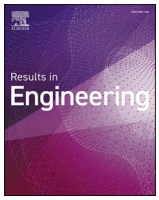
Results in Engineering 20 (2023) 101589

Contents lists available at ScienceDirect

Results in Engineering

journal homepage: www.sciencedirect.com/journal/results-in-engineering



Internet of things for smart manufacturing based on advanced encryption standard (AES) algorithm with chaotic system

Xiaoyan Huo [a,*], Xuemei Wang [b]

[a] Information Construction and Management Center, Jiaozuo University, Jiaozuo, 454003, China
[b] Academic Affairs Division, Jiaozuo Technical College, Jiaozuo, 454000, China

ARTICLE INFO

Keywords:
AES
Chaotic system
IoT
Recurrent learning
Smart manufacturing

ABSTRACT

Smart manufacturing using the Internet of Things (IoT) ensures uninterrupted and human intervention-less automation in industries for precision outcomes. As the smart manufacturing encloses chaotic systems the point of security is always demandable due to external threats. For mitigating the authorization issues in chaotic systems, a Smart Reviving Authorization Model using Advanced Encryption Standard (SRAM-AES) is designed in this article. This model is selective for chaotic systems for reviving their conventional operation cycles and preventing failures. A machine/controller's performance is monitored for its point of instability through differential access. The malicious access and its cause for controller unstableness are verified using IoT elements (remotely) and deep recurrent learning algorithms. Such identified instances are recovered by providing alternate controller recommendations from the IoT platform. In the recurrent learning process, the unstable to stable point possibilities are verified; the passing controllers are equipped with AES mitigating the previous authorizations. For a stable-functioning controller, the AES deficiency in authorization is verified in its completion cycles for consecutive production instances. Thus this model stands reliable for preventing unauthorized access, controller downtime reduction, and production failures.

1. Introduction

Device or controller authorization is a process that provides access to the devices. The authorization process verifies the identity of users using id and password. The device and controller are mainly used to monitor the performance range of the systems [1]. Ensuring the security in authentication and authorization are complicated tasks to perform in every Internet of Things (IoT) based application [2,3]. Security policies are a must in every IoT system which provides necessary services to the users. Proper authorization security schemes are used in IoT-based smart manufacturing systems [4]. A secure security framework is commonly used in smart manufacturing systems to identify threats. The security framework detects the optimal details of users during the authorization process [5]. The security framework improves the effectiveness level of authorization that reduces the complexity of the access control process [6]. A privacy-preserving scheme is also used for the authorization process. The privacy-preserving scheme verifies the information which is provided by the user for the authorization process. The privacy-preserving scheme improves the security level of devices in smart manufacturing systems [7].

Smart manufacturing systems are widely used to fulfill the demands of customers. Chaotic systems are those which does not have any rules and regulation to perform tasks that are summoned by the users [8]. A chaotic system required an optimal security scheme to ensure the safety of the systems. The security of chaotic systems is used to reduce the issues and threats that are presented in the manufacturing process [9,10]. An effective authentication policy is used to verify the identity of the users. The authentication policy provides secret keywords to the users which are used during the authentication process [11]. The authentication policy detects the similarities of keywords which reduces the difficulties in the anomaly detection process. The authentication policy reduces the latency in authentication which enhances the feasibility range of smart manufacturing systems [12]. An optimal threat detection method is also used to detect unpredictable issues in chaotic systems. The detection method provides high-quality privacy and security services to the users that improve the capabilities of smart manufacturing systems. The threats are detected based on the priorities of tasks that manage the performance level of the tasks [13,14].

Advanced encryption standard (AES) is a technology that is used to protect classified information for an application. AES is mostly

* Corresponding author.
E-mail address: xiaoyan_huo@outlook.com (X. Huo).

https://doi.org/10.1016/j.rineng.2023.101589
Received 30 June 2023; Received in revised form 1 November 2023; Accepted 10 November 2023
Available online 15 November 2023

implemented in the software to encrypt sensitive data for the systems [15]. AES-based security is used for chaotic systems in smart manufacturing. A lightweight advanced encryption standard (LAES) based method is used for the security management process in chaotic systems [16]. The LAES identifies the sensitive data and provides proper encryption keys for further processing. The LAES reduces the overall time consumption level in encryption that protect the data from attack [17]. The LAES method analyzes the content of the text which is protected for the users. A hybrid algorithm based on AES is used in chaotic systems for security purposes [18]. The hybrid algorithm identifies the unstable data which are presented in the system. The detected data is verified which ensures the safety and security range of sensitive data from third-party members. The hybrid algorithm-based AES scheme provides strong security services to the users that improve the performance level of smart manufacturing systems [19,20].

The Contributions of this study is as follows:

(1) Designing a reviving authorization model for confining unauthorized access to the smart manufacturing controllers between consecutive operation cycles.
(2) Defining the consistency of the chaotic system operation cycles for preventing unstable and unauthorized outcomes through access control and learning recommendations.
(3) Performing a comparative analysis study using definite metrics and methods from the previous works.

2. Related works

In Table 1 the results of the previous works are summarized with the key areas and the techniques used.

The smart manufacturing-assisted chaotic systems, the point of security is demandable at the time of identifying any external threats. In the smart manufacturing process, selective chaotic systems are used for reviving their conventional operation cycles and reducing failures. Smart manufacturing based on the AES algorithm is connected with chaotic systems and processed through IoT. The deficiency check and point of change are administered to prevent authorization issues and malicious access. The IoT technology ensures a stable point between the smart manufacturing industries. The operations of stable and unstable point possibilities in the IoT are used for point of change and deficiency verification for consecutive prediction instances.

3. Smart reviving authorization model using advanced encryption standard

The design goal of SRAM-AES is to improve the response rate of smart manufacturing by reducing unauthorized access in IoT-combined chaotic systems in smart manufacturing platforms. The AES authorization issues in chaotic systems are controlled using IoT experiences and various privacy measures to be suppressed for authorized and reliable operations. The proposed model is capable of maintaining controller stableness and the malicious access is identified for controller unstableness is verified using IoT elements and deep recurrent learning algorithms. The malicious access identified instances are recovered using

Table 1
Summary of results, key area, and techniques used.

