RAS ENGINEERING & TECHNOLOGY

Review Article: Sensing e-Banking Cybercrimes Vulnerabilities via Smart Information Sciences Strategies

Issue Type: Volume1 Issue1

Author Name:
Faiza Al-Shaarani, Nouf Basakran, Adnan Gutub
Computer Engineering Department, Umm Al-Qura University, Makkah, Saudi Arabia

Corresponding Author:
Adnan Gutub

Citation: Adnan Gutub
Sensing e-Banking Cybercrimes Vulnerabilities via Smart Information Sciences Strategies

Received Date: 22nd Nov-2020

Published Date: 3rd Dec-2020

Abstract:
Smart information data sciences strategies can be utilized for possible cybercrimes inquiry within e-banking activities. This paperwork studies samples of cyber security attacks on e-banking systems covering overview analysis of different required models of data mining techniques. The data mining of client segmentation and productivity, and credit scores and authorization, as well as predicting payment, default advertising, and sensing fake transactions, are all considered as hints adopted to help in possible protection of e-banking system data. We perform comparative analysis of three standard classification techniques as J48, Naïve theorem and zeroR, to ascertain effectivity factors that will provide better results of victimization real crime sensing information. The research found different preferences offering the sorting procedures considering predictive analytics and many confusion matrices factors of processing delay, prediction accuracy, true positive rate, false positive rate, kappa coefficient, precision optimistic predictive value, and recall sensitivity offering options variety of wining methods. The work can be considered a clue to help in researching active information data sciences techniques dedicated for banking cybercrimes possible protection.

Keywords: Banking Cybercrime; Data mining; e-Banking breaches; clustering; Influenced Association Classification; J48; Naïve theorem; zero

1 INTRODUCTION: Today technology has become a part of every single piece in our life from work to our personal life, also in business sector and banking that include to technology. However, from the other side, it also brings a lot of security challenges from intentional or unintentional acts of accessing employees and users [1]. The rapid improvement within e-technology makes us forget about the value of resources, as it starts by people taking easy way and not following the essential and necessary steps to protect their assets [2]. In addition to that, technology can make a revolution in laws with negatively effecting the e-banking industry, i.e. because it's one of importance taking a large number of cyber-attacks on their valuable data. E-banking takes the largest number of cyber-attacks on their data privacy especially that which includes cards net banking and transaction [3]. Therefore, cybercrime can be extremely taught as well on the online business transaction and hectic network traffic, as examples are found of serial criminal cases with technology rising higher and higher to deal and overcome fraud [4]. The ongoing e-life is taking the best classification techniques but found needing help in sensing crimes as investigation and detection to solve this out and take a new role to make it works [3].

Technology can be utilized to provide an effective sensing tool as cybercrimes vulnerabilities models. Its utilization and effectiveness need on-going running as well as separate future prospective cybercrime data mining pattern exposure forecasting, which admits the need for novel methods of security and further secret sharing [5]. Banking sector has been a known hotspot for cybercrime [6]. Technology has

also become an indispensable part of e-Banking work, making it easier for users and administrators to access all services [7]. Banking sectors are prone to many interruptions originated by an assortment of categories of threats; numerous threats are distinct under diverse groups that is cyber fraud, trade permanence development and information safety measures. Cybercrimes that are committed in banks include hacking, Credit card fraud, money laundering, DoS attacks, phishing, salami attacks, ATM card cloning etc. Cyber threats such as pharming, phishing, tempted reveal of private details like identity theft are the security qualms that subsist in the brains of clients in banking and financial sectors [8]. Perceiving cybercrime can be extremely tough as well, as of numerous online business transactions and hectic network traffic which generate enormous quantity of data and just a segment of which relay to prohibited actions.

At present, it has become important to control cybercrime, as it develops with the expansion of technology [9]. To deal and overcome fraud, clustering and classification techniques are implemented to help in this issue [8]. In fact, fraud detection is considered one of the difficult processes not only technically, but also in crime vulnerabilities investigations. The method of fraud detection is based on comparisons, and also based on association, clustering, prediction and outlier detection. Association Rule mining as generates "n" best association rules based on n selected and Classification and Regression Tree (CART) that predict categorical class labels [9]. This work performs comparative analysis of three standard sorting procedures, known as J48, Naïve theorem and zeroR, to form figure-of-merit analysis factors that will provide better results of victimization e-banking crime sensing information benefitting from the crime prevention research presented in [10]. The research found different preferences offering the sorting procedures considering predictive analytics and many confusion testing variables of processing delay, prediction accuracy, true positive rate, false positive rate, kappa coefficient, precision optimistic predictive value, and recall sensitivity offering options variety of wining methods. The work shows many indicators of interesting feedback from the classification ways making the selection based fully on the user priority.

