implementation the cost of a particular device which is already present in industrial system is not added. However, in the proposed model network cost is also added with different sensors, i.e., only external cost of installation is added and no internal costs have been simulated. The simulated value of total cost is shown in Figure 6.

Figure 6 is plotted by varying the network size from 47 to 193 and number of sensors is considered as 2 and 3. For five different network dimensions total value of cost is simulated and it is observed that even when network size is higher the proposed model provides only low cost of implementation. For example if network size is 117 and number of sensors in this case is 3 then total cost of implementation for existing method [2] is 413 dollars whereas for the same network size the proposed method implements only 312 dollars where cost of implementation is much reduced. This proves that if proposed model is implemented then cost of sensor implementation for cyber twin technology will be reduced.

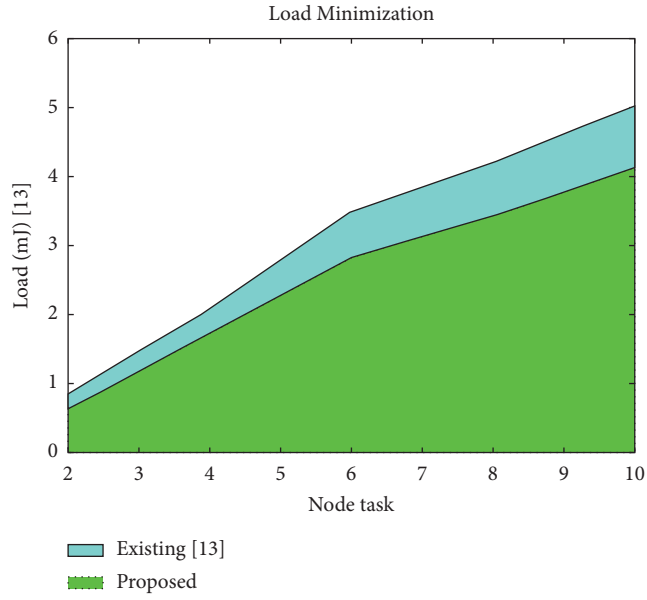

Figure 4: Minimization of load with the nodal task.

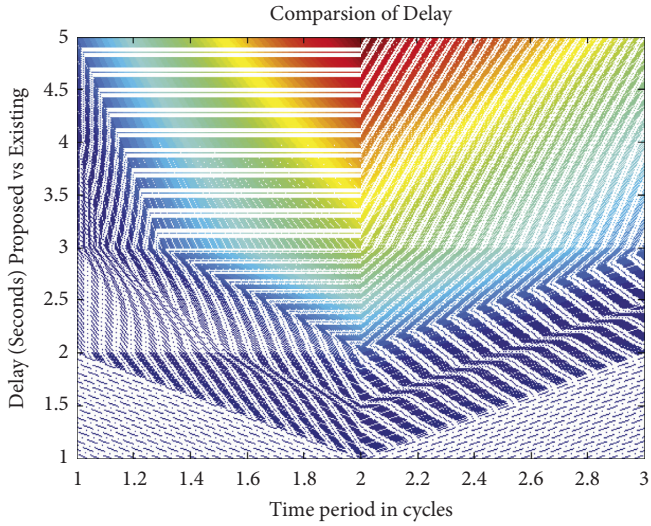

Figure 5: Minimization of delay with time periods.

4.5. Scenario 5. The limiting behavior of intelligent algorithm in the proposed model can be evaluated using big O notation at constant time period functionalities which is expressed using O(1). Even though the size of input that is provided for the operation of cyber twin is much higher it takes the same amount of time to execute the complete setup with a physical entity. At the starting of input functions it is necessary to consider a linear time function as variation will transpire all input data in outer loop conditions. After some iteration period the linear function will change to a constant function where all data have achieved maximum inner loop conditional periods thus indicating that complete data has been executed. The time complexity function of cyber twin with SVM can be represented using (13) and simulation plot of SVM complexity is represented in Figure 7.

$$O(1) = \sum_{i=1}^{n} f(SVM(n)), \tag{13}$$

where $SVM(n)$ denotes the maximum constant time function of SVM.

It can be observed from Figure 7 that number of iterations is limited to 100 at outer loop and for varying iterations time complexity of SVM is plotted and compared with existing algorithm [2]. As a comparative analysis the proposed method performs better as constant time period is achieved at iteration number 50 for a period of 1.6 seconds. But with the same big O complexity existing method can be able to achieve O(1) at iteration of 80 and the time complexity is observed to be 2.8 seconds which indicates that much long time is needed for achieving speed advancement.