Author	Method	Key areas	Technique used	Results
Tang et al. [21]	A feature management system for assembly devices.	Provide optimal trustable mechanisms and services for the users.	A permission blockchain technique is used here to control the devices.	Increases the performance range in security analysis.
Cui et al. [22]	An anonymous and outsourcing multiauthority access control scheme for edge-enabled Industrial Internet of Things (IIoT).	The main aim is to improve the overall manufacturing efficiency range of industries.	Attribute-based encryption (ABE) is used to ensure the safety of data.	Improves the effectiveness level of IIoT systems.
Cui et al. [23]	An anonymous cross-domain authentication scheme for IIoT.	It provides necessary communication and interaction services among the organizations.	Blockchain technology is used here to identify the necessary features for the authentication process.	Reduces the error rate in providing authentication services to the users.
Choi et al. [24]	An anomaly detection framework for manufacturing systems.	The actual goal is to predict the predictive maintenance risks which are presented in a system.	It is a data-driven framework that identifies the exact cause of risks.	Increases the accuracy of the anomaly detection process.
Zhao et al. [25]	A trustworthy authorization method for IIoT systems.	The aim role is to improve the security and privacy level of the systems.	Biological information is used here that provides optimal data for the authorization process.	Recognize the relevant patterns for IIoT systems.
Ferretti et al. [26]	A verifiable and auditable authorization method for IIoT.	It regulates the devices to access information in industries.	A delegation technique is used to identify the characteristics of the authorization process.	Reduces the latency in the computation process.
Demertzis et al. [27]	A new anomaly detection method for Industry 4.0.	It is a real-time detection method that identifies anomalies using autoencoders.	Deep learning smart contracts are implemented in the method to detect anomalies.	Minimizes the complexity of anomaly detection.
Kim et al. [28]	A behavioral anomaly detection framework for artificial intelligence (AI) enabled smart manufacturing systems.	The actual goal is to improve the security level of the systems.	The industrial network is used in the framework to analyze the necessary features for the detection process.	Improves the performance range of manufacturing systems.
Tang et al. [29]	Public-key encryption with keyword search (PEKS) for IIoT.	PEKS reduces the computational cost ratio in the identification process.	A lattice assumption technique is sued in PEKS to identify the risks in security issues.	Increases the accuracy of the keyword encryption process.
Fröhlich et al. [30]	Secure gateway architecture for a trusted execution environment in IIoT.	It provides relevant security policies to the users.	Operational technology (OT) and information technology (IT) are used to secure the authentication process.	Improves the performance level in the execution process.
Liu et al. [31]	Multi-gateway authentication scheme for IIoT-based systems.	It identifies the risks in complex production environments.	Blockchain technology is used in the scheme to analyze the characteristics of gateways.	Increases the security range of IIoT systems.
Cabrera-Gutiérrez et al. [32]	An efficient hardware security module (HSM) for IoT networks.	The main aim is to improve the mobility and robustness level of IoT-based systems.	A public-key encryption algorithm is implemented to improve the security mechanism of the systems.	Maximizes the effectiveness range of IoT systems.
Wu et al. [33]	A blockchain-based trust evaluation method for IIoT.	It detects the malicious users in the systems.	Blockchain technology detects the exact access control ratio of the systems.	Increases the performance range of IIoT systems.

alternate controller recommendations from the IoT platform. In Particular, the possibilities of unstable to the stable point are verified and the remaining passing controllers are equipped with AES deficiency check through IoT in its completion cycle is secured from malicious access to improve the performance of smart manufacturing. The proposed SRAM-AES design is illustrated in Fig. 1.

The operation of this proposed model is to monitor a machine/controller's performance for identifying its point of instability through differential access. If a stable to unstable point identifies, then a deficiency check is performed in its completion cycles for consecutive prediction instances instead the point of change is true in this chaotic system, and the change of controller is performed. The process of monitoring the point of instability in chaotic systems is analyzed using a deep recurrent learning algorithm. The aforementioned processes are briefly explained in the following sections.

3.1. Chaotic system setup and its process

The IoT platform is defined using two types of points namely stable and unstable. The stable point is responsible for deficiency verification and the unstable point administers monitoring and identifying malicious access and then performs point of change. The stable point communicates with a set of chaotic systems $CH^S = \{1, 2, \ldots, N\}$; the selective chaotic system is denoted as ch^s from the IoT platform. These systems are capable of changing new controllers from the IoT platform using recommendations. The chaotic system shares various quantities of data at any instance i. Let us consider MA to represent the number of malicious access that is occurred in smart manufacturing. Based on the above, the chaotic systems process P per unit of time T such that, the AES authorization $(AES_{authorz})$ is given as

$$AES_{authorz} = \begin{cases} CH^S \times P \times T \forall ch^s::i, MA = 0 \\ Rs_r \times \dfrac{CH^S - MA}{T} \forall (ch^s, MA)::i, MA \neq 0 \end{cases} \quad (1)$$

Such that,

$$\left.\begin{aligned} ch^s::i = \sum_{i=1}^{N} P_T \\ and \\ (ch^s, MA)::i = \sum_{i=1}^{N} P_T - Rs_r \sum_{i=1}^{MA} P_T \end{aligned}\right\} \quad (2)$$

where,

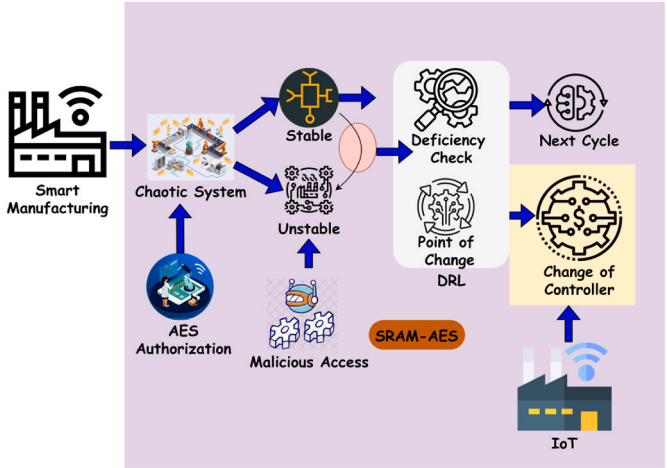


Fig. 1. Proposed SRAM-AES design.

$$Rs_r = \frac{(pr_f)_T}{(ch^s)_T + P_T} \quad (3)$$

In the above equations, the variables Rs_r and pr_f represents the response rate and prediction failure from the IoT platform. As per equation (2), the constraints $ch^s::i$ and $(ch^s, MA)::i$ used for mapping the chaotic systems process and malicious access in different instances. The initial system setup for different operation cycles is presented in Fig. 2.

The initialization process of the CH^s is determined based on P allocated in any i. Depending on the availability and controlled access the MA and completed T are performed. If $A \in S$ author is the maximum defined limit, then P completion is high and consecutive cycles are assigned in the next i. The initialized P determines the state of the CH^S provided in Rs_r is high (matching T) then it is stable and proceeds for the next i. The failing condition results in CH^S instability (Refer to Fig. 2). The AES authorization of the chaotic systems from the IoT platform is processed in two levels namely stable point and malicious access for unstable point. In the stable point identified instances, the deficiency verification and $AES_{authorz}$ are the added-up metrics for ensuring uninterrupted and human intervention-less automation in smart industries for mapping the instances achieved. For mitigating the authorization issues in chaotic systems, the unstable point was identified for the point of change and change of controller using DRL and SRAM-AES. The classification of stable and unstable point possibilities between $ch^s \in T$ and MA are processed using the chaotic systems for the timed response. Equation (1) computes the condition $MA > ch^s$ outputs in fewer authorization issues and controller downtime reduction in the IoT platform. The time-mapping for the chaotic systems and the consecutive $AES_{authorz}$ based on $ch^s::i$ and $(ch^s, MA)::i$ are the verifying conditions for classification expressed as

$$T_{MA} = \sum_{i=1}^{N} \frac{(CH^S)_i - (Rs_r + pr_f)}{T_i} \quad (4)$$

And,

$$\daleth AES_{authorz} = \frac{AES_{authorz}}{(CH^S - MA)} - (P - pr_f) \quad (5)$$

In the above equation T_{MA} and $\daleth AES_{authorz}$ used to represent the timed mapping and consecutive prediction instances. From the above equations, the reliable authorization of the chaotic systems (α_s) is estimated for each instance. This estimation is analyzed for detecting the condition $MA \neq 0$ and $MA = 0$ for all t instances using DRL. The DRL is dependent on controller stableness and unstableness such that α_s is determined for all the DRL output (Δ^O). The linear output of $\daleth AES_{authorz}$ in T_{MA} is the unstableness identified instances for maximizing $(ch^s \times P)$. The Δ^O and final output $\exists$ is crucial in determining precision outcomes. The inputs for its point of instability are $AES_{authorz}$ for both the conditions $ch^s::i$ and $(ch^s, MA)::i$ for mapping through differential access. The AES process for instantaneous and consecutive timed initialization is illustrated in Fig. 3.