The paper arrangement is as follows. Section 2 covers the literature survey of related works. Section 3 focus on discussing several common cyber security attacks on banks. Section 4 presents our used model for sensing e-banking cybercrime vulnerabilities clarifying several possible classification options. Section 5 gives idea of the experimentations and affecting feedback results. Section 6 concludes the work.

2 LITERATURE SURVEY

Many research attempts studied real-life banking breaches as part of data mining useful probable predictions. For example, Mahdavi in 2015 [11] tried to test theoretical models of reinforced data processing techniques like cluster and sorting to real lawbreaking dataset investigation. They linked their analysis to available verified police reports noted between 1990 to 2011. Interestingly, they selected marks to the different choices in order to formulate a standard, i.e. to serve their model and removed low worth from them. They utilized genetic rule for enhancing outlier discovery operator restrictions exploitation as quick laborer tool [11].

Similarly, Sonaqwanev [12] as well as McClenden [13] both in 2015 had classified misconduct evidences by studying many types of crimes activities. Sonaqwanev studied frequent states and cities of Asian nations that found most interruption occurring against girls with very high percentages. The research [12] used K-means algorithmic program for agglomeration, Pearson's coefficient of correlation for correlating crimes between two variables and regression for crime prediction unlike McClenden [13] investigation using smart machine learning and data processing rail tool to predict violent crime patterns as effective and correct in predicting than Additive regression and call stamp algorithms, i.e. once enforced them with same finite set of options on the communities and crime dataset. Both works presented in [12] and [13] were influenced by Zubi [10] research presented in 2014 related to hack prevention research. Zubi [10] discussed investigation of criminal activities by deeply using data mining analyses with k-means. The exploitation in [10] and [12] are different than [11] by adoption of straightforward K-means method for cluster and priori formula as information connotation rubrics. Zubi conjointly works on data scrutiny hoping to determine trends or patterns, building associations, generating guesses, and possible enlightenments for drawing criminal paths and characteristic realistic respondents. They detailed auspicious remarks from their assumptions projected model as attributes for crime linked to K-means formula. The work [10] gave elaboration on the general applied math data regarding the criminal age versus crime kind which connected the inputs to the K-means approximations.

Earlier in 2014, Hosseinkhani [14] discussed web crime mining by means of clever data analysis techniques running evaluation for mining supportive info to seek-out crime hot spots that forecast lawbreaking or illegal data movements. The work, furthermore, assessed liberal styles for retrieving cooperative info via data mining innovations. In same pace, but a year before in 2013, Chitra [6] examined the info mining procedures and its applications focused on banking sectors. Chitra studied possible fraud recognition and interference, customer preservation, marketing and risk management. The research declared the obligation of data mining procedures as needed essential within the banking sectors for advanced targeting of current clients, Most well-intentioned users retention, automatic credit agreement that is employed for deception discovery and interference in real time, providing section based mostly merchandise, analysis of the shoppers, dealings patterns over time for higher relationship, risk management and selling, have all been investigated within

the work [6] differently than the general crimes data mining coverage of [11] and protecting medical records against cybercrimes of [15] as well as and educational technology security [16] and specific students systems protections of [1].

An intelligent analysis of crime data using data mining and auto correlation models was previously discussed by Mande in 2012. Their research put basic assortment for crime detection from governmental dataset collected by local state departments intended to spot illegal supported witness on crime spots. The old analysis [17] used binary accumulation practices to research the unlawful information aiming to map the wrong victimization approaches focused on automotive vehicle connection as well as the means of incident and their selections of corruption. Likewise, Patidar in [18] attempted to remove untruthful cluster action through neural network combined to genetic rule. Genetic algorithm in [18] showed possible methodology picks concerning topology, diversity of unseen layers, assortment of nodes, i.e. employed in the look of neural network, for downside of banking Mastercard fraud detection. For the artificial neural network training purpose, the research in [18] used supervised learning feed forward back propagation rule showing important remarks to be considered.

Lately in 2016, Agarwal [19] proposed analysis and prediction of crime notation using data mining frequent patterns with association elaboration analyzing varied misconducts approached by criminals. Agrawal projected the vision of every crime that may be performed later, linked to its history. This prediction has been very useful linking to attributes like cataloguing, schooling, profession, contact circle, personal background and other influences [1]. Agarwal enforced specific regulation for creating recurrent element sets. Interestingly, the work in [19] focused to associate nursing application that may be accessed and obtainable to the licensed users anytime and anyplace, alongside the most practicality of estimate of the more wrongdoings by separate criminals [19].

