

RESEARCH ARTICLE

A Zero-Trust Network-Based Access Control Scheme for Sustainable and Resilient Industry 5.0

KHALED ALI ABUHASEL 

Mechanical Engineering Department, Industrial Engineering Program, College of Engineering, University of Bisha, Bisha 61922, Saudi Arabia

e-mail: kabuhasel@ub.edu.sa

This work was supported by the Deanship of Scientific Research, University of Bisha, through the Fast-Track Research Support Program.


ABSTRACT This new era of the industry is characterized by the integration of artificial intelligence and the Internet of Things (IoT) to optimize production processes. To ensure sustainability and continuous industrial performance, Industry 5.0 integrates automated technology, robots, humans, and others. This modern paradigm relies on data and high-level security to achieve sustainability and error-free production operations. For improving the resilience of Industry 5.0 through adversary mitigation, this manuscript introduces a Zero-Trust Network-based Access Control Scheme (ZTN-ACS). This scheme extends its remote and limitless support for managing, monitoring, and controlling devices and operation schedules. For its limiting network over the available controllers, deep learning aids access control. The industrial controller output over the defined access is verified for efficiency and consistency compared to the expected and previous production outputs. In the verification scheme, access interrupts the controllers, and the schedules are initiated using the learning paradigm. This learning process considers the achievable production outcome and the low or high variations in the current access-based output. Therefore, the access control and security features are extended depending on the learning output over the adversaries. This scheme leverages consistency and reduces controller denials, failures, and false positives in Industry 5.0.

INDEX TERMS Access control, deep learning, Industry 5.0, zero-trust.

I. INTRODUCTION

Industry 5.0 mostly uses robots and smart machines for working and manufacturing. Industry 5.0 reduces the workload of laborers, which enhances the production range of the companies [1]. Industry 5.0 faces various issues and problems while performing tasks. Various security features and functionalities are used in Industry 5.0 [2]. Human-centricity, sustainability, and resiliency are the three fundamental principles of Industry 5.0. These principles aim to create an intelligent manufacturing system that prioritizes the rights to privacy, autonomy, and human dignity. Industry 5.0 is also able to adapt to adverse situations and reduce environmental impacts. Industry 5.0 seeks to balance technological advancements with social and environmental responsibility. Industry 5.0 has three main pillars: sustainability, human-centricity,

and resilience, as shown in Fig. 1. Cyberattacks are the main problem that occurs in every industry. Issues such as unauthorized authentication and access problems are faced by smart industries [3]. A cyber-attack security policy is used to solve issues in industries. The actual cyberattacks are detected, which also identifies the exact cause of the issues [4]. The cyberattack policy provides feasible solutions that enhance the efficiency of smart industries. The Internet of Things (IoT) is also used for security policies [5]. A human-centric solution based on IoT is implemented in industries to reduce the challenges. The human-centric solution analyzes the issue and produces optimal features to solve the problems. IoT identifies the exact interaction details that are communicated among the software [6], [7]. Zero trust network access (ZTNA) is an information technology (IT) security solution. ZTNA provides remote access solutions to solve issues in organizations. ZTNA connects the users without transmitting data, which reduces the latency

The associate editor coordinating the review of this manuscript and approving it for publication was Zhangbing Zhou .

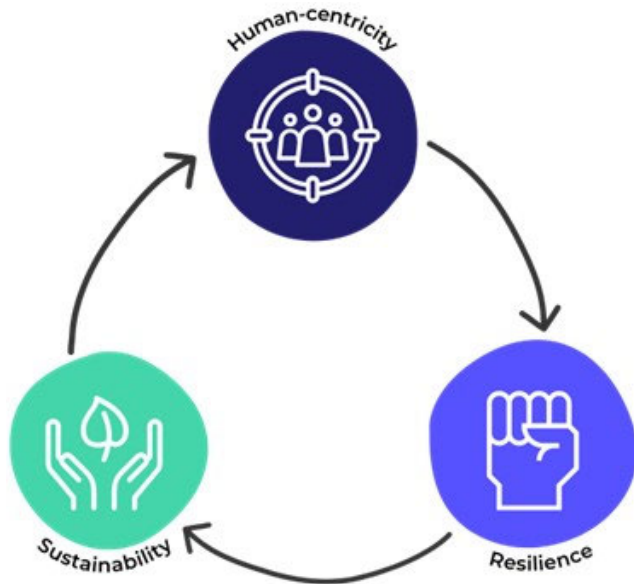


FIGURE 1. Industry 5.0 features [1].

in the computation process [8]. ZTNA is used in Industry 5.0, which enhances the efficiency and security level of organizations [9]. The ZTNA-based security framework is used to organize and access the network. ZTNA provides effective authorization and authentication services to users in industries [10]. The ZTNA security framework detects the management issues that are presented in Industry 5.0. ZTNA provides a secure authentication policy that prevents third-party members from accessing the network [11]. ZTNA-based applications are also used in Industry 5.0. Industrial Internet of Things (IIoT)-enabled applications are commonly used to enhance the effectiveness of the manufacturing process [12]. The ZTNA achieves high accuracy in security prediction and detection processes. The ZTNA application provides necessary services that minimize both time and energy consumption levels in production processes [13].

Security feature verification is a process that verifies the exact security features for Industry 5.0. Security feature verification is a crucial task to perform in every organization and application [14]. Deep learning (DL) is commonly used for the detection and prediction processes. The main aim of DL is to improve prediction accuracy, which reduces the latency in the identification process [15]. DL-based security feature verification methods are used in Industry 5.0. Deep reinforcement learning (DRL) algorithm-based verification methods are widely used [16]. The DRL algorithm uses a feature extraction technique that extracts the important features. The extracted data produces optimal information for the security feature verification process [17]. The DRL algorithm maximizes the accuracy of security feature verification, which ensures the safety level of industrial data. A lightweight deep learning model is also used for the security feature

verification process [12], [15]. The DL model uses the convolutional neural network (CNN) algorithm to recognize the exact features for the verification process [16]. The CNN algorithm minimizes energy consumption in the computation process, which reduces the complexity of verification services. The DL model improves the overall performance and efficiency of Industry 5.0 [18]. The key contributions of this work are as follows:

- Designing a secure access control scheme for industrial controllers that confronts interrupts and adversaries for consistently scheduled outputs.
- Identifying the controller schedule outputs for their variations and providing defined access through deep learning assessments.
- Performing a data and metric-based analysis for validating, verifying, and confirming the proposed scheme's performance.

The rest of the paper is organized as follows: Section II presents the state-of-the-art related to access control, and zero trust in industries. In Section III, some preliminaries and system models are presented. This section presents the proposed zero trust network access scheme (ZTN-ACS) and its analysis. Section IV presents the simulation results and performance evaluation. Finally, a conclusion is presented in Section V.

II. RELATED WORKS

Xu et al. [19] have presented an anonymous authentication and dynamic group key agreement scheme for Industry 5.0. The main aim is to secure the data from third parties, which enhances the performance level of the applications. Both blockchain and time-sensitive token mechanisms are used in the scheme to validate the authentication process. The presented work improves the energy efficiency of the industries. While into another work by Xu et al. [20] have presented a transmit antenna selection (TAS)-based secrecy scheme for Industry 5.0. The proposed scheme is mainly used to predict the exact secrecy performance level of Industry 5.0. An amplify-and-forward (AF) relaying technique is used here to transmit the relevant data for the tasks. Maximizes the accuracy of the prediction process. In another work by, Zhang et al. [21] where authors have presented a new framework for the construction of knowledge-sharing intelligent machine tool swarms. The main aim of the framework is to provide an explicit tool for Industry 4.0. The multi-access edge computing (MEC) technique is implemented in the framework to identify the key values for the sharing process. The proposed scheme increases the effectiveness ratio of the industries.

