Lightweight Cyber Security for Decision Support in Information Security Risk Assessment

Khoshal Rahman Rahmani, Md Sohel Rana, Md Alamin Hossan,
and Wali Mohammad Wadeed

***Abstract* — Cyber-Security on the Internet of Things (IoT) is a major concern for information exploitation which hinder the growth of information system. To address security levels and issues, security risk assessment is considered an effective tool for system security, products, process, and readiness. Effective system vulnerabilities guidance is involved in the prioritization of security risk assessment. At present, the differential equation provides a significant tool for risk assessment. However, for second-order derivatives, the error rate is higher which impacts on overall risk assessment model. To overcome those limitations, this paper presented Decision Support Light Weight Risk Assessment Model (DSLiRAM). The proposed DSLiRAM is the domain-specific framework for security assessment. The proposed DSLiRAM is adopted in four stages for the specification of practices applied for cybersecurity and organizational characteristics. The proposed DSLiRAM includes a fuzzy differential equation with a second-order derivative. To minimize error rate Taylor series expansion is integrated with Fredholm for risk assessment. The proposed DSLiRAM is examined in three scenarios, RT server, BPCS, and HMI. Analysis of results stated that the proposed DSLiRAM significantly predicts risk and prevents the attack.**

***Keywords* — Cyber risk assessment, Risk Prediction, Differential Equation, DSLiRAM, Human Machine Interface (HMI), Basic Process Control System (BPCS).**

I. Introduction

Internet of Things (IoT) is involved in the transfer of data through interrelated computing. IoT performs data transmission without the intervention of interaction between human-to-human or human-to-computer. In the present era, the drastic development of social media rises the number of IoT devices and applications, this exhibits the advantage of technological data transfer and capture between users. On another hand, a vast range of applications is developed for smartphone applications involved in the collection of user information. However, to protect those user data several rules and regulations are evolved. When information about users is paired with IoT, collected data are captured this leads to failing in rules, regulation, and policy for data security. In this scenario, the administration is struggling to understand the cybersecurity threat in IoT. Also, administration highly focused on cybersecurity issues relies on IoT and the users. However, a significant number of researchers evaluated IoT explicit and implicit values of IoT cybersecurity need to be improved. To withstand security Cyber-Physical System (CPS) is evolved which includes physical elements for automation and controlling process, for actuation, actuation, communication, and computation [1]. CPS is widely utilized in vast domains like traffic management, energy infrastructure, health care, and manufacturing. This CPS includes open-source software, a standard protocol for communication, and a commercial protocol for reducing cost with ease of integration incorporate networks [2]. However, CPS is subjected to a vast range of security threats that are targeted by cyber-attackers that impact normal operations. Even these security threats impact on public safety of the network and the economic stability of the network. To protect CPS, these require cyber-attack vulnerable component infrastructure [3,4]. The framework of the IoT cybersecurity model focused on risk assessment mechanisms for the decision-making process. Those cyber systems are involved in the systematic assessment and management of risk associated with the organization. As stated, cybersecurity is involved in the static evaluation of critical problems associated with real-time applications [5]. In the case of a static environment, the admin able to take decisions with network assessment for the decision-making process in CPS. Even this provides accurate, and evaluation of problems associated with cybersecurity those requires for static factors to maintain system [6], [7]. In the case of a sophisticated attack environment, IoT cyber system demands an effective mechanism to evaluate the management of risk. Additionally, the developed cybersecurity mechanism concentrates on designing safety and security. In the case of conventional cyber risk assessment International Standards are evolved [8]. At present, CPS comprises several standards in those IEC 62443 is adopted for automation and control in industrial processes. However, those standard fails to provide security independently for industrial monitoring. This requires a well-established CPS design with safety and security. To overcome those limitations associated with IoT cybersecurity automation systems with operational safety need to be defined [9]. At present, to withstand cybersecurity fractional calculus is evolved and widely adopted in industrial applications. Fuzzy-based fractional calculus is based on the condition of non-local boundary values applicable in a theoretical and practical scenario. However, this does not provide a significant solution for the boundary problem for

Submitted on December 24, 2021.
Published on January 20, 2022.
Koshal Rahman Rahmani, Afghanistan.
(e-mail: khoshalrahman.rahmani@gmail.com)
Md Sohel Rana, NUIST, China, Bangladesh.
(e-mail: sohelrana117373@gmail.com)
Md Alamin Hossan, Daffodil Int University, Bangladesh.
(e-mail: alamin311293 @gmail.com)
Wali Mohammad Wadeed, Afghanistan.
(e-mail: wadeed.walid@gmail.com@gmail.com)

second-order derivatives [10]. Several researchers and scholars focused on boundary problems with second-order derivatives for resolving boundary value estimation. Those boundary values have resolved through consideration of infinite, fractional boundary, Non-linear boundary, finite boundary conditions, etc. provides significant performance [11]. Based on this consideration, this paper derived fuzzy-based fractional derivatives for risk assessment. This paper proposed a Decision Support Light Weight Risk Assessment Model (DSLiMAP) model for cybersecurity risk assessment and prediction. The proposed model includes a lightweight model for the assessment of cyber risk. The proposed DSLiMAP is adopted in four stages for cyber risk assessment. This incorporates fractional differential equation integrated with Fredholm integral and Taylor series expansion for risk assessment. The derivatives are based on second-order derivatives. The developed integral is applied to fuzzy for the classification of attacks. Simulation of proposed DSLiMAP is performed under three scenarios RT server, BPCS, and HMI. The results demonstrated that the proposed DSLiMAP effectively prevents attacks and improves cybersecurity.