3 CYBER SECURITY ATTACKS ON BANKS

Banks square measure exposed to variety of cyber security attacks. run batted in in [7] identifies Phishing, Cross web site scripting, Vishing, Cyber-Squatting, larva networks, E-mail connected crimes, Malware, SMS spoofing, Denial of service attacks, Pharming, corporate executive threats because the rising data security attacks on banks.

3.1 Phishing

One of the foremost common cyber frauds is ―Phishing. Phishing is an attack during which an endeavor to get sensitive data of user like usernames, passwords, MasterCard details, etc. by an aggressor by deceit to be a reliable body in any transmission. Phishing is often disbursed by email spoofing or instant electronic messaging during which users are asked to click on a link usually for securing their accounts. The users are then directed to dishonorable web site that look alike the initial banking website in order that the user is deceived and is asked to enter his personal data like usernames, passwords, MasterCard details, etc. Once the user enters his/her personal data, the fraudster then has access to the customer's on-line checking account and to the funds contained therein account. There are a range of tools and techniques employed by phishers that serve a range of functions, as well as email delivery, phishing website hosting, and specialized malware. These tools embody Botnets, Phishing Kits, Abuse of name Service (DNS), Technical Deceit, Session Hijacking and specialized Malware [20].

3.2 Cross site scripting

Cross-site scripting (XSS) may be a quite cyber security vulnerability sometimes found in net applications and that they permit code injections by malicious net users into the net pages that are viewed by alternative users [7]. samples of such code embrace client-side scripts, HTML code, etc. A cross-site scripting vulnerability may be exploited by attackers to bypass access controls. Their impact ranges from a petty nuisance to a major security risk, reckoning on the sensitivity of the info that's handled by the vulnerable website and therefore the nature of any security mitigation enforced by the site's owner.

3.3 Vishing

Vishing could be a cyber-attack within which social engineering and voice science (VoIP) are accustomed access the personal and money info from the general public for obtaining money reward [7]. It combines "voice" and ―phishing‖. Vishing is associate degree felonious observe wherever associate degree aggressor calls a user associate degreed pretends to be from a bank within which the user has an account. He typically asks to verify the user's account info (stating that user's account has been suspended, etc.) and once the user offers his credentials like username, password, MasterCard variety, etc., the aggressor has easy accessibility to the user's account and therefore the cash in it. There has additionally been a thieving of payment card information of the shoppers of U.S. banks by numerous vishing attacks. In associate degree attack in 2014, customers of a midsize bank received SMS text messages that claimed their charge account credit was deactivated and asked users to produce the cardboard and PIN numbers to activate it.

3.4 Cyber Squatting

Cyber-squatting could be used as method within which a notable name is registered and so it's oversubscribed for a fortune. Cyber Squatters register domain names that are the same as common service providers' domains thus on attract their users and have the benefit of it. Some countries have specific laws against cyber-squatting that are on the far side the traditional rules of trademark law. For instance, the us has the U.S. Anticybers-quatting shopper Protection Act (ACPA) of 1999 that provides

protection against cybersquatting for people and additionally house owners of distinctive proprietary names [7].

3.5 Bot Networks (Botnet)

Bots square measure programs that infect a system to supply remote command and management access via a range of protocols, like communications protocol, instant electronic communication, and peer-to-peer protocols. many of bots beneath common management square measure ordinarily stated as a Botnet. Computers get related to botnets once unaware users transfer malware like a Trojan Horse‖ that is distributed as associate e-mail attachment. The systems that square measure infected square measure termed as - zombies‖. Illicit activities will be dole out with bots by the controller that embrace relays for causation spam and phishing emails, updates for existing malware, DDOS, etc. larva Networks produce distinctive issues for organizations as a result of they'll be upgraded terribly quickly remotely with new exploits, and this might facilitate attackers stop security efforts [8].

3.6 Malware

Malware may be a maliciously crafted computer code program that accesses and alters the pc system while not the consent of the user or owner. Malware includes viruses, Trojan horses, worms, etc. Malware will heavily influence the confidentiality, integrity and availableness of the banking industry. Malwares have the aptitude to compromise the data within the banking systems and should result in a loss of value millions to the bank. Malwares will target each the user's system and therefore the bank itself. e.g; Zeus [8].