Murphy et al. [22] have proposed a new strategy to highlight the ethical personalization of smart human-centered Industry 5.0. The actual goal is to identify the behavioral aspects of personalization. The actual concerns and ethics are detected for further processing. The strategy maximizes

the privacy and security range of the industries. In another work by Shijie and Yingfeng [23] where authors have proposed a credit-based dynamical evaluation method for manufacturing services (MS). This method provides effective security services to organizations. The IIoT is used here for communication services. The proposed method reduces the computational cost of performing tasks in industries. While Fang et al. [24] have proposed a Gaussian distribution-based comprehensive trust management system (GDTMS) for fog computing-enabled industrial wireless sensor networks (F-IWSN). The main aim is to provide trust services to the users. Trust management-based secure routing schemes are also provided to F-IWSN. The proposed system promotes the significance level of F-IWSNs. In Cui et al. [25] work, where authors have presented an anonymous access control scheme for edge enabled IIoT systems. The authors have introduced a scheme that secures the user's privacy during the authentication process. Attribute-based encryption (ABE) is used in the scheme to ensure the security range of the systems, which improves the performance and efficiency level of IIoT systems.

Qi et al. [26] have presented an efficient data access control scheme for data protection in the cloud assisted IIoT. The proposed scheme is used as a fine-grained access control policy in IIoT. The ABE protocol is used here to improve the safety level of the systems. The presented scheme reduces the data loss ratio, which improves the effectiveness of IIoT. In another work by, Zhao et al. [27] where authors have presented a secure edge computing scheme for artificial intelligence (AI)-driven IIoT. The main goal is to improve the flexibility ratio of the systems. In this work, the authors have presented an optimization scheduling algorithm for the optimization process that increases the overall performance range of AI-driven IIoT. While Fröhlich et al. [28] have developed a secure Industrial Internet of Things gateway architecture-based trust execution environment. Both information technology (IT) and operational technology (OT) are performed in the gateway execution process. A machine learning algorithm is used here for resource scheduling and allocation processes. The developed strategy secures the IoT domain and reduces the latency in performing tasks. The developed strategy improves the security level of the IIoT.

Liu et al. [29] have proposed a deep reinforcement learning (DRL) algorithm-based security policy for IIoT. The main purpose of DRL is to identify the threats and problems that are faced by the IIoT. The DRL algorithm also produces optimal solutions to solve the problems, which reduces the complexity of the IIoT systems. The proposed DRL-based security policy ensures the safety and privacy of users in IIoT systems. Shuai et al. [30] have developed a secure authentication scheme using the Rabin cryptosystem for the IIoT. The Rabin cryptosystem analyzes the key values that are required for the authentication process. The proposed scheme trains the datasets that secure

the data in the IIoT. The developed scheme is used as a privacy-protection scheme that reduces the error ratio in the authentication process. Experimental results show that the developed scheme maximizes the security level of users during the authentication process. While Ali and Khan [31] have introduced a new feature-oriented evaluation framework for secure authentication in the IIoT. A graph theory matrix (GTM) approach is implemented in the framework to evaluate the best authentication process. The actual authentication features are identified from the database, which minimizes the latency in the computation process. The introduced framework enhances the security level via authentication in IIoT systems. In the work by Tariq et al. [32], where authors have designed a context-aware autonomous security for the IIoT. The actual goal is to identify the risks that have occurred in IIoT. A convolutional neural network is used here for the risk evaluation process in IIoT. The designed security measures the protection policies which improves the prevention process in IIoT systems. The designed method maximizes the accuracy of vulnerability assessment, which enhances the performance range of IIoT-enabled systems. Rafique et al. [33] have developed an efficient, secure, and certificateless protocol for the IIoT. A secure authentication key agreement scheme is used in the protocol. The developed protocol is used to identify the attacks that occurs during the authentication process. The developed protocol provides effective services for legitimate users to access the device via remotes. When compared with other protocols, the developed protocol maximizes the safety of users from third parties. While Wu and Ansari [34] have proposed a blockchain-based method for the trust evaluation process in the IIoT. The actual key values are identified, which produce optimal information for the authentication and authorization processes. The blockchain technique is mainly used here to reduce the energy consumption level in the evaluation process. The proposed method achieves high accuracy in evaluation, which enhances the efficiency level of the systems. In another work, Khan and Alghamdi [35] have designed a robust security model for attack detection in the Industrial Control System (IICS). The designed model is mostly used in intrusion detection systems (IDS), which detect attacks in IICS. A deep autoencoder is used in the model to predict attacks based on failures and priorities. The designed model improves the accuracy of the attack detection process.

This article addresses the interruption problem in scheduling industrial operations through 5.0 technological paradigms. The issues in job allocation and its denial by the remotely operated controllers are mitigated through verification based on consistency and sustainability. Different from the methods discussed above, the proposed scheme focuses on variations in consistency and sustainability from the previous production outputs. The continuous and discrete production outcomes are accounted for this purpose, which is robust against different interrupts.

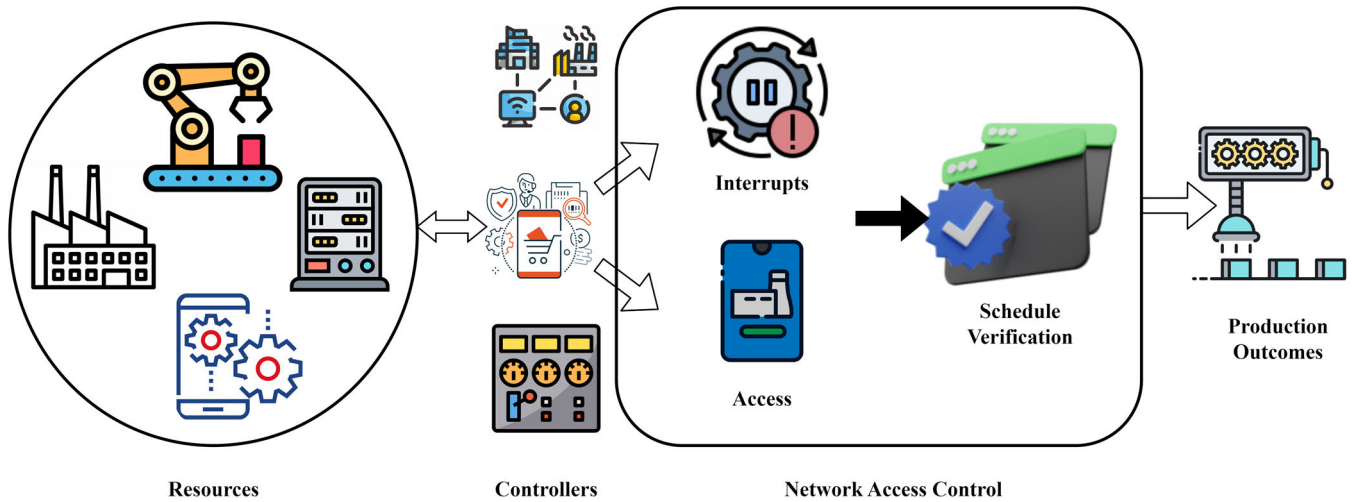


FIGURE 2. ZTN-ACS illustration.

III. ZERO-TRUST NETWORK-BASED ACCESS CONTROL SCHEME

The proposed access control scheme is designed to regulate the operations of the device controllers employed in Industry 5.0.

In the Industry 5.0 scenario, different controllers are used to achieve error-free production operations and sustainability in smart industries through intelligent controllers. The intelligent controller devices are a combination of software and hardware items used to gather and analyze the data accumulated from Industry 5.0. The intelligent controllers in smart industries are equipped with multiple sensing units to process and maintain data and high-level security to reduce adversaries using ZTN-ACS. This observed data from Industry 5.0 is exploited for verifying the access interrupts over the controllers for scheduling reliable production using the deep learning paradigm. In the proposed scheme, precise smart industry data assessment and high-level security maintenance are processed using the recommendations of the access controls. Fig. 2 presents a high-level view of the proposed scheme.

Industry 5.0 consists of different centralized controllers that regulate the functions of devices through access controls. The function of the controllers is to manage, monitor, control, and schedule operations using deep learning. The ZTN-ACS operates between Industry 5.0 and the control unit to achieve maximum sustainability and consistent industrial performance. The ON (or) OFF of the smart industrial devices is controlled by the controllers, where production schedule verification, intelligent decisions, and limitless support are made. In smart industries, the intelligent decision to control the devices is pursued by verifying the consistency and efficiency of the defined access. The defined access over the industrial controller output is processed by verifying the expected consistency and efficiency are compared with the previous production outcome to ensure that a high

TABLE 1. Symbols and description.

