

Received 16 June 2023, accepted 24 July 2023, date of publication 1 August 2023, date of current version 7 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3300650

## RESEARCH ARTICLE

# A Linear Probabilistic Resilience Model for Securing Critical Infrastructure in 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, for supporting this work through the Fast-Track Research Support Program.

**ABSTRACT** Critical infrastructures are designed for securing interconnecting networks from different influencing factors such as adversaries, unauthorized platoons, cyber threats, etc. These infrastructure hosts include human, physical elements, and cyber paradigms. The vital part is cyber resilience against weak and volatile authentication and security administrations. For strengthening cyber security, this article introduces the Artificial Intelligence-induced Constructive Resilience Model (AI-CRM). The proposed model accounts for the security requirements of the adversary impacting infrastructure elements based on probability. This probability is computed using previous adversary impacts on infrastructure failures and session drops in handling operational services. The computation for linearity or stagnancy is validated using a recurrent learning paradigm over different service transitions. The resilience is improved by augmenting security measures that are identified as an output of linear impacts over the services. Based on the linear incremental probability the resilience between two successive service transitions is computed. Identifying the non-linear or stagnant probability is the converging solution of recurrent learning. The recurrent learning optimizes the stagnancy and linear impact (probability) by repeatedly computing the failures and drops due to adversary injection. This improves resilience through security augmentations and modifications. This model is analyzed using adversary detection ratio, session drops, infrastructure failures, time lag, and service dissemination ratio.


**INDEX TERMS** Critical infrastructure, linear processing, recurrent learning, resilience.

## I. INTRODUCTION

Critical Infrastructure (CI) is a vast network that connects bridges, highways, railways, tunnels, and buildings to maintain the efficiency of daily life. CI is mostly used in transportation systems which minimizes the energy consumption level of the systems [1]. The critical infrastructure required proper security models to ensure the feasibility of the systems. Various methods and techniques are used for CI that protect the security range of the networks [2]. A convolutional security technique is used to identify the risks and issues which are presented in critical infrastructure [3]. The convolutional security technique addresses the risk based on economic losses, network losses, and cyber-attacks. The convolutional security technique identifies the exact cause

of security issues which produces an optimal solution to solve the problems [4]. A CI security model is also used to ensure the security range of the systems. The CI security model detects security issues in various fields. The CI security model also identifies the attacks via cyber security policies [5]. The CI security model maximizes the accuracy in attack detection which improves the security level of CI systems [6].

CI resilience is a process that identifies, provides, and prioritizes a plan which protects both the physical and cyber layers of the systems. CI resilience improves the performance range of CI which enhances the efficiency range of the applications [7]. CI resilience is the ability that adapts or change the conditions and functions to perform tasks in a system. CI resilience against adversaries causes various issues in CI [8]. Many approaches and techniques are used in CI to maintain the effectiveness level of

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

the systems. A comprehensive approach is used in CI to improve resilience against adversaries [9]. The comprehensive approach addresses the efforts which are made by CI that provide necessary services to perform tasks. The comprehensive approach provides proper security policies to create an effective service to the users [10]. A detection model is also used for CI resilience that improves the overall performance and feasibility range of CI. The detection model detects the threats based on adversaries [11]. The adversary-based issues are identified using a tool that filters the threats which are relevant to adversaries. The detection model minimizes the failure range of the system which improves the reliability and efficiency level of CI resilience [12], [13].

Artificial intelligence (AI) is a technology that utilizes human knowledge to perform tasks in an application. AI technology is commonly used in various fields to perform tasks efficiently [14]. AI-based solutions are used in CI which ensures the security and safety range of the systems. The AI-based five-dimensional framework is used in CI. The AI-based framework identifies the critical issues and attacks which are occurred during performing a task [15]. The AI-based framework provides relevant key solutions to solve the issues in CI that improves the security range of CI systems [16]. Smart grids (SG) based security model is also used in CI. SG monitors CI and identifies the risks based on the grids monitoring system. A deep reinforcement learning (DRL) algorithm-based method is also used for the CI security management process [17]. The DRL algorithm uses a feature extraction technique that extracts the important features from the database [18]. The extracted data produce optimal information for the security management process. The DRL-based method provides proper security services and policies to CI that reduces the complexity of the systems [19]. The contributions are listed below:

- Introducing a constructive resilience model for detecting and mitigating adversary impacts in critical infrastructures.
- Estimating and identifying linear impacts with incremental transition probabilities for failure-preventing and better service dissemination.
- Providing a comparative analysis using different metrics and self-analysis using the limited features discussed throughout the proposal.

## II. RELATED WORK

Fang et al. [20] proposed a new optimization model for resilient critical infrastructure planning. The main goal of the model is to minimize the investment cost of the systems. The proposed optimization model identifies the arranging pairs which are required for planning. A quantitative analysis technique is used in the model which analyzes the exact investing actions for decision-making processes. The proposed model enhances the accuracy of critical infrastructure planning.

Liu et al. [21] introduced a hierarchical resilience enhancement framework for interdependent critical infrastructure

(ICI). The introduced framework detects the multi-objective optimization (MOO) problems that are presented in ICI. The actual relationship between the impacts and solutions is identified that relevant information for the enhancement process. The introduced framework increases the effective range of ICI systems.

Galbusera et al. [22] designed a game-based training method for critical infrastructure (CI) protection and resilience. Computer-assisted exercises are implemented in CI which reduces the complexity of the designing process. The designed training method trains the whole CI to prepare the functionalities for the evaluation process. The designed method improves the awareness of resilience using scientific tools.

Cheng et al. [23] developed a multi-hazard resilience model for critical infrastructure (CI). The actual aim of the model is to recover the resources which are damaged due to severe hazards. The developed model is used as a stochastic recovery model which improves the availability and recovery range of CI systems. The developed model maximizes the performance and efficiency range of the systems.

Xu et al. [24] presented resilience-driven repair sequencing decision-making for critical infrastructure systems (CIS). The proposed model detects the time consumption ratio which is the required scenario. A heuristic algorithm is used in the model which repairs the time scenarios in decision-making processes. The proposed model achieves high accuracy in decision-making that enhances the feasibility level of CIS.

Wu et al. [25] proposed a blockchain and edge computing-based security policy for the Industrial Internet of Things (IIoT). The proposed policy is mostly used for critical infrastructure in Industry 4.0 which ensures the safety of the organizations. The actual availabilities of CI are also identified by the method. The proposed method improves the performance and efficiency range of CI in Industry 4.0.

Sousa et al. [26] proposed a new security scheme is named, ELEGANT for critical infrastructure (CI). In this work authors used digital twins that provides trustable services. The results show that it increases the development and improvement range of CI which ensures the safety of the users.

Fioravanti et al. [27] proposed a risk assessment framework for CI using an analytic hierarchy process. The actual risk factors and causes are identified by the framework. The hierarchy process is used in the framework which predicts the risks. The results shows that it maximizes the accuracy of the risk assessment process.

Sharifi et al. [28] proposed a fog layer-based Internet of Things (IoT) attack detection method for critical infrastructure (CI). The proposed method predicts the bugs and problems based on priorities using machine learning (ML) algorithms. The proposed method improves the performance and efficiency level of CI.

Ashley et al. [29] proposed a game-based security method for critical infrastructure (CI). The proposed method is a gamification method that detects the exact cyber-attacks in CI.

The scenarios are detected using cyber-attack events which enhances the effectiveness range of CI systems.

Otoum et al. [30] have proposed a blockchain-based federated learning method for critical IoT infrastructures. The proposed method provides adaptive solutions to solve the security issues in CI. This method improves the accuracy of the problem-detection process which increases the trustworthiness of CI.

Memos et al. [31] proposed a secure cloud infrastructure for e-health data transmission. The active malware and issues are identified. The proposed method secures the overall safety level of the systems which has achieved high accuracy in the data transmission process.