3.7 Denial of Service (DOS) Attack

A DOS is Associate in Nursing attack within which a user or Associate in Nursing organization is prevented from accessing a resource on-line. whereas as in Distributed denial-of-service Attack (DDOS), a selected system is targeted by an oversized cluster of compromised systems (usually known as a Botnet) and create the services of the targeted system unavailable to its users. truly the targeted system is flooded with incoming messages that causes it to close upend so the system is unavailable to its users. Although DOS attacks don't sometimes lead to loss of data or security to a bank, it will price the bank an excellent deal of your time, cash and customers and might additionally destroy programming and files in affected laptop systems [8].

3.8 SMS Spoofing

It is a comparatively new technology that during which within which} a user receives a SMS message on phone which seems to be coming back from a legitimate bank. during this SMS the originating mobile range (Sender ID) is replaced by alphabetic text. Here a user is also fooled to offer his/her on-line credentials and his/her cash is also in danger of felony.

3.9 TCP/IP Spoofing

It is one in every of the foremost common styles of on-line camouflage. In science spoofing, outlaw access is tried on a system by causing associate email message to a victim that seems to return from a sure machine by spoofing‖ the machines' science address. science address spoofing could be a powerful technique because it will change associate assaulter to send packets to a network while not being blocked by a firewall. this can be as a result of sometimes firewalls filter packets supported sender's science address and that they would ordinarily strain any external science address. but victimization science spoofing, the attacker's information packet seems to return from legitimate science address (internal network) and so firewall is unable to intercept it. the most goal here is to get root access to the victim's server (here the banking system), permitting a backdoor entry path into the targeted systems [20].

3.10 Pharming

It is conjointly known as farming or DNS poisoning. during this attack whenever a user tries to access an internet site, he/ she's going to be redirected to a pretend web site. Pharming will be worn out 2 attainable means: one is by dynamical host's files on a victim's pc and different way is by exploiting vulnerability in DNS server computer code [8].

3.11 Insider Threats

With the rise within the use of data technology by banks, there's a high security risk to bank's knowledge by insiders or staff of banks WHO will disclose, modify or access the knowledge illicitly. conjointly unintentional errors by staff will have devastating results. sturdy security processes should be employed by banks to mitigate such threats [8].

4 SENSING E-BANKING CYBERCRIMES VULNERABILITIES MODEL

Discovering and exploring cybercrimes and inquisitor their affiliations with virtual criminals' square measure concerned in evaluating cybercrime progression. This planned work presents the model over cybercrime prediction with K-Means agglomeration technique, and classifiers. For the cybercrime prediction in e-banking activities, the planned model grants an increased prediction outcome. Influenced Associative Classifier affords a well-organized thanks to utilize the classification technique with Association Rule Mining, which boosts the prediction accuracy for classification. It conjointly employs the influenced support and confidence structure for dig out the Association rule from crime information [20].

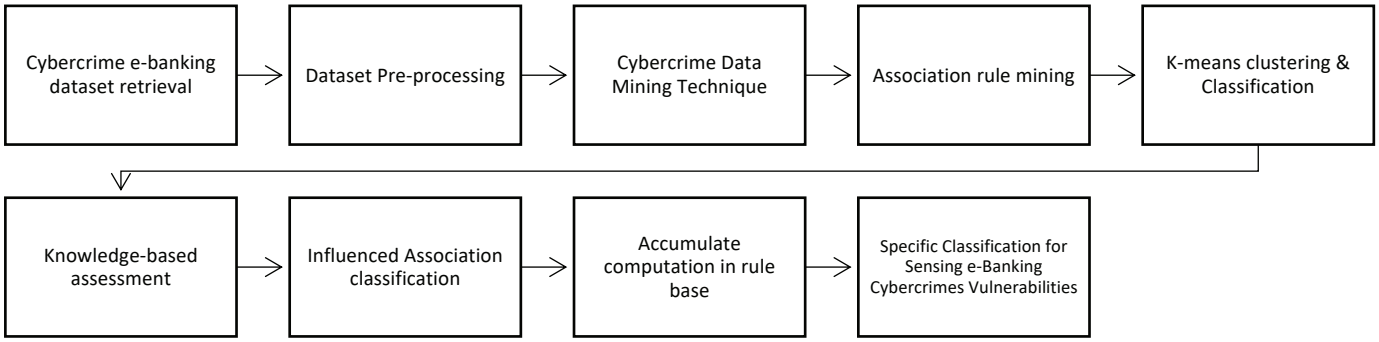

Fig. 1. Sensing e-Banking Cybercrimes Vulnerabilities Model

A. Collection of cybercrime dataset

A diversity of cybercrime knowledge has got to be collected for the prediction of cybercrime category in banking sector by the analysis of crime pattern. Thus, this knowledge has got to be collected from numerous news feeds, articles and blogs, department of local government websites over the net. The collected cybercrime knowledge is hold on in crime information for additional handling of knowledge.

