© MAR 2026 | IRE Journals | Volume 9 Issue 9 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I9-1715357

# Design and Implementation of Machine Learning Models to Detect Cybercrime: A Perception for the Gen-z(S)

SUNDAY ELIJAH ADEYEMO[1], JELILI IDRIS OLAWALE[2], YINUSA AISHAT BUKOLA[3], OSOBA DANIEL[4]

[1]*Christopher University Mowe, Nigeria, Department of Computer Science*
[4]*Maranatha University Okota-Lagos, Nigeria, Department of Cybersecurity*

***Abstract-*** ***This project focuses on the trade-off between the concept of cyber-psychology among the Nigerian Gen Z's attitude that involves exploitation of cyberspace users and super smart society 5.0 subset features like Machine Learning Algorithms to combat network intrusion. A survey using google form questionnaire was taken as a sample at the Maranatha University, Lagos campus among the undergraduates of about 200 students. Apparently, the survey depicts Gen Z predominately depending on cyberspace as means of living. To further analyse the detection of cyberattack on the cyberspace which this age group mainly rely on. At the cross road of approaches to detect network intrusion, using Machine Learning techniques serves as the renaissance through which simulation of network scenario using Network Traffic Data for Intrusion Detection dataset which was implemented with the use of Waikato Explorer Knowledge Analysis (WEKA) as a data mining tool to build Machine Learning models like Naïve Bayes, J48, Random Forest and AdaboostM1. The best model in the experiment was Random Forest with evaluation metrics of precision, accuracy, Root Relative Squared Error (RRSE) and sensitivity as 1.00,0.985,0.389 and 1.00 respectively. The outcome of the simulation shows perfection of the Random Forest model to predict intrusion as cyberattacks after considering the independent variables of the dataset. The real-life scenario further suggests the need for Gen Z to substitute their cyber-psychology curiosity with Machine Leaning techniques as a perception to curb cybercrime.AI-driven driven cybersecurity is the future, which is undoubtedly needed by the Gen Z to leverage the benefits of the society 5.0 epoch.***

***Keywords: Machine Learning, Model, WEKA, Precision, Accuracy, Sensitivity, RRSE, Cyber-Psychology, Society 5.0***

## I. INTRODUCTION

The perception of many Nigerian youths especially the very active ones popularly known as the Generation Z (Gen Z) to use the internet has been negatively sensed to make a strategic advantage of exploiting individuals, institutions, organizations and companies. The escalating number of cybercrimes poses significant challenges for ensuring the security of networked and standard systems. However, the high awareness of cybercrime by this age group is very high yet with wrong perception of the use.

Cybercrime is a global issue that has transcended various geographical boundaries, its development as changed forms overtime; it continues to evolve into divergent phases according to (Fajemirokun, 2025).Even though the awareness of cybercrime amount to very high percentage among the youths , undergraduates intersecting with the Gen-Z yet comprehensive knowledge of the awareness should trigger their curiosity to acquire knowledge especially in the new epoch of AI using the Machine Learning techniques as it subset to combat cybercrime. In as much it is global issue, yet the peculiarity of cybercrimes among the Nigerian Gen-Z(s) is based on the social economic problems, unemployment, according to many research articles on this subject.

Following the trend through the society 1.0 to society 5.0 ,the latest society 5.0 has a lot of privileges than others via AI, Internet of Things and 5G network just to mention a few .So the age group focuses more really and efficiently on the correlation between the physical world and the cyber world(Nicholson et al., 2023) but despite their accessibility to all these opportunities –there is still wrong perception to their awareness to this renaissance. The prevalence of problem is the wrong perception to the leverage of opportunities at hand.

While many of these intellectual findings (Sani et al., 2024) (Eberechukwu Nwodu, 2025) (Balogun et al., 2024) proved the unconducive environment for many Nigerian Gen Z to venture into cybercrime(s) even with high rate of awareness to cyberattacks notwithstanding it has a way of de-moralizing their attitude. In the world of cyber age, cybercrime is spreading its root extensively. Supervised classification methods such as the Support Vector Machine (SVM), Naïve Bayes, J48, Random Forest and AdaBoostM1 models are employed for the classification of cybercrime data using WEKA (Waikato Environment for Knowledge Analysis) as data mining tool. Likewise, the unsupervised mode of classification involves the techniques of K-means clustering, Gaussian mixture model, and cluster random via fuzzy C-means clustering and fuzzy clustering. Neural networks are employed for determining synthetic identity theft. formation of clusters takes place using these clustering techniques, which fetches crime data from the overall data as noted by(Kaur et al., 2023) (Veena et al., 2022). Yet, little has the Nigerian youths utilize of the strategic advantage of Machine Leaning techniques to solve challenges, that can attract wealth legitimately without fraudulent means.