Masi et al. [32] proposed a cyber-security digital twin (DT) based security policy for critical infrastructure (CI) which detects the attacks using DT tools. Also, minimizes the latency in the computation process. The method obtains an increase in the safety and privacy level of user data from third parties.

The methods discussed above bank on third-party validation systems/ methods for identifying the resilience of different infrastructures. The application and service-bound infrastructures require diverse validation and security implications. This purely relies on the user demands and the application-level security for resilience improvement. However frequent alterations in existing security adaptable to the application demands become prominent in meeting the security requirements. This is less feasible for non-adaptable methods discussed above that increase time lag and session drops. For addressing these issues, a constructive resilience model is designed in this article. The discussions of the same are presented in the next section with appropriate illustrations.

### III. PROPOSED AI-BASED RESILIENCE MODEL

Critical Infrastructure is those possessions, arrangements, and structures that execute actions which is necessary for daily life. Critical infrastructure produces assistance that is fundamental for everyday life such as communications, interactions, and finance. The protected and resilient infrastructure corroborates fecundity and helps to operate the business exertion that establishes the pecuniary backlogs. Critical infrastructures are schemed for tethering interrelating networks from distinguishable authoritative factors such as rivals, unconstitutional brigades, cyber threats, etc. These infrastructures swarms include human, physical elements, and cyber exemplars. The important part is cyber resilience against sapless and eruptive validation and guardianship orchestrations. For enhancing cyber security, this article introduces the Artificial Intelligence-induced Constructive Resilience Model (AI-CRM). Linear processing in critical infrastructures is the establishment in which something transfers straight from one stage to another and has a starting point and an ending point where the results change according to the critical infrastructures. Recurrent neural networks (RNNs) are a class of neural networks that help model sequence data.

Derived from feed-forward networks, RNNs exhibit similar behavior to how human brains function. Simply put: recurrent neural networks produce predictive results in sequential data that other algorithms can't. Resilience is the procedure and results of fortuitously accommodating difficult experiences, especially affability, and improvement to extraneous and intramural requirements. Service transition refers to altering the level of an indulgence based on service risk and tabulating service knowledge. Service risk is important for employment in transporting standard results, and curating service knowledge includes embracing informed determinations with contributors. Service transition includes high-level activities such as designing and collating service changes, building and testing new or changed service components, and redistributing new or changed service components into the existing environment.

In critical infrastructures, the adversaries are extracted to determine the probability of the service transition procedure. The proposed model accounts for the security necessities of the adversary impacting infrastructure elements based on probability. The adversaries are the impacts where the resilience level is identified for the probability state. This probability is determined using previous adversary impacts on infrastructure failures and session falls in governing operational services. From the service transition, the non-linear and the incremental impacts are determined by using the recurrent learning technique. If there are non-linear impacts are identified, then some of the recommendations are given to enhance the security level to increase the resilience state of the critical infrastructure. The estimation for linearity or stagnancy is validated using a recurrent learning exemplar over different service transition sessions.

The critical infrastructures are used here for the enabling of communication in the information transfer. From this, the resilience level is extracted in the adversaries for further service transition procedures. The critical infrastructures are used in the enhancements of the security administrations and the volatile authentications. These infrastructures are used in the different exemplars in the base of artificial intelligence for security necessities and also for further service transfer procedures. Then the reductions of the non-linear impacts are reduced by enhancing the high-security level to it. The process of simulating the critical infrastructures for the extortion of the resilience level and the adversaries are explained by the following equation (1) below:

$$\left. \begin{aligned} \beta_{n+1} &= \beta_n + f(\beta_n) \\ \beta_{n+1} &= \beta_n + gf(\beta_n) \\ \frac{d(g_n)}{dt} &= f(g(t), t, n) \\ g_{t+1} &= g_t + f(g_t, \partial t) \\ f_{i+1} &= f_i + (g(f_i, \partial t)) \\ \frac{d(g(t))}{dt} &= f(g_t, t, \partial t) \end{aligned} \right\} \quad (1)$$

where  $\beta$  is denoted as the critical infrastructure,  $f$  is represented as the communication in the session,  $g$  is represented as the information in the infrastructure,  $t$  is denoted as the information transfer procedure. Now from the critical

infrastructure, the resilience level is extracted for the service transition procedure. The adversaries are also determined due to the lag of the backend support in the critical infrastructure. The impacts of the infrastructure are identified for the determination of the robustness strength. The session drops and the infrastructure failures may lead to adversaries and a low resilience level. The values of the resilience level range from 0-1 and then the probability is determined for the further service transition procedure during the detection of the non-linear and the incremental impacts of the critical infrastructure by using recurrent learning. The process of determining the adversaries from the critical infrastructure is explained by the following equation (2) given below:

$$\left. \begin{aligned} \alpha_n &= (\alpha_1, \alpha_2, \dots, \alpha_n) \\ \alpha &= (\alpha_1, \alpha_2, \dots, \alpha_n) \\ E &= \{(\alpha_1, \beta_1), (\alpha_2, \beta_2), \dots, (\alpha_n, \beta_n)\} \\ \alpha(t) &= f(\alpha(t-1), \alpha(t-2), \dots, \alpha(t-m-1)) \\ \alpha(t+g) &= f(\alpha(t), \alpha(t-1), \dots, \alpha(t-m-1)) \\ F &= \alpha_1, \alpha_2, \dots, \alpha_t \end{aligned} \right\} \quad (2)$$

where  $\alpha$  is represented as the adversary detected from the critical infrastructure,  $E$  is denoted as the lag of backend support. The resilience level is identified to determine the validity strength and then these adversaries are determined from the failures of the critical infrastructure and the failures of the sessions in it. The resilience level determination from the critical infrastructure is explained by the following equation (3) given below:

$$\left. \begin{aligned} H_t &= f_t \odot H_{t-1} + (g_t \odot \alpha_t) \left[ \begin{array}{c} f^{t_1 \alpha} \\ \dots \\ f^{t_2 \alpha} \end{array} \right]^T \in \alpha^{t \times g} \\ \alpha_t &= \sum_{\alpha \beta} (W_{\alpha \beta} + H_{\alpha \beta} + \beta_t) \in H^T \\ f_t^\alpha &= (W_\alpha^{-1} + H_\beta^{-1} + \beta_t) \in H^{-1} \\ f_t^\beta &= (W_\beta^{-1} + H_\alpha^{-1} + \alpha_t) \in H^{-2} \\ f_t &= f_t^1 \otimes f_t^2 \in H^{t \times g} \\ &= f_t^1 \cdot f_t^2 \end{aligned} \right\} \quad (3)$$

where  $H$  is denoted as the resilience level of the infrastructure,  $W$  is represented as the determination of the validation strength.