B. Pre-processing of cybercrime dataset

The cybercrime dataset keep in Crime information must be preprocessed before applying data processing techniques on them. as a result of preprocessing removes screaky information, missing values etc.

For Pre-processed knowledge, data processing techniques and algorithms area unit enforced to spot or forecast fraud through data innovation from abnormal patterns and conjointly it achieves recognition in combating cyber credit-card fraud data processing aids by tributary in finding tribulations in banking sector by discovering patterns, relationships and links that area unit unseen within the business data accumulated within the crime databases.

4.1 Association Rule mining

Based on frequent occurrences of the crime patterns, Association rule mining produces rules for cybercrime dataset. These generated rules assist the assessment producer of defense society to require a hindrance action. The procedure includes the next measures [20]:

• The methodology of crucial ordinarily occurring item sets within the cybercrime info.

• The identification of patterns in program implementation and client behaviors as association rules referred to as intrusion recognition.

4.2 Clustering

Splitting from a collection of records or things to variety of teams is named cluster. cluster is implicit on discovering interactions linking cybercrime and criminal characteristics having some past mysterious general characteristics. for locating frauds in banking sectors, cluster techniques square measure used. cluster is phrased as unattended learning as a result of its categories don't seem to be definite and determined ongoing and association of information is thru exclusive of superintendence [21]. K-means partition rule is enforced in cluster cybercrime datasets thanks to its minimal art and fewer procedure elaboration. At first, the number of information things square measure assembled and precise as 'k' clusters. Between the mean distances of objects, the norm is meant. The positioning reiterative methodology is employed to recover the partitions by transferring things from one cluster to different. Then till the union happens, the quantity of iterations is disbursed.

4.3 Classification

Classification is that the most often used data processing technique, that executes a collection of pre-classified examples to make up a model which will classify the instances of attributes at Brobdingnagian scale. The classification technique creates subordinate association between variable related mapping of the information points inside the given dataset. Classification is employed to bring get into that cluster every information prevalence as to be fully associated [20]. Classification is used to form many models of unknown patterns and prospect assessment on the idea of the higher cognitive process. Automatic credit authorization is that the nearly major procedure within the banking sector and monetary organizations. Frauds will be prohibited by building a superior assessment for the credit consents victimization the classification illustration supported call trees like J48, CART etc.

4.4 Influenced Association Classification

For accomplishing a lot of preciseness, the associative classification is extraordinarily novel and improved technique that assimilates the mining of association rule and classifications of the model prediction. This technique is being enforced for ruling out the link and association over item sets. The associative category if action comes beneath unattended learning since it will have interaction of any class characteristic for rule extraction as two steps can be utilized to extract association rules area unit [20]:

through cybercrime knowledge set, categories generated to support the association rule.

within the category labels, perform analysis on the dataset classification.

The Influenced Association classification is entirely novel perception for rule categorization. It additionally intends weighted confidence and support structure for information mining association rules over the cybercrime knowledge set. Varied steps enforced in Influenced Association Classifier has been summarized below:

Initially, Pre-process the cybercrime dataset thus any mining practices may be achieved on them.

To duplicated the assessment within the replica of prediction, each component is assigned inside a variety of weight (0-1). Attributes having further significance are allotted most weight of (0.9) and having fewer significance are allotted minimum weight of (0.1), pretending to benefit from same philosophical approach of figure of merit study within expansion rules for more users accessing multimedia secret sharing [22] as well as AT figure of merit estimation within pipelined crypto models designing [23]. Influenced Association Rule Mining instruction is enforced on pre-processed cybercrime information set for getting fascinating pattern invention. Influenced Association Classification uses weighted support and confidence and therefore the rules spawned by this method are referred to as Classification Association Rule. The extracted Classification Association Rules are kept within the Rule base index.

At any time if any new cybercrime record is updated, this automotive rule forecast the category label from the Rule base.

4.5 Sensing Cybercrimes Vulnerabilities

For the classification of problems and issues within the cybercrime sensing analysis, prediction rule is a lot of high-pitched and precise, which is organized to be performed in 2 steps [20]:

Formation of tree.

Validate the engineered tree over the cybercrime information set.

5 EXPERIMENTS AND COMPARISONS

This work performed an overview comparative analysis of three standard classification techniques J48, Naïve theorem and zeroR to examine the preference [21]. We perform comparative analysis of these three techniques to ascertain effectivity factors that will provide better results of victimization real crime sensing information. The work used a machine learning package developed at university of Waikato in New Zealand, known as WEKA, for testing purposes. It is to be noted that WEKA is built for different intention but found very benefitable as open supply package freely downloaded from this information processing system address http://www.cs.waikato.ac.nz. It remarks accepts its information in ARFF (Attribute connected File Format) as algorithmic data processing utilized used platform [24].