The authorization is differentiated for the cycle instigation and the consecutive cycles through T_{MA}. For the first P cycles the access information is simply fetched for validation provided $A \in S_{authors}$ is high. Based on the Rs_r the consecutive intervals are determined across various T and P. If the access key is valid for $P = Rs_r$ satisfying condition, then $(P+1)$ is the $TM_A \forall \alpha_S$. The failing $(i.e.) pr_f$ identifies the CH^S point-of-change (at any $T \in i$). This is analyzed recurrently using DRL (Fig. 3). The deep recurrent learning process for both the instances mapping based on the constraints $MA \neq 0$ and $\daleth AES_{authorz} = (ch^s - MA) AES_{authorz}$. If the deficiency verification is true in the mapping then it is 1 else 0. The output of the DRL, the first mapping $ch^s::i$ outputs in precious outcome whereas $(ch^s, MA)::i$ outputs in the change of controller with $MA \neq 0$. Using equations (5) and (6), the DRL output and final output $\exists$ for $ch^s::i$ is validated. The validations are performed for both the instances and the conditional assessment of $\varepsilon = 1$ or $\varepsilon = 0$ from the IoT platform.

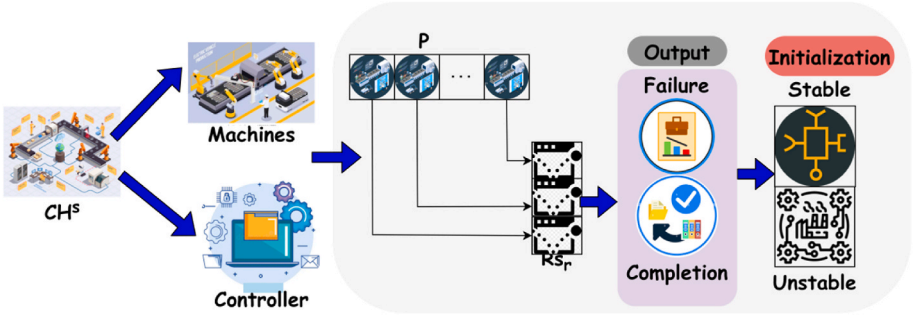


Fig. 2. Chaotic system setup.

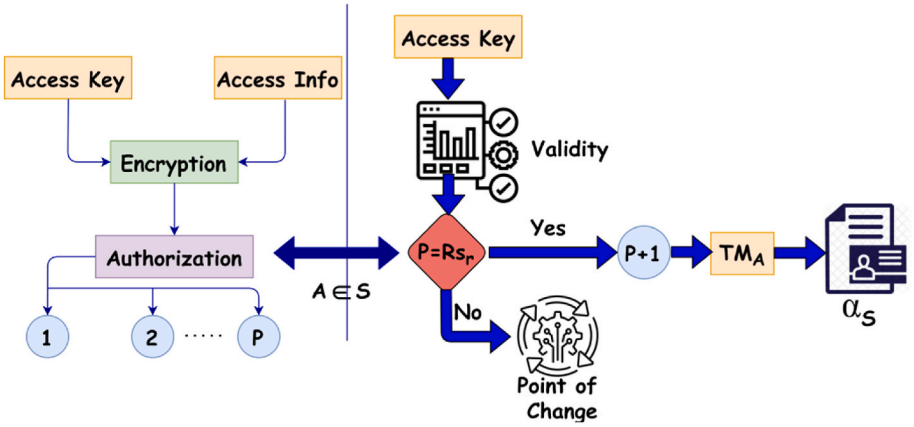


Fig. 3. AES process for instantaneous and consecutive timed initialization.

Therefore, the outputs are required for the work reallocated time interval T. From the above mapping process, MA serves as an input, after the identification of Rs_r in $ch^s::i$ mapping is expressed as

$$\left.\begin{aligned}
\Delta^{O^1} &= \daleth AES_{authorz_1} T_1 + P_1\varepsilon_1 \\
\Delta^{O^2} &= \daleth AES_{authorz_2} T_2 - pr_{f_1} + P_2\varepsilon_2 \\
\Delta^{O^3} &= \daleth AES_{authorz_3} T_3 - pr_{f_2} + P_3\varepsilon_3 \\
&\vdots \\
\Delta^{O^i} &= \daleth AES_{authorz_i} T_i - pr_{f_i} + P_i\varepsilon_i
\end{aligned}\right\} \tag{6}$$

$$\left.\begin{aligned}
\exists_1 = \Delta^{O^1} \quad & \exists_1 = \daleth AES_{authorz_1} T_1 + P_1\varepsilon_1 \\
\exists_2 = \Delta^{O^2} - Rs_{r_1} P_1 \quad & \exists_2 = \daleth AES_{authorz_2} T_2 - pr_{f_1} + AES_{authorz_1} - Rs_{r_1} P_2\varepsilon_2 \\
\exists_3 = \Delta^{O^3} - Rs_{r_2} P_3 \quad & \exists_3 = \daleth AES_{authorz_3} T_3 - pr_{f_2} + AES_{authorz_3} - Rs_{r_2} P_3\varepsilon_3 \\
\vdots \quad & \vdots \\
\exists_i = \Delta^{O^i} - Rs_{r_i} P_{i-1} \quad & \exists_i = \daleth AES_{authorz_i} T_i - pr_{f_i} + AES_{authorz_{i-1}} - Rs_{r_i} P_i\varepsilon_i
\end{aligned}\right\} \tag{7}$$

Based on equations (6) and (7), the linear output is given as $\exists = \daleth AES_{authorz} T - pr_f + AES_{authorz} - Rs_r P\varepsilon$ and if $MA = 0$, then $\varepsilon = 1$ and $\daleth AES_{authorz_i} = NAES_{authorz}$. Hence, the precision outcome is achieved. Therefore, the identification of such authorization issues and malicious access is retained at 1. The IoT technology stores (α_s, ch^s, T) for the instance and this AES deficiency in authorization is verified for the chaotic systems. Instead, $(ch^s, MA)::i$ based DRL output and final output are computed as per equations (8) and (9) respectively.

$$\left.\begin{aligned}
\Delta^{O^1} &= \daleth AES_{authorz_1} \\
\Delta^{O^2} &= \daleth AES_{authorz_2} - Rs_{r_1}\varepsilon - MA_1 P_1 \\
\Delta^{O^3} &= \daleth AES_{authorz_3} - Rs_{r_2}\varepsilon + MA_2 P_3 \\
&\vdots \\
\Delta^{O^i} &= \daleth AES_{authorz_i} - Rs_{r_i}\varepsilon - MA_i P_{i-1}
\end{aligned}\right\} \tag{8}$$

equation (8) states that this identification process maintains a high accuracy level, denoted by the value "1," implying near-perfect precision. IoT technology is noted to store certain parameters represented by $\alpha_s, ch^s and\ T$ The text further emphasizes the verification of deficiencies in authorization related to the use of AES (Advanced Encryption Standard) within chaotic systems. Additionally, the computation of outputs based on variables like ch^s and MA, possibly using mathematical equations presented in equation (8).

$$\left.\begin{aligned}
\exists_1 = \Delta^{O^1} &= \daleth AES_{authorz_1} \\
\exists_2 = \Delta^{O^2} - T_{MA_1} + \daleth AES_{authorz} &= AES_{authorz_1} - pr_{f_1} + AES_{authorz_1} - Rs_{r_1} P_2\varepsilon_2 \\
\exists_3 = \Delta^{O^3} - T_{MA_2} + \daleth AES_{authorz} &= AES_{authorz_3} - pr_{f_2} + AES_{authorz_2} - Rs_{r_2} P_2\varepsilon_2 \\
&\vdots \\
\exists_i = \Delta^{O^i} - T_{MA_i} + \daleth AES_{authorz} &= AES_{authorz_{i-1}} - pr_{f_i} + AES_{authorz_i} - Rs_{r_i} P_i\varepsilon_i
\end{aligned}\right\} \tag{9}$$

Equations (7) and (8) is required by computing the condition $\daleth AES_{authorz} = (ch^s - MA) AES_{authorz}$ and $\varepsilon = 1$ or $\varepsilon = 0$ is verified in a step-by-step manner for preventing prediction failures. From this DRL output, the deficiency verification leads to the next cycle whereas the point of

change leads to the change of controller through differential access. If the first system relies on stable conditions, then AES deficiency in authorization is verified in its complete cycle. The DRL process is illustrated in Fig. 4.

