International Journal of Science and Research Development
Vol. 03, Issue 08, pp.063-072, August, 2024
Available online at http://www.scienceijsrd.com

ISSN: 2583-4231

Research Article

INTELLIGENT DISCRETE EVENT SYSTEM SPECIFICATION FOR MONITORING CYBER-ATTACKS IN AIRPORT

[1,7,*]Samuel S. Udoh, [2]Kufre C. Ekong, [3.7]Patience U. Usip, [4,7]DanielE.Asuquo, [5,6]Imoh U. Moffat, [1,7]Uduak D. George and [4,7]Uduak A. Umoh

[1]Department of Data Science, Faculty of Computing, University of Uyo, Nigeria
[2]Department of Information Technology, Faculty of Sciences, National Open University of Nigeria
[3]Department of Computer Science, Faculty of Computing, University of Uyo, Nigeria
[4]Department of Information Systems, Faculty of Computing, University of Uyo, Nigeria
[5]Department of Statistics, Faculty of Physical Sciences, University of Uyo, Nigeria
[6]Ministry of Science and Technology, Akwalbom State, Nigeria
[7]Tetfund Centre of Excellence in Computational Intelligence Research, University of Uyo, Nigeria

Received 20th June 2024; **Accepted** 26th July 2024; **Published online** 30th August 2024

Abstract

In recent years,cyber-attacks on airport computers and digital devices have increased thereby generating problems on airport check-in and screening systems with ripple effect of increasing passengers waiting time, halting air transportation business, cancellation of flights and frustration of airport operations. The aftermath of cyber-attacksculminates in compromise of customers and staff personal data, financial loss to airline owners and threat to life of airline operators and customers. Periodic status monitoring of airport digital devices enables early detection and mitigation of cyber-attacks.This research is aimed at developingan intelligentdiscrete event system to monitor, identify, classify andguide mitigation ofcyber-attacks at airport.A knowledge repository of cyber-attackswas created.An adaptive neuro-fuzzy discrete event model for monitoring cyber-attacks was designed. K-nearest neighbor (KNN) model was deployed forclassification ofcyber-attack patterns. The model was implemented using Java programming tools, Matrix laboratory tools and My structured query language (MYSQL). Effects of some cyber-attacks such as Trojan virus, distributed denial of service (DDOS), Brute Force, Man-in-the-middle (MITM), Ransomware and Session Hijacking on airport check-in computers were investigated. Dataset comprising 1440 records of cyber-attacks were obtained and split in the ratio of 8:1:1 for model training, validation and testing respectively. Assessment of the model's effectiveness showed acceptable performance accuracy level of 95.14% on the tested data. DDOS was observed to be the most frequent cyber-attack on airport check-in computers followed by Trojan.The model could be adapted to tackle other forms of airport attacks and aviation terrorism. Further research in monitoring cyber-attacksusing other classifiers, inductive inference tools and variants of adaptive discrete event-based modelsare recommended.

Keywords: Discrete event system, cyber-attacks, airport attacks, aviation terrorism.

INTRODUCTION

A cyber-attack is any intentional effort to steal, expose, alter, disable, or destroy data, applications or other assets through unauthorized access to a network, computer system or digital device. Threat actors deploy variety of tactics such as malware attacks, social engineering scams and password theft, to gain unauthorized access to their target systems. In recent years, attacks on airports and hijacking of aircrafts have increased thereby generating fear and psychological trauma for air travelers. Attacks and terrorist activities could lead to loss of lives and property as well as degradation of national and international economy [1][2][3]. The World Economic Forum report of year 2018 raised cyber-attacks as the third top global risk domain. The motivations behind cyber-attacks can vary, but there are three main categories: criminal, political, and personal. Criminally motivated attackers seek financial gain through monetary theft, data theft, or business disruption. Politically motivated attackers are often associated with cyber warfare, cyber terrorism, or "hacktivism." In cyber warfare, nation-state actors often target their enemies' government agencies or critical infrastructure. Activist hackers, called "hacktivists," may not cause extensive damage to their targets. Instead, they typically seek attention for their causes by making their attacks known to the public.

Corresponding Author:** ***Samuel S. Udoh,
Department of Data Science, Faculty of Computing, University of Uyo, Nigeria.

Some disgruntled current or former employees primarily seek retribution for some perceived slight.Hence, they arepersonally motivated to carry out attacks. Attackers may potentially hack different airport booking and check-in systems as well as air navigation systems such as automatic direction finder (ADF), radar navigation system (RNS), Global navigation satellite System (GNSS) and many others with a view to change or control the aircraft routes for purposes of attack. Cyber attackers usually target ground-based infrastructures within the airport because they have fewer security controls than the aircraft itself which is intelligently furnished with security features [4]. Many researchers had worked on real-time models forcyber-attack monitoring and anomalydetection incomputer networks [5][6][7]. Daum [8] suggested that, if a cyber-attack occurs in the system, protective measures should be automaticallyinvoked to repulse the attack. Adaptive neuro-fuzzy inference system (ANFIS) is an intelligent inference mechanism that combines the learning techniques of neural networks as well as the human-like computing paradigm of fuzzy logic.Discrete eventsystem specification (DEVS) is a set theoretic formalism formodelling and simulation of complex real-life systems.Classical DEVS are goodat studying complex and dynamic systems as well as modelling and analyzing eventsthat evolve with time but lacks inbuilt facility for intelligent decision making [9] [10] [11]. Cyber-attack on Airport infrastructure apart from itscomplexityand dynamicity also evolves with time and requires intelligent decision model

to guide remedy decisions. Hence, the deployment of ANFIS and DEVSto facilitateinvestigation and mitigation of the impact of cyber-attacks on airportcheck-in computers and digital devices. This work utilizes simulated data from Ibom International Airport, Uyo, Nigeria as a testbed to visualize and validate the modeling results. Several set of simulations and experiments were conducted on cyber-attacks on airport booking and check-in systems and their effects on passengers waiting time to provide important managerial insights for decision making. The remainder of the work is organized as follows: Section 2 deals with review of related works on cyber-attacks. The methodology and design of knowledge base of attacks as well as discrete event-based model for monitoring cyber-attacks are presented in Section 3. The model implementation, results and discussion are presented in Section 4 while Section 5 focusses on researchconclusion and recommendations for future work.