II. Related Works

The CPS security is considered as a research community based on international standards. A review of CPS security challenges, security, and the solution are examined in [14]. In [15] focused on run time attack environment with a CPS security development mechanism. The developed approach performance is examined through assessment of attack and prevention mechanisms for the industrial control system. In [16] performed as risk analysis for security enhancement through the integration of bowie analysis and attack tree. Also, [17] evaluated the testbed for water treatment with consideration of security risk assessment. The CPS security tested provides components for software and hardware for industrial communication standards. The analysis defined that in chemical process cyber threat is challenging for the implementation process. [18] focused on CPS attack detection and estimation. The analysis is conducted in a wireless sensor network (WSN). The analysis stated that False Data Injection (FDI) exhibits adversary performance for physical later security. The physical layer is altered due to the existence of jamming attacks in the cyber layer. To improve CPS resilience, [19] proposed an integrated topology with the integration of multiagent in distributed middleware. The developed CPS model comprises of CSTR model for Wireless Sensor Actuator Network (WSAN) with remote control through HMI. The constructed model exhibits significant performance in the case of jamming and loss attacks. In [20] developed a control design for the CSTR process in a nonlinear scenario. The developed mechanism provides an effective mechanism for cyber safety in an injection attack environment. In [21] integrated Neural Network (NN) with Lyapunov-based for predictive controller for the non-linear system. The CSTR exhibits a constant column for handling cyber-attack. [22] developed an abnormal event for Industrial treatment using the Internet of Things (IoT). The adopted method is for detection of an anomaly for processing correlation variable for detection of cyber-attack with CSTR model. In [23] evaluated the control system for measuring data for cyber-attack for control signal commanded for spoofing attack. The closed-loop system provides spoofing attacks for testbed with the implementation process. In [24] presented CSTR approach for elucidating the feedback control dynamic interaction and system for classical model-based system. The model-based system provides interaction with Model Predictive Control (MPC) system in a thermal plant. Through analysis tested involved in the estimation of control-theoretical approach for cyber-attack detection in risk assessment. The proposed model is stated as DSLiRAM for cybersecurity. The proposed model incorporates a fuzzy fractional differential equation for achieving cyber-security. The proposed DSLiRAM estimate the error values are measured for evaluation of cybersecurity risk assessment and prediction.

III. Proposed Methodology

To provide cybersecurity-related information in industrial applications, this paper proposed a DSLiRAM security risk evaluation framework. The proposed DSLiRAM focused on industrial security applied in a lightweight manner with consideration of various attack scenarios. The proposed DSLiRAM utilizes a partial differential approach for measuring risk in CPS. The proposed DSLiRAM focused on security activity in the CSP of the industry with the identification of future security activity. The proposed DSLiRAM is performed in four phases with a fractional-order differential equation for risk assessment. The proposed DSLiRAM is adopted in four stages within the inclusion of differential equations. The proposed DSLiRAM performs risk assessment and prediction using fractional fuzzy differential equations. In Fig. 1 the performed phases for DSLiRAM are described as follows:

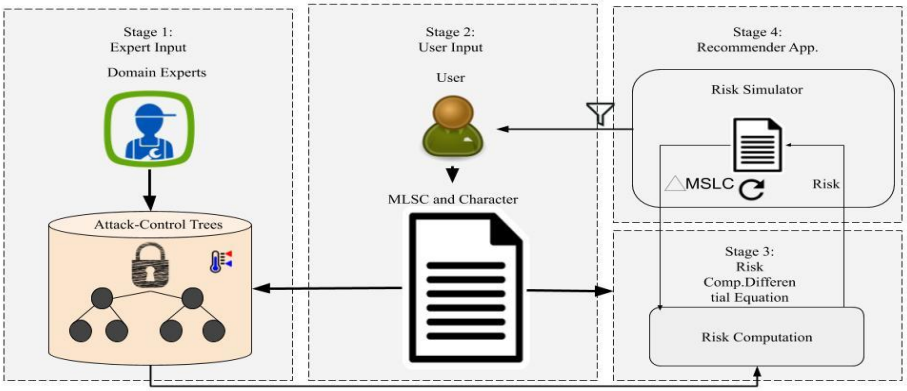

Fig. 1. Overall Architecture of DSLiRAM.