In Fig. 4 the Rs_R and T_{MA} are the inputs for Δ and $\exists$ analysis such that Δ^{o^1} to Δ^{o^i} is repeated. If the repetition pursues then $\rho_{W_{all}}$ is induced for P assignment. Based on the available Δ^{o^i}, the pr_f is computed. In this case, the output is extracted for T generates $\exists_i$. The proposed model distinguishes P and pr_f post the Δ^{o^i} output for which $\exists_i$ is the output. In this case, the validations using equations (8) and (9) pursues T_{MA} other than the existing Rs_r. Therefore, the precision outcome along with work reallocation and change of controller is performed in the IoT platform and hence the chaotic systems are unchanged. In the consecutive prediction instances, the precision outcome on its previous instance is determined for improving smart manufacturing. If the consequence is observed in $MA > ch^s$, then the controller is terminated to prevent authorization in the deficiency and point of change verification. The IoT platform gives an alert sound to the smart manufacturing industry to take appropriate actions to identify authorization issues and malicious access. This prevents unauthorized access and controller downtime reduction by processing authorization whereas, the response rate is high. The change of controller ensures delay-less manufacturing within the IoT environment. However, the chances for external threats in the IoT platform are high, and therefore end-to-end authentication is performed to secure the process.

3.2. Change of controller

In the IoT platform, the allocation of work is performed for authorization verification, and the controller unstableness identified instances in the chaotic systems based on $\urcorner AES_{authorz}$ is the considering factor. The possibilities of allocating work $(\rho_{w_{all}})$ sequentially is computed as

$$\left.\begin{aligned} \rho_{w_{all}} &= (1-\rho_{cdr})^{i-1} \forall T \in i \\ &\quad and \\ \rho_{cdr} &= \left(1 - \frac{ch^s \in N}{ch^s \in T}\right) \end{aligned}\right\} \tag{10}$$

In equation (10), the consecutive prediction instances follow the idle possibility of the selective chaotic system such that there is work reallocation and hence the reviving authorization is performed using AES is computed. Therefore, the reallocation of work for $\rho_{w_{all}}$ follows

$$ReAllocation(N) = \frac{1}{|ch^s - MA + 1|} \cdot (\rho_{w_{all}})_i \forall i \in T \tag{11}$$

However, the work reallocation, deficiency verification, and point of change for all N instances are valid for both $ch^s::i$ and $(ch^s, MA)::i$ ensuring human intervention-less automation. The converging process of reassigning work is to reduce the impact of controller downtime reduction. Therefore, the identifiable instances of $MA > ch^s$ and ρ_{cdr} is less to satisfy stable to unstable points. Contrarily, the prolonging ρ_{cdr} and hence the processing time outputs in predicting failures. The controller change process is illustrated in Fig. 5.

The CH^s is validated for α_S for different P such that if α_S is true then pr_f is identified. Contrarily if $\exists_i$ is yes then the point of change is observed for the current CH^s. Therefore the controller change is observed due to which new allocations are optimal without deficiency. Thus the alternate allocation case relies on $\Delta^{o^i} \forall \exists$ such that reallocation is confined. Therefore the ρ_{wall} is pursued by the consecutive operation cycles for new P (Fig. 5).

3.3. Recurrent learning process assessment

The chaotic systems are responsible for monitoring the controller's performance from the IoT platform. The input can be of any type related to smart industry manufacturing. In this instance, the conventional operation cycles (OP_C) is computed as

$$OP_C = \frac{(MA_{max} - MA_{min})}{T} + \urcorner AES_{authorz_i} \tag{12}$$

And,

$$Dfc = 1 / \sqrt{2\pi} \left[\frac{\left(\frac{\urcorner AES_{authorz_i}}{\rho_{cdr}}\right)}{2(Rs_{r_i}\varepsilon - MA_i P_{i-1})} \right] \tag{13}$$

where, ch^s is the selective chaotic system from the IoT platform and $ch^s \in N$ are observed in differential access. The variables Dfc and cdr denote the deficiency verification and controller downtime reduction. The prediction failure is identified due to external threats at different intervals. There are some cases of prediction failures in chaotic systems due to malicious issues and unauthorized access to the controller. Therefore, these issues impact the chaotic systems at any instance for which the reliable recommendations $\gamma(ch^s)$ is given as

$$\gamma(ch^s) = \frac{cdr^2}{\left(\frac{\urcorner AES_{authorz_i}}{\rho_{cdr}} - \vartheta\right)^2} \tag{14}$$

And,

$$\vartheta = \frac{1}{T} \sqrt{\frac{1}{ch^s - 1} \sum_{i=1}^{N} \urcorner AES_{authorz_2} - Rs_{r_1}\varepsilon - MA_1 P_1} \tag{15}$$

In the above equation, the consecutive prediction instances of the complete cycle are verified using AES deficiency in authorization following the maximum authorized access for the controllers and the unauthorized access ϑ. The above equation computes the prediction failure for a sequence until is active in the change of controller from the IoT platform. In this smart manufacturing, point of change and deficiency verification is performed based on stableness and unstableness

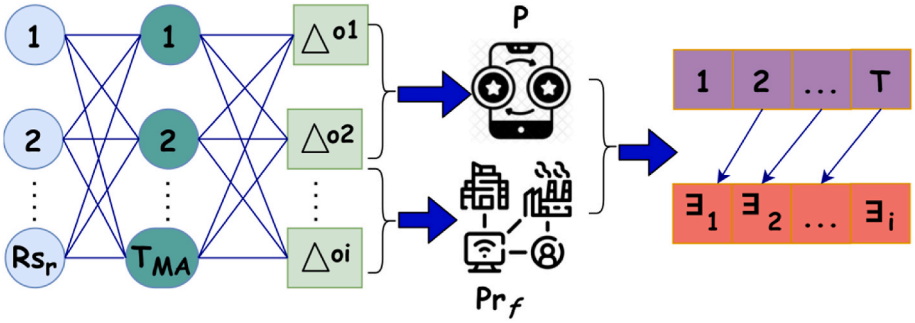


Fig. 4. DRL process representation.

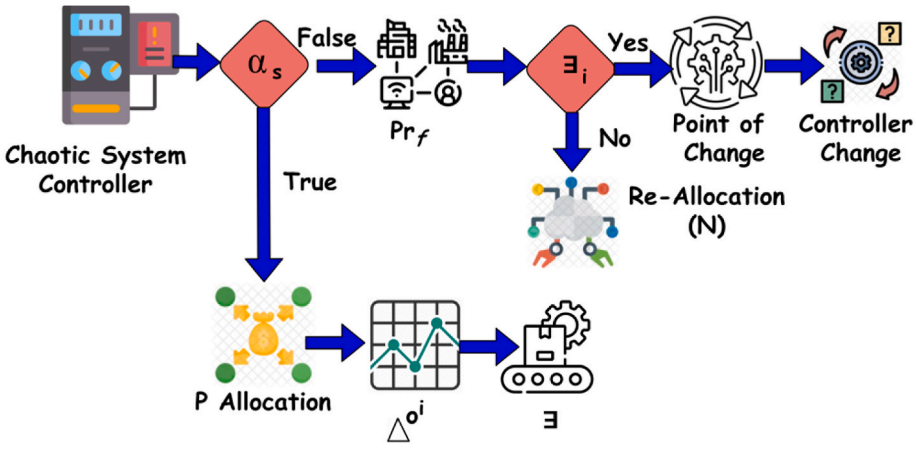


Fig. 5. Controller change process.

for the instances to improve the synchronized working of all the machines/controllers. This proposed model and DRL are used to improve the precision outcome of the chaotic systems.