REVIEW OF RELATED WORKS

Ukwandu *et al.* [12] presented areview of cyber-security attacks and operations withinthe aviationsector for the period2001-2021. The aimwas to identify common threat actors, their motivations, attacks types and map the vulnerabilities within aviation infrastructures that are most commonly subject to persistent attacks. Evidence was provided that the main threats to the industry arise from advance persistent threat (APT) groups that operate, in collaboration withother actors, to steal intellectual property in order to advance their domestic aerospace capabilities as well as monitor, infiltrate and subvert other sovereign nations' capabilities. Information Technology (IT) infrastructure was identified as a segment of the aviation industry commonly attacked. The most prominent type of attack was identified asmalicious hacking with intent to gain unauthorized access. The analysis of the range of attack surfaces and the existing threat dynamics was used as a foundation to predict future cyber-attack trends. The work recommended the deployment of artificial intelligence tools and machine learning approach for proactive measures towards protecting critical infrastructures against cyber-incidents that could damage the confidence of customers in theaviation industry.Alnajim *et al.* [13] described malware as malicious software that can render infected systems inoperable. Malware could destroy data, steal information, or even wipe files critical to the operating system's ability to run. Social engineering attacks manipulate people into doing things they should not do, like sharing information they should not share, downloading software they should not download, or sending money to criminals.Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks flood computer systems with fraudulent traffic. This traffic overwhelms the system, preventing responses to legitimate requests and reducing the system's ability to perform [2]. Kirkliauskaite [14] reported on Pro-Beijing hackers who defaced a website belonging to Vietnam airlines and flight information screens at Ho Chi Minh City and the capital, Hanoi, thereby enabling it to display messages supportive of China's maritime claims in the South China Sea. Narendra [15] presented a phishing attack on Air New Zealand Airpoints which compromised the personal information of approximately 112,000 customers. Ishtiaq and Rahman [16] assayed that in year 2015 there was a DDoS attack on Poland'sairport system which led to cancellation of 22 flights and unforeseen negative imprints on 1,400 passengers. Sanapala [2] reported a cyber-attack on British airline company which culminated in disclosure and compromise of personal data of nearly 9 million customers together with the credit card information of over 2000 customers. The airline notified its customers about the attacks four months after the attack had occurred thereby leading to lawsuit against the company. The work also reported that a Canadian airline faced cyber-attack in April, 2022. The attack caused flight delays and operational glitches for five days. It was revealed that the attack was due to data breach at the Company's third-party service provided, which provides passenger management software solutions such as check-in and boarding modules for the airlines. The work recommended the deployment of real-time continuous monitoring model based on artificial intelligence and machine learning techniques for pattern recognition and response to anomalies of cyber-attacks.

Advances in Internet of things (IoT)technologies and device integration within the aviation sector have triggered the emergence ofsmart airport with the aimof excellent service deliveryand automated control in daily operations [17]. Threats against IoT infrastructures and applications within smart airports are grouped into: malicious software attacks, network and communication attacks and airport smart devices tampering attacks. Since it isvery difficult to completely prevent intrusionattempts on airport sensitive digital devices, there is need for constant monitoring, early detection and mitigation of attacks on these devices. Sanapala (2022) suggested the deployment of artificial intelligence-enabled techniques based on machine learning methodology to address the menace of IoT-inspired cyber-attacks.

Prasanna *et al.* [18] deployed Fuzzy-DEVS technique to handle imprecise data in the task of detection of intruders in a computer network environment. A combination of crips and fuzzy rules were used to simulate a network security system which encompasses both prevention and detection features. Several intrusion detection classifications were carried out, such as: invalid logins, abnormal connections, anomalies, suspicious modification of files, denial of service and protocol violation. Denial of service (DoS) attack was demonstrated, which the intruder or hacker sends large number of ICMP packets in small amount of time. The work suffered from lack of learning model to tune the fuzzy rules for optimum performance.

Udoh [19] incorporated adaptive neuro-fuzzy model into DEVS formalism and proposed adaptive neuro-fuzzy discrete event system specification (ANFIS-DEVS) for intelligent monitoring of computer networks and provision of situational awareness as well as reports on physicalinfrastructure monitoring.ANFIS-DEVS model has been successfully applied in proffering solution to prediction, pattern recognition and anomaly detection problems [20][21][22].

Kara *et al.* [11] implemented a DEVS-based cyber-attack simulator for cybersecurity. The aim was to use simulation technique to understand and detect cyber-attacks as well as understand security weaknesses and vulnerabilities in digital devices. DEVS modelling approach was adopted using DEVS-Suit development environment. Application was developed to simulate and test cyber-attacks scenarios in a virtual network environment. Different attack models such as DoS and DDoS were selected and their respective attack settingswere made at the control interface.Evaluation and detection alert generated appropriate intrusion detection signals.However, the signals

generated were not duly classified to facilitate corresponding response to detected anomaly.This research seeks to utilize the real-time complex modelling capabilities available in DEVS with the human-like intelligence embedded in ANFIS for investigation,detection and classification of cyber-attacksto trigger corresponding action and response.

METHODOLOGY

The methodological workflow of the proposed Adaptive neuro fuzzy discrete event-based model for monitoring cyber-attacks is depicted in Figure 1. The major components of the system are Knowledge base, ANFIS, User Interface, DEVS Engine, KNN and Output.

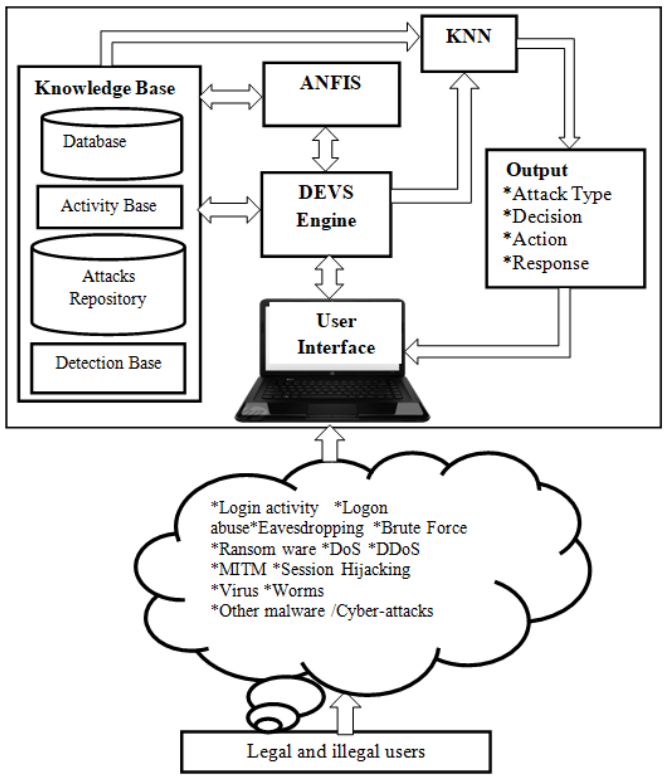

Figure 1. DEVS Based Platform for Cyber Attacks Monitoring

Knowledge Base Design

The knowledge base (KB) accommodates the database which contains both structured and unstructured knowledge about the activities and operations of the airport. These include assets, staff, customers, passengers, business partners, flight information, accounting data and many others. The structured knowledge consists of organized facts about the organization, events and its attributes while the unstructured knowledge are knowledge gotten from expert through observations of past activities happening around the institution. The Activity base keeps records of events and activities that occur within the system such as thelogin_attempts, login_time, login_details and IP address of the systems used in accessing the database. Events and activities carried out by both authorized or unauthorized users are noted. The activity base tracks the number of trials and the time interval the user tries to gain access to the airport booking and check-in system. It also logs the type of applications, files as well as operations performed by the user. The attacks repository stores the patterns of known cyber-attacks operations for future reference. The attack base helps similarity matching with new signals received from the user interface. A typical data attributes for customer, activity, attacks and detection repositories are given as follows:

Customer_attributes:{Customer_id, Name, Passport, Sex, Age, Address, Occupation,
Booking_date, Booking_time,Flight_date, Flight_time, Flight_type, Purpose_of_travelling, Flight_origination, Flight_destination, Round_trip, One_way_going, One_way_returning, amount_paid, Payment_evidence}

Activity_attributes:{Activity_id, Activity_code, Activity_name, Operation_type, Operation_mode,
Login_attempts, Login_time, login_duration}

Attack attributes:{Attack_id, Attack_type, Attack_name, Attack_time, Attack_date,
Attack_duration, Attack_mode, Attack_pattern, Attack_target, Attack}

Detection attributes:{Detection_id, Detection_type, Detection_name, Detection_time,
Detection_date, Detection_class, Response_guide}

ANFIS Design

The architecture of Adaptive Neuro-Fuzzy Inference System (ANFIS) consists of five layers. The first and the fourth layers consists of adaptive nodes which have parameters to be learnt while the second, third and fifth layers are fixed nodes and contain no learning parameters. The system is based on Sugeno inference mechanism whose reasoning methodology shows the output of each rule as a sequential combination of each rule input variable plus the constant term as shown in Equations 1 and 2

R_1: IF x is A_1 AND y is B_1 AND… AND z is C_1 THEN $f_1 = p_1x + q_1y + \ldots + r_1z + s_1$ (1)

. . .

R_n: IF x is A_nAND y is B_n AND… AND z is C_n THEN $f_n = p_nx + q_ny + \ldots + r_nz + s_n$ (2)

where x,y,z are the inputs or antecedent parameters, A, B, C are the fuzzy sets of inputs parameters, f is the fuzzy set of output parameters and p, q, r and s are consequent parameters.

Layer 1 is the input layer. Every node $i$in layer 1 has a node function as given in Equation 3.

$$O_i^1 = \mu A_i(x) \quad (3)$$

where x is the input to node i, and A_i is the linguistic label (Very Low, Low, Moderate, High and Very High) associated with this node function. In other words, O_i^1 is the membership function of A_i and it specifies the degree to which the given x satisfies the Quantifier A_i. In this work, the triangularmembership function(MF) as shown in Equation 4 is adopted as follows:

$$\mu A_i(x) = \frac{x-a}{b-a} \quad (4)$$

where μ represents the MF, $A_i$is the linguistic variable, x is the external input and signals from Users, a and b are the

parameters of the MF governing triangular shape such that $a \le x < b$.

Layer 2 is the rule node. Every node in layer 2 is labeled*M* which multiplies the incoming signals as denoted in Equation 5.

$$w_i = \mu A_i(x) * \mu B_i(y) * \mu C_i(z) \quad (5)$$

i= 1,2…,n. Each node output represents the firing strength of a rule.

Layer 3 is the normalization node which calculates the ratio of the ith rule's firing strength to the sum of all rules's firing strengths. Outputs of layer 3 are called normalized firing strengths

$$O_i^3 = \overline{w}_i = \frac{w_i}{\sum_{1=1}^{n} w_i} \quad (6)$$

Layer 4 is the deffuzification node. It comprises the consequent nodes for computing the contribution of each rule to the overall output as shown in Equation 7

$$O_i^4 \equiv \overline{w}_i f_i = \overline{w}_i (p_i x + q_i y + \ldots + r_i z + s_i) \quad (7)$$

where $\overline{w}$ is the output of layer 3, and f_i is the fuzzy set of signals. *p,q,r,s*are consequent parameters.

Layer 5 is the output node. It computes the overall output as the summation of all incoming signals as given in Equation 8.

$$O_i^5 = Y = \sum_i \overline{w}_i f_i = \frac{\sum_i w_i f_i}{\sum_i w_i} \quad (8)$$

DEVSDesign

DEVS is the central component of the system which receives input from userinterface. DEVS engine depicted in Figure 2 periodically checks the user interface for cyber events signal received directly from users or via the network. DEVS coordinates the parallel processing of signals and resolution of conflict resulting from random signal transmission.

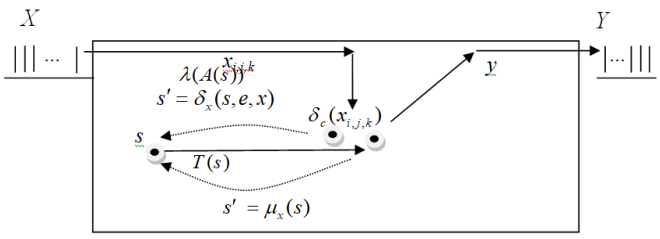

Figure 2 . DEVS Transition for Cyber Attack Monitoring

The DEVS model, maintains an internal coupling mechanism which enables the output of one component to be connected to the input of another component as illustrated in Figure 2, at the initial time the Airport systems for booking, check-in or screening of passengers is inthe Normal state.The system continues in the normal state until some events such as virussignal,worm invasion, eavesdropping, denial of service (DOS) attack, distributed denial of service (DDOS) attack, brute force attack, ransomware attack,session hijacking and other attacksoccur at Time $T_t(s)$ and change the system state to either Abnormal or Highly Abnormal or Extremely Abnormal depending on the severity of attack. The system state could also be restored to normal via repair operation at specified time. Attack signals at time $T_t(s)$ are ordered by the confluent function and submitted to the external transition function for processing. The outputs of external transition function are deployed by the internal transition function to determine the new state of the system via the output function. ANFIS function provides the means for mapping the ordered data to fuzzy domain as well as use the knowledge acquired from previous cyber-attacks patterns to draw inference on the current state of the system. The result of inference is sent to the KNN for pattern recognition and classification to guide response. The ANFIS-DEVS model for monitoring cyber-attacks is shown in a set form as follows:

$$ANFIS - DEVS = \langle X, \delta_c, \delta_x, T_t, \mu_x, S, A, \lambda, Y \rangle \quad (9)$$

where X is a set of cyber events input variables

$\delta_c : X \to S,$ is the confluent function

$\delta_x : X \to S,$ is the external transition function

$T_t : S \to \Re^{+}{}_{0,\infty}$, is time assigned for monitoring cyber events

$\mu_x : S \to S,$ is the internal transition function based on fuzzy membership

S is the set of cyber events internal state

Internal state ={Very Low, Low, Moderate, High, Very High}

$A : S \to S$, isthe ANFIS function;

$\lambda : S \to Y$,isthe output function;

$$\lambda(s) = \begin{cases} \text{Very Low} & \text{if } s<0.1 \\ \text{Low} & \text{if } 0.1 \le s < 0.4 \\ \text{Moderate} & \text{if } 0.4 \le s < 0.6 \\ \text{High} & \text{if } 0.6 \le s < 0.8 \\ \text{Very High} & \text{if } 0.8 \le s < 1.0 \end{cases} \quad (10)$$

Y is a set of system output status

{Normal (NO), Abnormal (AB), Highly Abnormal (HA), Extremely Abnormal (EA)}

$$Y(s) = \begin{cases} \text{Normal} & \text{if } s < 0.1 \\ \text{Abnormal} & \text{if } 0.1 \le s < 0.6 \\ \text{Highly Abnormal} & \text{if } 0.6 \le s < 0.8 \\ \text{Extremely Abnormal} & \text{if } 0.8 \le s < 1.0 \end{cases} \quad (11)$$