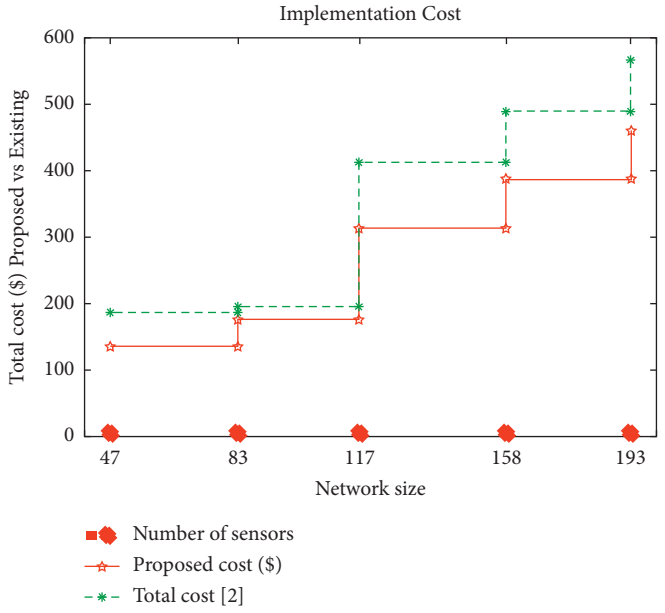

Figure 6: Comparison of total cost ($).

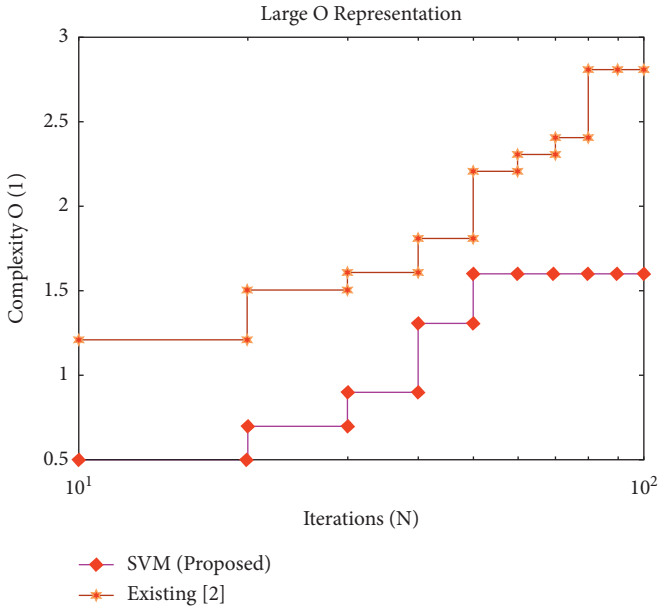

Figure 7: Time complexity of SVM.

5. Conclusions

The concept of cyber twin for industrial applications is analyzed as a triobjective case study for improving life time of application components which is highly useful to the society where a new projected design model will provide much easy way for users to create real time twins using a physical entity. This type of decision making approach will route a path to realistic implementation in future appliances as all business people can communication in real time thus improving the economic benefits within short span of time. Although more advantageous process is introduced in communicating fields with cyber twin it is necessary to have an additional security for end-to-end business applications; thus the data is transferred as separate blocks. Also, the physical entity which is used for assimilation with equipment is termed as sensor which can be distinctively identified using an authentication or encrypted key. Further, the system model is combined with SVM algorithm where accurate processing of cyber twin and blockchain technologies transpires. After observing several design issues a triobjective case study is performed under four different scenarios where the entire predesigned prototype is tested using Node MCU and all tested data have been stored in cloud platform using Github. By using the stored data analysis and management process, data has been

accomplished using a simulation setup where the results are plotted using MATLAB for better understanding. After observing the simulation results it has been proved that proposed model operates well for creating real twins and outperforms the existing methods at a rate of 72%. In future, the same model can be applied in real time for all medical applications to avoid emergency conditions with rapid guidance from experts by creating dark shadows. Moreover, imminent virtual representation models can be driven completely using sensors with IoT integration for maintaining optimal intervals in manufacturing industries.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] A. Hafid, A. S. Hafid, and M. Samih, "New mathematical model to analyze security of sharding-based blockchain protocols," *IEEE Access*, vol. 7, pp. 185447–185457, 2019.