## II. LITERATURE REVIEW

Through the literature review exploration into the past and recent research papers pertaining to the awareness of the Generation Z to cybercrime, also the trajectory to the future by using Artificial Intelligence was done. Despite the cyber-crime awareness among the Generation Z **( Gen Z )** especially the university students) in Nigeria is very high as stated by (Nsude et al., 2021) to about 68% , yet weak ethical comprehensive knowledge of internet fraud, cybersex-terrorism, malware attacks , spam-emails , identity theft and other sexually related cyber-crime had proved the youths wrong perception of cyberspace as reflected in (Hamisu et al., 2021). The abuse of the awareness and the perception among the Gen-Z is still trending and very destructive to the future. Society 5.0 is a hyper-connected society with advanced technological integration. With the emergence of Society 5.0, characterized by the integration of cyberspace and physical space. Understanding the awareness of Generation Z (Gen-Z) regarding cybercrimes becomes imperative(Sharma et al., 2024).

The conceptual review and the empirical review are the two (2) subsections that make up the activities are explicitly investigated in the conceptual review paragraph, while the empirical review subsection evaluates and discusses the empirical contributions of researchers in the field and articles. thematic style of literature that was used. Scholarly explanations of cybercrime and related

### 2.1 Conceptual Review

#### 2.1.1 Definitions of Research Context

Gen Z sometimes referred to as the Generation Z, were born approximately between 1997 and 2012. In contrast to other generations, Gen Z was raised in an era where digital technology was widely used. Due to their early exposure to the internet, cellphones, and other connected gadgets, this generation is regarded as the first to be completely "digital native."

Cyber is a prefix used in describing any related activity involving computer and/or it networks (for example, the internet), it also connotes the relationship with information technology, while *Crim*on the other hand can be defined as a violation of law, a behaviour not in conformity with the rules and norms of the society. Putting together, cyber and crime, cybercrime is a form of crime that occurs in the cyberspace (meaning, it happens in our world of modern technology and computer). Cybercrime delineates offences that have the potential of causing geopolitical and mental or psychological distress through the use of a computer and internet. The Council of Europe Convention on Cybercrime,(Nsude et al., 2021) defines cybercrime as a broad range of malevolent activities, which includes an unauthorized access to data, system hijack that disrupt or violate network integrity and availability, and copyright infringement.

Cyber security is a set of strategies and processes for defending computers, networks, databases, and applications against assaults, illegal access, modification, or destruction (Perwej et al., 2021). Cyber-attacks are raising concerns about privacy, security, and financial compensation. Moreover, cyber security is a set of technologies, processes, and

practices aimed at preventing attacks, damage, and illegal access to networks, computers, programmes, and data

The digital age has made our virtual identity an expedient component of our everyday life. As the computer has become central of commercial activities, entertainment and government, cybercrime has grown into importance. By the 21st century, hardly any hamlet would be found anywhere in the world that had not been affected by cybercrime of one form or the other (Dennis, 2019). It consists of illegal activities such as, internet fraud, identity theft, human trafficking, child pornography, intellectual property, violating privacy, among others.

Furthermore,(Gajjar & Taherdoost, 2024) made the point that, the traditional form of criminalities does not involve the use of computers in its penetration and it requires the physical presence of the criminal, while the computer is the core of cybercrime. New technologies produce new folds of criminal opportunities and the major difference between the traditional criminal penetration and cybercrime is the fact that there is now the involvement and utilization of digital computers, but then, technology alone is not sufficient for distinguishing between the realms of criminal activity, as perpetrators do not necessarily need a computer to initiate their activities such as fraud, human trafficking, fake job posting, unusual calls and messages for auto teller machine (ATM) pin and bank details, purchase and/or sale of cards of another and others.

Cybercriminals may target an individual's private information, corporate database or government data for resale or personal theft as perceived by (Eberechukwu Nwodu, 2025). The necessity of connectivity to the internet has enabled an increase in the proportion and rate of cybercrime activities, as perpetrators no longer need to be physically present in the scene of the crime. The internet's speed, anonymity, and lack of traceable medium (through the use of VPN - virtual private network) make computer-based variations of financial related crimes - for example, internet fraud, money laundering, credit card scam - easier to execute (Brush & Cobb, 2021). These criminal activities can be carried out by individuals (or groups) with relatively low technical skills, or by highly organized global criminal groups that may include skilled programmers and other expertise.

2.1.2 Misconception of Nigerian Gen Z towards Cybercrime

Misconception of Nigerian Gen Z Towards Cybercrime is rich and important, especially considering the intersection of youth culture, digital literacy, and ethics in Nigeria(Martins, 2024). So it is important to know that Many Nigerian Gen Z may have a skewed understanding of cybercrime due to, media glorification that is social media and popular culture e.g., Afrobeats lyrics, Nollywood, influencers) sometimes glamorize "Yahoo Yahoo" or internet fraud. Also, socioeconomic frustration which explicitly indicate the high unemployment and limited opportunities, some youth perceive cybercrime as a form of survival or a "smart hustle. Another misconception is Peer influence and normalization where Cybercrime may be downplayed or accepted within certain peer groups, with perpetrators seen as successful or brave. Lastly, lack of digital ethics education as a result of limited focus on cyber-ethics and the legal implications of online behavior in school curricula.