K- Nearest Neighbour Design

KNN classifies patterns based on the nearest similarity matching technique. It works by forming a majority vote between k instances of an event which bear the greatest similarity. In order to achieve the similarity metric, the KNN algorithm directly searches through all the training examples provided by calculating the distances between the testing samples and that of the training data using the Euclidean metric in Equation 12 and compressed in Equation 13 to identify its nearest neighbours and predict the classification output.

$$d(x_{ij}, x_{lj}) = \sqrt{(x_{i1} - x_{l1})^2 + (x_{i2} - x_{l2})^2 + \cdots + (x_{ip} - x_{lp})^2} \quad (12)$$

$$d(x_{ij}, x_{lj}) = \sqrt{\sum_{i=1}^{n} (x_i - p_i)^2} \quad (13)$$

The detected and classified cyber-attack patterns trigger remedy actions and provide useful guide for corresponding response by stakeholders.

RESULTS AND DISCUSSION

The minimum hardware required to provide reliable support for the proposed ANFIS-DEVS system is aquad-core computer with a clock speed of at least 4.8 GHzand 8 GB of RAM. It allows multi-tasking and multi-threading of ANFIS-DEVS program thereby providing parallel and speedy processing of data and program instructions.This research used Ibom International Airport, Uyo, Akwa Ibom State, Nigeria as a case study. Ten (10) data instances were available and collected from the Airport. Althoughreal data collected for the study was small in quantity, it served as a reliable template for generating 1440 data instances of cyber-attackvia simulation. In the simulation of Trojan virus attack, A virus and worm simulator was deployed. Afully connected network was selected having a network size of 100 computers. The10 computers used for checking-in of passengers at the airport were tagged as vulnerable with one (1) computer initially infected with virus. The simulation time was set to 86400seconds with status report given every 60 seconds. Time for a computer to be fully infected was set to 50 seconds and time to spread to other computers was set to 5 seconds. Time of repairing the infected system varied between 3600 to 86400 seconds at every simulation run. The virus simulation parameters and resultsare shown in Figure 3

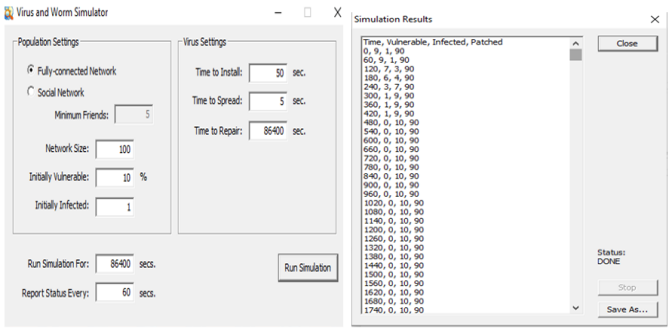

Figure 3. Trojan virus attack simulation

The Trojan virus spreads to other vulnerable computer at a given time via an infected computer which dispenses the virus at random to any computer directly connected to it.The virus could be removed via software patches and deployment of anti-virus programs within a given time tagged "Time to Repair". A successful repair operation changes the state of the computer system from either abnormal, highly abnormal or extremely abnormal to normal. Data attributes captured from the simulation environment for further investigation were: Time of status report (TR), number of computers vulnerable at that time (NV), number of computers infected at that time (NI), Number of computers repaired or patched at that time (NR).Other cyber-attack data were obtained using appropriate simulation tools. For instance, ransomware attack data were obtained via Infection Monkey's ransomware simulation. Brute force attack data were obtained via brute force attack simulation and so on. A dataset comprising 1440 records were obtained and split in the ratio of 8:1:1 for model training, validation and testing respectively.

System Training Procedures

System training procedures in Udoh et al. [10] is adopted. ANFIS procedure istriggeredby a click on"ANFIS" button in the main menu. This createsa link to ANFIS editor in the MatLab environment which facilitates FL operations of fuzzification, inference and defuzzifcation as well as ANFIS training as depicted in Figure 4.

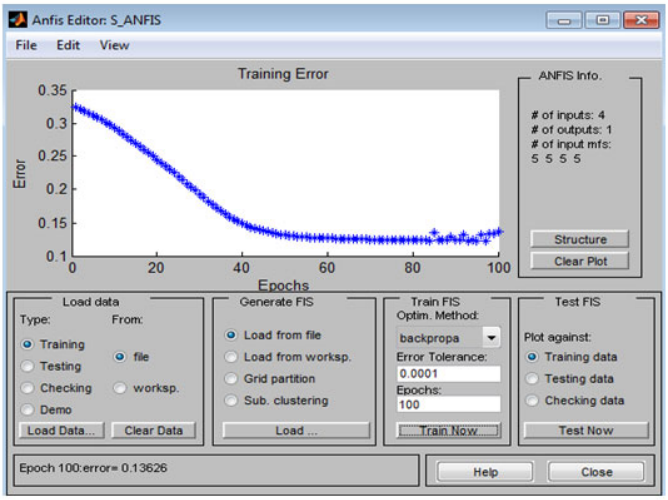

Figure 4. ANFIS Training Error Window

The maximum epoch shown in Figure 4 is set to 100 and the threshold is 0.0001. Training cycle could be aborted without reaching the maximum epoch if the MSE specified by the threshold value is reached in the course of ANFIS training. The ANFIS training editor as shown in Figure 4 is made up of six (6) major components namely: Load data, Generate FIS, Train FIS, Test FIS, Output and ANFIS Information. The load data window frame enables the loading of training, checking and testing data from either file or workspace. The Generate FIS window frame enables the loading of FIS structure whose premise and consequent parameters are modified using the Train FIS and assessed using the Test FIS. As shown in Figure 4, Backpropagation algorithm is selected as the training algorithm with error tolerance of 0.0001. The training curve decreases from epoch 1 to epoch 40, from epoch 41 the curve maintains a constant value and rises at epoch 100 with the error value of 0.13826. The observed error value is far greater than the error tolerance value of 0.0001 specified in the Train FIS optimization frame. This indicates that more cycles of training are required to equip ANFIS with knowledge of generalization into unseen patterns. The ANFIS training was repeated with varying number of epochs for optimal results. ANFIS-DEVS application software for monitoring Cyber attack is activated by clicking on its icon on the computer desktop where it is installed. A successful authentication is established when the correct user name and password are entered.A click on the "Ok" button displays the welcome screen and grants access into the main menu. The main menu comprises seven menu options namely: File, Neural Network, ANFIS, DEVS, Decision Support, Report and Help as depicted

in Figure 5. A click on the DEVS menu item in the main menu displays aninterface in Figure 6that facilitates the monitoring of cyber-attacks in the systemon click of the start button. Figure 7 shows Cyber-attack active monitor which checks the user interface every 60 seconds for arrival of new signals. A report of "No new sensor log data found" is displayed when there are no new signals at the interface.The major item in the File submenu is the data input interface as shown in Figure 8. It provides a temporary store and receptacle for a random collection of input data from all kinds of users.