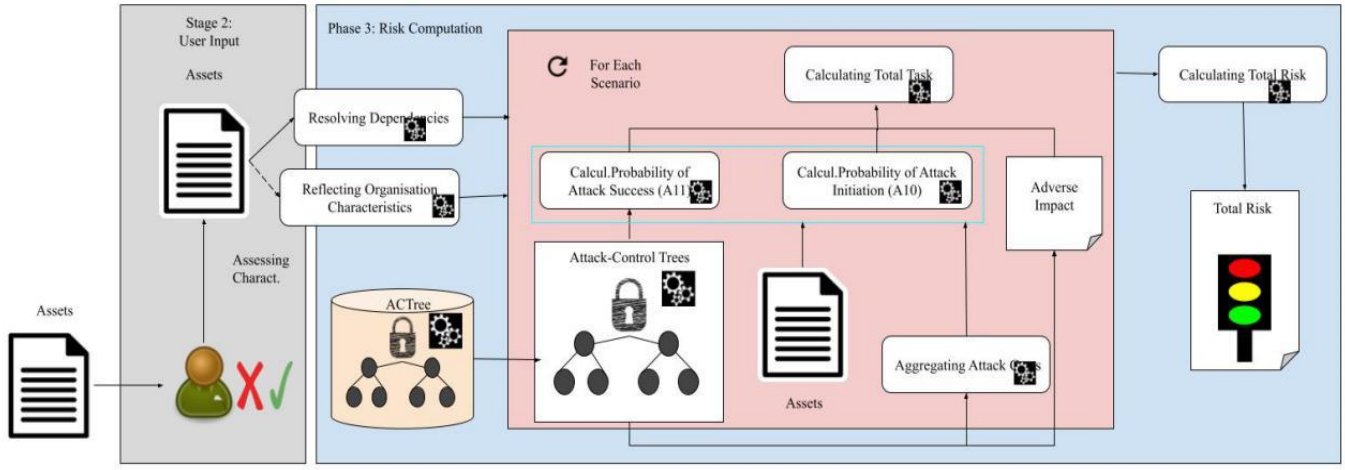

Fig. 2. Risk Computation using DSLiRAM.

Stage 1: Input by Admin

Initially, domain admin creates set of frameworks for different domains of the sector. The domain construction is based on the construction of an attack tree with a set of parameters for security. Based on the operational sector of the organization user can be able to select a particular domain from a set of framed domains. This facilitates the assessment of risk for selected domains based on the attack tree. These stage steps are illustrated in Fig. 3.

Stage 2: Input assigned by User

It is adopted in the advanced stage of security in organization security which provides security practices that need to be implemented in a lightweight manner.

Stage 3: Computation of Risk

The computation of risk is performed after the dependencies are resolved. The general process in the computation of risk is presented in Fig. 2. This stage derives the suspected risk and estimates the probability based on severity. The probability of impact adverse relies on attack initiated and estimated through constructed attack trees. In this stage, fuzzy computation is applied for risk effective prediction of risk to offers security.

Stage 4: Recommender Application

This provides information about security activity to an organization which is more effective and cost-effective. The proposed DSLiRAM integrates the above-mentioned four-stage with fuzzy fractional derivation for cybersecurity risk assessment. Through fractional-order derivation risks are estimated and prediction is performed through constructed DSLiRAM with fractional derivation.

A. *Cyber Security Risk Assessment with Fractional Order*

To assess risk associated with cybersecurity fractional derivatives is applied with the lightweight protocol. For risk assessment, this paper selected Fredholm integral equation applied with Taylor Series expansion. In existing, several fractional derivatives such as Riemann-Liouville-type, Grunwald-letnikov-type, WeyL-type, Resz-type and Caputo-type. Based on the integral equation it is difficult for achieving analytical solutions. By general integral solution, numerical solutions are achieved using kernels.

Let consider Fredholm integer with the introduction of Taylor Series expansion in the second type as stated in (1):

$$\phi(x)+\int_a^b K(x,t)\phi(t)d_t = f(x), x\in[a,b] \quad (1)$$

In above equation (1), $K(x,t)$ and $f(x)$ are defined as known equation which lies in finite closed interval range of $[a,b]$. The parameter $\phi(x)$ stated as Taylor series expansion with set of Taylor level point set. After estimation of Taylor level those are substituted in integral term, for construction of algebraic equation for obtaining derivative. Using $\phi(x)$ approximate solution is achieved through integral equation. The value of each point with algebraic values are derived for obtaining derivative values and Taylor series expansion provides slow convergence value. In Taylor series large range of error is achieved when $b_{-a}>1$. To overcome those limitation piecewise Taylor series method of second type is integrated with Fredholm integral is applied. To estimate the risk assessment and prediction error rate are estimated in DSLiRAM with second order Fredholm integral. The Taylor series error estimation at second order with expansion for convergence is presented follows:

For analysis, Taylor series expansion considers isometric values are considered as stated in (2):

$$a = x_0 \prec x_1 ..... \prec x_m = b(m \geq 1) \quad (2)$$

The error estimation values are presented in (3)-(5):

$$x_q = a + qh(q = 0,1....m), h = \frac{b-a}{m} \quad (3)$$

$$\phi(x)+\sum_{q=0}^{m-1}\int_q^{q+1} K(x,t)\phi(t)d_\tau = f(x) \quad (4)$$

$$t = x_q + hr$$

$$\phi(x)+h\sum_{q=0}^{m-1}\int_0^t K(x,x_q+hr)\phi(x_q+h\tau)d_\tau = f(x) \quad (5)$$