The critical infrastructure performs  $F \forall t$  such that  $W$  is computed for the preference of  $\alpha$ . If  $\alpha$  is detected, then  $g$  those swings in  $t$  due to  $\alpha$  are computed for which  $E$  support assessment is performed. If support is provided, then the probability for resilience is computed. This probability computation is discussed in the pursuing equations. Contrarily if there is no support then  $f$  is terminated; the  $H$  is computed only if  $W$  ensures there is no  $\alpha$  at any  $t$  such that  $E$  is required/ withheld. Based on the previous infrastructure failures and session fall while handling the operational services, the probability is

computed.

$$\left. \begin{aligned} \beta_t &= P \left( \alpha_0 + \sum_{j=1}^f \alpha_j F \left( \sum_{i=1}^P \beta_{ij} \beta_{j-1} \right) \right) \\ F(\alpha) &= \frac{1}{1+t-\alpha} \\ P(\alpha) &= \alpha \\ P(\alpha)^{-t} &= \begin{bmatrix} P\alpha_{11} & P\alpha_{12} & \dots & P\alpha_{1n} \\ P\alpha_{21} & P\alpha_{22} & \dots & P\alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ P\alpha_{n1} & P\alpha_{n2} & \dots & P\alpha_{nn} \end{bmatrix} \end{aligned} \right\} \quad (4)$$

In equation (4), where  $P$  is represented as the probability of the resilience level of the adversaries. From the outcome of the resilience level detection process, the service transition takes place. The services are changed in the critical infrastructure simultaneously due to the attackers/adversaries. The services are changed to enhance the resilience level in the infrastructure by eliminating infrastructure failures and session drops. The output of the service transition helps to identify the non-linear and incremental impacts of the infrastructure. The processes of changing the services are happening according to the level of the adversaries and the resilience probability level. The different transitions are made for the further security enhancement process and then to repeatedly assume the incremental impacts of the critical infrastructure. The process of service transition from the outcome of the adversaries and the resilience level from the critical infrastructure is explained by the following equation (5) given below:

$$\left. \begin{aligned} T[\alpha + \beta] &= \sigma(\alpha(t) W_{\alpha t} + \sigma(\Delta t \Delta t \alpha w t t + \beta t)) \\ W[\alpha] &= f[\alpha] \odot W[\alpha - 1] + i[\alpha] \odot T[\alpha] \\ &= \sigma \alpha (\alpha[\beta] W_{\alpha \beta} + h[\beta - 1] W_{\beta \beta} + \beta_\alpha) \\ T[\alpha] &= \sigma_0(\alpha[\beta] W_0 + t[\alpha] W t_0 + f \alpha \\ &= 1 W f_0 + W t_0 \odot f[\alpha] + \beta_0 \\ T_1[\alpha] &= \sigma_1(\alpha(W) + \sigma \Delta t (\Delta t[\alpha])) \\ &\text{such that } W_{t1} \leq 0 \\ T_2[\alpha] &= \sigma_2(\beta(W) + \sigma \Delta t (\Delta t[\beta])) \end{aligned} \right\} \quad (5)$$

where  $T$  is denoted as the service transition operation,  $\sigma$  is represented as the outcome of the resilience probability detection procedure,  $i$  is denoted as the impacts of the procedure. The service transition is happening based on the acquired adversaries and then according to that the changes in the service distribution to the infrastructure are done. From the outcome of the service transition, the incremental and the non-linear impacts which are used in the enhancement of the security level are determined.

$$\left. \begin{aligned} \frac{\partial \alpha_j}{\partial W_{jT} Q} &= \alpha_j Q \\ \frac{\partial \beta_j}{\partial W_{jT} Q} &= \alpha_j Q_1 \\ \frac{\partial \alpha_j(1)}{\partial W_{jT} Q} &= -\alpha_j Q \\ \frac{\partial \beta_j(1)}{\partial W_{jT} Q} &= -\alpha_j Q_1 \end{aligned} \right\} \quad (6)$$

In equation (6), where  $Q$  is represented as the service-changing procedure according to the adversaries,  $j$  is denoted as the level of the attackers. Now from the service transition outcome, the incremental and the non-linear impacts

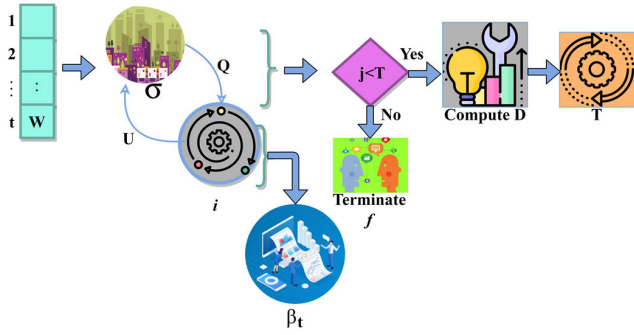


FIGURE 1. Transition operation.

are derived by using the recurrent learning technique. The transition operation is portrayed in Fig. 1.

The  $W \forall t$  is estimated using equation (3) from which  $T$ 's significance is validated. If  $Q$  to  $i$  is observed then it results in  $f$  termination if  $j > T$  else  $D$ -based  $T$  operations are pursued. If  $i$  increases  $\sigma$  from  $U$  mitigation, then  $\beta_t \forall P$  is estimated in the intermediate  $t$ . This does not require any  $T$ , retaining the previous state. In Table 1, the possibility of  $P$  and  $T$  for the varying users is presented.

The  $P$  and  $T$  probabilities are estimated under  $E$ ,  $\sigma$ , and  $i$ ; the estimations are validated using the  $T$  if  $\sigma$  to  $i$  transitions are high else  $i$  is low; this is less. For marking this feature, if  $T = 1$ , then  $i$  is high else  $i$  is low; this is prevented by terminating  $f$ . Based on the varying features of  $H \forall W$ , the  $j$  is suppressed for any condition defined in equation (8). If the  $Q$  is initiated, then the  $\beta_t$  is suppressed for  $E$  such that  $t$  is abrupt for increasing the  $\sigma$  such that  $i$  is less (Table 3). The non-linear impacts are the ones with no improvements in the resilience level after the service transition procedure. The lesser resilience level leads to non-linear impacts which are not helpful in the critical infrastructure. If the non-linear impacts are identified in the service transition, then security-level enhancements are made to reduce them. The process of extracting the non-linear impacts from the service transition by using the recurrent learning algorithm is explained by the following equations (7) given below:

$$\left. \begin{aligned} \frac{\partial U}{\partial W_j Q} &= \frac{\partial U}{\partial t} \left( \frac{\partial t^i}{\partial \alpha_j} \frac{\partial \alpha_j}{\partial W_j Q} + \frac{\partial t^i}{\partial \beta_j} \frac{\partial \beta_j}{\partial W_j Q} \right) \\ &+ \frac{\partial U}{\partial t} \left( \frac{\partial t^i}{\partial \alpha_j} \frac{\partial \alpha_j}{\partial W_j Q} + \frac{\partial t^i}{\partial \beta_j} \frac{\partial \beta_j}{\partial W_j Q} \right) \\ &= -\partial_j Q \left( u_\alpha^i \alpha_i Q + \alpha_\beta^j \alpha_i Q \right) \\ &= -\partial_j T \left( \beta_u^i \beta_i Q + \beta_\alpha^j \beta_i Q \right) \\ \frac{\partial U_1}{\partial W_j Q} &= \frac{\partial U}{\partial t} \left( \frac{\partial t^i}{\partial \alpha_j} \frac{\partial \alpha_j}{\partial W_j Q} + \frac{\partial t^i}{\partial \beta_j} \frac{\partial \beta_j}{\partial W_j Q} \right) \\ &+ \frac{\partial U_1}{\partial t} \left( \frac{\partial t^i}{\partial \alpha_j} \frac{\partial \alpha_j}{\partial W_j Q} + \frac{\partial t^i}{\partial \beta_j} \frac{\partial \beta_j}{\partial W_j Q} \right) \\ &= -\partial_j Q \left( u_\alpha^i (-\alpha_i Q) + \alpha_\beta^j (-\alpha_i Q) \right) \\ &= -\partial_j T \left( \beta_u^i (-\beta_i Q) + \beta_\alpha^j (-\beta_i Q) \right) \end{aligned} \right\} \quad (7)$$

where  $U$  is denoted as the non-linear impacts. The resilience level which has no improvements in-between the two transitions are non-linear impact. This impact may cause infras-

TABLE 1. Properties probability of  $P$  and  $T$ .