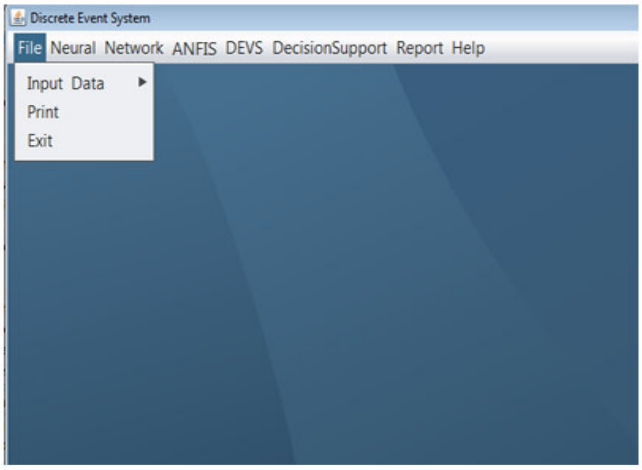

Figure 5. Main Menu

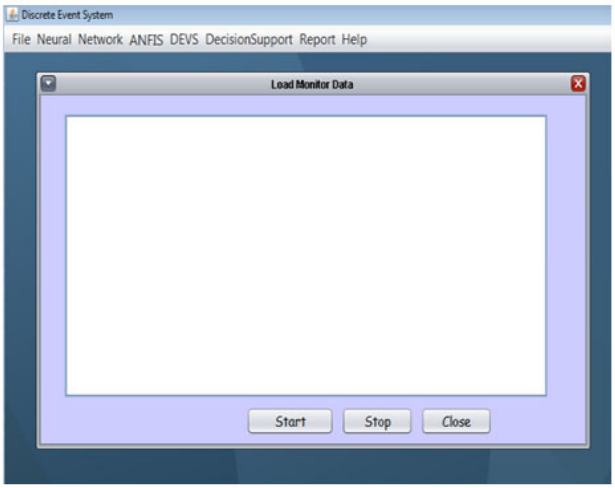

Figure 6. Cyber-attack Monitoring Window

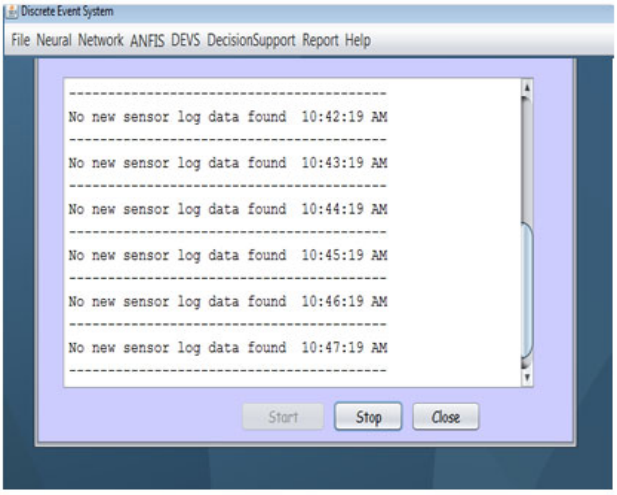

Figure 7. Cyber-attacks Events Active Monitor Window

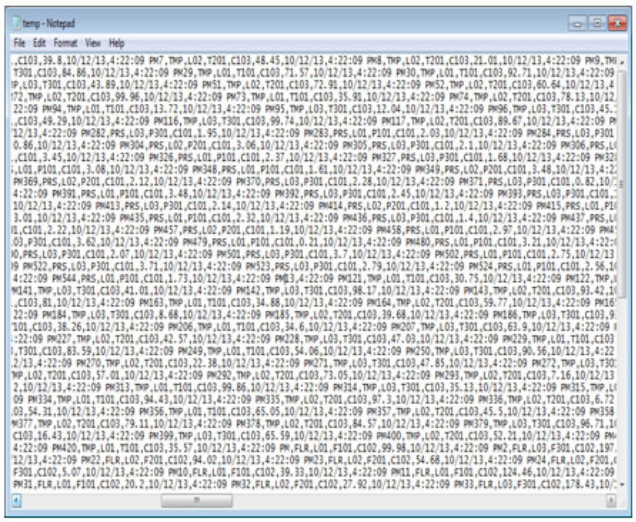

Figure 8: Signal Interface

In subsequent checking of the interface, if data are found, they are read and processed using ANFIS-DEVS in-built components such as: confluent, time advance, external, internal, state, ANFIS and output functions until the final output is produced. The signal interface depicted in Figure 6 receives signals at random from both legal and illegal users. The ANFIS-DEVS controller periodically checks the data interface, reads and processes the data using its components and transitions functions to facilitate detection and classification of attacks on the system as shown in Figure 9. The analysis of nearest neighbors (k) to mean value of attacks as presented in Figures 10 (a-d) shows that at k = 1 to 4, DDOS attack is the nearest neighbor to the mean of combined attacks. The frequency and percentage of attacks on airport check-in computers are presented in Figures 11 (a-b) respectively. DDOS was observed to have the highest frequency of attack and highest percentage in intensity followed by Trojan.

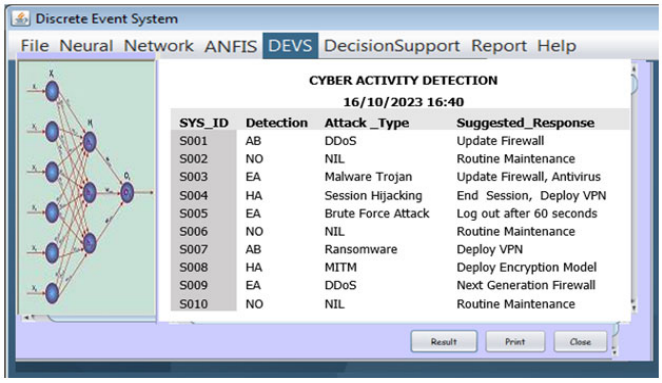

Figure 9. Cyber Activity Output Window

Results Extracted from ANFIS-DEVS Model

The final ANFIS-DEVS cyber activity presents the output as either Normal (NO), Abnormal (AB), Highly Abnormal (HA) or Extremely Abnormal (EA). The model also intelligently suggests some responses to guide decisions towards detected activity as presented in Table 4.Analysis of the results obtained from the ANFIS-DEVS system showed that within three (3) days, DDoS attack occurred 8 times, Brute Force and Session Hijacking attacks occurred 2 times each, Trojan attack occurred 3 times, while Man-in-the-middle (MITM) and Ransomware attacks occurred 1 time each.