In above equation, polynomial degree $\phi(x)$ is higher than m, then Lagrange expansion value function $\phi(x)$ stated in (6) as follows:

$$\phi(x)+h\sum_{q=0}^{m-1}\int_0^l K\left(x,x_q+h\tau\right)\left[\sum_{j=0}^{n}\frac{\phi^j\left(x_q\right)}{j!}\left(h\tau\right)^j\right]=f\left(x\right) \quad (6)$$

Here, i = 0,1, ..., n, if $x=x_p\left(p=0,1....m-1\right)$ is obtained using (7):

$$\phi_p^i+h\sum_{q=0}^{m-1}\sum_{j=0}^{n}\frac{\phi_q^i h}{j!}\int_0^l K_s^i\left(x_p,x_q+h\tau\right)d_\tau=f^i\left(x_p\right) \quad (7)$$

It is necessary to estimate the discontinuities with finite number for deriving kernel function $K\left(x,t\right)$. The numerical solution is obtained using differential piecewise Taylor series expansion for achieving differential solution. The similarities exist between kernel function and Green function is denoted as $K\left(x,t\right)$ and $G\left(x,t\right)$. The green function differential values for kernel function $K\left(x,t\right)$.

Consider second order Fredholm integral equation for Taylor series expansion is defined using following (8):

$$\phi(x)-\frac{1}{2}\int_0^1(x+1)e^{-st}\phi(t)dt=e^{-x}-\frac{1}{2}+\frac{1}{2}e^{-(s+1)},x\in[0,1] \quad (8)$$

For error estimation Taylor series expansion is selected as n = 4. In this, scenario, fuzzy is applied for classification of risk in cyber security. For error estimation this paper selects n = 4, m = 2,4,8 for estimation of pair value m and n. The Taylor series expansion with n = 4 is represented as (m, n) = (2, 4), (m, n) = (4, 4) and (m, n) = (4, 8) with symbol (m, n) = (1,4). Additionally, for symbol S (8, 0) calculation for complex Simpson formula is estimated when m =8. The risk error rate estimation for Piecewise Taylor Series is presented in Table I.

TABLE I: ABSOLUTE ERROR EXTRACTION

Fractional Differential Type	Piecewise Taylor Series Expansion		
0.00	(2,4)	(4,4)	(8,4)
0.25	3.267e-5	1.856e-6	3.267e-8
0.50	4.167e-5	1.357e-6	3.675e-8
0.75	4.167e-5	1.267e-6	4.156e-8
1.00	4.267e-5	1.476e-6	4.367e-8

Above Table I provides absolute error for real and numerical solutions for different values on the Taylor series. This provides that Taylor series expansion provides minimal error rate which can be effectively processed.

B. Fuzzy Differential Equation for Risk Prediction

Cybersecurity risk prediction is performed based on the present historical security information and quantitative prediction of network security. This provides an effective solution for suppressing attacks in the system. To predict risk autoregressive moving average model (ARMA) is utilized and it is represented as $ARMA(p,q)$. In this p and q define the order and autoregressive process for the model. The parameter r is stated as moving average order process, with the application of differential equation as stated in (9).

$$r_t-\phi_1 r_{l-1}-\phi_2 r_{l-2}.....-\phi_p r_{l-p}=a_1-\theta_1 a_{i-1}.....-\theta_q a_{t-q} \quad (9)$$

The network security is defined as nonstationary process, and it can be defined as differential operator of $\Delta r_l=r_l-r_{l-1}$ with first-order differential transformation. The network security sequence is stated as $R(t)=\left\{r\left(t_1\right),r\left(t_2\right).....r\left(t_n\right)\right\}$ for non-stationary process. The first-order differential sequence is represented as $R_s^1(t)=\begin{Bmatrix}-1\\-t\end{Bmatrix}$ and cyber security risks are obtained as $\begin{Bmatrix}-1\\-t\end{Bmatrix}=\Delta r_l=(1-B)r_l$.

In this manner, the ARMA model with differential equation provides trends in periodic changes in time series manner with a stable platform.

For a stationary process, parameters estimated with covariance function are defined using (10):

$$\gamma_l=\phi_1\gamma_{l-1}-\phi_2\gamma_{l-2}.....-\phi_p\gamma_{l-p} \quad (10)$$

The parameters in $ARMA(p,q)$ model is solved, and it is rewritten as in equ (11) as follows:

$$r_{t+h}=\phi_1 r_{t+h-1}+\phi_2 r_{t+h-2}.....+\phi_p r_{t+h-p}+a_{t+h}-\theta_1 a_{t+h-1}-\\-\theta_2 a_{t+h-2}....-\theta_q a_{t+h-1},h\succ 0 \quad (11)$$

C. DSLiRAM for Cyber Security Risk Assessment

Initially, DSLiRAM was involved in risk assessment adopted in 4 phases for the construction of a risk framework for the application of a specific domain. At this phase, information related to various attack scenarios is examined. It involved the transformation of the tree structure for tree and utilized for security. That constructed tree is stated as an attack control tree (ACTree) which is involved in the determination of designing a security control scheme for protecting attacks. The constructed attack tree includes different parameters which define the various attack control efficiency and reduced costs. In Fig. 3, the overall process in risk assessment structure for DSLiRAM is presented.