Symbol	Description
SMI_d	Smart device data instances
CON_n	Set of controllers
con^*	Active controllers
e^{sust}	Sustainability factor
c^{const}	Consistency factor
$AC_{ctrl_{min}}$	Min. access control requests
$AC_{ctrl_{max}}$	Max. access control requests
PPO^*	Production output instances
$N(AC_{ctrl})$	Normalized access control requests
Std_{Ac}	Standard defined access control limit
α_D	Number of adversaries detected
ρ_{Ac}	Probability of access control
Δ	Abnormality factor
M_{Int}	Delta measuring instances
\exists_1, \exists_2	Deep learning inputs
V	Output sequences
$F\{.\}$	Access function
$\rho_{\exists_2}, \rho_{\exists_1}$	Probability of scheduled operations
Q	Sequence after $F\{.\}$
ϑ^θ	Verification schedule factor

production is achievable. The input from Industry 5.0 is processed by the number of controllers CON_n and then appropriate production is scheduled to improve sustainability and consistency of industrial performance. Hence, the proposed scheme is designed into two segments, namely access control and operation schedule. Table 1 presents list of important symbols and their descriptions used in the modeling.

A. ZERO-TRUST NETWORK-BASED ACCESS CONTROL SCHEME

The deployed controllers are responsible for regulating the devices in Industry 5.0 in different scenarios. The input data can be of any type related to robots, technologies, and humans, etc. For this instance, the smart industrial data

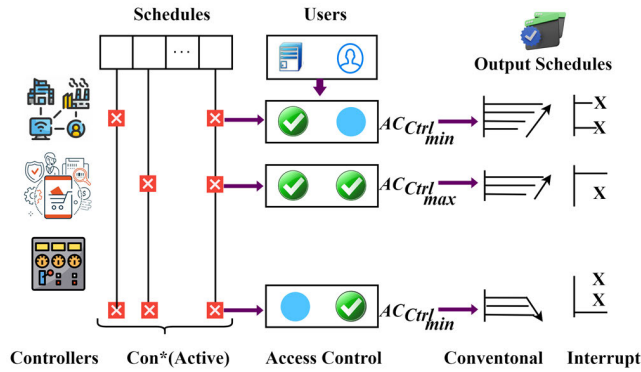


FIGURE 3. Controller functions.

received from the controllers (SMI_d) is computed as in equation (1)-(3).

$$SMI_d = \frac{(AC_{ctrl_{max}} - AC_{ctrl_{min}})}{CON_n} + t(\alpha_D) \quad (1)$$

$$\epsilon^{sust} = \frac{1}{\sqrt{3\pi} \left[\frac{(AC_{ctrl_{min}} - con^*)}{(AC_{ctrl_{max}} - CON_n)} \right]} \quad (2)$$

$$C^{const} = \frac{SMI_d}{PPO^*} - \alpha_D \quad (3)$$

where, con^* are the active controllers in Industry 5.0 then $con^* \in CON_n$ based on the data and high-level security is managed for performing error-free production operations in different periods t . The variables $AC_{ctrl_{min}}$ and $AC_{ctrl_{max}}$ represent minimum and maximum access control observed in different instances in the smart industry. The variable ϵ^{sust} and C^{const} used to denote the sustainability and consistency of industrial performance which is computed with previous production outcome PPO^* . The conventional and interrupt-based controller functions are shown in Fig. 3. The controller operations are responsible for defining consecutive schedules for PPO^* . This relies on con^* and the timed controllers in the previous schedules. Based on the active con^* , the $AC_{ctrl_{min}}$ or $AC_{ctrl_{max}}$ are classified.

The classification provides different output schedules for maximizing further PPO^* . If the schedules are interrupted, then new controllers with improved AC_{ctrl} are assigned for PPO^* (Refer to Fig. 3).

The sustainability is verified as the number of adversaries detected α_D in particular controllers. In this case, some interrupts can be occurred in SMI_d due to physical and operational problems of controllers in Industry 5.0. Therefore, this identified access interrupts the impact SMI_d at any sequence. Therefore, the normalization of access control is performed as shown in equation (4):

$$\mathcal{N}(AC_{ctrl}) = \frac{M_{Int} \cdot t}{(AC_{ctrl_{min}} - Std_{Ac})^2} \quad (4)$$

where,

$$Std_{Ac} = \frac{1}{CON_n} \sqrt{\frac{1}{con^* - 1} \sum_{t=1}^{CON_n} (SMI_d - PPO^*)^2} \quad (5)$$

In equation (4)-(5), the normalization of AC_{ctrl} requires the maximum interrupts M_{Int} and the standard access Std_{Ac} observed from the Industry 5.0 controllers. Here, the Std_{Ac} is a normalized measure instead M_{Int} is the abnormal measure for which the accurate and appropriate function is performed using the zero-trust method. From the SMI_d and $\mathcal{N}(AC_{ctrl})$, the sequence of abnormality Δ relies on current access and interrupts in Industry 5.0 is estimated as shown in equation (6):

$$\Delta(SMI_d, \mathcal{N}(AC_{ctrl})) = \begin{cases} \left[\frac{\mathcal{N}(AC_{ctrl})}{SMI_d} \right]_2^2 \\ \left[\frac{\mathcal{N}(AC_{ctrl})}{SMI_d} \right]_2 \\ \vdots \\ \left[\left(1 - \frac{PPO^*}{SMI_d}\right) M_{Int} \right]_{con^*}^2 \end{cases} \quad (6)$$

Equation (6) verifies the abnormality in a sequence until the controllers are active in monitoring and managing devices.

In the handling of the current data, the controller depends on the access interrupts until which the smart industry requires operation schedules. Based on the instance, the abnormality in Industry 5.0 is analyzed using the learning paradigm for time. In this scenario, the observed information from the industry 5.0 is to be converted into controls for appropriate operation schedules at the time of production. Controls must be shared in accurate periods to increase the synchronized working of all the devices in Industry 5.0. Besides, the shared access control and its limitless support are instantaneous to meet the user demands. Therefore, the deep learning paradigm like the zero-trust method is used for ϵ^{sust} and C^{const} assessment. The zero-trust method output is to identify and segregate the access interrupts over the controllers through SMI_d computation and PPO^* based training for achieving high sustainability and error-free production operations. The first step of this deep learning paradigm is the sequence of SMI_d , if high ϵ^{sust} and C^{const} is observed in the current access-based output. The error-free production operation is achieved through $\left(1 - \frac{PPO^*}{SMI_d}\right) M_{Int}$ from the previous production outputs for identifying the access interrupts. For this purpose, two types of SMI_d is handled at different time instances as \exists_1 and \exists_2 , which is serving as the input for deep learning. For ϵ^{sust} and C^{const} assessment, these input sequences are modeled as shown in equation (7):

$$\exists_1 + \exists_2 = SMI_d, \quad (7a)$$

$$\exists_1 + \exists_2 = \mathcal{N}(SMI_d) + \frac{Std_{Ac}}{M_{Int}} \quad (7b)$$

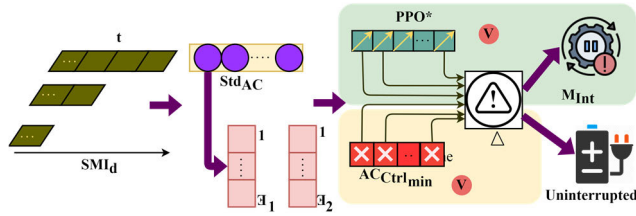


FIGURE 4. Variation detection in consecutive schedule inputs.

Equation (7a) is for initial or first instance of input analysis while as consecutive input analysis is performed using equation (7b). The access interrupt over the controllers and the schedules are initiated from the sequence of input data analysis with the first training performed as SMI_d . In this instance, if the expected production outcome is achieved in any instance, low or high variations are observed. The variation detection in the consecutive schedule input sequence is diagrammatically illustrated in Fig. 4.