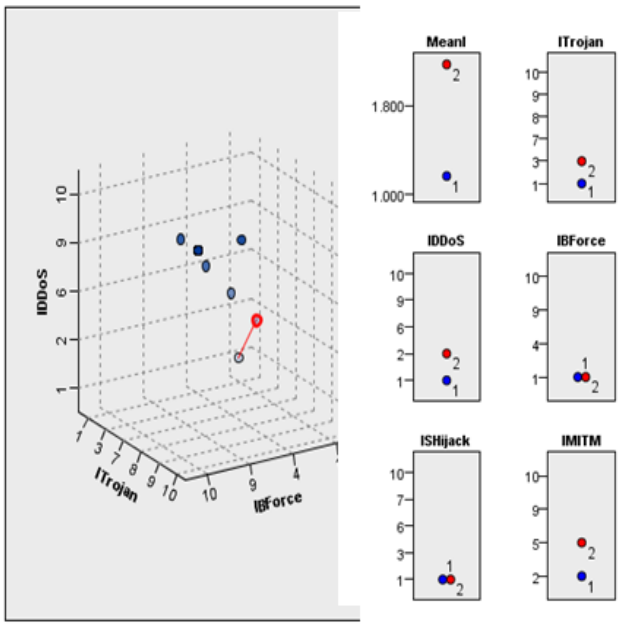

Figure 10a: Malware model nearest neighbor at k = 1

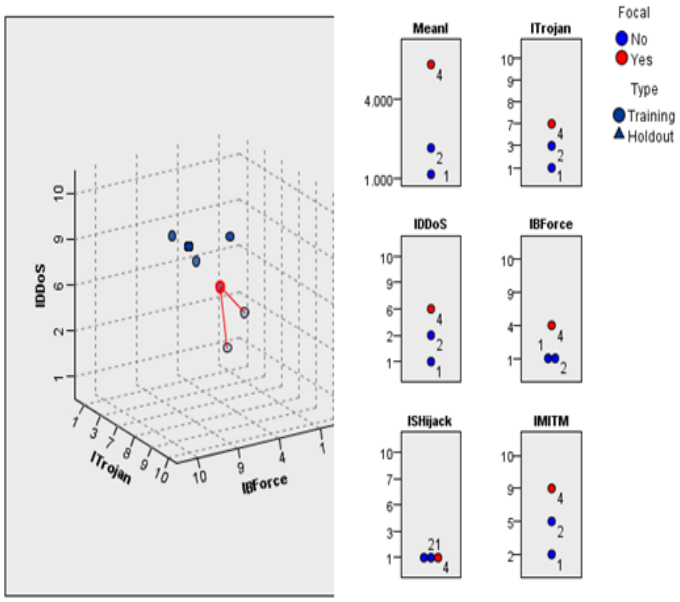

Figure 10b: Malware model nearest neighbor at k = 2

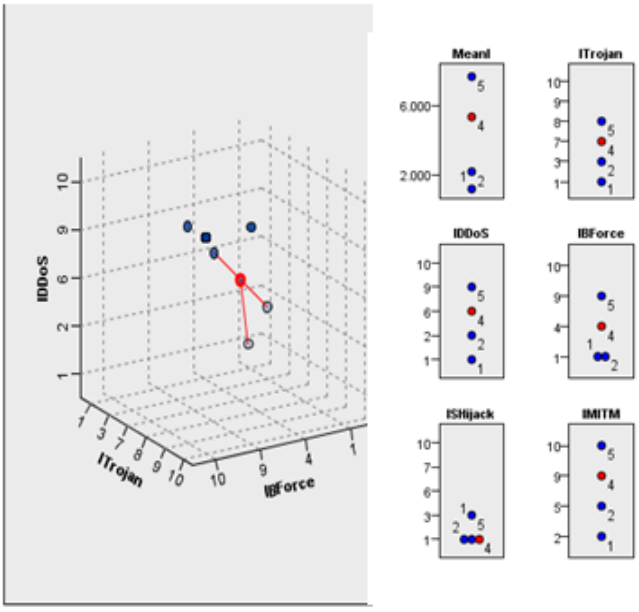

Figure 10c: Malware model nearest neighbor at k = 3

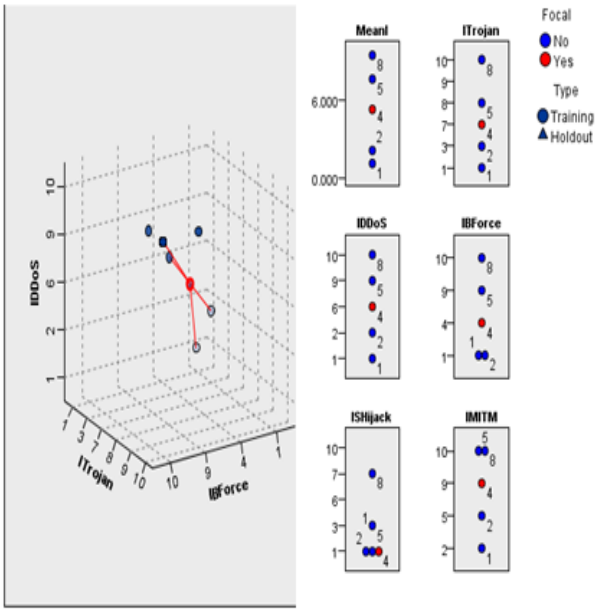

Figure 10d: Malware model nearest neighbor at k = 4

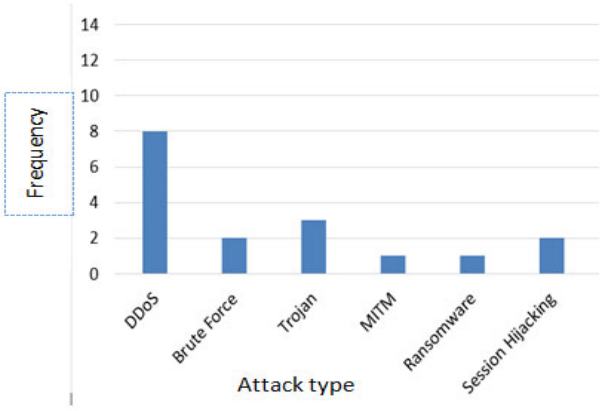

Figure 11a: Frequency of Cyber-Attacks Check-in System

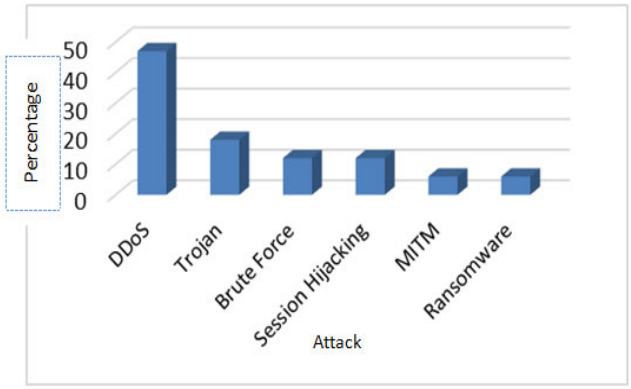

Figure 11b: Percentage of Cyber-Attacks

Table 4. Extracts of Cyber Activity Monitoring Operation

Test_ID	SYS_ID	Date	Time	Detection	Attack_Type	Suggested Response
Te1	S001	16/10/2023	4.40pm	AB	DDoS	Update Firewall
Te2	S002	16/10/2023	4.40pm	NO	NIL	Routine Maintenance
Te3	S003	16/10/2023	4.40pm	EA	Malware Trojan	Update Firewall, Antivirus
Te4	S004	16/10/2023	4.40pm	HA	Session Hijacking	End Session, Deploy VPN
Te5	S005	16/10/2023	4.40pm	EA	Brute Force Attack	Log out after 60 seconds
Te6	S006	16/10/2023	4.40pm	NO	NIL	Routine Maintenance
Te7	S007	16/10/2023	4.40pm	AB	Ransomware	Deploy VPN
Te8	S008	16/10/2023	4.40pm	HA	Malware Trojan	Update Firewall, Antivirus
Te9	S009	16/10/2023	4.40pm	EA	DDoS	Update Firewall
Te10	S010	17/10/2023	4.40pm	NO	NIL	Routine Maintenance
Te11	S001	17/10/2023	9.00am	NO	NIL	Routine Maintenance
Te12	S002	17/10/2023	9.00am	HA	Session Hijacking	End Session, Deploy VPN
Te13	S003	17/10/2023	9.00am	EA	Malware Trojan	Update Firewall, Antivirus
Te14	S004	17/10/2023	9.00am	NO	NIL	Routine Maintenance
Te15	S005	17/10/2023	9.00am	NO	NIL	Routine Maintenance
Te16	S006	17/10/2023	9.00am	NO	NIL	Routine Maintenance
Te17	S007	17/10/2023	9.00am	NO	NIL	Routine Maintenance
Te18	S008	17/10/2023	9.00am	NO	NIL	Routine Maintenance
Te19	S009	17/10/2023	9.00am	EA	Brute Force Attack	Log out after 60 seconds
Te20	S010	17/10/2023	9.00am	EA	MITM	Deploy Encryption Model
Te21	S001	18/10/2023	12.00pm	NO	NIL	Routine Maintenance