After the application of phase 1, attacks are estimated with the identification of relevant attacks. Attack scenario involved in the identification of various scenarios like domain-independent and specific scenarios for various domains. Based on organization operation user selects a domain for assessment of risk for examination of various attack scenarios. The domain-specific scenario is linked explicitly for different domains, this is applicable for both scenarios because the organization is exposed to different attack environments. The admin of a specific domain is involved in the collection of different attack scenarios for risk assessment for the management of risk. The proposed lightweight risk assessment is involved in the prediction of risk in the organization. Through estimated differential equation risk error are examined and risk is predicted for cybersecurity.

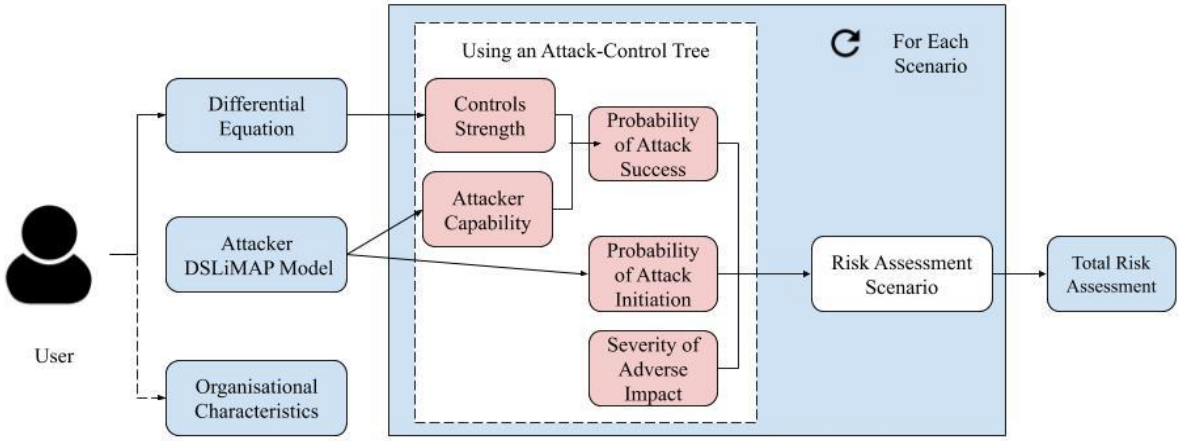

Fig. 3. Cyber Security Risk Assessment Tree Structure for DSLiRAM.

IV. Results and Discussion

The proposed DSLiRAM is examined with Real-Time (RT) server for legitimate access used for data logging. The performance of the proposed DSLiMAP is examined under three scenarios such as RT server, BPCS, and HMI. In table II description of the risk assessment model for DSLiRAM is provided.

TABLE II: Description of Risk Assessment Model

Design Variables	Description
p_c	The PC compromising probability
C_5	The probability of data transmission from I/O and Modbus
C_6	The probability of storing document configuration for prevention and storage in local server. This offers guaranteed security to C_7.
C_7	This provides probability value of information loss
C_8	This estimates the period of BPCS command higher than the setup time.
C_{13}	Estimate the probability of success for brute-force mysql login attack
C_{14}	The effective password recovery forms the hash table
C_{15}	The effective monitoring probability for disabled data from mysql
C_{17}	The probability value of RT server
C_{18}	The value of probability for leakage of password.
C_{21}	The value probability for activation of workstation

In Table II RT server nmap port is used for information in terms of mysql and ssh services. MySQL was involved in authentication bypass utilized for password hash dump and brute-force attack based on server setting. The Mysql information about risk assessment for nmap based on RT server is provided. In table 3 provides the focused service, version, and vulnerabilities considered for analysis of DSLiMAP is presented. The parameters are for the RT server scenario.

TABLE III: Vulnerabilities in RT Server

Port	Service	Version	Vulnerabilities
3306/tcp	Sql	5.7.28, Protocol 10	Authentication, Dumping of passwords dump, Brute force attack
22/tcp	Ssh	OpenSSH 7.9p1 Ubuntu 10	

In RT server attack tree for cybersecurity assessment is approximated as follows:

$$P\left[Srv-Comp\right]=c_{14}c_{15}\left(c_{16}+c_{17}\right)\left(c_{11}c_{12}+c_{13}\right) \quad (12)$$

With (12) the attack probability is estimated for RT server with nmap for cybersecurity risk assessment.In the case of the Basic Process control system (BPCS), the proposed DSLiMAP provides the list of services related to cybersecurity risk assessment are provided. In table 3, presented about nmap for RT server for scanning is listed with provided services and service version. Additionally, nmap provides RT server target as NI cRI0 9049 operates in the Linux platform. The distinct port for open source is based on the provision of services by vendor-specific with the exploitation of hardware and software knowledge. Based on presented services and open ports BPCS involved in the construction of an attack tree with a specified register address for the configuration of control data stored in the local control drive. The BPCS vulnerabilities are examined for a different version, services and vulnerabilities are listed in Table VI.