Nigeria has the biggest economy and population in Africa, which helps explain why ICT and Internet usage there are growing and spreading quickly. The Internet has been utilized by both good and harmful people, just as prior technologies (Hamisu et al., 2021). Billions of dollars are being lost by the worldwide economy as a result of criminals using computers and the internet. The vast majority of Nigerians use the Internet for constructive purposes, although a small percentage utilize it for illegal purposes like fraud. Nigerian cybercriminals, sometimes referred to as Yahoo Boys, are experts at online scams that mostly target victims from other countries (Nsude et al, 20220. The government of Nigeria is making steps to stop these criminals' operations since they damage nation's reputation. Even if the government's efforts have produced some encouraging outcomes, Nigeria remains at high risk of cybercrime because criminals continue to exploit weaknesses in the tactical method used by law enforcement to combat the crime.

© MAR 2026 | IRE Journals | Volume 9 Issue 9 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I9-1715357

In spite of this, (Aransiola & Asindemade, 2011) co ntended that descriptive research that aims to identif y the tactics used by the offenders in Nigeria is still lacking, which is a crucial prerequisite for practical and trustworthy policy guidance to deal with the iss ue.Along with highlighting the government's shortc omings, it also talks about its accomplishments and areas of strength in the battle against cybercrime.Th ere are recommendations and ideas on how Nigerian law enforcement and the government at large might better combat cybercrime. Additionally, (Aransiola & Asindemade, 2011) explain in their study that they have addressed this gap by utilizing data from 40 cybercriminals who were chosen via the snowballing technique. The results showed that the majority of Nigerian cybercriminals are between the ages of 22 and 29, belong to the Gen-Z social group, and lead different lifestyles from other young people , also pointed out in (Sani et al., 2024) . Their tactics include working along with bank officials and security personnel, networking both domestically and abroad, and utilizing voodoo, or traditional supernatural power. It was evident that the majority of cybercriminals engaged in online dating, as well as purchasing and selling under false pretenses. To vividly delve into how the Gen-Z arrive at their prominent attitudes to the use of internet of things, cloud, AI and other technologies, there is a need to review the evolution of various societies.

2.1.3. Evolution of Societies

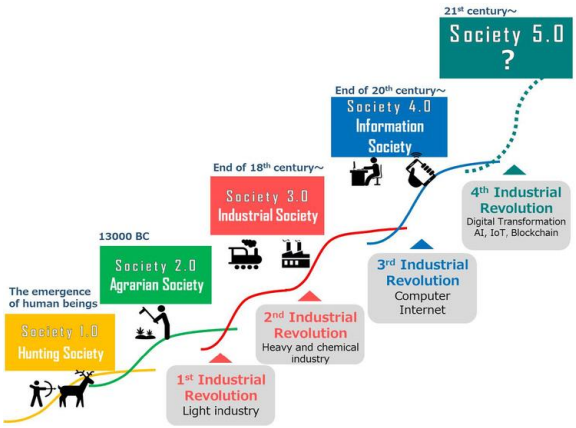



Fig. 2.1 Diagram of the Evolution of Societies 1.0 through 5.0

Actually, Society 5.0 was mentioned above but much in-depth knowledge is needed through the evolution from society 1.0 through society 5.0 as much understanding will aid in mitigating the differences of these societies as we classify them based on their salient features:

Society 1.0: The Hunting and Gathering Society

The first society was led by nomads responsible for food gathering and hunting. They constructed temporary shelters and did not remain in one location throughout the year. The primary goal of the nomads, who traversed familiar territories, was to find sustenance. This challenge made their survival more difficult as they had to search for food sources. They hunted and foraged a variety of items, including roots, fruits, and vegetables. However, they were skilled at adapting to new environments, as demonstrated by their tendency to stay in groups to communicate and share information.

Society 2.0: The Farming Society

Agriculture was established and developed within this community. Consequently, civilization progresses into a new level of development. The production of land and crops enabled more previously nomadic family groups to split into tribes. They were now able to establish permanent homes near rivers for fishing as well as in areas suitable for planting and gathering food. With the need to transport cattle and crops being impractical, humans transitioned to a sedentary lifestyle. Community members were compelled to build durable houses to live in and harvest food throughout the year. Thus, they depended on what they could cultivate, raise, or produce independently to achieve self-sufficiency. The economy utilized various resources from the land, such as grains, fruits, and vegetables.

Society 3.0: Industrial Society

This civilization is consistent with the myriad of production, or the introduction of factories and machinery that supplanted manual labour. Furthermore, mass production was encouraged by the technological advancements of the era, which led to meaningful reductions in prices and times as well as an increase in resources obtained. These factors ultimately resulted in higher worker salaries and revenue. People began to make money as a result that did not even exist before. The first industry was the textile sector, which relied heavily on coal. The way that humans began to think was significantly altered

by this transformation. The emergence of social class structures was also influenced by the way that material items owned by individuals and families defined economic inequalities. In addition, people began to acquire rights throughout this time.