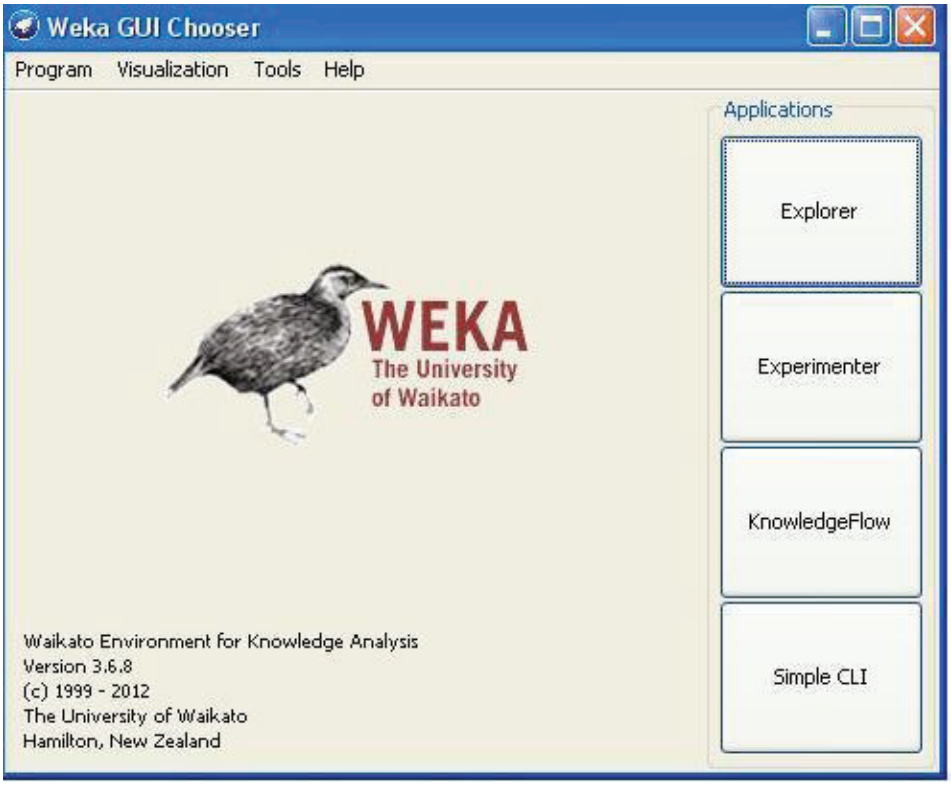

Fig. 2. WEKA Testing Interface

The research found different preferences offering the sorting procedures considering predictive analytics and many confusion matrices factors of processing delay, prediction accuracy, true positive rate, false positive rate, kappa coefficient, precision optimistic predictive value, and recall sensitivity offering options variety of wining methods. The work can be considered a clue to help in researching active information data sciences techniques dedicated for banking cybercrimes possible protection.

A. Decision tree algorithm J48

J48 classifier may be an easy C4.5 call tree for classification. It creates a binary tree from the choice tree approach, as known most helpful in classification downside [21]. With this J48 system, a tree is made to model the classification method applied to every tuple within the info data leading to classification for that tuple. While building the tree, J48 further ignores the missing values i.e. the worth for that item are often expected supported what's proverbial concerning the attribute values for the opposite records. The fundamental plan is to divide the information into vary supported attribute values for that item that square measure found within the coaching sample. In fact, J48 permits classification via either call trees or rules generated from them to get the results.

B. Naive Bayes classifier

The Naive Bayes formula could be an easy probabilistic classifier that calculates a collection of chances by reckoning the frequency and mixtures of values in an exceedingly given information set. The formula uses Bayes theorem and assumes all attributes to be freelance given the worth of the category variable. This conditional independence assumption seldom holds true in world applications, thence the characterization as Naïve, however the formula tends to perform well and learn quickly in numerous supervised classification issues, as detailed in [21].

C. ZeroR classifier

ZeroR is a classification technique that depend on the goal disregarding different predictors aiming to be simple. ZeroR strategy merely detects the mainstream sorting group loosing or avoiding other certainty influences. It is reported beneficial for defining a starting point (zero) performance level as a scale references for any further sorting approaches. In other words, ZeroR constructs a frequency table for the target and select its most frequent value [3].