TABLE IV: BPCS Vulnerabilities

Vulnerability	Risk	Exploit	Exploit	Notes
RDP - Brute-force	Yes	Hydra	Success	user: admin, pass: "reactorws" successfully deduced. HMI access gained
Contiguous address in Modbus	Yes	Metasploit	Success	Process and Modbus configuration knowledge assumed

To improve the attack detection probability success rate Modbus write on a similar register. The BPCS is involved in successive communication rates with an open SSH port. Through privileged access, with incoming DoS attack, BPCS controller shut down immediately. The controller problem is overwritten with the integration of attack with the assumption of sufficient hardware knowledge with the inclusion of appropriate software. At last, Modbus with DoS attack exploit provides significant functionality with the inclusion of SYN flood attack in SSH port. The BPCS controller for real-time scheduling for attack control. It is observed that with proposed DSLiMAP provides significant performance for DoS attacks for output process and configuration. From BPCS attack tree construction with DSLiMAP involved in the estimation of attack probability using (13):

$$P[BPCS-Comp]=c_9[c_3c_4+(c_1+c_2)+a_1c_3c_4+ \\ +c_8[a_2c_7+(c_5c_6)] \quad (13)$$

In the attack scenario, HMI compromised with attack data over HMI-BPCS data as presented in Table V. Table V provides the HMI vulnerabilities applied for the DSLiMAP algorithm is presented for analysis.

TABLE V: VULNERABILITIES IN HMI

Port	Service	Version	Vulnerabilities
502/tcp	mdps	Modbus or TCP	Modbus, stop
3306/tcp	mysql	MySQL	
3389/tcp	rdp		

In the proposed DSLiRAM, running windows are provided with a mechanism for the identification of attacks. The analysis exhibited that the proposed DSLiMAP scheme provides efficient security for a brute-force attack. The server of RT users is relying on HMI and mysql for attack identification. It is identified that a fewer number of mysql users are subjected to vulnerabilities. Through the developed approach mysql eliminates side attacks with the construction of an HMI for construction of attack tree. The probability value for HMI-BPCS data is estimated using (14):

$$P[HMI-BPCS]=c_5c_7+c_{21}(c_{18}+c_{19}c_{20}) \quad (14)$$

The developed HMI involved identification of Man in the Middle (MITM) attack with removal of RT server in DSLiMAP firewall.

A. *Cyber Security Risk Assessment with DSLiMAP*

The proposed DSLiMAP is examined for the cybersecurity risk prediction and assessment with tolerable risk assessment. The CPS component upper bound values probability values are performed for assessment of cyber failure. The risk assessment process is based on the evaluation of risk assessment with actual failure prediction of cybersecurity threats. Even the proposed DSLiRAM exhibits a backward approach involved in a proactive approach for suitable runtime scenarios. In table 6 exhibited different tools, modules and the purpose of the proposed DSLiMAP in the organisation server is provided.

TABLE VI: DIFFERENT SERVER MODULES

Node	Tool	Module	Purpose
RT Server	nmap	-	Scan
RT Server	Metasploit	mysql_authbypass_hashdump	Bypass auth
RT Server	Metasploit	mysql_login	Brute- and SQL login
BPCS	nmap	-	Scan
BPCS	Metasploit	modicon_command	Start/Stop control through remote
BPCS	Metasploit	synflood	BPCS SYN Flood attack
BPCS	Metasploit	ssh_login	SSH login - Brute-force
BPCS	Metasploit	modbusclient	Manipulated data in Modbus
BPCS	Metasploit	modbusclient	Manipulated multiple data in Modbus
HMI	nmap	-	Scan
HMI	Hydra	-	RDP - Brute-force
HMI	Metasploit	modbusclient	Manipulated multiple data in Modbus

To perform the effective designing process in risk assessment with consideration of various variables. Based on the assigned configuration for the RT server, BPCS and HMI risk assessment and prediction are examined. The observed results are presented in Table VII, Table VIII, and Table IX. In Table VI presented about risk assessment using DSLiMAP for RT server.

TABLE VII: DSLIMAP RESULTS FOR RT SERVER

Vulnerability	Notes	Tool	Result
Bypass mysql Authentication	mysql server configured to enforce authentication	Metasploit	Fail
Brute-force mysql login	Weak mysql root password used	Metasploit	Success
Linux password in hashing	Apparmor disabled for mysql	Metasploit	Success
Hashed passwords for cracked linux	root password recovered	Metasploit	Success

In Table VIII, DSLiMAP risk assessment performance for BPCS is provided with exploitation of tools and functional characteristics notes.

TABLE VIII: DSLIMAP RESULTS FOR BPCS

Vulnerability	Hazard Caused	Tool	Result	Notes
Modbus STOP CPU Attack	No	Metasploit	Fail	In CPU attack BPCS not supported
SYN Flood Attack to ports 22, 502	No	Metasploit	Fail	The SYN attacks does not affect communication
SSH login - Brute-force	Y/N	Metasploit	Success	user: admin, pass: "niroot" successfully identified. DoS was not significant. Integrity attack performance is reduced with utilization of software tools
Contiguous address in Modbus	No	Metasploit	Success	The process is not affected with Random write in Modbus
Contiguous address in Modbus register	No	Metasploit	Success	The communication is periodic for BPCS communication for data written in every 5 sec.

In Table IX, performance of DSLiMAP for HMI is provides. The performance of is stated for HMI.