Society 4.0: Information Society

Modern technology has made using information easier. Since social, cultural, and economic activities are primarily focused on people and interconnected technical developments that enable information to move properly and swiftly throughout the world, this is more apparent as expressed by (Ahamed et al., 2024) . Thanks to the preparation and dissemination of information, modern society is undergoing a transformation that encompasses information access and interpersonal communication through ICTs. Everywhere in the world is connected to things and people. For instance, it's simple to find answers to our queries using the Google search engine, which exponentially promotes knowledge availability. Social media also informs users about news, current affairs, and events occurring across the globe.

Society 5.0: Super smart society

This is a human-centred society where social problems are resolved by systems created by integrating sustainability and cyberspace, thanks to economic advancement (Sharma et al., 2023). To address contemporary societal concerns, this unique societal model focuses more effectively and efficiently on the relationship between the physical world and the cyber world, which was defined and evolved in the Fourth Industrial Revolution. This new social model, which is based on a unified system, directly addresses the needs and interests of individuals while managing social and economic challenges. From an organisational perspective, Society 5.0 aims to develop innovative approaches to managing individualistic systems in which businesses, academic institutions, and governmental bodies independently work to develop a cooperative operational concept enhanced by the interconnectedness of today's society.

A high degree of convergence between cyberspace (virtual space) and physical space (real space) is achieved by Society 5.0 of which many Nigerian youths just have the concept but lack the technicality to operate ethically-this wrong conception has not enable the Gen-Z to reap the benefits of Cyberspace at their fingertips and take advantage of the future. “Cyberspace” is a term used to describe a digital environment where real-world data is gathered and examined to provide answers. The phrase was created to refer to a hypothetical or virtual space where vast amounts of unprocessed data are publicly accessible and transformed into insightful knowledge that may be distributed to others. The real world, from which unprocessed data are gathered and solutions are implemented, is referred to as “Physical space”.

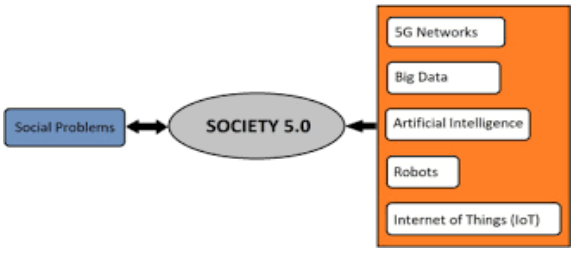



Fig.2.2 Pictorial View of Society 5.0

Figure 2.2 shows that in Society 5.0 popularly known as Super Smart Society and the Gen-Z being the major stakeholders, depicts the physical space will be used to collect enormous amounts of data in cyberspace. Cyberspace artificial intelligence (AI) examines this massive amount of data and provides individuals in physical space with a variety of information types. Additionally, in society 5.0, all entities—people, things, and systems—are linked online, and artificial intelligence (AI) generates results that are better than those of humans and then transfers them back into the physical world this is not limited other trending technologies like 5G Networks, Big Data, Robots and Internet of Things (IoT). This method has hitherto unimaginable benefits for industry and society (Perwej et al., 2021).

2.1.4. Awareness and Technical Knowledge of Cybercrime

The level of knowledge by average Nigerian youths in cyber security should exceed the point of sensing firewall as the ultimate defense of the system. So more sophisticated parameter of firewall like source address, destination address, source ports, destination port, protocol, direction, priority, time etc

© MAR 2026 | IRE Journals | Volume 9 Issue 9 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I9-1715357

Organizations require cyber security experts and specialists to deal with the numerous types of cybersecurity attacks that come with varying technicalities (Perwej et al., 2021). The larger organisations, on average, are the ones who have paid the most for an internet presence. This is unsurprising given that they were also the most extensively targeted. More than half of all businesses with 1,000 or more employees (51%) reported they have had at least one cyber incident. Cybercrime has a significantly higher cost and intensity. The following are the common cybercrimes in Nigeria and need a cautious awareness and perception (Nzeakor et al., 2022)

Machine Learning Techniques to Detect Cybercrime
The fact that AI has taken over many tasks in recent years is not new. Cyberspace is not excluded either. In his research, (Rizvi, 2023) noted that "Artificial intelligence (AI) has emerged as a key component of cyber security due to its (AI) ability to evaluate security threats in real-time and take appropriate action." The primary focus of this article is on the machine learning subfield of artificial intelligence, which is a very vast area. These days, to name a few applications, machine learning (ML) is used in cybersecurity to find irregularities in system logs, user activity, and network traffic. To recognize malware attacks and phishing efforts, even if they lack a known signature. Vulnerabilities assessment and automated incident response. Also, ML is used for monitoring user activities to detect suspicious behavior, flagging insider threats and disgruntled employees.

Machine Learning is about designing algorithms that automatically extract valuable information from data. The emphasis is on automatic directed toward the use of dataset. Concepts like data, algorithm, model and learning. Data is at the core of machine learning. The goal of machine learning is to design general purpose methodologies to extract valuable patterns from data, ideally without much domain-specific expertise. More also, algorithm for Machine Learning (ML) is a collection of guidelines and statistical techniques for discovering insights pertaining to data. Another important context in Machine Learning is Model ,it is meant to learn from data ,if it task is to improve after the data is taken into consideration. The main purpose of model is to optimally get the best in data by generalizing well even in the utilization data in the future. Models are usually trained using Machine Learning Algorithm while the algorithm perform the execution of sequence of steps that must be taken by a model. Learning is the act of automatically finding patterns and structure in data by optimizing the parameters of the model which can be implied as predicting variable. So, a good model is capable of predicting what would happen in the real-world scenario.