Users	$E$		$\sigma$		$i$	
	$T$	$P$	$T$	$P$	$T$	$P$
40	0	0.11	0.13	0.04	0.52	0.17
80	1	0.19	0.23	0.35	0.77	1.35
120	1	0.25	0.26	0.02	0.74	1.02
160	0	0.31	0.34	0.11	0.30	0.62
200	1	0.34	0.39	0.22	0.61	0.78
240	0	0.28	0.46	0.15	0.38	0.46

tructure failures and session drops such that in equation (8)

$$\left. \begin{aligned} w_i^{-\alpha m} &= w_i^{-\alpha m} + \frac{D\alpha m}{(n_{m-1}+1)} \beta_{i,m-1,1=1,\dots,n} \\ w_0^{-\alpha m} &= w_0^{-\alpha m} + \frac{D\alpha m}{(n_{m-1}+1)} \in \alpha_m \\ w_i^{-\alpha j} &= w_i^{-\alpha j} + \frac{D\alpha j}{(n_{j-1}+1)} \beta_{i,j-1,1=1,\dots,n} \\ w_0^{-\alpha j} &= w_0^{-\alpha j} + \frac{D\alpha j}{(n_{j-1}+1)|\beta_j|} \in \alpha_j \\ w_i^{-\alpha 1} &= w_i^{-\alpha 1} + \frac{D\alpha 1}{(n+1)} \in \alpha_1 \alpha_{2,1=1,\dots,n} \\ w_0^{-\alpha 1} &= w_0^{-\alpha 1} + \frac{D\alpha 1}{(n+1)|\beta_j|} \in \alpha_j \\ \frac{1}{n} \sum_{n=1}^T \sum_{\alpha} (\alpha m)^2 (w) &= \frac{1}{n} \sum_{n=1}^T \alpha_t \leq w \end{aligned} \right\} \quad (8)$$

The computation for linearity or stagnancy is validated using a recurrent learning paradigm over different service transitions. This linearity of resilience is identified over the multiple transition procedures and then by determining the adversary levels in the transition process. Where  $D$  is represented as the improvement level of the resilience in the infrastructure,  $m$  is denoted as the multiple transitions. Now the incremental impacts are derived from the service transition by using the recurrent learning algorithm. It denotes the maximum resilience level in-between the transitions. The incremental impacts are computed over the transitions which reduce the infrastructure failures and session drops. The process of extorting the incremental impacts after the service transition by the recurrent learning technique is explained by the following equation (9) given below:

$$\left. \begin{aligned} f(\alpha) &= \frac{1}{1+Z(\frac{-\alpha}{\sigma})} \\ \beta(t) &= Z(t) + N(t) \\ \hat{\beta}(t) &= \hat{Z}(t) + \hat{N}(t) \\ G &= \{u, \alpha, \beta\} \\ B &= \{(w_{ij})\}_{j=1}^m \\ \alpha(t) &= f(\alpha(t)) \end{aligned} \right\} \quad (9)$$

where  $Z$  is represented as the incremental impacts of the service transition. The impacts must compute the incremental outcome which leads to the reduction of the session drops and then the infrastructure failures. The recurrent learning process for incremental and non-linear impact differentiation is presented in Fig. 2.

In the recurrent learning process  $\frac{\partial U}{\partial t}$  and  $\frac{\partial U}{\partial W}$  differentiations are induced for  $T = 0$  and  $T = 1$  conditions. In particular, the differentiations are induced for  $\alpha$  in detecting  $D$  or  $N$ . If  $D$  or  $N$  are extracted then  $f \in T$  is segregated

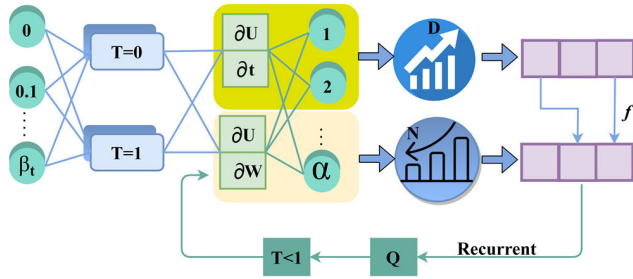


FIGURE 2. Incremental and non-linear impact differentiation.

for preventing new security lags. The recurrent learning is thus instigated for  $Q$  from the  $\sigma$  to  $i$  (or)  $ito\sigma$  transition for preventing frequent  $T = 1$ . Thus, in the consecutive  $f$  the impact validations are subsequent in leveraging security implications (Fig. 2). After consummating the impacts after the service transition, the security enhancement procedure takes place. Then the modifications are done based on the outcome of the impact determination process.

$$\left. \begin{aligned} f &:= U_t + N[t] \\ f &:= U_t - N(t\alpha, U_\alpha, U_{\alpha\alpha}, \dots) \\ \beta_{i+1} &= \beta_i + f(\beta_i, \sigma_i) \\ \dot{\alpha}(t) &= f(\alpha(t)) \\ \dot{\alpha}(t) &= \hat{f}(\alpha(\beta + t)) \\ \alpha(t_0) &= \alpha_0 \\ \alpha(t) &= \alpha(t_0) + \int_0^t f(x(h)) dh \\ \forall t \in (\alpha, \beta) \end{aligned} \right\} \quad (10)$$

In equation (10), where  $N$  is represented as the results of the determination of the impact process. Now if there is a non-linear impact from the service transition process, then the security level is enhanced for the reduction of the non-linear impacts. Some of the modifications are made at the security level to prevent non-linearity impacts. The resilience is improved by augmenting security measures that are identified as an output of linear impacts over the services. Again, after increasing the security level, the linearity is also increased then the probability of the resilience level is identified. The procedure of enhancing the security level after acquiring non-linear impact is explained by the following equations (11) given below:

$$\left. \begin{aligned} \alpha(a + b) &= \alpha(a) + h\alpha(b) + \beta(h^2) \\ \alpha(t + h) &= \alpha(a) + hf(\alpha(a)) \\ \alpha(t_0) &= \alpha_0 \\ \alpha(a + b) &= \alpha(a) + hf(\alpha(t), \sigma(t)) \\ \alpha(t_0) &= \alpha_0(b_0 + f(t_0)) \\ \dot{\alpha}_1(t) &= f_i(\alpha_i(t) \dots \alpha_n(t), t, \sigma(t)) \quad i = 1, \dots, n \\ \alpha_1(t_0) &= \tilde{\alpha}_0 \dots, \alpha_n(t_0) \\ &= \tilde{\alpha}_n \end{aligned} \right\} \quad (11)$$

where  $a$  is denoted as the enhancements of the security level,  $b$  is represented as the existing security level. After assuming the impacts of the service transition process, the security level

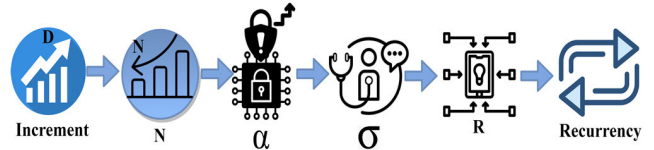


FIGURE 3. Security level enhancement process.

is increased if there is a non-linear impact. This helps in the elimination of the session and infrastructure failures.

$$\left. \begin{aligned} \phi_i(\alpha_1(t_1), \dots, \alpha_n(t_1)) &= 0 \\ \text{where } i &= 1, \dots, P \leq n \\ \varepsilon(\alpha_1(t_1), \dots, \alpha_n(t_1)) & \\ \sigma^*(t) &= u(\alpha_1, \dots, \alpha_n, t) \\ \alpha_i(t + \Delta t) &= \alpha_i(t) + \dot{\alpha}_i(t) \Delta t + 0(\Delta t^2) \\ &= \alpha_i(t) + f_i(\alpha_i(t), \dots, \alpha_n(t), t, \sigma^*(t), \Delta t + 0(\Delta t^2)) \end{aligned} \right\} \quad (12)$$

As per equation (12), where  $\phi$  is denoted as the alterations made in the security level,  $\varepsilon$  is denoted as the security level after enhancements. This process is done repeatedly between the two service transitions to enhance the resilience level in the critical infrastructure. Fig. 3 presents the security level enhancements in critical infrastructure.