5.1 Evaluation Metrics

The parameters thought of whereas evaluating the chosen classifiers are:

Accuracy: This shows the proportion of properly classified instances in every classification model [14]

Kappa: Measures the connection between classified instances and true categories. it always lies between [0, 1]. the worth of one suggests that excellent relationship whereas zero suggests that random shot [18].

TP Rate: is that the statistics that shows properly classified instances [14].

FP Rate: is that the report of instances incorrectly tagged as correct instances [14].

Recall: Measures the proportion of all relevant knowledge that was came by the classifier. A high recall suggests that the model returns most of the relevant knowledge [18].

Time: Delay time taken to perform the classification [14].

5.2 Datasets

A real crime knowledge collected from hand-picked prisons in Nigeria were used to perform this experiment. The dataset was reborn to Attribute connected File Format (ARFF) kind for straightforward process by rail. The dataset was divided into two: coaching set and check set. the previous was accustomed train the model whereas the alternative was used to check the designed model. A cross validation method was applied in dividing the dataset into coaching and check set. the method divides the info into equal elements typically and also the model was trained victimization [24].

Table 1 shows the tabulation of various results obtained from the three-classifier tested within this work. The study shows that the J48 classifier has higher accuracy of 59.15% whereas each Naïve theorem and ZeroR classifier has same slightly less accuracy of 56.78% each. The J48 running time took longer time than the rest of 0.76 seconds to make the model compare to 0.09 seconds for Naïve theorem and ZeorR classifier. The other metrics showed that J48 is preferable than both others making the recommendation to use it if the time constraint is not a problem. In other words, if time isn't the most dominant metric for analysis of the performance, the j48 classifier may be aforementioned to own higher performance than both Naïve theorem as well as ZeroR classifiers.

Evaluation Metrics	J48	Naive Bayes	ZeroR
Time	0.76 sec	0.09 sec	0.09 sec
Accuracy	59.15 %	56.78 %	56.78 %
TP Rate	0.591	0.568	0.568
FP Rate	0.456	0.496	0.568
Kappa	0.15	0.0813	0
Precision	0.51	0.478	0.322
Recall	0.591	0.568	0.568

Table 1 Comparison result

6. CONCLUSION

The dependency of banks on technology is increasing by time. Nowadays, Banks are facing an exponentially increasing privacy and security risk to their valuable assets. As result of that, the cyber-crimes related to banks is also increasing stupendously making its prediction and analysis of real-life essential need.

This paper presents samples of different cyber security attacks on banks. The work general idea is about utilizing active model of data mining techniques to relate between them and the incidents. The research performed a comparative analysis study of three standard classification techniques: J48, Naïve theorem and zeroR, to ascertain which one of them provided the preferred result as victimization real crime information. The work showed interesting remarks depending on the evaluation metric considered. In general, if time delay is not a concern, the classifier J48 is providing the best results, otherwise Naïve Bayes or ZeroR may show attractive features, i.e. based on the focused parameter influencing.

Although the research found different favorites offering the classification measures, considering predictive analytics and many confusion matrices factors, such as delay, prediction accuracy, true positive rate, false positive rate, kappa coefficient, precision value, and recall sensitivity, offering choices of recommendations, the work is used in sensing active information data sciences techniques dedicated for banking cybercrimes possible protection. The research is considered in its early stage though it is essential and important in todays' e-business life applicability.

For related future research, other models' concepts can be tested for cybercrime prediction, such as running data mining using K-Means as well as influenced association classification with prediction tree. The coming research can utilize weighted support and confidence measures to assess cybercrime datasets, statistical algorithm bunches the item sets. The Classification concert and precision can be enhanced with K-Means, Influenced Association Classification with Prediction tree J48. In the banking sectors, the clients have to be aided through precise requirements in the application software to discover alert while a stern interruption is recognized. Intrusion tools ought to be established wherever it is practicable and appraised on a standard basis. To scrap beside cyber-attacks, customer tutoring must be prepared in association with government and other confidential organizations. Awareness agenda as well as verifying correct usage should be put into practice to guarantee that clients.

Acknowledgment

Thanks to Umm Al-Qura University for motivating this research.

Ethical approval:

This article does not contain any studies with human participants or animals performed by any of the authors.

Informed consent:

Informed consent was obtained from all individual participants included in the study.

Conflict of Interest:

The authors declare that they have no conflict of interest.

REFERENCES

[1] Almutairi S., Gutub A., Al-Ghamdi M. (2019) Image Steganography to Facilitate Online Students Account System. Review of Business and Technology Research (RBTR) 16(2):43-49.

[2] Farooqi N., Gutub A., Khozium M.O. (2019) Smart Community Challenges: Enabling IoT/M2M Technology Case Study. Life Science Journal 16(7):11-17.