TABLE IX: DSLIMAP RESULTS FOR HMI

Vulnerability	Risk	Exploit	Exploit	Notes
RDP - Brute-force	Yes	Hydra	Success	user: admin, pass: "reactorws" successfully deduced. HMI access gained
Contiguous address in Modbus	Yes	Metasploit	Success	Process and Modbus configuration knowledge assumed

From Table VII-IX, it is observed that for varying RT servers, BPCS and HMI proposed DSLiMAP exhibits significant performance for prevention of attack with an effective assessment of cybersecurity risks. At first, information probability information leaking is similar to the software configuration process. Through c5 and c7 the proposed DSLiMAP provides effective processing. Secondly, similar password privacy is enforced with various

server systems such as database server, remote desktop, and OS. This implies that c13=c14=c18. The third stage, it is observed that HMI-BPCS for communication is higher than small practice which means c8 = 0. In RT server SSH provides configuration for remote operation for remote desktop capability for c17 = 1. At last, it is observed that HMI offers operational inconvenience with c21=0. This provides the reduced (15) as follows:

$$\left(c_5^2 c_{13}^2 c_{15}\right) P_c \le 10^{-5} \tag{15}$$

In RT server probability of failure in cyber attack offers CPS drawback. In above equation P_c presented about the probability of cyber attack failure. In CPS IT security higher risk value tolerance is increases failure probability with the decreased target level.

B. Simulation Analysis

Through the analysis of proposed DSLiMAP evaluation is examined with consideration of residual energy and throughput of IoT network. The proposed model is target cybersecurity in IoT communication for industrial application. In this section after deployment the performance of proposed model with IoT is presented.

C. Residual Energy

The residual energy provides the remaining energy available in the IoT environment with consideration of 100, 200, and 300 nodes. The simulation analysis is considered for 100 sec. In table 10 comparative analysis of the proposed DSLiMAP is provided with EADUC and ECDC with different node count such as 100, 200 and 300.

The analysis expressed that residual energy for 100, 200, and 300 nodes residual energy decreases for 100 sec. The comparative analysis expressed that the proposed DSLiMAP residual energy is higher than the existing EADUC and ECDC. This expressed that the proposed DSLiMAP significantly minimizes energy utilization with reduction of attack.

TABLE X: ANALYSIS OF RESIDUAL ENERGY

Time (sec)	Residual Energy (J)								
	100 nodes			200 nodes			300 nodes		
	EADUC	ECDC	DSLiMAP	EADUC	ECDC	DSLiMAP	EADUC	ECDC	DSLiMAP
0	49.13	49.24	49.96	100	100	100	150	150	150
10	49.03	49.12	49.93	99.67	99.73	99.93	149.43	149.57	149.92
20	48.96	49.04	49.90	99.37	99.65	99.74	149.18	149.34	149.83
30	48.91	48.97	49.89	99.14	99.46	99.53	148.87	149.19	149.78
40	48.83	48.93	49.86	98.68	99.03	99.42	148.46	148.95	149.67
50	48.78	48.89	49.83	98.46	98.67	99.36	148.29	148.67	149.56
60	48.31	48.86	49.81	98.32	98.45	99.12	147.78	148.49	149.43
70	48.28	48.83	49.73	97.84	98.31	98.94	147.56	148.15	149.37
80	48.24	48.81	49.71	97.29	98.21	98.83	147.32	147.87	149.24
90	48.19	48.06	49.69	97.01	98.01	98.72	147.16	147.65	149.16
100	47.87	49.96	49.67	96.86	97.87	98.67	146.87	147.45	149.09

D. Throughput

Throughput provides the successful transmission of data between sender and receiver. In table XI shows the average throughput of the IoT network for the proposed DSLiMAP and the existing methods.

TABLE XI: ANALYSIS OF THROUGHPUT

Time (sec)	EADUC	ECDC	DSLiMAP
0	8000	9500	10000
5	9600	11000	13000
10	12000	13000	17000
15	17000	18000	21000
20	21000	22000	24000
25	26000	27000	28000
30	29000	30000	32000
35	33000	34000	36000
40	37000	40000	42000
45	39000	43000	46000
50	43000	44000	50000

The comparative analysis of the proposed DSLiMAP provides a significant energy consumption balance in data transmission. The proposed DSLiMAP is effectively involved in the maintenance of residual energy and increased throughput rather than the existing EADUC and ECDC approach. These results prove that DSLiMAP outperforms other protocols and increases the number of available nodes.

V. CONCLUSION

This paper, presented about security approach for system security in CPS. The proposed DSLiMAP includes a fuzzy differential equation with a lightweight model for risk assessment and prediction. Through analysis, it is observed that an attack takes a long time to assess the system and it becomes nullified with an attack scenario. The proposed model includes a successful application for industrial application integrated with physical cyber domain design. The proposed model is designed for deployed IoT environment in industrial control system. The analysis presented about performance of IoT communication after deployment of proposed model. Further, the proposed DSLiMAP offers an effective security scheme for MITM. DoS, and Brute Force attack with improved security. In the future, the proposed approach can be implemented in control industrial applications.