The most important aspect of the ML is the learning aspect given a dataset and suitable model. Training is another concept that means the use of available data to improve some parameters of the model with respect to a utility function that evaluates how the model predicts the training data. The training data is used to construct the machine learning model while the testing data is the predictive ability of a model is determined by its testing once. The model learns to identify important trends and pattern that enhances accurate prediction.

The model is the important target to perform well on unseen data, so performing well on already test-run data (Training data) implies just to memorize data prediction lies on unseen data.

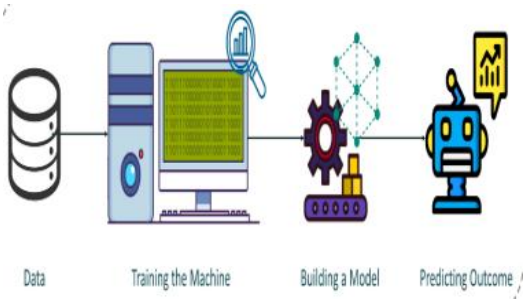


Fig. 2.7 Machine Learning Task

Machine learning entails constructing a Predictive model which can be used for the Problem Statement to determine an appropriate course of action. Assuming you have indeed been given an issue to tackle as clarified by . Machine Learning process contained the following phases according to (Dua & Du, 2016):

i Define Objective Phase

© MAR 2026 | IRE Journals | Volume 9 Issue 9 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I9-1715357

ii Data Gathering Phase
iii Preparing Data Phase
iv Data Exporation Phase (Exploratory Data Analysis)
v Model Evaluation Phase
vi Prediction Phase
vii

Machine Learning Model Classification
Every Machine Learning are classified into three:

i Superverised Machine Learning
ii Unsupervisied Machine Learning
iii Reinforcement Machine Learning

(i)Supervised ML models learn from labeled datasets where the input data and corresponding outputs are provided. Each data point in the training set has both input features (e.g., email title, email body, etc.) and a corresponding target label (e.g., "spam" or "not spam"). The model learns to map inputs to outputs and can then predict labels for unseen data. Supervised ML solves two types of problems:

- Regression, that predicts continuous values for example monitoring network traffic usage to predict peak times and prepare for potential Distributed Denial-of-Service (DDoS) attacks, and other examples.
- Classification, that predicts categories (e.g., email is spam or not, Malware detection and Intrusion detection)

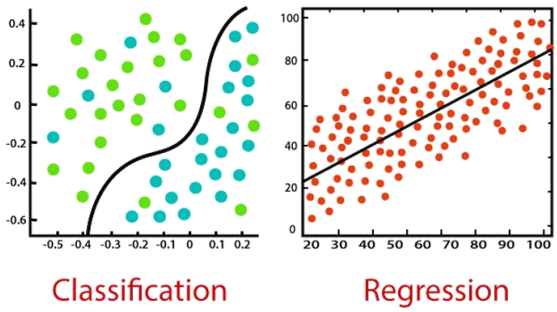



Fig.2.8 Visualized Graph of Classification and Regression Models

(ii) Unsupervised learning is a kind of machine learning in which the model is trained with data that has not been labelled and then given the freedom to make decisions independently.

(iii) Reinforcement Learning -The field of machine learning known as Reinforcement Learning involves placing a virtual agent in a real-world setting and teaching it how to act appropriately by watching the consequences of its choices and adjusting its behavior accordingly.

The Image below was depicted by[cited] in his article to show pictorial view of Machine Learning Model Categories.

| Supervised | Unsupervised | Reinforcement |
|---|---|---|
| Linear Regression | K-Means Clustering | Deep Q-Networks |
| Logistic Regression | DBSCAN | Proximal Policy Optimization |
| Support Vector Machines | Isolation Forest | Soft Actor-Critic |
| Decision Trees | Transformers (BERT, GPT) | |
| Random Forest | | |
| Gradient Boosting Machines | | |
| Naïve Bayes | | |
| k-Nearest Neighbors | | |
| Neural Networks | | |

Fig.2. Machine Learning Categories and Model

## III. METHODOLOGY

The awareness and perception of Gen-Z towards the cyber structure should go beyond exploiting others, rather the need to innovatively automate the cyber structure using the society 5.0 technological features such as AI, robots, Internet of Things, Big Data and 5G Network should be leveraged to proactively induce Intrusion Detection System (IDS). The IDS serves as a surveillance or monitoring system for Network traffic and cyber treats, IDS helps in identifying potential intrusions or malicious activities on a network by analysing the packet data, security professionals can detect signs of common attack techniques like port scanning, network reconnaissance. In this project survey, questionnaire was distributed using Online Google Form to the Undergraduates students at Maranatha University, Okota Campus of Lagos State, Nigeria (about 200 in population) to study the opinion and perception of young youths towards their participation in cyberspace as a sole medium of business, means of living and they being actively involved. Leveraging the benefits of AI and Data mining techniques on the cyber structure requires previous knowledge of combating cybersecurity threats at two levels that is the network- and host-based defense system. Network-based defense systems control network flow

© MAR 2026 | IRE Journals | Volume 9 Issue 9 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I9-1715357

by network firewall, spam filter, antivirus, and network intrusion detection techniques. Host-based defense systems control upcoming data in a workstation by firewall, antivirus, and intrusion detection techniques installed in hosts.