The $SMI_d \in t$ requires Std_{Ac} such that $\exists_1 + \exists_2$ assimilation generates PPO^* and $Ac_{ctrl_{min}}$ variations. Therefore PPO^* with M_{Int} generates a sequential V whereas $Ac_{ctrl_{min}} \in \Delta$ generates uninterrupted sequences. Therefore, for a continuous operation and schedule outputs, the V detection after the first sequence is analyzed. The end of this analysis is the ϵ^{sust} and C^{const} using deep learning paradigm for $Ac_{ctrl_{min}}$ and $Ac_{ctrl_{max}}$ as shown in Fig. 4.

For instance, the consecutive $\exists_1 + \exists_2 = \mathcal{N}(SMI_d) + \frac{Std_{Ac}}{M_{Int}}$ is addressed for unleashing the abnormal instances over the controllers. The deep learning paradigm consists of two segments such as interrupts, and access followed by the industrial controller output. The sustainability and consistent industrial performance and its associated operations are processed by the learning paradigm. Therefore, this sequential industrial function is computed as shown in equation (8) and (9):

$$F \{ \epsilon^{sust}(SMI_d, \mathcal{N}(Ac_{ctrl})) \} = \exists_1.In - \exists_2.SMI_d - In.SMI_d.V \quad (8)$$

such that,

$$\left. \begin{aligned} \exists_1(In | SMI_d) &= \psi(SMI_d + V.In) \\ &\text{and} \\ \exists_2(SMI_d | M_{Int}) &= \psi(\exists_1 - V.In) \end{aligned} \right\} \quad (9)$$

where In is the access interrupt identified over the controllers and V is the low or high variations detected by mapping \exists_1 and \exists_2 with In for achieving error-free production outcomes. Based on equation (9), $\exists_1(In | SMI_d)$ and $\exists_2(SMI_d | M_{Int})$ are the schedule operations that are verified for satisfying the constraint $F \{ \epsilon^{sust}(SMI_d, \mathcal{N}(Ac_{ctrl})) \}$. If ψ used to indicate the schedule verification. From the defined access is pursued by verifying the efficiency and consistency, the abnormality function satisfies either $\exists_1(In | SMI_d)$ or $\exists_2(SMI_d | M_{Int})$ using the zero-trust method-based ($SMI_d = V.In$) and ($\exists_1 \neq V.In$). The comparison of expected and previous production outputs for the available controllers, the efficiency and consistency of the defined access generate the linear

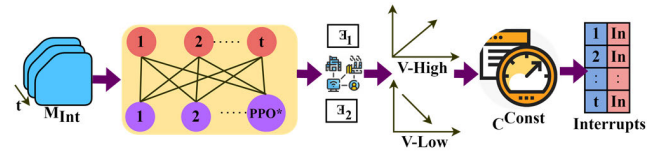


FIGURE 5. Deep learning process for consistency verification.

output of $\exists_1 \neq \exists_2$ is to satisfy the schedule operation verification. As per the abnormality identified instances of $\exists_1(In | SMI_d)$ and $\exists_2(SMI_d | M_{Int})$, the non-linear computation of M_{Int} and $\mathcal{N}(Ac_{ctrl})$ jointly produces the output $F \{ \epsilon^{sust}(SMI_d, \mathcal{N}(Ac_{ctrl})) \}$ for production time interval at its nearest possible efficiency and consistency. In this manner, the deep learning for the zero-trust method follows $\exists_1, \exists_2 \epsilon^{sust}(SMI_d, \mathcal{N}(Ac_{ctrl}))$ followed by the access control and security features for identifying adversaries through PPO^* and M_{Int} . Consistency in PPO^* is analyzed using deep learning as illustrated in Fig. 5.

The M_{Int} serves as the input for identifying $In \in t$ in either \exists_1 or \exists_2 . Based on the available PPO^* , the V (high or low) is classified; if the C^{const} is observed (same as PPO^*) then variations are suppressed by scheduling an idle controller. This is required for interactive C^{const} maintenance without preventing PPO^* retention. Therefore, the interrupts are suppressed for the high $C^{const} \forall M_{Int}$ (Refer to Fig. 5). As illustrated in the initial and sequential instances of this scheme extending its remote accessibility and limitless support for controlling devices and precise operation schedules, the schedule verification using the training is validated. In this first instance, the access interrupt is defined, and therefore ($M_{Int} = Std_{Ac}$) = 0 is the learning output observed for the instance and hence, the expected production outcome of SMI_d is retained without abnormality or adversaries. Instead, the sequential instances vary and the variations are identified in the current access-based outputs using the constraints $\exists_1(In | SMI_d)$ and $\exists_2(SMI_d | M_{Int})$ that impacts the training set. Therefore, the access interrupt occurrence in the industrial performance is either $\exists_1(In | SMI_d)$ or $\exists_2(SMI_d | M_{Int})$ is achieved. In particular, the serving inputs of \exists_1 and \exists_2 is classified based on access control and safety features such that the probability of function degradation is which is assumed to be 0.5 for the current industrial performances. Based on this instance, the low or high variations in V , where $V > \frac{Std_{Ac}}{M_{Int}}$ or $V \leq \frac{Std_{Ac}}{M_{Int}}$ is verified for maximizing production outcomes. Using equation (10), the identified variations and their limiting network of \exists_1 and \exists_2 mapping to In is verified as shown in equation (10).

$$\left. \begin{aligned} V &= 1 - \frac{\rho_{\exists_2}}{\rho_{\exists_1}} \\ &\text{and} \\ \text{if } \exists_1(In | SMI_d) \text{ maps to } SMI_d, \quad V &> \frac{Std_{Ac}}{M_{Int}} \\ \text{else} \\ \exists_1(In | SMI_d) \text{ maps to } Std_{Ac} \text{ or } M_{Int}, \quad V &\leq \frac{Std_{Ac}}{M_{Int}} \end{aligned} \right\} \quad (10)$$

In the above equation (10), the variables ρ_{\exists_2} and ρ_{\exists_1} means the access control of \exists_2 and \exists_1 to the possible schedule operation verification for the instance. The verification scheme is used to address that not all access controls can be associated with both \exists_2 and \exists_1 . Therefore, the achievable production outcome and the low or high variations observed in the current access-based output for the conditions $V > \frac{Std_{Ac}}{M_{Int}}$ and $V \leq \frac{Std_{Ac}}{M_{Int}}$ is evaluated as shown in equation (11)-(12):

$$\left. \begin{aligned} In_1 &= \mathcal{N}(SMI_d)_1 \\ In_2 &= \mathcal{N}(SMI_d)_2 - \left(\frac{Std_{Ac}}{M_{Int}}\right)_1 - \left(\frac{\epsilon^{sust} + C^{const}}{con^*}\right)_1 \\ In_3 &= \mathcal{N}(SMI_d)_3 - \left(\frac{Std_{Ac}}{M_{Int}}\right)_2 - \left(\frac{\epsilon^{sust} + C^{const}}{con^*}\right)_2 \\ &\vdots \\ In_Q &= \mathcal{N}(SMI_d)_Q - \left(\frac{Std_{Ac}}{M_{Int}}\right)_{Q-1} - \left(\frac{\epsilon^{sust} + C^{const}}{con^*}\right)_{Q-1} \end{aligned} \right\} \quad (11)$$

$$\left. \begin{aligned} Ac_1 &= SMI_{d_1} - \exists_2(SMI_d | M_{Int})_1 \\ Ac_2 &= SMI_{d_2} - \exists_2(SMI_d | M_{Int})_2 - \left(\frac{\epsilon^{sust} + C^{const} - \alpha_D}{con^*}\right)_1 \\ Ac_3 &= SMI_{d_3} - \exists_2(SMI_d | M_{Int})_3 - \left(\frac{\epsilon^{sust} + C^{const} - \alpha_D}{con^*}\right)_2 \\ &\vdots \\ Ac_Q &= SMI_{d_Q} - \exists_2(SMI_d | M_{Int})_Q - \left(\frac{\epsilon^{sust} + C^{const} - \alpha_D}{con^*}\right)_{Q-1} \end{aligned} \right\} \quad (12)$$

From equations (11) and (12), the above learning paradigm output follows Q instance of sequence over the defined access where normalized measure and abnormality measure are the augmenting metrics for determining the current access-based output. Now, the adversaries are identified and verified the operation schedules for its limiting network for the conditions $V > \frac{Std_{Ac}}{M_{Int}}$ and $V \leq \frac{Std_{Ac}}{M_{Int}}$. This computation requires an appropriate production schedule to be allotted for the controllers in Industry 5.0. Here, the allocation process is for a particular data with high-level security for controlling and managing devices. The sensitive information observed from the smart industry is segregated for access and control which is processed at the time of the controller's classification. Therefore, time sensitiveness is retained through access control and safety features for achieving sustainability and consistent industrial performance. The access control is extended with the learning output over the adversaries identified by the zero-trust network in Industry 5.0.