3.4. Self-analysis

The data analysis is performed using the [34] data; the data provides security information for Industrial Control System (ICS). This ICS emulates steam turbine and hydropower control operations through testbed functions. The testing and training dataset provides the operation time stamp, the cycles, and the maximum access/controller. The optimal operation time is 24 h for an uninterrupted power supply. Similarly, unauthorized access is identified for multiple denials under varying intervals. Based on this, the analysis of Rs_r for the varying operation time and T_{MA} is presented in Fig. 6. Besides the analysis the manufacturing process setup is presented.

The Rs_f for two operations (i.e.) 505 controller to motor control and value control are analyzed for the different operation times and T_{MA} respectively. Deep recurrent learning identifies the chances of pr_f under different Δ^{o^i} and $\exists$ such that $\rho_{W_{all}}$ are assigned. In this process, the different operation times are handled independently under T_{MA}. Contrarily or $\urcorner AES$ the Δ° and $\exists_1$ to $\exists_i$ is used for reallocating the process from motor to valve control using previous outputs. Thus Rs_f varies accordingly under distinguishable factors (Fig. 6). Fig. 7 presents the pr_f for the varying T_{MA} and P between different instances.

Based on the output of the deep recurrent learning, $\gamma(ch^s)$ is identified for stabilizing multiple outputs across different cycles. This process is valid until various features are suppressed for preventing failures. The failures induce distinguishable T_{MA} sequences for leveraging $A \in S_{authors}$. Thus the mediate $\exists_1$ to $\exists_i$ is satisfied by rectifying deficiencies between

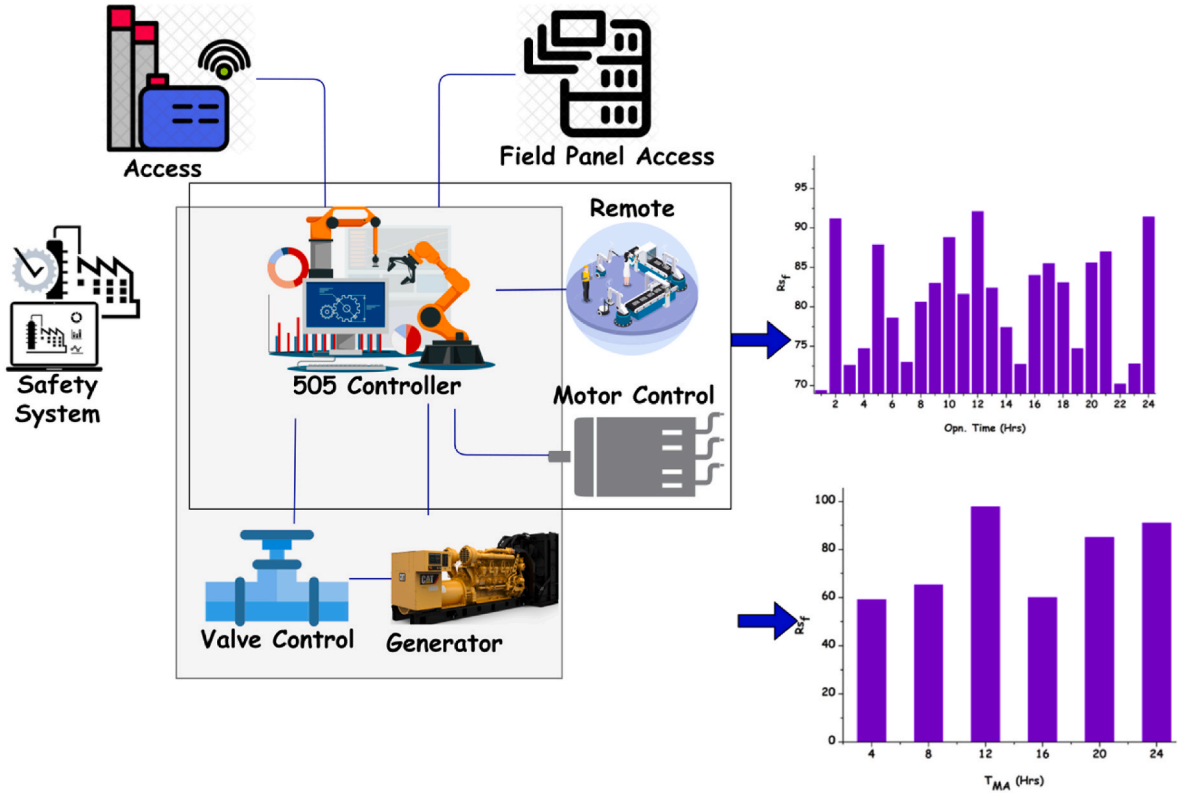


Fig. 6. Rs_f analysis.

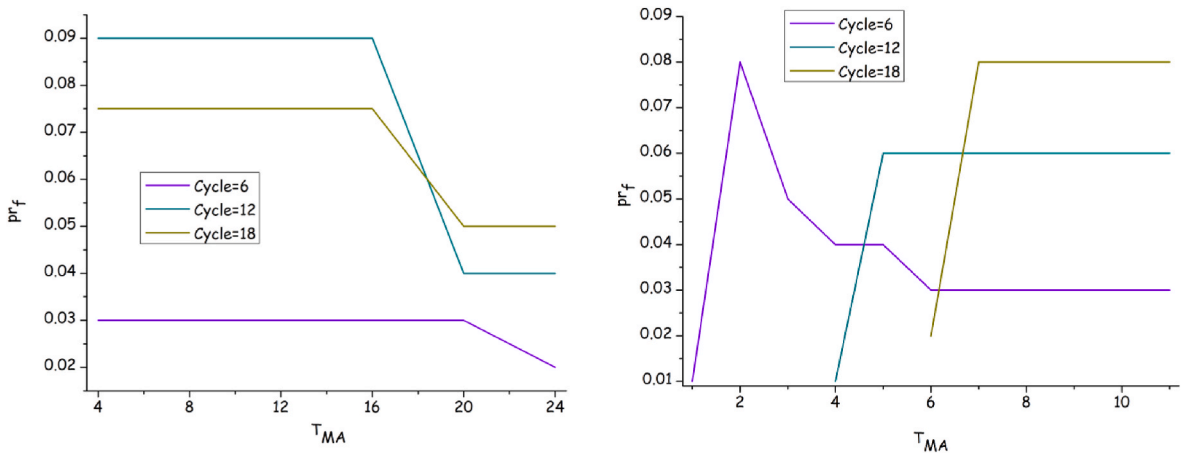


Fig. 7. $pr_f \forall T_{MA}$ and ρ

successive authorized access intervals.

4. Comparative analysis

The comparative analysis is performed using the metrics of unauthorized access, downtime, production failure, authorization overhead, and authorization deficiency. The number of operation cycles (up to 18) and the access/controller (up to 10) are the X-axis variants in this comparative analysis. In this comparative analysis, the existing RAM-BI [25], EADF [24], and SGA-TEE [30] are allied with the proposed model.