However,the use of data mining and Machine Learning Algorithm through a WEKA as a datamining software is the state-of-art that can be of aid by depicting various Machine learning Algorithm to build models of Random Forest,Niave Bayes, J48, AdaBoostM1 and Decision Tree. As data mining is the extraction, or "mining, of knowledge from a large amount of data. The strong patterns or rules detected by data-mining techniques can be used for the nontrivial prediction of new data (Dua & Du, 2016). The built models are used to learn from the dataset (Network Traffic Data) gotten from Kaggle (a Data Sciencist platform to get data for analysis, survey and sharing of knowledge). The evaluation metrics will be based on classification of wether there will be a cyberattack ornot using Precision, Recall, F-measure and others on the various Machine Learning built Models that will be examined and elaborately discussed in chapter four of this project.

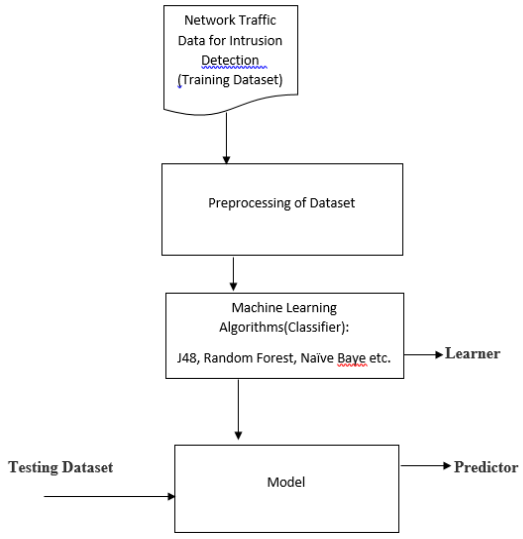



Fig 3.5 Model Design Diagram

## IV. DATA REPRESENTATION AND ANALYSIS

Evaluation Metrics

Machine Learning models built are evaluated based on metrics like precision, accuracy, F-measure, Root Relative Square Error (RRSE), execution time and confusion matrix.

Precision is defined as the proportion of cases found that were actually relevant and it given as :

$$\text{Precision} = \frac{TP}{TP + FP}$$

Recall is defined as the proportion of the relevant cases that were actually found among all the relevant cases.It denoted as :

$$\text{Recall} = \frac{TP}{TP + FN}$$

Accuracy is defined as the ability of the classifier to select all cases that need to be selected and reject all cases that need to be rejected. It is formula is stated as :

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

Sensitivity is the ability of a classifier to select all the cases/instances that need to be selected. A perfect classifier will select all the actual instances and will not miss any actual instance.

$$\text{Sensitivity} = \frac{TP}{TP + FN}$$

The Root Relative Squared Error (RRSE) represents the square root of the relative squared error. It adjusts the model's error by contrasting it with a basic model that forecasts the average of the real values that is the naïve model.

$$\text{RSSE} = \sqrt{\frac{\sum_{i=1}^{n}(x_i - x_j)^2}{\sum_{i=1}^{n}(x_i - \mu)^2}}$$

$x_i$ = actual value

$x_j$ = the predicted value

© MAR 2026 | IRE Journals | Volume 9 Issue 9 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I9-1715357

$\mu$ = mean of the actual value

$n$ = number of data point

Interpretation:

RRSE <1: The model performs better than a naïve model ( a naïve model is a simple and not too sophisticated model used as a an average baseline)

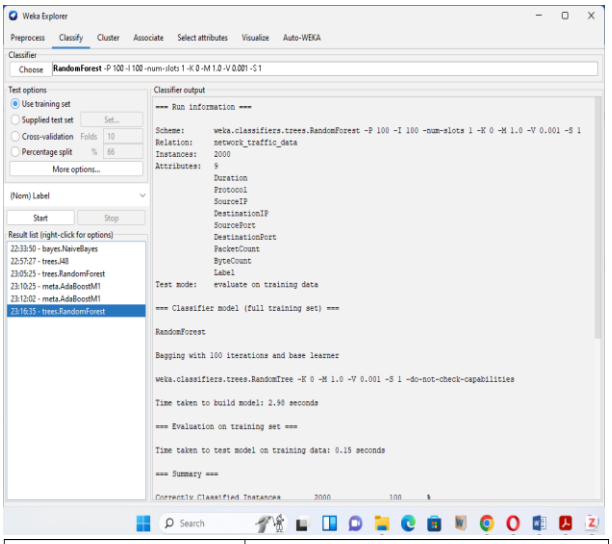
RRSE = 1 : The model performs as well as naïve model

RRSE >1 : the model performs more than naïve model

The main benefit of using RRSE is due to it scale independent metric to be compared with other models across different datasets

Confusion Matrix: this is mostly 2×2 matrix metric that is very useful in this context as the class label of the dataset shows whether there was an attack or normal .So, the accuracy of the confusion matrix can be viewed with four parameters that can be very useful with other metrics explained above.