[2] H. R. Hasan, K. Salah, R. Jayaraman et al., "A blockchain-based approach for the creation of digital twins," *IEEE Access*, vol. 8, pp. 34113–34126, 2020.

[3] R. Xie, M. Chen, W. Liu, H. Jian, and Y. Shi, "Digital twin technologies for turbomachinery in a life cycle perspective: a review," *Sustainability*, vol. 13, no. 5, pp. 2495–2521, 2021.

[4] M. Bevilacqua, E. Bottani, F. E. Ciarapica et al., "Digital twin reference model development to prevent operators' risk in process plants," *Sustainability*, vol. 12, no. 3, pp. 1088–1117, 2020.

[5] S. B. Elmamy, H. Mrabet, H. Gharbi, A. Jemai, and D. Trentesaux, "A survey on the usage of blockchain technology for cyber-threats in the context of industry 4.0," *Sustainability*, vol. 12, no. 21, pp. 9179–9219, 2020.

[6] E. F. Jesus, V. R. L. Chicarino, C. V. N. De Albuquerque, and A. A. d. A. Rocha, "A survey of how to use blockchain to secure internet of things and the stalker attack," *Security and Communication Networks*, vol. 2018, pp. 1–27, 2018.

[7] Y. S. Rao, A. K. Rauta, H. Saini, and T. C. Panda, "Mathematical model for cyber attack in computer network," *International Journal of Business Data Communications and Networking*, vol. 13, no. 1, pp. 58–65, 2017.

[8] D. K. Saini, "Cyber defense: mathematical modeling and simulation," *International Journal of Applied Physics and Mathematics*, vol. 2, no. 5, pp. 312–315, 2012.

[9] A. Moser, C. Appl, S. Brüning, and V. C. Hass, "Mechanistic mathematical models as a basis for digital twins," *Advances in Biochemical Engineering*, vol. 176, pp. 133–180, 2020.

[10] L. V. Massel and A. G. Massel, "Development of digital twins and digital shadows of energy objects and systems using scientific tools for energy research," *E3S Web of Conferences*, vol. 209, p. 02019, 2020.

[11] A. El Saddik, "Digital twins: the convergence of multimedia technologies," *IEEE MultiMedia*, vol. 25, no. 2, pp. 87–92, 2018.

[12] R. Stark, C. Fresemann, and K. Lindow, "Development and operation of Digital Twins for technical systems and services," *CIRP Annals*, vol. 68, no. 1, pp. 129–132, 2019.

[13] F. Tao, Q. Qi, L. Wang, and A. Y. C. Nee, "Digital twins and cyber-physical systems toward smart manufacturing and industry 4.0: correlation and comparison," *Engineering*, vol. 5, no. 4, pp. 653–661, 2019.

[14] J. Szpytko and Y. Salgado Duarte, "A digital twins concept model for integrated maintenance: a case study for crane operation," *Journal of Intelligent Manufacturing*, vol. 32, no. 7, pp. 1863–1881, 2020.

[15] C. Mandolla, A. M. Petruzzelli, G. Percoco, and A. Urbinati, "Building a digital twin for additive manufacturing through the exploitation of blockchain: a case analysis of the aircraft industry," *Computers in Industry*, vol. 109, pp. 134–152, 2019.

[16] A. Saad, S. Faddel, and O. Mohammed, "IoT-based digital twin for energy cyber-physical systems: design and implementation," *Energies*, vol. 13, no. 18, p. 4762, 2020.

[17] A. A. Akanmu, C. J. Anumba, and O. O. Ogunseiju, "Towards next generation cyber-physical systems and digital twins for construction," *Journal of Information Technology in Construction*, vol. 26, no. June, pp. 505–525, 2021.

[18] P. Radanliev, D. De Roure, R. Nicolescu, M. Huth, and O. Santos, "Digital twins: artificial intelligence and the IoT cyber-physical systems in Industry 4.0," *International Journal of Intelligent Robotics and Applications*, no. 1, 2021.

[19] S. Juneja, M. Gahlan, G. Dhiman, and S. Kautish, "Futuristic cyber-twin architecture for 6G technology to support internet of everything," *Scientific Programming*, vol. 2021, pp. 1–7, 2021.