4.1. Unauthorized access

This proposed model is used for improving the authorized access and controller performance based on the AES algorithm from the IoT platform for identifying failures and delaying chaotic system processing due to points of instability. The classified stableness and unstableness points of possibilities are used for reallocating the work using recommendations. In these two instances, stable to unstable systems are identified and terminated for protecting machines/controllers. The AES deficiency in authorization is identified through instability points and the malicious access or issues identified instances are recovered by providing alternate controller recommendations to identify failures using a deep recurrent learning process. Based on the controller stableness analysis, the consecutive prediction instances are processed through differential access, preventing unauthorized access. The controller deficiency is verified from the IoT platform using SRAM-AES along with DRL for completing the process cycle. The differential access is performed without security threats outputs in malicious access and unauthorized issues. The proposed model classifies the point of change depending on the stability of the machines, this leads to less unauthorized access as represented in Fig. 8.

4.2. Downtime

The possibility of a point of stability and instability is computed through AES deficiency in authorization for overcoming malicious access from the IoT platform is represented in Fig. 9. Using this proposed model to perform deficiency and point of change verification from the chaotic systems satisfies fewer prediction failures. By computing the chaotic system classification based on the stable and unstable points at different time intervals for reducing unauthorized access. At that time identifying prediction failures and disconnection occurrences in the IoT platform through differential access is performed for reviving their conventional operation cycles. The authorization issues in chaotic systems are mitigated through DRL and the proposed model depending upon the point of change from the IoT platform is preceded using equations (6)–(9) computations. In this proposed model, the unstable to stable point satisfies more precision outcomes. This smart reviving authorization using AES prevents failures [as per equations (11) and (12)]. In this model, the controller downtime reduction is observed for new controller changes at malicious access identified instances.

4.3. Production failure

In this proposed smart reviving authorization model, the maximum

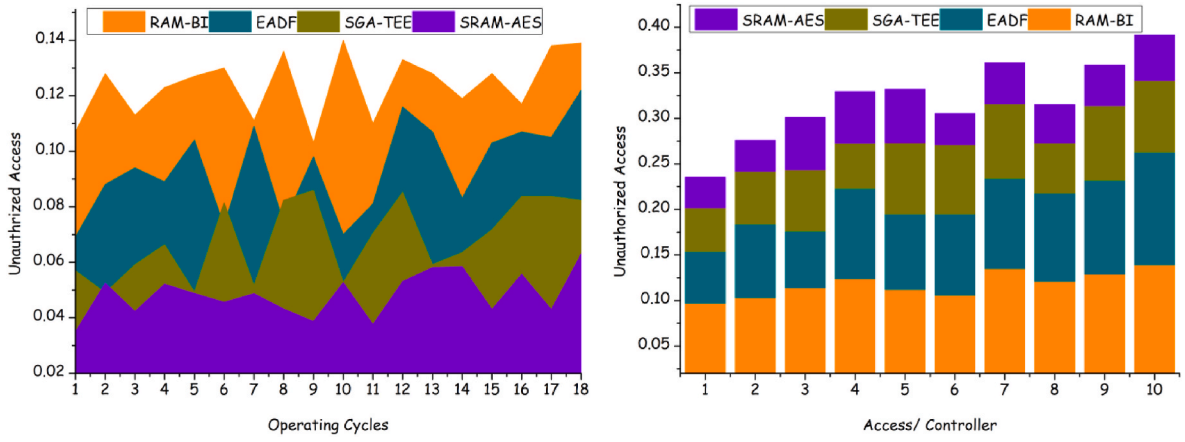


Fig. 8. Unauthorized access analysis.

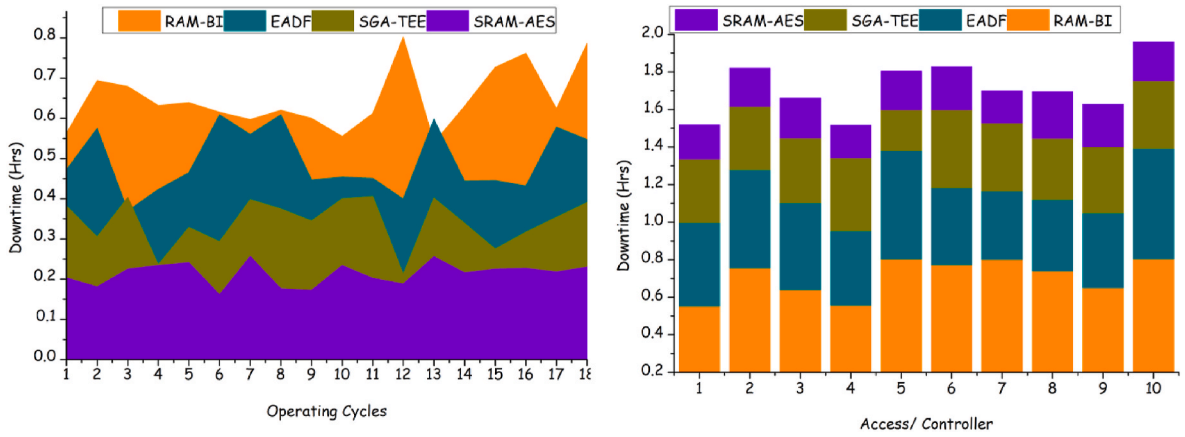


Fig. 9. Downtime analysis.

possibilities of deficiency and point of change are verified without failures achieving a high change of controller compared to the other factors as represented in Fig. 10. The conventional operation cycles and preventing failures is verified using deep recurrent learning algorithm for selective chaotic systems in this article due to external threats and authorization issues. The failure occurrence is identified in smart manufacturing using the SRAM-AES model. Reducing production failure using the proposed model and DRL is the best way to reduce unauthorized access and controller downtime through differential access. From the chaotic system processing, the change of controller is compared with previous successful outcomes and is verified using IoT elements and DRL. The less production failure is satisfied by the proposed model for improving precision outcome. This is difficult for verifying the AES deficiency in authorization at different time intervals. Thus the proposed model achieves fewer production failures in this article.

4.4. Authorization overhead

In this proposed model, the authorization overhead occurs due to external threats, and malicious access is verified and controlled by the IoT elements and DRL algorithm for chaotic systems, reducing production failures using the proposed model (Refer to Fig. 11). This classification improves authorized access using minimum or minimum point of change from the IoT platform and AES deficiency in authorization is verified as compared to the other factors in this proposed model. Based on the DRL output, the maximum precision outcome is satisfied by the proposed model for improving authorized access for production intervals. In this manner, these consecutive prediction instances help to identify and differentiate production failures based on the AES algorithm with chaotic systems to maximize the controller's performance. The final output satisfies both the conditions of $ch^s::i$ and $(ch^s, MA)::i$ ensuring human intervention-less automation is to reduce failures. This proposed model achieves less authorization overhead as compared to the other factors.

4.5. Authorization deficiency

The AES authorization deficiency is less compared to the other factors in this proposed model using the DRL algorithm and the failure identified instances are recovered by providing alternate controller recommendations is high for improving precision outcomes as illustrated in Fig. 12. In this article satisfies less authorization deficiency for stable to unstable point based on AES algorithm is verified in its completion cycles is to reduce controller downtime and unauthorized access and failures. After applying the AES algorithm, the stability analysis is performed for completing the cycle with less processing time. In this manuscript, the identifiable instances of $MA > ch^s$ and ρ_{cdr} is less to satisfy stable to unstable points. The prediction failure is identified due to external threats in any instance. There are some cases of prediction failures in chaotic systems identified by malicious issues and unauthorized access for the controller. In this proposed model, based on this two instance validation, the authorization deficiency is less compared to the other factors in this model. The comparative analysis results with the inference is tabulated in Table 2 (Operating Cycles) and Table 3 (Access/Controller).