- The predicted class is Y, and the actual class
- 
- is also Y - this is a True Positive or
- TP
- The predicted class is Y, and the actual class is N - this is a False Positive or FP
- The predicted class is N, and the actual class is Y - this is a False Negative or FN
- The predicted class is N, and the actual class is also N - this is a True Negative or TN




| • | | Actual Class (observation) | |
|---|---|---|---|
| | | Y | N |
| Predicted Class (expectation) | Y | TP<br>Correct instances | FP<br>Unexpected instances |
| | N | FN<br>Missing instances | TN<br>Correct absence of instances |

Table.4.2 Confusion Matrix Table

The Performance of the Classifiers

The four selected classifiers were evaluated using the WEKA tool , the training data was chosen in preference to 10 cross-validation folds which reshuffles the dataset and split it equally into 10 or "n" equal datasets. The training dataset was adopted due to the pre-analysed and cleaning of the dataset even with WireShark to represented the dataset in a real scenario.

The performance of these classifier was based on 2000 instances which can be an under sampled form of dataset , however the evaluation of the Machine Learning Classifiers based on building perfect model is feasible with this experiment. The full details of the outputs of this experiment is shown at the appendix of this project.

| Classifier | Precision | Accuracy | Recall | F-Measure | RRSE | Sensitivity | Execution time (s) |
|---|---|---|---|---|---|---|---|
| Naïv | 0.69 | 0.71 | 0.7 | 0.70 | 0.8 | 0.698 | 0.03 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| e Bayes | 8 | 6 | 16 | 7 | 80 | | 5 |
| J48 | 0.864 | 0.876 | 0.876 | 0.870 | 0.620 | 0.867 | 0.085 |
| Random Forest | 1.000 | 0.985 | 1.000 | 1.000 | 0.389 | 1.00 | 0.345 |
| Ada Boost | 0.551 | 0.516 | 0.516 | 0.533 | 0.997 | 0.5380 | 0.195 |

Table.4.3 Classifier Evaluation Metrics (for attacks prediction)

4.5 Summary of Finding through Classifiers Interpretations

- The Random Forest (RF) performed better than the other three classifiers, followed by the J48 in terms of precision, accuracy, recall, F-measure, RRSE and sensitivity. Although the Random Forest has the longest duration of the execution time as a result of many decision trees ensemble together to yield accurate result.
- The RRSE value of the Random Forest with 0.39 is a confirmation of the reality of building a perfect model with WEKA. The value is less than 1 which means RF model performs better than a naïve model.
- However, other classifiers values are also lesser than one according to Table 4.3, this also showed the level perfection in RF model as the sensitivity is 1.00 That is ability to select all instances needed to be selected. For this experiment all the 2000 instances of the dataset were selected that implied the correlation and importance of the 9 attributes with the classification to detect network intrusion as a possible attack. The execution time is the time taken to test the model on training data, considering the time taken to build the Random Forest Model in this experiment was longer than other classifiers. This underscores complex data structure of trees used in the model to enhance the model at different levels of the tree. The ensemble of RF model enables improved prediction accuracy.

## V. SUMMMARY AND CONCLUSION

Cyber-psychology among the Gen Z in Nigeria towards cybercrime has to be improved with the aid of machine learning task that requires a collective effort of acquiring veiled knowledge of data mining and machine learning models. Undoubtedly, this project through the summary of findings has necessitated the need for the young youths to go beyond superficial knowledge of using cyberspace as means of exploitation, awareness and perception of cybercrime only without the machine learning task to thrive in the huge amount of data as benefactors of society 5.0. The way-out to thrive is through AI (Artificial Intelligence) through the building of Machine Learning models for accurate prediction of cybercrime.

The experiment performed so far will remove the cover of deluge in network intrusion which is a common problem in cyberspace. The Gen Z are over dependent on the use of cyber structure without the need to explore the wide variety of opportunities accompanying the society 5.0. The accuracy, RRSE and sensitivity are best evaluation metrics to detect intrusion through Machine Learning classifiers to even forecast the possibilities of cybercrime by building the model that gives the cyberspace users wide range privilege to avoid catastrophic havoc that could be caused by cyberattacks. Therefore, the need to leverage the ML task to forecast cybercrime is a very important challenge for the cyberspace users while physically handling these features : duration (the duration of the network connection in seconds),protocol (the protocol used (TCP, UDP, ICMP),source IP(the source IP address of the traffic),destination IP (the destination IP address of the traffic),Destination Port (the destination port number.),Packet Count (the number of packets in the connection),Source Port (the source port number.) and Byte count (the number of bytes transferred).