The increment classified inputs are validated for the  $N$  before and after  $\alpha$  such that  $\phi$  performed the recurrency is pursued validating security. Therefore, the available & recommendations are pursued  $\alpha$  improvements. However,  $\frac{\partial U}{\partial W}$  alone classifier further recurrency in  $T = 0$  constraints for preventing failures (Refer to Fig. 3). By this, the probability can be increased and improves resilience through security augmentations and modifications. The process of identifying the impacts simultaneously between the service transitions is explained by the following equations (13) & (14) given below:

$$\left. \begin{aligned} O &= \sum_{\sigma} \left[ \sum_{i=1}^n \frac{\partial R}{\partial \alpha_i} f_i \Delta t + \frac{\partial R}{\partial t} \Delta t + 0(\Delta t^2) \right] \\ O &= \sum_u \left[ \sum_{i=1}^n R \alpha_i f_i + Rt \right] \\ \sum_{i=1}^n R \alpha_i f_i + Rt &(\alpha_1, \dots, \alpha_n, t, u^*) \\ \text{where } \frac{\partial R}{\partial U} &= 0 \\ \frac{d}{dt} \begin{bmatrix} h(t) \\ \alpha(t) \end{bmatrix} &= f \left( \begin{bmatrix} h(t) \\ \alpha(t) \end{bmatrix}, t \right) \\ \begin{bmatrix} h(0) \\ \alpha(0) \end{bmatrix} &= \begin{bmatrix} \alpha \\ 0 \end{bmatrix} \end{aligned} \right\} \quad (14)$$

where  $O$  is represented as the increased resilience level,  $R$  is denoted as the converging solution by recurrent learning. This process helps in the reduction of infrastructure failures, session drops and time lags. This also enhances the adversary detection ratio within a short period and service distribution to critical infrastructures. The security level is also enhanced if there is a non-linear impact occurred. By using the recurrent learning technique, the incremental impacts are determined

after the service transition. Table 3 presents the algorithmic representation for  $R$  focused  $\alpha$  from  $T = 1$  to  $T = 0$  sequence.

**Algorithm 1** Representation for **R**

```

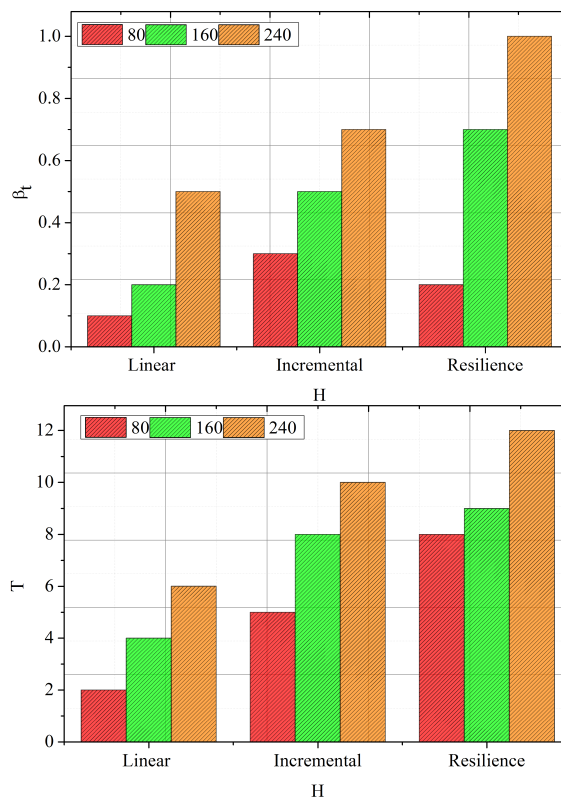
Input:  $D, \phi$ 
1:  $\forall \beta_t \in fdo\{$ 
2:   Compute  $I$  from equation (5) // impact estimation.
3:   if  $\{Q > T\}$  then // Transition condition
4:     Validate  $\frac{\partial U}{\partial t} \forall j = 1, 2, \dots, Q$  // non-linearity estimation.
5:     if  $\{\frac{\partial U}{\partial t} = D\}$  in any  $j$  then
6:       break; computer  $N$ ; goto step 2
7:     end if
8:     Update  $\alpha$  using equation (11) // security level.
9:   end if
10:  Compute  $O \forall \beta_t = \{0.1, 0.2, \dots, 1\}$ 
11:  if  $\{\beta_t * D = \varepsilon\}$  then
12:    Compute implication of  $\phi$ 
13:    Goto step 4  $\forall \frac{\partial U}{\partial W}$  and repeat till step: 13
14:  end if
15: end loop
    
```

This short section presents the self-analysis from the equation explanations presented above. This analysis presents the free flow in the increasing and connecting order of the explanations. In Fig. 4, the  $H$  based on  $\beta_t$  and  $T$  are validated by varying the users.

The proposed model maximizes  $H$  for three factors namely linearity, incremental, and resilience. These features are maximized based on the available  $W \forall f$ . If  $\sigma$  is consistently high  $\forall \frac{\partial W}{\partial t}$  and  $\frac{\partial W}{\partial U}$  then the available users consented to low  $j$ . This is due to less  $i$  such that  $(N, Z)$  are condensed for the successive  $\phi$ . If the alterations are non-applicable, then  $\alpha$  requirements are satisfied. Therefore the  $\alpha$  and  $H$  improvements are validated for increasing  $\beta_t$  such that  $D$  requires  $Q \forall T$ . The recurrent learning process requires  $N$  and  $D$  validation for suppressing  $\alpha$ . If the suppressions are successful, then  $H$  is increased for which  $Q$  dual  $f$  and  $t$  based recurrent validations are optimal. Therefore, the output for  $R$  is leveraged towards a common assessment of  $O$ , preventing  $\alpha$  impacts.

**IV. RESULTS AND DISCUSSION**

This section presents the comparative analysis using the experimental simulations using the OPNET modeler. In the simulation, 240 users accessing 14 resources of varying intervals say 10min-40mins are considered. The simulation setup is modeled for accessing 8 services considering 13 transitions for a single user. The simulation utilizes the following metrics for analysis: detection ratio, session drops, infrastructure failure, time lag, and service dissemination ratio. The service transitions and users are varied across different sharing intervals; the methods p-ROM [20], IFogLearn [28], and ATM [30] are augmented in the comparative analysis.



**FIGURE 4.** H Analysis for  $\beta_t$  and  $T$ .

**A. DETECTION RATIO ANALYSIS**

The detection ratio is efficacious by using the resilience probability level. Based on the previous infrastructure failures and session fall while handling the operational services, the probability is computed. From this outcome, the service transition takes place. The impacts of the infrastructure are identified for the determination of the robustness strength. The session drops and the infrastructure failures may lead to adversaries and a low resilience level. The resilience level is identified to determine the validity strength and then these adversaries are determined from the failures of the critical infrastructure and also the failures of the sessions in it. From this outcome, the service transition is used to determine the non-linear impacts and the incremental impacts. The adversaries are enhanced by altering the security levels if there are non-linear impacts are identified after the service transition. Based on the resilience and the probability level, the detection ratio is increased to improvise the adversaries. After detecting the adversaries in the critical infrastructure, the service transition takes place based on the outcome (Fig. 5).