B. OPERATION SCHEDULE VERIFICATION

In the operation schedule verification process, the different controllers-based data analysis is performed by the deep learning output to decide the appropriate production schedule of the devices in Industry 5.0.

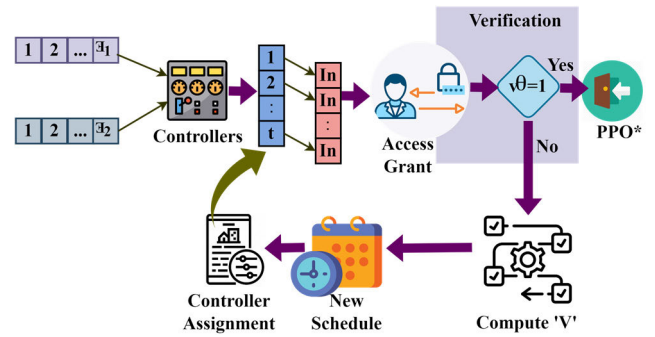


FIGURE 6. Schedule verification process.

Synchronized/periodic working of the industrial devices depends on $F\{\epsilon^{sust}(SMI_d, \mathcal{N}(AC_{ctrl}))\}$ outputs without adversaries. Assume the initial operation schedule verification $v^\theta = 0$. If $v^\theta = 1$ then the industry 5.0 devices are controlled through an access point. This sequential verification scheme relies on V and $F\{\epsilon^{sust}(SMI_d, \mathcal{N}(AC_{ctrl}))\}$ such that the probability of the access control (ρ_{Ac}) is computed as shown in equation (13):

$$\rho_{Ac} = \frac{(count(v^\theta))^{con^*} \times (\psi)^{Q-1}}{\sum_{con^* \in CON_n} (count(v^\theta))^{con^*} \times (1 - V)^{Q-1}} \quad (13)$$

In equation (13), the probability of operation schedule verification is performed to ensure that the industrial devices are remotely accessed and controlled so that the adversaries are mitigated through the zero-trust method. If $\rho_{Ac} > 0 \forall V > \frac{Std_{Ac}}{M_{Int}}$, then the count of the operation schedule is incremented by one, which means the devices are synchronously working without interrupts, else it is identified any access interrupts over the controllers. The schedule verification process is illustrated in Fig. 6.

The \exists_1 and \exists_2 probabilities are analyzed for their interrupts for providing access grants. If the $v^\theta = 1$ then PPO^* is validated for V and its consecutive schedules. If v^θ fails then new schedules for mitigating $V(\max)$ are initiated and therefore previous and new controllers are concurrently allocated for output generation (Fig. 6). The device condition is sent to the controller for scheduling operation with high efficiency and consistency. The segregation of normal and abnormal instances from the industrial performances helps to retain the accuracy of the schedule verification. This verification scheme increases the production outcome in a shortest time with less computational complexity. These access control and safety features increases the controller's performance and decreases the failures and false positives by using the zero-trust method.

C. DATA-BASED ANALYSIS

The data-based analysis is presented using ‘‘Smart Grind Power Monitoring System’’ available as open source [36]. The information is about power-generated schedules and their

TABLE 2. Data explanation-controller/attacks.

Controller ID	Description	Purpose	Schedules	Event
BR1	Breaker Controllers	Voltage/phase shift	48 in 30min duration	Tripping
BR2		Frequency Shifter	12 (2 in 1 Hour)	Command Changes
BR3		Heat Regulator	90-96 (4 in 1 Hour)	Command Changes
BR4		Turbine Monitoring	Full Day	Disabled
IR1	Intelligent Electronic Device Controllers	Distance Protection	24 (1 in 1 Hour)	Fault Intervals
IR2		Remote Access	Variable	Denials

TABLE 3. Data explanation-controller/attacks.

Controller	Schedule							
	4	8	16	20	24	28	32	36
BR1	5/3	8/4	6/3	10/8	6/3	15/12	13/10	12/8
BR2	7/3	16/7	12/10	17/9	17/13	5/3	15/12	16/16
BR3	15/10	9/3	11/9	12/6	15/4	13/7	10/9	7/6
BR4	17/9	11/6	13/13	9/5	13/7	17/13	5/4	17/13
IR1	7/5	15/6	10/3	7/4	6/5	10/0	12/4	12/5
IR2	4/3	13/10	13/4	17/12	13/9	15/14	13/6	15/15

interruption due to cloud-based attacks. The components are remotely accessible for scheduling power generation and distribution. The detailed explanation and components associated with data are presented in Table 2.

The above information is recorded for 676 entries and 496 records for 37 power generation instances. The adversary-detecting events are marked as abnormal/normal based on their occurrences. Using this information, the proposed scheme is verified for its functions discussed. The analysis of C^{const} and ϵ^{sust} is presented for the 4 breaker controllers given in the data source [36]. The maximum power generated, and interrupts faced by the breakers across 24 hours production schedule are considered. The functions, number of schedules, and the output (expected) generated are the ideal conditions for validation. If a breaker generates considerably the same power with precise neat dissipation is said to be natural. Contrarily the overlapping and non-overlapping schedules determine the PPO^* for consecutive allocations. Followed by this process the average access per production time and its success rate are presented in Table 3.

Based on the available SMI_d and Con^* , the $AC_{ctrl_{min}}$ and $AC_{ctrl_{max}}$ is determined. These two cases are inverse post the $N(AC_{ctrl})$ without M_{Int} and therefore $\exists_1 + \exists_2$ is performed. If the mapping is successful, then V minimization

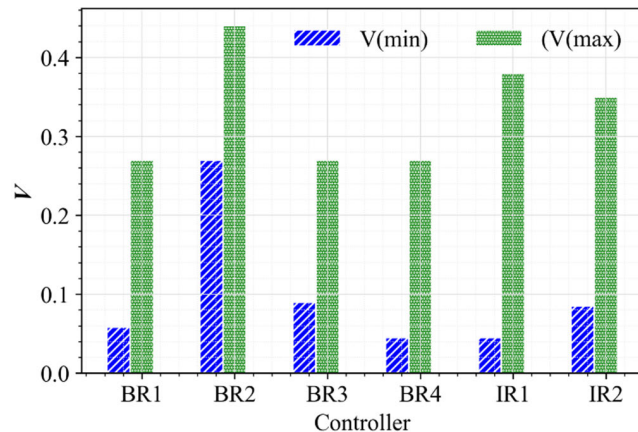
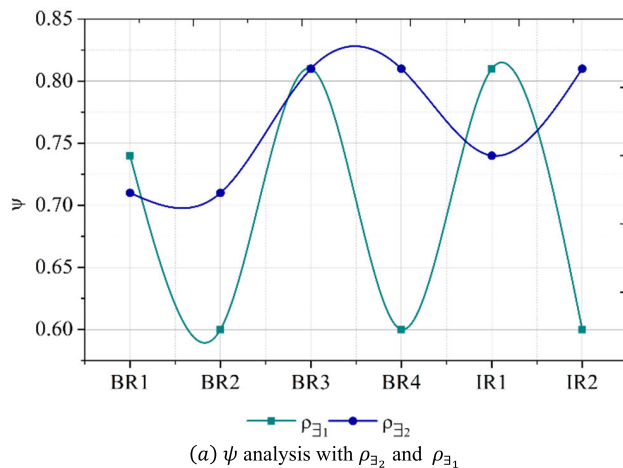
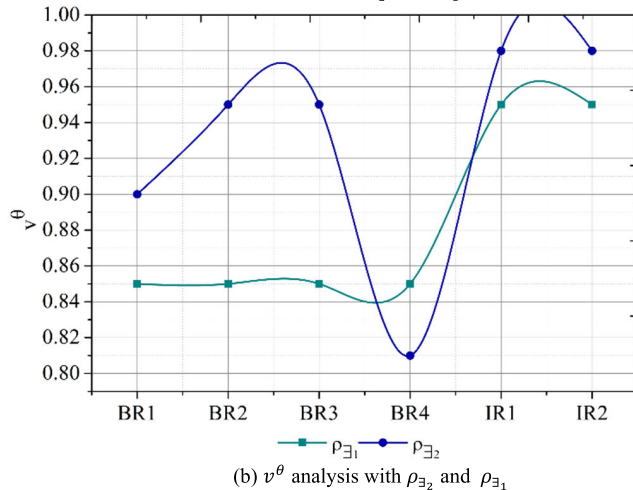


FIGURE 7. V (min and max) analysis.