The dataset from the experiment needs to be improved tremendously as a large one to build models that can really predict cyberattacks on real scenarios of cyberspace.

Nigeria has the biggest economy and population in Africa, with high dominance and usage by the Gen Z which underscores why ICT and Internet usage are growing and spreading quickly.

The dominance has encroached into many organizations, institution and bodies depending on cybersecurity as a means of sustenance, models applicable to very large datasets and real life situation are highly encouraged to be explored.

The Generation X (Gen X), Generation Y (Gen Y) can never attain the unprecedented thriving privileges ever achieved by the Generation Z (Gen-Z) through the use of AI,5G Networks, Internet of Things, big data and robots while using the cyberspace. Gen-Z need to gear up with their awareness and perception towards deep exploration into detection of cybercrime with Artificial Intelligence epoch not by mere conventional means because that is the future.

REFERENCES

[1] Ahamed, B., Polas, M. R. H., Kabir, A. I., Sohel-Uz-Zaman, A. S. M., Fahad, A. A., Chowdhury, S., & Rani Dey, M. (2024). Empowering students for cybersecurity awareness management in the emerging digital era: The role of cybersecurity attitude in the 4.0 industrial revolution era. Sage Open, 14(1), 21582440241228920.

[2] Balogun, N. A., Abdulrahaman, M. D., & Aka, K. (2024). Exploring the prevalence of internet crimes among undergraduate students in a Nigerian University: A case study of the university of Ilorin. Nigerian Journal of Technology, 43(1), 71–79.

[3] Dua, S., & Du, X. (2016). Data mining and machine learning in cybersecurity. CRC press.

[4] Eberechukwu Nwodu, G. (2025). Awareness and Perception of the Use of Artificial Intelligence for Learning Among Select Communication Undergraduates in Nigeria. African Journal of Social Sciences and Humanities Research, 8, 113–130. https://doi.org/10.52589/AJSSHR-QKE2A0EG

[5] Fajemirokun, O. (2025). NIGERIA'S SECURITY DYNAMICS AND THE FIGHT AGAINST CRIME. Open Journal of Social Science and Humanities (ISSN: 2734-2077), 5(2), 1–9.

[6] Gajjar, V. R., & Taherdoost, H. (2024). Cybercrime on a global scale: Trends, policies, and cybersecurity strategies. 2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI), 668–676.

[7] Hamisu, M., Idris, A. M., Mansour, A., & Olalere, M. (2021). Analysis of cybercrime in Nigeria. 2020 IEEE 2nd International Conference on Cyberspac (CYBER NIGERIA), 73–79.

[8] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804.

[9] Martins, S. (2024). The Firm and Its External Stakeholders. In Business Ethics in Africa, Volume I: Values, Profits and Responsibility (pp. 43–59). Springer.

[10] Nicholson, J., Marcum, C., & Higgins, G. E. (2023). Prevalence and Trends of Depression among Cyberbullied Adolescents-Youth Risk Behavior Survey, United States, 2011–2019. International Journal of Cybersecurity Intelligence & Cybercrime, 6(1), 45–58.

[11] Nsude, I., Elem, S. N., & Uwaoma, A. N. (2021). Combating cybercrime through artificial intelligence for sustainable Development in Nigeria. Artificial Intelligence and the Media, G s, 63.

[12] Nzeakor, O. F., Nwokeoma, B. N., Hassan, I., Ajah, B. O., & Okpa, J. T. (2022). Emerging trends in cybercrime awareness in Nigeria. International Journal of Cybersecurity Intelligence & Cybercrime, 5(3), 41–67.

[13] Perwej, D. Y., Qamar Abbas, S., Pratap Dixit, J., Akhtar, D. N., & Kumar Jaiswal, A. (2021). A Systematic Literature Review on the Cyber Security. In International Journal of Scientific Research and Management (Vol. 9, Number

12, pp. 669–710). International Journal of scientific research and management. https://hal.science/hal-03509116

[14] Rizvi, M. (2023). Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. International Journal of Advanced Engineering Research and Science, 10(5), 055–060.

[15] Sani, K. M., Hassan, M. A., Saidu, M., Kabiru, S., & Tata, U. D. (2024). Investigating Undergraduate Students Levels of Cybercrime Awareness: A Study of Northwest University Sokoto, Sokoto State, Nigeria. International Journal of Social Sciences & Educational Studies, 12(1), 19–39.

[16] Sharma, V., Manocha, T., Garg, S., Sharma, S., Garg, A., & Sharma, R. (2023). Growth of Cyber-crimes in Society 4.0. 2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM), 1–6.

[17] Sharma, V., Verma, Pranay, Singh, A., Verma, Pradeep, Manocha, T., & Srivastava, A. (2024). Awareness of cybercrimes in society 5.0: Perception of generation-z. 2024 International Conference on Intelligent Systems for Cybersecurity (ISCS), 1–6.

[18] Veena, K., Meena, K., Kuppusamy, R., Teekaraman, Y., Angadi, R. V., & Thelkar, A. R. (2022). Cybercrime: Identification and prediction using machine learning techniques. Computational Intelligence and Neuroscience, 2022(1), 8237421.