**B. SESSION DROP ANALYSIS**

The drop of the session is less in the critical infrastructure by enhancing the security level and then service transition without any time lag. From the service transition process, the non-linear and the incremental impacts are determined. If there is a non-linear impact, then some of the alterations

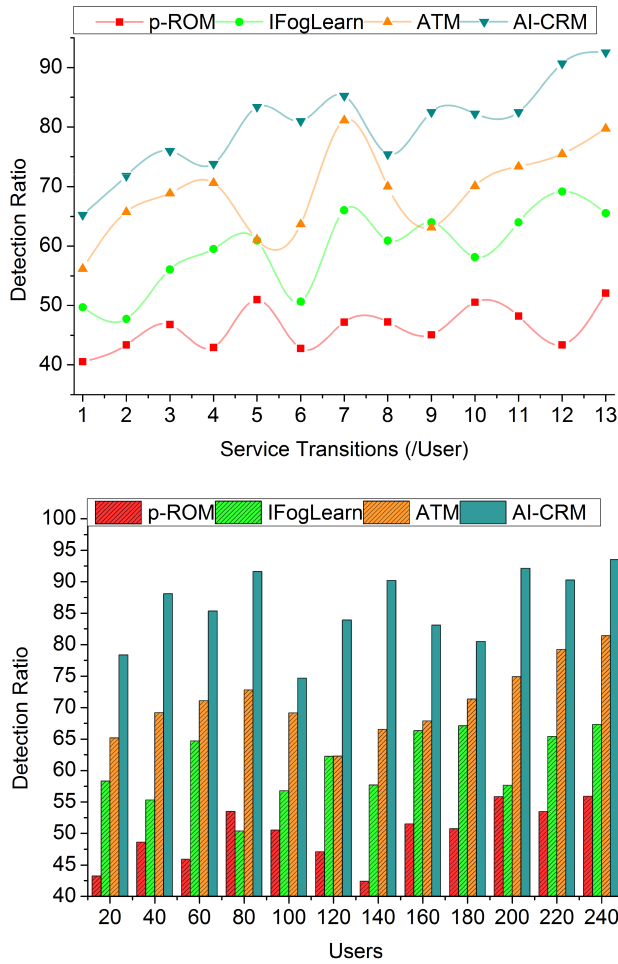


FIGURE 5. Detection ratio analysis.

are made for the security level to enhance the resilience level in critical infrastructure. The session drops and the infrastructure failures are eliminated by using recurrent learning for the determination of the impacts of the critical infrastructure. By improving the resilience level in the adversary, the non-linear impacts are reduced which leads to the elimination of the session drops. With the service transition process, the impacts are determined simultaneously based on the previous infrastructure failures and session drops. With these procedures, the session drops are less with the help of the recurrent learning technique in the determination procedures of impacts (Fig. 6).

C. INFRASTRUCTURE FAILURE ANALYSIS

The infrastructure failures are less in this process by enhancing the resilience probability level. The recurrent learning technique is used in the identification of the impacts of critical infrastructure. From the outcome of the resilience level detection process, the service transition takes place. The services are changed in the critical infrastructure simultaneously due to the attackers/adversaries. The services are changed to enhance the resilience level in the infrastructure

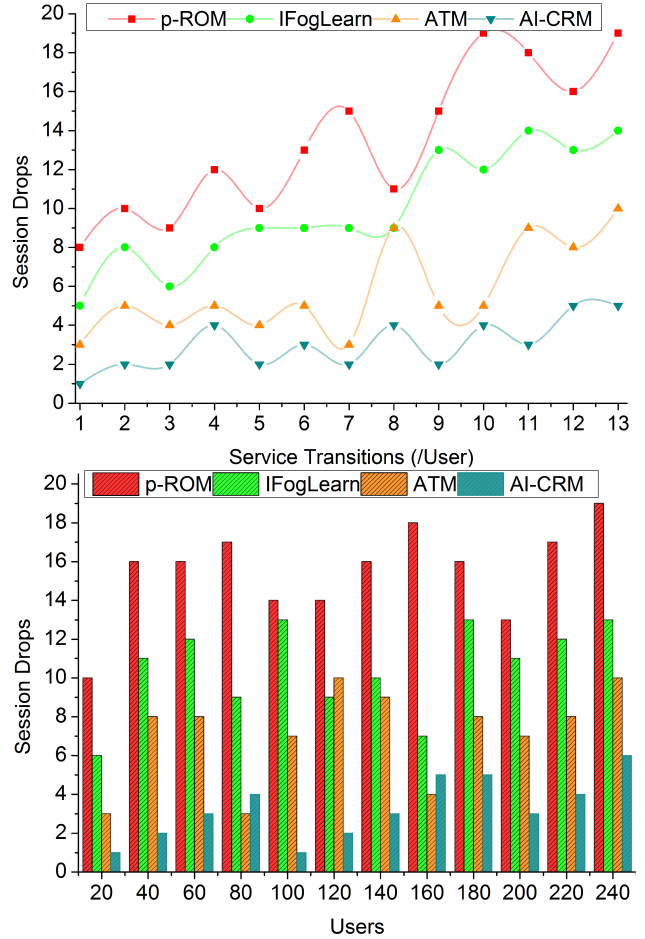


FIGURE 6. Session drop analysis.

by eliminating infrastructure failures and session drops. Then the impacts are identified if the incremental impacts are computed over the transition which reduces the infrastructure failures and session drops help in reducing the session drops and failures. After assuming the impacts of the critical infrastructure between the service transition processes, the security level is increased if there is a non-linear impact. This helps in the elimination of the session and infrastructure failures. By using the recurrent learning technique infrastructure failures are reduced by identifying the impacts in it (Fig. 7).

D. TIME LAG

The time lag is reduced in this process by increasing the robustness strength during the service transition process. If there is no backend support, then the resilience level is made low and then the adversaries are low. By enhancing the security level in critical infrastructure, the resilience level is increased. Based on the previous infrastructure failures and the session drops, this process is preceded to avoid time lags during the procedure of enhancing the service transition. The communication enables information transfer in the service transition and security enhancement operations. If the non-linear impacts are identified by using the recurrent learning



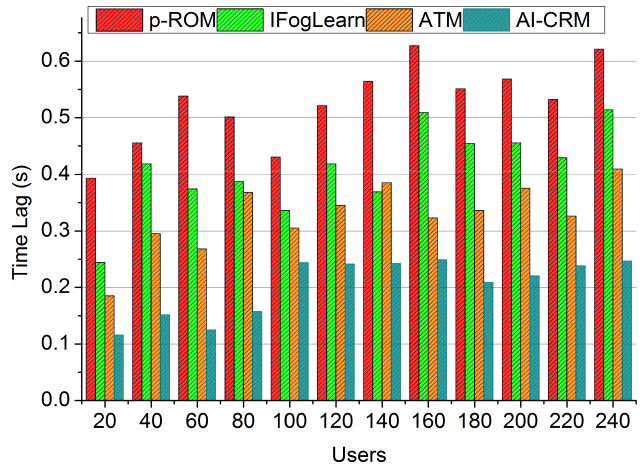
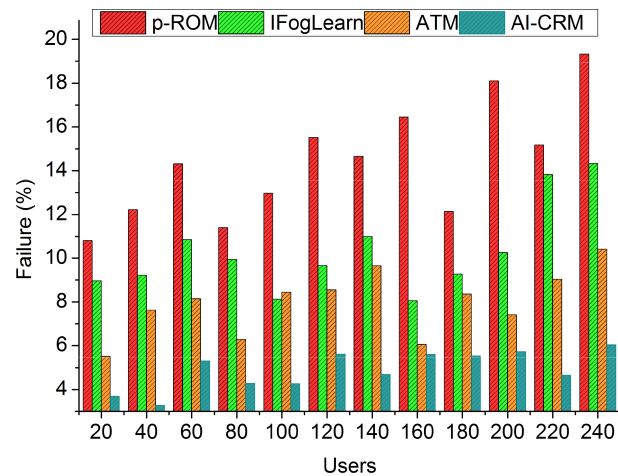
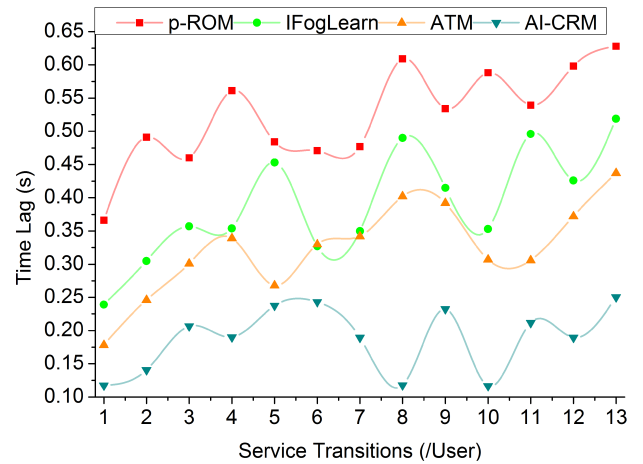
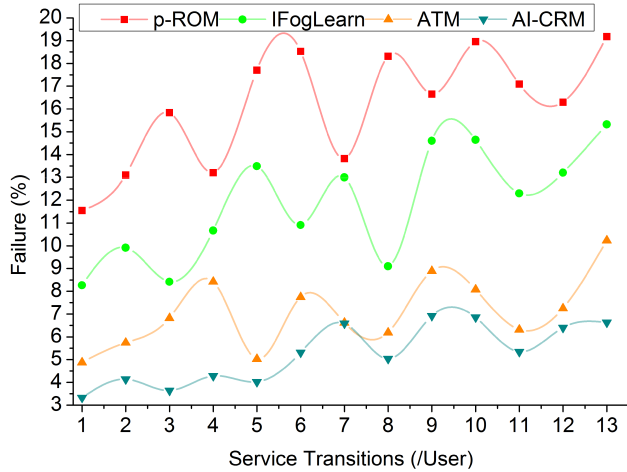