Te22	S002	18/10/2023	12.00pm	NO	NIL	Routine Maintenance
Te23	S003	18/10/2023	12.00pm	NO	NIL	Routine Maintenance
Te24	S004	18/10/2023	12.00pm	EA	DDoS	Next Generation Firewall
Te25	S005	18/10/2023	12.00pm	EA	DDoS	Next Generation Firewall
Te26	S006	18/10/2023	12.00pm	AB	DDoS	Update Firewall
Te27	S007	18/10/2023	12.00pm	AB	DDoS	Update Firewall
Te28	S008	18/10/2023	12.00pm	AB	DDoS	Update Firewall
Te29	S009	18/10/2023	12.00pm	EA	DDoS	Next Generation Firewall
Te30	S010	18/10/2023	12.00pm	NO	NIL	Routine Maintenance

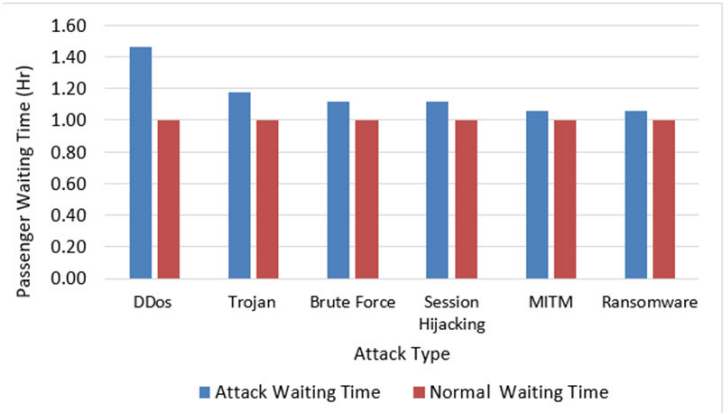

Figure 12: Effect of Cyber Attack on Waiting Time in First Hour of Attack

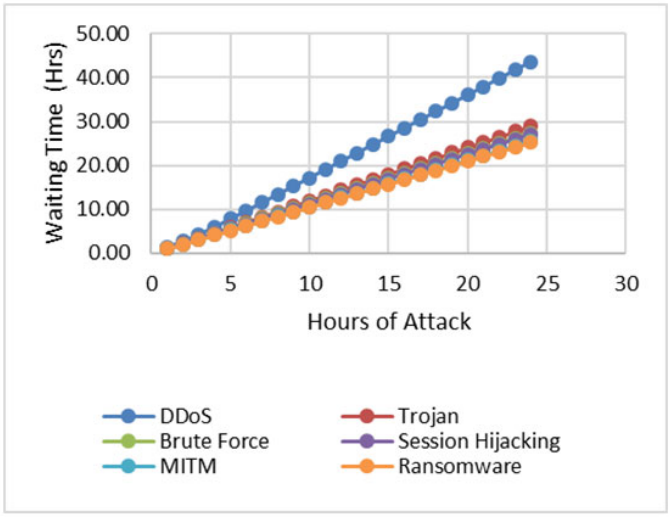

Figure 13a: Effect of Cyber-Attacks on Waiting Time

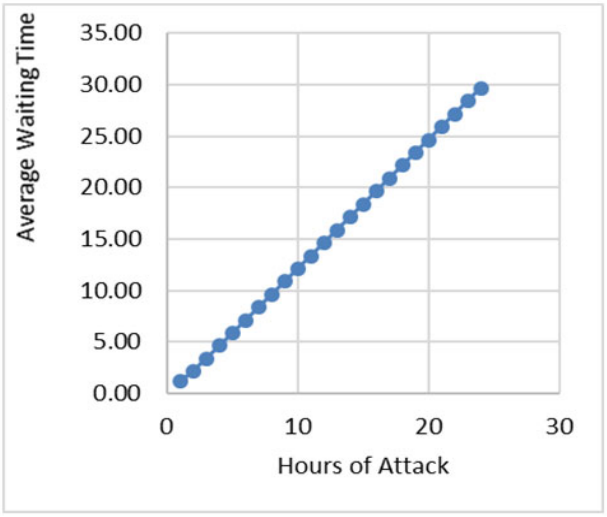

Figure 13b: Effect of Combined Attack on Average Waiting Time

The results indicated that Airport check-in and screening systems were more vulnerable to DDoS attacks followed by Trojan attacks as well as Brute Force and Session Hijacking attacks.In the first hour of attack, the effect of the cyber-attacks on waiting time of passengers to board flight at the Airport is depicted in Figure 12. The normal waiting time to board flight at the Airport is one (1) hour. The computation of average waiting time showed that in the first hour of attack, DDoS increases the waiting time by 47 minutes, Trojan increases the waiting time by 18 minutes, Brute Force increases the waiting time by 13 minutes, Session Hijacking increases the waiting time by 11 minutes, MITM increases the waiting time by 6 minutes while Ransomware increases the waiting time by 5 minutes. The waiting time of passengers increases substantially for all attack types in subsequent hours of attack. Figures 13a presents the effects of individual malware attacks on passengers waiting time while Figure 13b shows the combined effects of all attacks on average waiting time. As seen in Figure 13a, the greatest impact on passengers waiting time is caused by DDoS.