(a) ψ analysis with ρ_{\exists_2} and ρ_{\exists_1}



(b) v^θ analysis with ρ_{\exists_2} and ρ_{\exists_1}

FIGURE 8. ψ and v^θ analysis.

is achievable such that Δ reduction is achieved. Therefore In_1 to In_Q and AC_1 to AC_Q are contrarily performed. This is invariable based on access grant and response through remote monitoring. Finally, the verification of controller is performed for ρ_{\exists_2} and ρ_{\exists_1} in Fig. 8. The ψ and v^θ are concurrent and invariant for ρ_{\exists_2} and ρ_{\exists_1} such that

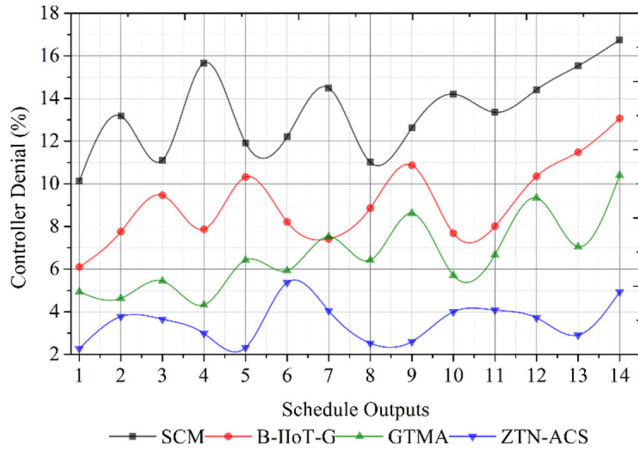


FIGURE 9. Controller denial.

the Δ identifications are high. Considerably the variations are suppressed for any M_{Int} . If the available M_{Int} is high then the controllers are re-scheduled for the rest of the PPO^* . By mapping Ξ_1 and Ξ_2 the v^θ is high and ψ is maximum as shown in Fig. 8.

IV. RESULTS AND DISCUSSION

This section presents the comparative analysis using controller denial, failure rate, false positives, access interrupt, and consistency. The schedule outputs are varied for this comparative analysis. The proposed ZTN-ACS is compared and analyzed with existing methods SCM [23], B-IIoT-G [34], and GTMA [31].

A. CONTROLLER DENIAL

The proposed access control scheme achieves fewer controller denials for securing the technologies, robots, and humans from the industrial devices. It also allows remote accessing and controlling the devices in both normal and abnormal scenario at different periods. The production operation schedule verification in Industry 5.0 is performed for preventing adversaries and controller denial. The controller output over the defined access is pursued verifying the efficiency and consistency, comparing the current achievable production outcome with the previous production outputs for verification time. Also, this identifies any variations in the network. Based on the schedule verification of both interrupts and access along with the control scheme is processed through a deep learning paradigm for preventing false positives.

The industry 5.0-based sensitive data is protected with high-level security for achieving sustainability and error-free production operations for accurate schedule verification for the available controllers without increasing the failure rate. The proposed scheme is used for adversary mitigation in Industry 5.0 and achieves less controller denial as presented in Fig. 9.

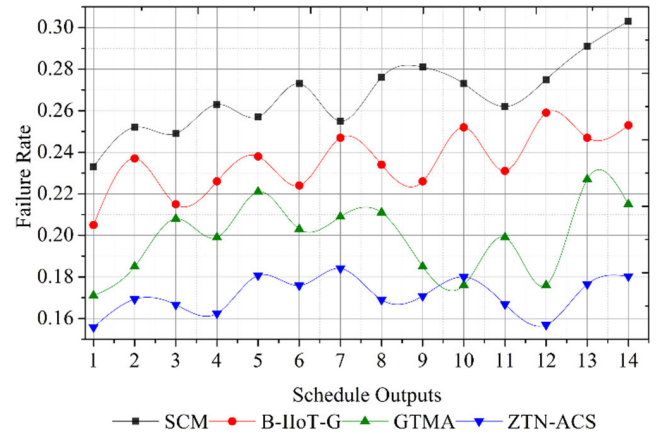


FIGURE 10. Failure rate.

B. FAILURE RATE

The presented ZTN-ACS achieves fewer failure rate for Industry 5.0 using deep learning for accurate operation schedule that is performed with limiting network as shown in Fig. 10. The proposed scheme verification and defined access verification is pursued improving the sustainability of industrial controllers without variations and adversaries.

This consideration is used for preventing failure rate using $F \{e^{sust}(SMI_d, \mathcal{N}(AC_{ctrl}))\}$ at different time intervals. The security features and access control are responsible for all the industrial devices. The schedule verification is computed for segregating the normal and abnormal instances, preventing access interrupts. The extracted security features are used for the protection of the sensitive information and its limiting network ensures schedule verification in Industry 5.0. The low or high variations are retained using deep learning for reducing false positives and failures. Therefore, access control is provided for all the devices in industries for monitoring, managing, and controlling devices through learning paradigm and security features for computing the accurate schedule verification, for which the failure rate is less in this proposed scheme.

C. FALSE POSITIVES

The proposed zero-trust method achieves fewer false positives compared to the other factors as represented in Fig. 11. The single device and use of sensitive information is secured, and proper operation schedule verification is performed through remote devices using the intelligent controllers, if e^{sust} and C^{const} assessment is less.

This production schedule is responsible for both access controls and access interrupts over the controllers by prolonging the industrial information for leveraging consistency. The schedule verification time is computed for the controller's access and interrupts which is identified per interval using the learning paradigm are again scheduled using the constraint $\Xi_1 + \Xi_2 = \mathcal{N}(SMI_d) + \frac{Std_{Ac}}{M_{Int}}$ as in equation (7). Hence, the pursued access control verification in Industry 5.0 by

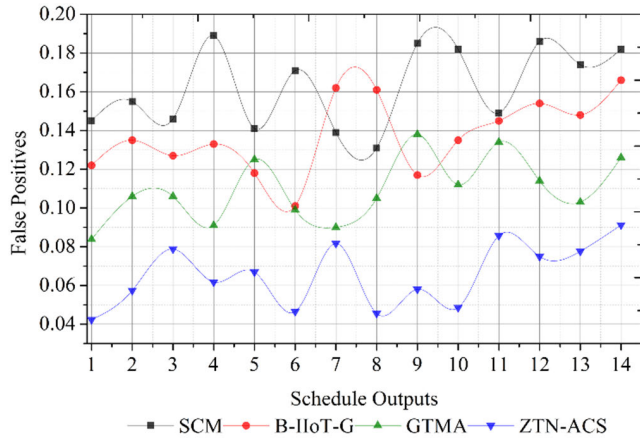


FIGURE 11. False positives.

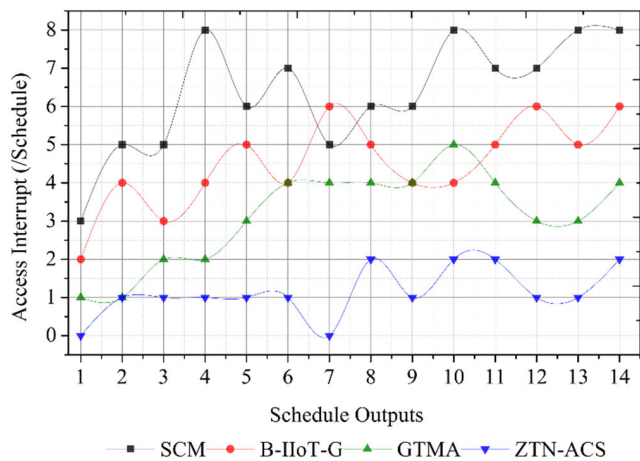


FIGURE 12. Access interrupt.

deep learning prevents false positives. This data analysis and high-level security is processed under different controllers for reducing false positives.