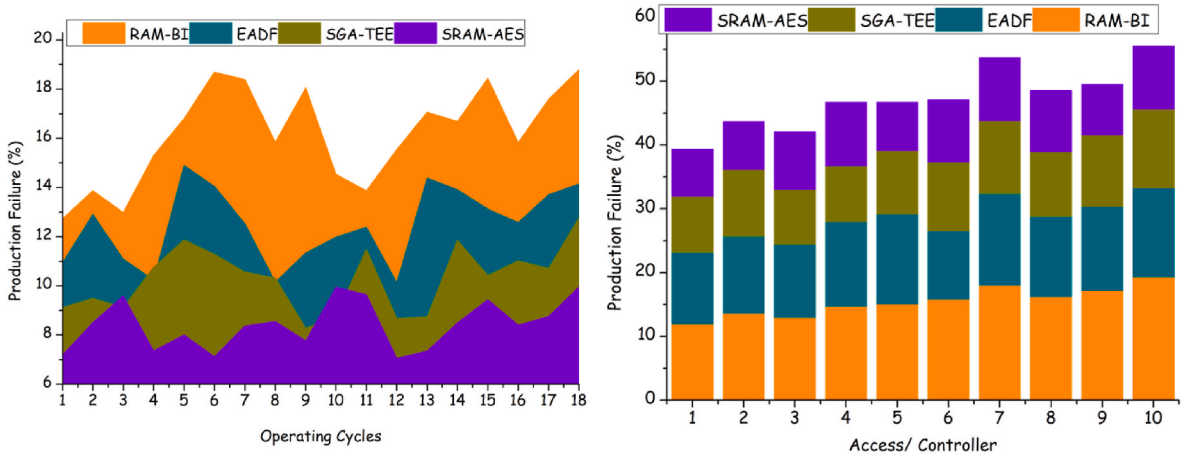


Fig. 10. Production failure analysis.

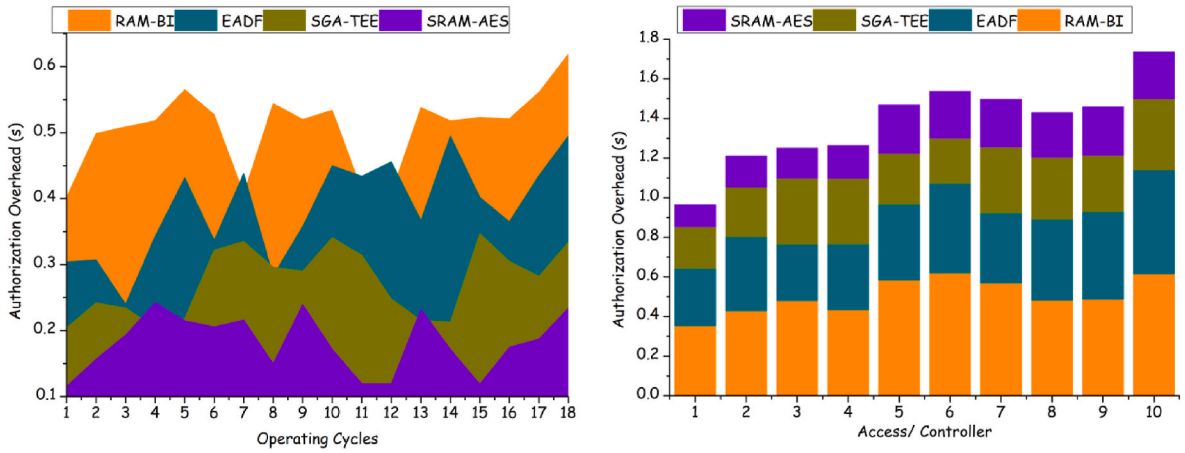


Fig. 11. Authorization overhead analysis.

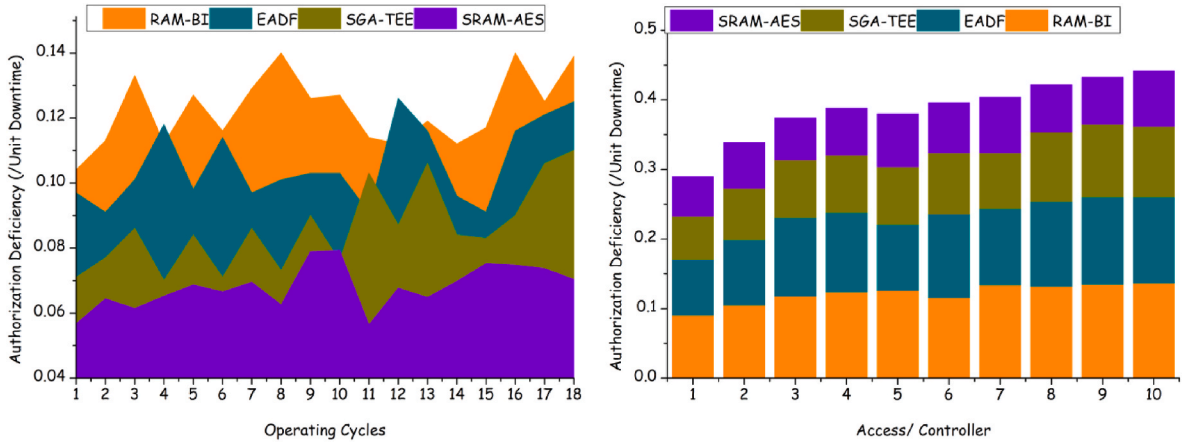


Fig. 12. Authorization deficiency analysis.

Table 2
Comparative analysis results (operating cycles).

Metrics	RAM-BI	EADF	SGA-TEE	SRAM-AES
Unauthorized Access	0.139	0.122	0.0823	0.0631
Downtime (Hrs)	0.786	0.547	0.391	0.23
Production Failure (%)	18.79	14.14	12.76	9.954
Authorization Overhead (s)	0.619	0.495	0.334	0.2341
Authorization Deficiency (/Unit Downtime)	0.139	0.125	0.11	0.0703

Inferences: The proposed model reduces unauthorized access, downtime, production failure, overhead, and deficiency by 10.27%, 9.99%, 10.55%, 8.58%, and 10.87% individually.

Table 3
Comparative analysis results (access/controller).

Metrics	RAM-BI	EADF	SGA-TEE	SRAM-AES
Unauthorized Access	0.139	0.124	0.0786	0.0498
Downtime (Hrs)	0.804	0.589	0.361	0.206
Production Failure (%)	19.35	13.94	12.34	9.922
Authorization Overhead (s)	0.615	0.527	0.357	0.2362
Authorization Deficiency (/Unit Downtime)	0.137	0.124	0.101	0.0795

Inferences: The proposed model reduces unauthorized access, downtime, production failure, overhead, and deficiency by 12.81%, 10.79%, 1058%, 8.78%, and 8.23% individually.

5. Conclusion

In the field of smart manufacturing unauthorized access to controllers results in chaotic operation cycles. Such process occurs due to external threats that are addressed by the proposed smart reviving authorization model. This model exploits the advanced encryption standard process for authorizing remote access requests due the consecutive operation cycles. The point of instability of the controller is the key factor for deciding the chaotic system response to the allocated operations. The deep recurrent learning process employed accounts the point of instability and stability reviving factors through consecutive analysis. This analysis is performed post the operation completion cycle ahead of different cycles. The definite possibility identified approves the implication of AES for secure authorization resulting in 10.27% less unauthorized access. The IoT-based data utilization and controller modification changes are revived using the learning recommendations for reducing the downtime by 9.99% and deficiency by 10.87% for the different operation cycles. Carrying forward with this feature, a concurrent private blockchain based access and remote control based systems are planned to be designed. Such systems integrate interoperational features between different locations unanimously.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

References

[1] K. Xia, C. Sacco, M. Kirkpatrick, C. Saidy, L. Nguyen, A. Kircaliali, R. Harik, A digital twin to train deep reinforcement learning agent for smart manufacturing plants: environment, interfaces and intelligence, J. Manuf. Syst. 58 (2021) 210–230.