REFERENCES

[1] Wang Z, Chen L, Song S, Cong PX, Ruan Q. Automatic cyber security risk assessment based on fuzzy fractional ordinary differential equations. *Alexandria Engineering Journal*. 2020 Aug 1;59(4):2725-31.

[2] van Staalduinen MA, Khan F, Gadag V, Reniers G. Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructure. *Reliability Engineering & System Safety*. 2017 Jan 1;157:23-34.

[3] Tantawy A, Abdelwahed S, Erradi A, Shaban K. Model-based risk assessment for cyber physical systems security. *Computers & Security*. 2020 Sep 1;96:101864.
[4] Schmitz C, Pape S. LiSRA: lightweight security risk assessment for decision support in information security. *Computers & Security*. 2020 Mar 1;90:101656.
[5] Venkatachary SK, Prasad J, Samikannu R. Cybersecurity and cyber terrorism-in energy sector–a review. *Journal of Cyber Security Technology*. 2018 Oct 2;2(3-4):111-30.
[6] Kumar VS, Prasad J, Samikannu R. A critical review of cyber security and cyber terrorism–threats to critical infrastructure in the energy sector. *International Journal of Critical Infrastructures*. 2018;14(2):101-19.
[7] Venkatachary SK, Prasad J, Samikannu R. Economic impacts of cyber security in energy sector: A review. *International Journal of Energy Economics and Policy*. 2017;7(5):250-62.
[8] Venkatachary SK, Prasad J, Samikannu R, Alagappan A, Andrews LJ. Cybersecurity infrastructure challenges in IoT based virtual power plants. *Journal of Statistics and Management Systems*. 2020 Feb 17;23(2):263-76.
[9] Benaroch M. Real options models for proactive uncertainty-reducing mitigations and applications in cybersecurity investment decision making. *Information Systems Research*. 2018 Jun;29(2):315-40.
[10] Nhlabatsi AM, Hong JB, Kim DS, Fernandez R, Hussein A, Fetais N, Khan KM. Threat-specific security risk evaluation in the cloud. *IEEE Transactions on Cloud Computing*. 2018 Nov 23.
[11] Khidzir NZ, Daud KA, Ismail AR, Ghani MS, Ibrahim MA. Information Security Requirement: The Relationship Between Cybersecurity Risk Confidentiality, Integrity and Availability in Digital Social Media. *In Regional Conference on Science, Technology and Social Sciences* (RCSTSS 2016) 2018 (pp. 229-237). Springer, Singapore.
[12] Kusyk J, Uyar MU, Sahin CS. Survey on evolutionary computation methods for cybersecurity of mobile ad hoc networks. *Evolutionary Intelligence*. 2018 Jun;10(3):95-117.
[13] Genge B, Haller P, Enăchescu C. Anomaly detection in aging industrial internet of things. *IEEE Access*. 2019 Jun 4;7:74217-30.
[14] Ashibani Y, Mahmoud QH. Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*. 2017 Jul 1;68:81-97.
[15] Ylmaz EN, Ciylan B, Gönen S, Sindiren E, Karacayılmaz G. Cyber security in industrial control systems: Analysis of DoS attacks against PLCs and the insider effect. *In2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG)* 2018 Apr 25 (pp. 81-85). IEEE.
[16] Abdo H, Kaouk M, Flaus JM, Masse F. A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie–combining new version of attack tree with bowtie analysis. *Computers & security*. 2018 Jan 1;72:175-95.
[17] Urbina DI, Giraldo JA, Cardenas AA, Tippenhauer NO, Valente J, Faisal M, Ruths J, Candell R, Sandberg H. Limiting the impact of stealthy attacks on industrial control systems. *In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* 2016 Oct 24 (pp. 1092-1105).
[18] Gupta A, Anpalagan A, Carvalho GH, Khwaja AS, Guan L, Woungang I. RETRACTED: Prevailing and emerging cyber threats and security practices in IoT-Enabled smart grids: A survey.
[19] Januário F, Cardoso A, Gil P. A distributed multi-agent framework for resilience enhancement in cyber-physical systems. *IEEE Access*. 2019 Mar 7;7:31342-57.
[20] Durand L. *Cyber security: a risky business*, 2018.
[21] Wu Z, Albalawi F, Zhang J, Zhang Z, Durand H, Christofides PD. Detecting and handling cyber-attacks in model predictive control of chemical processes. *Mathematics*. 2018 Oct;6(10):173.
[22] Sándor H, Genge B, Szántó Z, Márton L, Haller P. Cyber attack detection and mitigation: Software defined survivable industrial control systems. *International Journal of Critical InfrastructureProtection*. 2019 Jun 1;25:152-68.
[23] Paoletti N, Jiang Z, Islam MA, Abbas H, Mangharam R, Lin S, Gruber Z, Smolka SA. Synthesizing stealthy reprogramming attacks on cardiac devices. *In Proceedings of the 10th ACM/IEEE International Conference on Cyber-Physical Systems* 2019 Apr 16 (pp. 13-22).
[24] Liu L, De Vel O, Han QL, Zhang J, Xiang Y. Detecting and preventing cyber insider threats: A survey. *IEEE Communications Surveys & Tutorials*. 2018 Feb 1;20(2):1397-417.