As shown in Figures 13a and b, it is obvious that the effect of cyber-attacks on waiting time is insignificant and tends to zero in the first hour of attack for all types of attack. However, as hours of attack increases, waiting time significantly increases and assumes a funnel-like structure at the top with the highest deviation observed in DDoS.The average waiting time increases proportionally with increase in hours of attack. Out of the 30 instances of cyber-attack monitoring operations extracted from the ANFIS-DEVS model, 29 instances correctly identified the cyber-attack and proffered solutionsto guide responses by stakeholders in the aviation industry as indicated in Table 4.Also, out of the 144 data instances used to assess the effectiveness of the system in the test dataset, 137 instances correctly identified the cyber-attack and proffered solution to guide responses. Hence, the model exhibited 95.14 % accuracy on the tested data.

Conclusion

In this research, related works on cyber-attacks and its effect on corporate infrastructure have been reviewed. Various forms of cyber- attacks were studied with a view to deciphering their patterns and techniques of operation. Review of adaptive neuro-fuzzy inference system and discrete event system specification were carried out. ANFIS- DEVS based model for infrastructure monitoring was adopted for the study. ANFIS-DEVS model for monitoring cyber-attacks was furnished with Knowledge base of cyber-attack comprising database, activity base and attacks repository. K-nearest neighbor model was designed for classification ofcyber-attacks patterns. The model was implemented using Java programming tools and MYSQL data base. The system showed acceptable performance with accuracy level of 95.14% in the task of monitoring cyber-attacks at the airport check-in computers. It was observed that the effect of cyber-attacks on waiting time is insignificant and tends to zero in the first hour of attack for all types of attack. However, as hours of attack increases, waiting time significantly increases and crumbles the check-in and screening operations as well as the throughput of the Airport which could lead to cancellation of flights. Hence the need for proactive monitoring solution for cyber-attacks at Airport. Further research in monitoring cyber-attacks at airport using other classifiers and variants of adaptive discrete event-basedmodel are recommended.

Acknowledgements: The authors of this work are thankful to the Tertiary Education Trust Fund (TETFund) for their support of this research through the TETFund Centre of Excellence in Computational Intelligence Research, University of Uyo and the University of UyoManagement Team for the support and provision of enabling environment.

REFERENCES

Obot O. U., George U. D. &Udoh S. S. (2017): Managing information in fighting terrorism. *Journal of the Nigerian Association of Mathematical Physics,* Nigeria *40*(1), 265–272**.**

Sanapala, V. K. (2022). Cybersecurity in aviation: Risk and Mitigation. https://manageengine.com

George, U. D., Udoh, S. S., & Obot, O. (2023). An intelligent pattern recognition model for assessment of terrorists' activities in Nigeria. *International Journal of Science and Research Archive*, *09*(02), 231–244. DOI: https://doi.org/10.30574/ijsra.2023.9.2.0516

Mimesh, H. M. (2019). A discrete event simulation-based approach for managing cyber vulnerabilities in a full-service deep waterway port. *A Masters Degree Thesis in System Engineering. Mississippi State University, USA*. Pp 1-32.

Roy, J. (2008). Anomaly detection in the maritime domain. *In Optics and Photonics in Global Homeland Security International Society for Optics and Photonics.* IV (Vol. 6945, p. 69450W).

Riveiro, M., Falkman, G., and Ziemke, T. (2008). Visual analytics for the detection of anomalous maritime behavior. In 2008 12th IEEE International Conference Information Visualisation (pp. 273-279).

Chiappetta, A., &Cuozzo, G. (2017). Critical infrastructure protection: Beyond the hybrid port and airport firmware security cybersecurity applications on transport. In 2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS) (pp. 206-211). IEEE.

Daum, O. (2019). Cyber Security in The Maritime Sector. *Journal of Maritime Law & Commerce,* 50(1)

Zeigler, B. P., (2003): DEVS Today: Recent Advances in discrete event-based information technology", *Proceedings of the11th IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer Telecommunications Systems, Orlando*, pp. 148-161.

Udoh S. S., Akinyokun O. C., Inyang U. G., Olabode O., & Iwasokun G. B. **(**2017). Discrete event-based hybrid framework for petroleum products pipelineactivities classification. *Journal of Artificial Intelligence Research*, *6*(2), 39–50.

Kara, S., Hizal, S., & Zengin, A. (2022). Design and implementation of a devs-based cyber-attack simulator for cyber security. *International Journal of simulation model, 21*(2022)1, 53-64.

Ukwandu, E.; Ben-Farah, M.A.; Hindy, H.; Bures, M.; Atkinson, R.; Tachtatzis, C.; Andonovic, I.; Bellekens, X. Cyber-Security Challenges in Aviation Industry (2022): A Review of Current and Future Trends. Information, 13, 146. https:// doi.org/10.3390/info13030146

Alnajim, A. M., Habib, S., Islam, M., Albelai, R., &Alabdulatif, A. (2023). Mitigating the risks of malware attacks with deep learning techniques. *Journals Electronics 12(14) 3166.* https://doi.org/10.3390/electronics12143166

Kirkliauskaite, K. (2020). Main Cyber-Security Challenges in Aviation. Available online: https://www.aerotime.aero/ 25150-main-cyber-security-challenges-in-aviation.

Narendra, M., (2019). Air New Zealand Experiences Data Breach Available online: https://www.grcworldforums. com/news/2019/08/16/privacy-air-new-zealand-experiences-data-breach/

Ishtiaq, S. & Rahman, N. A. (2021). Cybersecurity vulnerabilities and defence techniques in aviation industry. *Atlantis Highlights in Computer Sciences, Atlantis Press International (4)559-567.*

Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P., Janicke, H. A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports. IEEE Access 2020, 8, 209802–209834. [CrossRef]

Prasanna, S., Shahab, S., Shan X. & Mo, J. (2003). Multi Agent Simulation Using Discrete Event and Soft-computing Methodologies. *IEEE Journal of Simulations* 4(2), pp1711 -1716.

Udoh, S. S. (2016). Adaptive neuro-fuzzy discrete event system specification for monitoringpetroleumproducts pipeline (Doctoral dissertation, PhD Dissertation, Department of Computer Science, School of Sciences, Federal University of Technology, Akure, Nigeria). Pp 178−212

Udoh, S. S., Asuquo D. E., Inyang U. G. (2018). Adaptive neuro-fuzzy model for oil pipelines monitoring in a cluster-based sensor network environment.*World Journal of Applied Science and Technology10* (1B)184–190.

Udoh, S. S**.,** George, U. D. &Etuk, U. R. (2023). Cassava yield forecasting using artificial neural network. In I. A. Ayandele; G. N Udom; E. O. Effiong; U. R. Etuk; I. E. Ekpo; U. G. Inyang; G. E. Edet& I. Moffat (Eds.), *Contemporary Discourse on Nigeria's Economic Profile: A festschrift in honour of Professor Nyaudoh, U. Ndaeyo.* A Publication of University of Uyo*,* pp. 667–679**.**

Udoh, S. S.,Usip, P. U., George, U. D., & Akpan I. E. (2024). Adaptive neuro fuzzy-based depression detection model for students in tertiary education. *Springer Nature, Applied Machine Learning and Data Analytics* AG 2024 M. A. Jabbar et al. (Eds.): AMLDA 2023, CCIS 2047, pp. 156–167, https://doi.org/10.1007/978-3-031-55486-5_12

****