[2] Y. Wu, Y. Zhang, An integrated framework for blockchain-enabled supply chain trust management towards smart manufacturing, Adv. Eng. Inf. 51 (2022), 101522.

[3] Rajasekhar Turaka, S. Ravi Chand, R. Anitha, R. Arun Prasath, S. Ramani, Harish Kumar, S. Gopalakrishnan, Yousef Farhaoui, A novel approach for design energy efficient inexact reverse carry select adders for IoT applications, Results Eng. 18 (2023), 101127.

[4] V. Terziyan, D. Malyk, M. Golovianko, V. Branytskyi, Encryption and generation of images for privacy-preserving machine learning in smart manufacturing, Proc. Comput. Sci. 217 (2023) 91–101.

[5] S. Costa, F.J. Silva, R.D.S.G. Campilho, T. Pereira, Guidelines for machine tool sensing and smart manufacturing integration, Procedia Manuf. 51 (2020) 251–257.

[6] P.D. Paraschos, A.S. Xanthopoulos, G.K. Koulinas, D.E. Koulouriotis, Machine learning integrated design and operation management for resilient circular manufacturing systems, Comput. Ind. Eng. 167 (2022), 107971.

[7] J. Gu, L. Zhao, X. Yue, N.I. Arshad, U.H. Mohamad, Multistage quality control in manufacturing process using blockchain with machine learning technique, Inf. Process. Manag. 60 (4) (2023), 103341.

[8] V. Majstorovic, V. Simeunovic, Z. Miskovic, R. Mitrovic, D. Stosic, S. Dimitrijevic, Smart manufacturing as a framework for smart mining, Procedia CIRP 104 (2021) 188–193.

[9] L.D. Nguyen, A. Bröring, M. Pizzol, P. Popovski, Analysis of distributed ledger technologies for industrial manufacturing, Sci. Rep. 12 (1) (2022), 18055.

[10] Ofori-Ntow Jnr Eric, Yao Yevenyo Ziggah, Maria Joao Rodrigues, Susana Relvas, A hybrid chaotic-based discrete wavelet transform and Aquila optimisation tuned-artificial neural network approach for wind speed prediction, Results Eng. 14 (2023), 100399.

[11] K. Li, T. Zhou, B.H. Liu, Internet-based intelligent and sustainable manufacturing: developments and challenges, Int. J. Adv. Des. Manuf. Technol. 108 (5–6) (2020) 1767–1791.

[12] S.W. Kim, J.H. Kong, S.W. Lee, S. Lee, Recent advances of artificial intelligence in manufacturing industrial sectors: a review, Int. J. Precis. Eng. Manuf. (2022) 1–19.

[13] D. Xu, K. Yu, J.A. Ritcey, Cross-layer device authentication with quantum encryption for 5G enabled IIoT in industry 4.0, IEEE Trans. Ind. Inf. 18 (9) (2021) 6368–6378.

[14] M.M. Khayyat, M.M. Khayyat, S. Abdel-Khalek, R.F. Mansour, Blockchain enabled optimal Hopfield Chaotic Neural network based secure encryption technique for industrial internet of things environment, Alex. Eng. J. 61 (12) (2022) 11377–11389.

[15] R. Elhabob, Y. Zhao, I. Sella, H. Xiong, An efficient certificateless public key cryptography with authorized equality test in IIoT, J. Ambient Intell. Hum. Comput. 11 (2020) 1065–1083.

[16] X. Li, T. Liu, C. Chen, Q. Cheng, X. Zhang, N. Kumar, A lightweight and verifiable access control scheme with constant size ciphertext in edge-computing-assisted IoT, IEEE Internet Things J. 9 (19) (2022) 19227–19237.

[17] W. Wang, H. Huang, Z. Yin, T.R. Gadekallu, M. Alazab, C. Su, Smart contract token-based privacy-preserving access control system for industrial Internet of Things, Digit. Commun. Network 9 (2) (2023) 337–346.

[18] H. Abdi Nasib Far, M. Bayat, A. Kumar Das, M. Fotouhi, S.M. Pournaghi, M. A. Doostari, LAPTAS: lightweight anonymous privacy-preserving three-factor authentication scheme for WSN-based IIoT, Wireless Network 27 (2021) 1389–1412.

[19] K.J. Yi, Y.S. Jeong, Smart factory: security issues, challenges, and solutions, J. Ambient Intell. Hum. Comput. (2021) 1–14.

[20] W. Shen, T. Hu, C. Zhang, S. Ma, Secure sharing of big digital twin data for smart manufacturing based on blockchain, J. Manuf. Syst. 61 (2021) 338–350.

[21] L. Tang, M. Törngren, L. Wang, A permissioned blockchain based feature management system for assembly devices, IEEE Access 8 (2020) 183378–183390.

[22] J. Cui, F. Bian, H. Zhong, Q. Zhang, S. Xu, C. Gu, L. Liu, An anonymous and outsourcing-supported multiauthority access control scheme with revocation for edge-enabled IIoT system, IEEE Syst. J. 16 (4) (2022) 6569–6580.

[23] J. Cui, N. Liu, Q. Zhang, D. He, C. Gu, H. Zhong, Efficient and anonymous cross-domain authentication for IIoT based on blockchain, IEEE Trans. Network Sci. Eng. (2022). Early access.

[24] H. Choi, D. Kim, J. Kim, J. Kim, P. Kang, Explainable anomaly detection framework for predictive maintenance in manufacturing systems, Appl. Soft Comput. 125 (2022), 109147.

[25] Y. Zhao, J. Yang, Y. Bao, H. Song, Trustworthy authorization method for security in industrial internet of things, Ad Hoc Netw. 121 (2021), 102607.

[26] L. Ferretti, F. Longo, G. Merlino, M. Colajanni, A. Puliafito, N. Tapas, Verifiable and auditable authorizations for smart industries and industrial Internet-of-Things, J. Inf. Secur. Appl. 59 (2021), 102848.

[27] K. Demertzis, L. Iliadis, N. Tziritas, P. Kikiras, Anomaly detection via blockchained deep learning smart contracts in industry 4.0, Neural Comput. Appl. 32 (2020) 17361–17378.

[28] H. Kim, T. Shon, Industrial network-based behavioral anomaly detection in AI-enabled smart manufacturing, J. Supercomput. 78 (11) (2022) 13554–13563.

[29] Y. Tang, Y. Ba, L. Li, X. Wang, X. Yan, Lattice-based public-key encryption with conjunctive keyword search in multi-user setting for IIoT, Cluster Comput. 25 (4) (2022) 2305–2316.

[30] A.A. Fröhlich, L.P. Horstmann, J.L.C. Hoffmann, A secure IIoT gateway architecture based on trusted execution environments, J. Netw. Syst. Manag. 31 (2) (2023) 32.

[31] X. Liu, M. Wang, T. Wang, R. Zhang, A blockchain assisted multi-gateway authentication scheme for IIoT based on group, Peer-to-Peer Network. Appl. 16 (1) (2023) 245–259.

[32] A.J. Cabrera-Gutiérrez, E. Castillo, A. Escobar-Molero, J.A. Álvarez-Bermejo, D. P. Morales, L. Parrilla, Integration of hardware security modules and permissioned blockchain in industrial IoT networks, IEEE Access 10 (2022) 114331–114345.

[33] D. Wu, N. Ansari, A trust-evaluation-enhanced blockchain-secured industrial IoT system, IEEE Internet Things J. 8 (7) (2020) 5510–5517.

[34] https://www.kaggle.com/datasets/icsdataset/hai-security-dataset?resource=download.