[3] Prasanthi M., Ishwarya, T. (2015) Cyber Crime Prevention & Detection. International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE) 4(3):45-48.

[4] Alassaf N., Gutub A., Parah S., AlGhamdi M. (2019) Enhancing Speed of SIMON: A Light-Weight-Cryptographic Algorithm for IoT Applications. Multimedia Tools and Applications 78:32633-32657.

[5] Gutub A., Al-Juaid N., Khan E. (2019) Counting-Based Secret Sharing Technique for Multimedia Applications. Multimedia Tools and Applications 78:5591-5619.

[6] Chitra K., Subhashini B. (2013) Data mining Techniques and its Applications in Banking Sector. International Journal of Emerging Technology and Advanced Engineering (IJETAE) 3(8):219-226.

[7] Gopalakrishna G. (2011) Report of the Working Group on information security, electronic banking, technology risk management, and tackling cyber frauds. RBI, Mumbai, Maharashtra.

[8] Ahmad M., Rosalim R., Beng L., Fun T. (2010) Security issues on Banking Systems. International Journal of Computer Science and Information Technologies 1(4):268-272.

[9] Dubhey N., Chaturvedi S., (2014) A Survey of Crime Prediction Technique using Data mining. Int. Journal of Engineering Research and Applications (IJERA) 4(3):396-400.

[10] Zubi Z., Mahmmud A. (2014) Crime Data Analysis using Data mining Techniques to Improve Crimes Prevention. International Journal of Computers 8:39-45.

[11] Kiani R., Mahdavi S., Keshavarzi A. (2015) Analysis and Prediction of Crimes by Clustering and Classification. International Journal of Advanced Research in Artificial Intelligence (IJARAI) 4(8):11-17.

[12] Sonaqwanev T., Shaikh S., Shaikh, S., Shinde R., Sayyad, A. (2015) Crime Pattern Analysis, Visualization and Prediction using Data Mining. International Journal of Advance Research and Innovative Ideas in Education (IJARIIE) 1(4):681-686.

[13] McClenden L., Meghanathan N. (2015) Using Machine Learning Algorithms to Analyze Crime Data. Machine Learning and Applications: An International Journal (MLAIJ) 2(1):1-12.
[14] Hosseinkhani J., Ibrahim S., Chuprat S., Naniz J. (2014) Web Crime mining by means of Data mining Techniques. Research Journal of Applied Sciences, Engineering and Technology 7(10):2027-2032.
[15] Samkari H., Gutub A. (2019) Protecting Medical Records against Cybercrimes within Hajj Period by 3-layer Security", Recent Trends in Information Technology and Its Application 2(3):1–21.
[16] Almutairi S., Gutub A., Al-Juaid N. (2020) Motivating Teachers to Use Information Technology in Educational Process within Saudi Arabia. International Journal of Technology Enhanced Learning (IJTEL) 12(2):200-217.
[17] Mande U., Srinivas Y., Murthy J. (2012) An Intelligent Analysis of Crime Data using Data mining & Auto Correlation Models. International Journal of Engineering Research and Applications (IJERA) 2(4):149-153.
[18] Patidar R., Sharma L. (2011) Credit card Fraud Detection using Neural Network. International Journal of Soft Computing and Engineering (IJSCE) 1:32-38.
[19] Agarwal A., Chougule D., Agarwal A., Chimote D. (2016) Application for Analysis and Prediction of Crime data using Data mining. IRF-EEEforum International Conference, India, pp. 35-38.
[20] Lekha K., Prakasam M. (2017) Data mining Techniques in detecting and predicting Cyber crimes in Banking sector. International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS).
[21] Patil T., Sherekar S. (2013) Performance Analysis of Naive Bayes and J48 Classification Algorithm for Data Classification. International Journal of Computer Science and Applications 6(2):256-261.
[22] Gutub A., Alkhodaidi T. (2020) Smart Expansion of Target Key for More Handlers to Access Multimedia Counting-Based Secret Sharing. Multimedia Tools and Applications, in press http://doi.org/10.1007/s11042-020-08695-y
[23] Gutub A. (2006) Merging GF(p) Elliptic Curve Point Adding and Doubling on Pipelined VLSI Cryptographic ASIC Architecture. International Journal of Computer Science and Network Security (IJCSNS) 6(3A):44-52.
[24] Obuandike N., Isah A., Alhasan J. (2015) Analytical Study of Some Selected Classification Algorithms in WEKA Using Real Crime Data. International Journal of Advanced Research in Artificial Intelligence (IJARAI) 4(12):44-48.