D. ACCESS INTERRUPT

This proposed access control scheme satisfies fewer access interrupts for protecting the industrial information using high-level security for addressing the normal and abnormal instances over the controllers.

The appropriate functions and operations are performed to improve consistency using the deep learning paradigm as shown in Fig. 12. This schedule verification is coined by deep learning for its limiting network over the controllers; it achieves less access interrupt and failure rate by estimating $\Xi_1 (In | SMI_d)$ and $\Xi_2 (SMI_d | M_{Int})$ is the schedule operations that are verified for satisfying the constraint $F \{ \epsilon^{sust} (SMI_d, \mathcal{N}(AC_{ctrl})) \}$. In this verification scheme, the access interrupts observed at the first instance are addressed due to variations in data and security features in Industry 5.0, preventing failures and complexity. This observed information from the industrial unit is protected between the

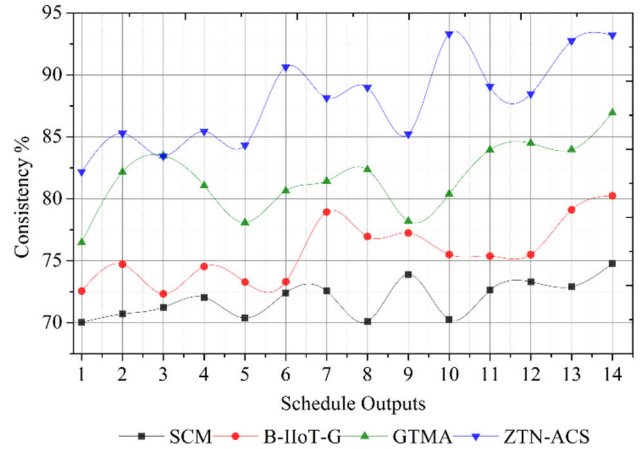


FIGURE 13. Consistency analysis.

TABLE 4. Comparative analysis.

Metrics	SCM [23]	B-IIoT-G [34]	GTMA [31]	Proposed ZTN ACS
Controller Denial (%)	16.75	13.07	10.4	4.929
Failure Rate	0.303	0.253	0.215	0.1803
False Positives	0.182	0.166	0.126	0.0912
Access Interrupt	8	6	4	2
Consistency (%)	74.79	80.25	86.94	93.214

controlling devices and security features wherein the different access interval is performed using equations (8) and (9) validation. The comparison of expected and previous production outputs over the available controllers for improving the efficiency and consistency of the defined access control, which generates the linear output of $\Xi_1 \neq \Xi_2$. Based on this verification scheme, the access interrupt is less.

E. CONSISTENCY

This proposed scheme satisfies a high consistency percentage for access control in Industry 5.0 using a deep learning paradigm with security features for securing the sensitive information using a zero-trust network for identifying the adversaries and variations (Refer to Fig. 13). The schedule verification failure and adversaries are mitigated using the learning paradigm for achieving the expected production outcome for time. The initial and sequential instance of this schedule verification extends its remote accessibility and limitless network support for controlling devices, the operation schedule is performed for training. Therefore, the Ξ_1 and Ξ_2 is classified based on access control and safety features such that the probability of function degradation is achieved in the current industrial performances. Schedule verification and variation identification are pursued by all the users and devices in Industry 5.0 using deep learning.

Therefore, the control access verification scheme is performed for augmenting the consistency and sustainability of industrial performances. Hence, the security features are also improved. From the different controllers in smart industries, the consistency percentage is high for access control. Table 3 summarizes the above comparison with the findings with state-of-the-art [23], [31], [34].

V. CONCLUSION

The next-generation Industry 5.0 paradigm requires secure access control and production consistency for economically sustainable reachability. As the major operations are remotely accessible, therefore, chances of adversary interruptions are high. For preserving the operational schedules of the controllers, this work has proposed a zero-trust network-based access control scheme. The proposed scheme provides boundaryless access control security for the controllers based on their schedules. Regardless of their overlapping or non-overlapping schedules, the outcomes based on consistency and sustainability are accounted for by security amendments. The sustainability and consistency factors are verified using the deep learning paradigm using previous outcomes. The remote access security is extended for monitoring, controlling, and allocations of schedules through persistent verifications. The verifications are performed for identifying variations that impact the production output at any interval. Considering the variations from the previous outputs, security amendments are included for preventing false rates. This scheme improves consistency by 12.55% and confined access interrupt by 11.11% compared to the existing methods in the varying outputs. Though the production sequences are continuously validated, concurrency is less supported in this scheme. Therefore, blockchain-supported access and storage control systems are planned to be fused with the proposed scheme for concurrency support.

ACKNOWLEDGMENT

The author is thankful to the Deanship of Scientific Research at University of Bisha for supporting this work through the Fast-Track Research Support Program.