FIGURE 7. Failure ratio analysis.

FIGURE 8. Time ratio analysis.

technique after the service transition, then the security level enhancements are made to reduce them. The resilience is improved by augmenting security measures that are identified as an output of linear impacts over the services which help in reducing the time lags in the further procedures. The time taken for the entire procedure is also less by using the learning technique after the service transition process (Fig. 8).

**E. SERVICE DISSEMINATION RATIO**

The service dissemination ratio is efficacious in this process with the help of the adversary extraction process. The services are changed in the critical infrastructure simultaneously due to the adversaries. The services are changed to enhance the resilience level in the infrastructure by eliminating infrastructure failures and session drops. The output of the service transition helps to identify the non-linear and incremental impacts of the infrastructure. The processes of changing the services are happening according to the level of the adversaries and the resilience probability level. The service transition is happening based on the acquired adversaries and then according to that the changes in the service distribution to the infrastructure are done. From the outcome of the ser-

TABLE 2. Comparative analysis of service transitions.

Metrics	p-ROM	IFogLearn	ATM	AI-CRM
Detection Ratio	52.06	65.53	79.73	92.547
Session Drops	19	14	10	5
Failure (%)	19.18	15.32	10.23	6.631
Time Lag (s)	0.628	0.519	0.437	0.2504
Dissemination Ratio	74.54	80.61	89.77	94.98

vice transition, the incremental and the non-linear impacts which are used in the enhancement of the security level are determined. The different transitions are made for the further security enhancement process and then to repeatedly assume the incremental impacts of the critical infrastructure (Fig. 9). The comparative analysis results are tabulated in Tables 2 and 3 for the service transitions and users.

This proposed model leverages detection ratio and dissemination by 13.39% and 13.34%. This model reduces the session drops, failure, and time lag by 10.88%, 8.28%, and 8.76% respectively.

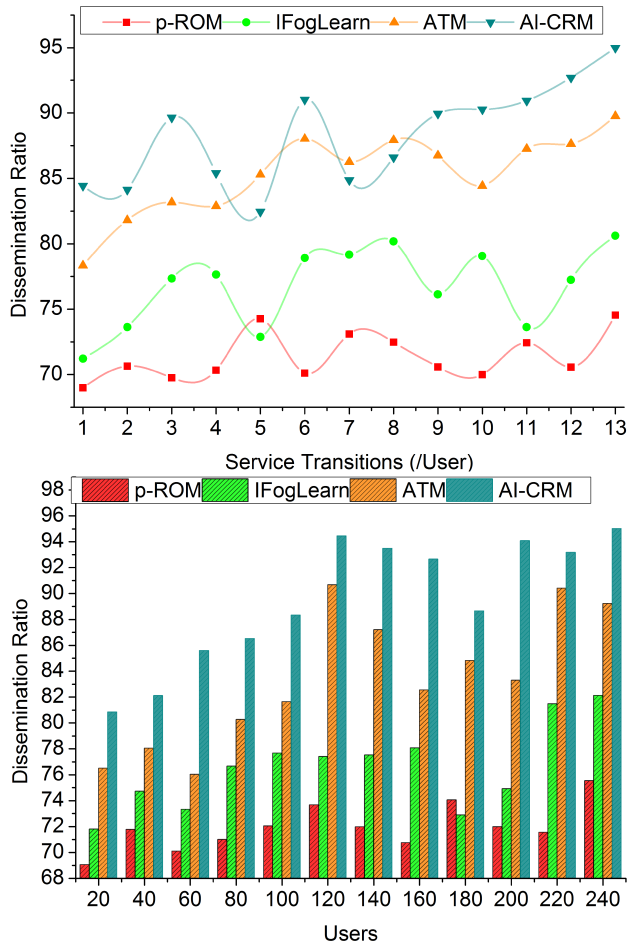


FIGURE 9. Service dissemination ratio analysis.

TABLE 3. Comparative analysis of users.

Metrics	p-ROM	IFogLearn	ATM	AI-CRM
Detection Ratio	55.91	67.3	81.4	93.506
Session Drops	19	13	10	6
Failure (%)	19.32	14.32	10.41	6.031
Time Lag (s)	0.621	0.514	0.409	0.2465
Dissemination Ratio	75.53	82.12	89.23	95.023

This proposed model leverages detection ratio and dissemination by 12.65% and 12.73%. This model reduces the session drops, failure, and time lag by 9.52%, 8.65%, and 8.68% respectively.

### V. CONCLUSION

For improving the session-level security of critical infrastructures, this article introduced a constructive resilience model backed by artificial intelligence. More specifically, recurrent learning-based resilience validation is performed in this proposed model. The learning performs the classification and detection of service transitions based on linear

and non-linear differentiations. Considering the transitions due to the adversary impact in the sessions the stagnancy in resilience is estimated and updated for maximum iterations. Therefore, the update process is recurrent for providing recommendations on security modifications and resilience level alterations. The adverse impact of the service sessions is measured using stagnancy, drops, and infrastructure failures. These metrics are rectified using new security augmentations and recommendation-based modifications in infrastructure application, security implication, and adversary detection. Thus, the proposed model is reliable in reducing session drops by 10.88% and failure by 8.28% under the varying service transitions. In the future, the blockchain paradigm is planned to be incorporated for increasing the processing of concurrency. This concurrency improvement is required for adversary detection, service reallocation, and resilience verification using adaptable learning paradigms.