REFERENCES

- [1] H. R. Chi, C. K. Wu, N.-F. Huang, K.-F. Tsang, and A. Radwan, "A survey of network automation for industrial Internet-of-Things toward industry 5.0," *IEEE Trans. Ind. Informat.*, vol. 19, no. 2, pp. 2065–2077, Feb. 2023, doi: [10.1109/TII.2022.3215231](https://doi.org/10.1109/TII.2022.3215231).
- [2] G. F. Prassida and U. Asfari, "A conceptual model for the acceptance of collaborative robots in industry 5.0," *Proc. Comput. Sci.*, vol. 197, pp. 61–67, Jan. 2022.
- [3] M. A. Khan and K. A. Abuhasel, "Advanced metameric dimension framework for heterogeneous industrial Internet of Things," *Comput. Intell.*, vol. 37, no. 3, pp. 1367–1387, Aug. 2021.
- [4] S. Huang, B. Wang, X. Li, P. Zheng, D. Mourtzis, and L. Wang, "Industry 5.0 and society 5.0—Comparison, complementation and co-evolution," *J. Manuf. Syst.*, vol. 64, pp. 424–428, Jul. 2022.
- [5] M. A. Khan and K. A. Abuhasel, "An evolutionary multi-hidden Markov model for intelligent threat sensing in industrial Internet of Things," *J. Supercomput.*, vol. 77, no. 6, pp. 6236–6250, Jun. 2021, doi: [10.1007/s11227-020-03513-6](https://doi.org/10.1007/s11227-020-03513-6).
- [6] E. G. Carayannis, J. Draper, and B. Bhaneja, "Towards fusion energy in the industry 5.0 and society 5.0 context: Call for a global commission for urgent action on fusion energy," *J. Knowl. Economy*, vol. 12, no. 4, pp. 1891–1904, Dec. 2021.
- [7] Z. A. E. Houda, B. Brik, A. Ksentini, L. Khoukhi, and M. Guizani, "When federated learning meets game theory: A cooperative framework to secure IIoT applications on edge computing," *IEEE Trans. Ind. Informat.*, vol. 18, no. 11, pp. 7988–7997, Nov. 2022.
- [8] K. A. Abuhasel and M. A. Khan, "A secure industrial Internet of Things (IIoT) framework for resource management in smart manufacturing," *IEEE Access*, vol. 8, pp. 117354–117364, 2020.
- [9] A. Mukherjee, P. Goswami, M. A. Khan, L. Manman, L. Yang, and P. Pillai, "Energy-efficient resource allocation strategy in massive IIoT for industrial 6G applications," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5194–5201, Apr. 2021, doi: [10.1109/JIOT.2020.3035608](https://doi.org/10.1109/JIOT.2020.3035608).
- [10] A. Mosteiro-Sanchez, M. Barcelo, J. Astorga, and A. Urbieto, "Securing IIoT using defence-in-depth: Towards an end-to-end secure industry 4.0," *J. Manuf. Syst.*, vol. 57, pp. 367–378, Oct. 2020.
- [11] M. Li, Z. Yin, Y. Ma, C. Wang, A. Chai, and M. Lian, "Design and verification of secure communication scheme for industrial IIoT intelligent production line system with multi-path redundancy and collaboration," *Neural Comput. Appl.*, vol. 35, pp. 13879–13893, Jul. 2023.
- [12] S. Otoum, I. A. Ridhawi, and H. Mouftah, "A federated learning and blockchain-enabled sustainable energy trade at the edge: A framework for industry 4.0," *IEEE Internet Things J.*, vol. 10, no. 4, pp. 3018–3026, Feb. 2023, doi: [10.1109/JIOT.2022.3140430](https://doi.org/10.1109/JIOT.2022.3140430).
- [13] Z. Jan, F. Ahamed, W. Mayer, N. Patel, G. Grossmann, M. Stumptner, and A. Kuusk, "Artificial intelligence for industry 4.0: Systematic review of applications, challenges, and opportunities," *Expert Syst. Appl.*, vol. 216, Apr. 2023, Art. no. 119456.
- [14] M. Golovianko, V. Terziyan, V. Branytskyi, and D. Malyk, "Industry 4.0 vs. industry 5.0: Co-existence, transition, or a hybrid," *Proc. Comput. Sci.*, vol. 217, pp. 102–113, Jan. 2023.
- [15] D. Battini, N. Berti, S. Finco, I. Zennaro, and A. Das, "Towards industry 5.0: A multi-objective job rotation model for an inclusive workforce," *Int. J. Prod. Econ.*, vol. 250, Aug. 2022, Art. no. 108619.
- [16] E. Oztemel and S. Gursev, "Literature review of industry 4.0 and related technologies," *J. Intell. Manuf.*, vol. 31, no. 1, pp. 127–182, Jan. 2020.
- [17] W. Zhang, H. Zhang, L. Fang, Z. Liu, and C. Ge, "A secure revocable fine-grained access control and data sharing scheme for SCADA in IIoT systems," *IEEE Internet Things J.*, vol. 9, no. 3, pp. 1976–1984, Feb. 2022.
- [18] D. Li, R. Chen, D. Liu, Y. Song, Y. Ren, Z. Guan, Y. Sun, and J. Liu, "Blockchain-based authentication for IIoT devices with PUF," *J. Syst. Archit.*, vol. 130, Sep. 2022, Art. no. 102638.
- [19] Z. Xu, W. Liang, K.-C. Li, J. Xu, A. Y. Zomaya, and J. Zhang, "A time-sensitive token-based anonymous authentication and dynamic group key agreement scheme for industry 5.0," *IEEE Trans. Ind. Informat.*, vol. 18, no. 10, pp. 7118–7127, Oct. 2022, doi: [10.1109/TII.2021.3129631](https://doi.org/10.1109/TII.2021.3129631).
- [20] L. Xu, X. Zhou, Y. Tao, X. Yu, M. Yu, and F. Khan, "AF relaying secrecy performance prediction for 6G mobile communication networks in industry 5.0," *IEEE Trans. Ind. Informat.*, vol. 18, no. 8, pp. 5485–5493, Aug. 2022, doi: [10.1109/TII.2021.3120511](https://doi.org/10.1109/TII.2021.3120511).
- [21] C. Zhang, G. Zhou, J. Li, F. Chang, K. Ding, and D. Ma, "A multi-access edge computing enabled framework for the construction of a knowledge-sharing intelligent machine tool swarm in industry 4.0," *J. Manuf. Syst.*, vol. 66, pp. 56–70, Feb. 2023.
- [22] C. Murphy, P. J. Carew, and L. Stapleton, "Ethical personalisation and control systems for smart human-centred industry 5.0 applications," *IFAC-PapersOnLine*, vol. 55, no. 39, pp. 24–29, 2022.
- [23] W. Shijie and Z. Yingfeng, "A credit-based dynamical evaluation method for the smart configuration of manufacturing services under industrial Internet of Things," *J. Intell. Manuf.*, vol. 32, no. 4, pp. 1091–1115, Apr. 2021.
- [24] W. Fang, W. Zhang, W. Chen, Y. Liu, and C. Tang, "TMSRS: Trust management-based secure routing scheme in industrial wireless sensor network with fog computing," *Wireless Netw.*, vol. 26, no. 5, pp. 3169–3182, Jul. 2020.
- [25] J. Cui, F. Bian, H. Zhong, Q. Zhang, S. Xu, C. Gu, and L. Liu, "An anonymous and outsourcing-supported multiauthority access control scheme with revocation for edge-enabled IIoT system," *IEEE Syst. J.*, vol. 16, no. 4, pp. 6569–6580, Dec. 2022, doi: [10.1109/JSYST.2022.3189219](https://doi.org/10.1109/JSYST.2022.3189219).

- [26] S. Qi, Y. Lu, W. Wei, and X. Chen, "Efficient data access control with fine-grained data protection in cloud-assisted IIoT," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2886–2899, Feb. 2021, doi: [10.1109/JIOT.2020.3020979](https://doi.org/10.1109/JIOT.2020.3020979).
- [27] Y. Zhao, N. Hu, Y. Zhao, and Z. Zhu, "A secure and flexible edge computing scheme for AI-driven industrial IoT," *Cluster Comput.*, vol. 26, pp. 283–301, Nov. 2021.
- [28] A. A. Fröhlich, L. P. Horstmann, and J. L. C. Hoffmann, "A secure IIoT gateway architecture based on trusted execution environments," *J. Netw. Syst. Manage.*, vol. 31, no. 2, p. 32, Apr. 2023.
- [29] X. Liu, W. Yu, F. Liang, D. Griffith, and N. Golmie, "On deep reinforcement learning security for industrial Internet of Things," *Comput. Commun.*, vol. 168, pp. 20–32, Feb. 2021.
- [30] M. Shuai, L. Xiong, C. Wang, and N. Yu, "A secure authentication scheme with forward secrecy for industrial Internet of Things using Rabin cryptosystem," *Comput. Commun.*, vol. 160, pp. 215–227, Jul. 2020.
- [31] Y. Ali and H. U. Khan, "GTM approach towards engineering a features-oriented evaluation framework for secure authentication in IIoT environment," *Comput. Ind. Eng.*, vol. 168, Jun. 2022, Art. no. 108119.
- [32] U. Tariq, A. O. Aseeri, M. S. Alkathiri, and Y. Zhuang, "Context-aware autonomous security assertion for industrial IoT," *IEEE Access*, vol. 8, pp. 191785–191794, 2020, doi: [10.1109/ACCESS.2020.3032436](https://doi.org/10.1109/ACCESS.2020.3032436).
- [33] F. Rafique, M. S. Obaidat, K. Mahmood, M. F. Ayub, J. Ferzund, and S. A. Chaudhry, "An efficient and provably secure certificateless protocol for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 18, no. 11, pp. 8039–8046, Nov. 2022, doi: [10.1109/TII.2022.3156629](https://doi.org/10.1109/TII.2022.3156629).
- [34] D. Wu and N. Ansari, "A trust-evaluation-enhanced blockchain-secured industrial IoT system," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5510–5517, Apr. 2021, doi: [10.1109/JIOT.2020.3030689](https://doi.org/10.1109/JIOT.2020.3030689).
- [35] M. A. Khan and N. S. Alghamdi, "A neutrosophic WPM-based machine learning model for device trust in industrial Internet of Things," *J. Ambient Intell. Hum. Comput.*, vol. 14, no. 4, pp. 3003–3017, Apr. 2023, doi: [10.1007/s12652-021-03431-2](https://doi.org/10.1007/s12652-021-03431-2).
- [36] *Smart Grid Monitoring Power*. Accessed: Jan. 10, 2023. [Online]. Available: <https://www.kaggle.com/datasets/bachirbarika/power-system>



KHALED ALI ABUHASEL received the B.Sc. and M.Sc. degrees in industrial engineering from the University of Central Florida, Orlando, FL, USA, in 2009 and 2010, respectively, and the Ph.D. degree in industrial engineering from New Mexico State University, Las Cruces, NM, USA, in 2012. He is currently a Professor with the Mechanical Engineering Department, University of Bisha, Saudi Arabia. He holds three U.S. patents and more than 65 publications in journals and proceedings of very reputable conferences. His current research interests include optimization, systems engineering, healthcare systems, intelligent systems, artificial neural network methodologies, and statistical analysis.

• • •