### 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] A. Al-abassi, A. N. Jahromi, H. Karimipour, A. Dehghantanha, P. Siano, and H. Leung, "A self-tuning cyber-attacks' location identification approach for critical infrastructures," *IEEE Trans. Ind. Informat.*, vol. 18, no. 7, pp. 5018–5027, Jul. 2022.
- [2] I. Barak, "Critical infrastructure under attack: Lessons from a honeypot," *Netw. Secur.*, vol. 2020, no. 9, pp. 16–17, Sep. 2020.
- [3] E. M. Wells, M. Boden, I. Tseytlin, and I. Linkov, "Modeling critical infrastructure resilience under compounding threats: A systematic literature review," *Prog. Disaster Sci.*, vol. 15, Oct. 2022, Art. no. 100244.
- [4] J. Mauro, P. Wood, S. Zanolgo, J. Silbermann, T. Sookoor, A. Lorenzo, R. Sleight, J. Rogers, D. Muller, N. Armiger, and C. Rouff, "Agile services and analysis framework for autonomous and autonomic critical infrastructure," *Innov. Syst. Softw. Eng.*, vol. 19, no. 2, pp. 145–156, 2021.
- [5] V. E. Kulugh, U. M. Mbanaso, and G. Chukwudebe, "Cybersecurity resilience maturity assessment model for critical national information infrastructure," *SN Comput. Sci.*, vol. 3, no. 3, p. 217, 2022.
- [6] G. M. Makrakis, C. Koliass, G. Kambourakis, C. Rieger, and J. Benjamin, "Industrial and critical infrastructure security: Technical analysis of real-life security incidents," *IEEE Access*, vol. 9, pp. 165295–165325, 2021.
- [7] A. H. K. Babar and Y. Ali, "Framework construction for augmentation of resilience in critical infrastructure: Developing countries a case in point," *Technol. Soc.*, vol. 68, Feb. 2022, Art. no. 101809.
- [8] R. Li and Y. Gao, "On the component resilience importance measures for infrastructure systems," *Int. J. Crit. Infrastruct. Protection*, vol. 36, Mar. 2022, Art. no. 100481.
- [9] A. Mottahedi, F. Sereshki, M. Ataei, A. N. Qarhasanlou, and A. Barabadi, "Resilience estimation of critical infrastructure systems: Application of expert judgment," *Rel. Eng. Syst. Saf.*, vol. 215, Nov. 2021, Art. no. 107849.
- [10] B. Zou, P. Choobchian, and J. Rozenberg, "Cyber resilience of autonomous mobility systems: Cyber-attacks and resilience-enhancing strategies," *J. Transp. Secur.*, vol. 14, pp. 137–155, Mar. 2021.
- [11] Y. Almoghathawi, A. D. González, and K. Barker, "Exploring recovery strategies for optimal interdependent infrastructure network resilience," *Netw. Spatial Econ.*, vol. 21, no. 1, pp. 229–260, Mar. 2021.
- [12] H. Li, D. Li, X. Zhang, G. Shou, Y. Hu, and Y. Liu, "A security management architecture for time synchronization towards high precision networks," *IEEE Access*, vol. 9, pp. 117542–117553, 2021.
- [13] L. Cui, Y. Qu, G. Xie, D. Zeng, R. Li, S. Shen, and S. Yu, "Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures," *IEEE Trans. Ind. Informat.*, vol. 18, no. 5, pp. 3492–3500, May 2022.

- [14] Z. A. Sheikh, Y. Singh, P. K. Singh, and K. Z. Ghafoor, "Intelligent and secure framework for critical infrastructure (CPS): Current trends, challenges, and future scope," *Comput. Commun.*, vol. 193, pp. 302–331, Sep. 2022.
- [15] G. E. I. Selim, E. E.-D. Hemdan, A. M. Shehata, and N. A. El-Fishawy, "Anomaly events classification and detection system in critical industrial Internet of Things infrastructure using machine learning algorithms," *Multimedia Tools Appl.*, vol. 80, no. 8, pp. 12619–12640, Mar. 2021.
- [16] L. Franchina, G. Inzerilli, E. Scatto, A. Calabrese, A. Lucariello, G. Brutti, and P. Roscioli, "Passive and active training approaches for critical infrastructure protection," *Int. J. Disaster Risk Reduction*, vol. 63, Sep. 2021, Art. no. 102461.
- [17] T. Zhao and L. Sun, "Seismic resilience assessment of critical infrastructure-community systems considering looped interdependences," *Int. J. Disaster Risk Reduction*, vol. 59, Jun. 2021, Art. no. 102246.
- [18] M. A. Husnoo, A. Anwar, R. K. Chakraborty, R. Doss, and M. J. Ryan, "Differential privacy for IoT-enabled critical infrastructure: A comprehensive survey," *IEEE Access*, vol. 9, pp. 153276–153304, 2021.
- [19] B. A. Alkhaleel, H. Liao, and K. M. Sullivan, "Risk and resilience-based optimal post-disruption restoration for critical infrastructures under uncertainty," *Eur. J. Oper. Res.*, vol. 296, no. 1, pp. 174–202, Jan. 2022.
- [20] Y.-P. Fang, C. Fang, E. Zio, and M. Xie, "Resilient critical infrastructure planning under disruptions considering recovery scheduling," *IEEE Trans. Eng. Manag.*, vol. 68, no. 2, pp. 452–466, Apr. 2021.
- [21] X. Liu, Y.-P. Fang, and E. Zio, "A hierarchical resilience enhancement framework for interdependent critical infrastructures," *Rel. Eng. Syst. Saf.*, vol. 215, Nov. 2021, Art. no. 107868.
- [22] L. Galbusera, M. Cardarilli, M. Gómez Lara, and G. Giannopoulos, "Game-based training in critical infrastructure protection and resilience," *Int. J. Disaster Risk Reduction*, vol. 78, Aug. 2022, Art. no. 103109.
- [23] Y. Cheng, E. A. Elsayed, and X. Chen, "Random multi hazard resilience modeling of engineered systems and critical infrastructure," *Rel. Eng. Syst. Saf.*, vol. 209, May 2021, Art. no. 107453.
- [24] M. Xu, M. Ouyang, L. Hong, Z. Mao, and X. Xu, "Resilience-driven repair sequencing decision under uncertainty for critical infrastructure systems," *Rel. Eng. Syst. Saf.*, vol. 221, May 2022, Art. no. 108378.
- [25] Y. Wu, H.-N. Dai, and H. Wang, "Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2300–2317, Feb. 2021.
- [26] B. Sousa, M. Arieiro, V. Pereira, J. Correia, N. Lourenço, and T. Cruz, "ELEGANT: Security of critical infrastructures with digital twins," *IEEE Access*, vol. 9, pp. 107574–107588, 2021.
- [27] C. Fioravanti, S. Guarino, B. Mazzá, M. Nobili, F. Santucci, and S. M. Ansaldi, "A risk assessment framework for critical infrastructure based on the analytic hierarchy process," *IFAC-PapersOnLine*, vol. 55, no. 40, pp. 277–282, 2022.
- [28] A. Sharifi and S. Goli-Bidgoli, "IFogLearn++: A new platform for fog layer's IoT attack detection in critical infrastructure using machine learning and big data processing," *Comput. Electr. Eng.*, vol. 103, Oct. 2022, Art. no. 108374.
- [29] T. D. Ashley, R. Kwon, S. N. G. Gouriseti, C. Katsis, C. A. Bonebrake, and P. A. Boyd, "Gamification of cybersecurity for workforce development in critical infrastructure," *IEEE Access*, vol. 10, pp. 112487–112501, 2022.
- [30] S. Otoum, I. A. Ridhawi, and H. Mouftah, "Securing critical IoT infrastructures with blockchain-supported federated learning," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2592–2601, Feb. 2022.
- [31] V. A. Memos, K. E. Psannis, S. K. Goudos, and S. Kyriazakos, "An enhanced and secure cloud infrastructure for e-Health data transmission," *Wireless Pers. Commun.*, vol. 117, no. 1, pp. 109–127, Mar. 2021.
- [32] M. Masi, G. P. Sellitto, H. Aranha, and T. Pavleska, "Securing critical infrastructures with a cybersecurity digital twin," *Softw. Syst. Model.*, vol. 22, no. 2, pp. 689–707, 2023.



**KHALED ALI ABUHASEL** received the B.Sc. and M.Sc. degrees from the University of Central Florida, Orlando, FL, USA, in 2009 and 2010, respectively, and the Ph.D. degree from New Mexico State University, Las Cruces, NM, USA, in 2012, all in industrial engineering. 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 proceed-

ing of very reputable conferences. His research interests include optimization, systems engineering, health care systems, intelligent systems, artificial neural network methodologies, and statistical analysis.

• • •