Designing Predictive Models for Cybercrime Investigation in Iraq

Mohammed Mahmood Abdullah[1]*
AlNoor University College

Ahmed H.[2]
Al-Farahidi University

Ayad Abas Hasan[3]
The Islamic university in Najaf

Dhafar Basim Ali[4]
Al-Mustaqbal University College

Mohammed Kadhim Abbas Al-Maeeni[5]
Al-Nisour University College

Salah Hasan Gdheeb[6]
Mazaya University College

Salem Dawood Salman[7]
Ashur University College

Abstract
Cyber threats have increased in Iraq with the introduction of new technologies. This study aimed to investigate the cyber security measures currently in place in Iraq and understand how predictive models can be adopted to investigate cybercrimes in Iraq. The study used a descriptive and explorative approach, with Literature review and documentation research as main data collection instruments. In a meta-review of past studies, the cybersecurity risks prevalent in Iraq were identified and explored whether predictive models can be used to eliminate cybercrimes. The study analyzed how predictive analytics proved a potential security application and assisted the law

[1] Department of Law, AlNoor University College, Bartella, Iraq.
Email: mohammed.m@alnoor.edu.iq
[2] college of Law, Al-Farahidi University / Iraq.
[3] College of media / The Islamic university in Najaf, Iraq.
[4] English Language and Literature Department, Al-Mustaqbal University College, Babylon, Iraq.
[5] Al-Nisour University College, Baghdad, Iraq.
[6] Mazaya University College / Iraq.
[7] Department of pharmacy / Ashur University College / Baghdad / Iraq.

enforcement agencies to cope up with cybercrimes against national security. While the study also encountered the frailty and vulnerability of cybersecurity in Iraq, it identified the benefits of Predictive AI models. The study concluded that Iraq needs an early warning system that can address to the cybercrime issues, reduce vulnerabilities, disseminate general cybersecurity best practices. The Iraqi government can also enact new cyber security laws and comply with the national and international norms. The study implies that predictive analytics models can best suit the needs of Iraq. It has been note significantly that each PA model is strong enough to optimize itself according to the required needs.

Keywords: Predictive analytics, Iraq, models, cybercrime, cyber security, law enforcement

Introduction

The science of predictive analytics (PA) in cybersecurity has a great potential and has surpassed all types of traditional solutions. PA helps businesses and security teams to stay ahead proactively and identify beforehand the emerging cyber threats through identified indicators like malware, phishing attacks and hacking. It also allows organizations to assess the likelihood of cyberattacks based on the past data. The security teams can visualize real-time insights into learn in advance about the potential risks and threats to their data security. The PA can also detect patterns of cybercrimes and make precise predictions by extrapolating forward in time and determine a likely outcome. As soon as the host organization becomes aware of future threats, immediate preventive actions are taken, often without human intervention through online measures. Such a potential to predict a crime with precision is made possible by artificial Intelligence(AI) and Machine Learning (ML) principles, which is missing in most other crime detection systems (Alhayani et al., 2021).

When current and past data merge together, data trends create a predictive model which helps to determine future events. This is called Predictive modeling, a type of data analytics that helps to forecast potential events that could take place in the future. This type of predictive modelling was first introduced in the banking sector to predict online frauds and detect identities based on the past data. Later, security personnel examined its potential to help mitigate cyberattacks. Predictive analytics is AI-enabled and is built with Machine Learning and Deep learning algorithms. Such AI enabled (predictive) models thus need technology to help businesses stay safe (Al Duhaidahawi et al., 2020; Harjan, Thabit, & Faaeq, 2015).

With the growth of technology, Predictive Analytics (PA) has a vast potential in cybersecurity. It is capable to catch a data breach before it actually takes place. When it comes to cybercrimes, it adopts statistical algorithms to determine future performance. Prior to the use of PA, a conventional approach was used to fight cybercrimes, which depended upon figuring out the origin of malware, causes of data breaches, phishing campaigns, and extracting information signatures, or information clusters that helped to identify a cybercriminal's attempt to exploit an operating system or its vulnerability (Nehme, 2020). Such a conventional method was used after a breach or a cybercrime had taken place and investigation was required. However, PA is now equipped with such analytical patterns that can raise a red flag if a cybercriminal attempts to penetrate into the security system.

In the current scenario, there is a great variety and volume of data, it might not be possible to prevent every data breach, but it is possible to minimize the risk. In other words, it is not possible to stop a determined hacker from getting into a system but it is possible to build a security wall to sustain the cyber-attack. Thus data breaches and cybercrimes are unavoidable but PA can minimize the risk. The risk mitigation is made much easier by using predictive analytics in cybersecurity. Predictive analytics can thus be used as an added form of security to sustain any kind of cyberattacks which though may be having fewer security measures at hand (Addae et al., 2019). Predictive analytics acts as a powerful to establish a security posture for the organizations. When it comes to risk mitigation, it is important that the predictive models should be accurate, otherwise, if the data is inaccurate or the user's behavior is biased, it could result in inaccurate models, which may not that overstate or understate risk and might result in a security breach (Sukhija et al., 2019).

In Iraq, new threats have emerged with the introduction of new technologies (Alem Al-Deen, 2019; Grimes, 2020; Kudhair & Shihab, 2018; Shires, 2022). It is therefore essential to focus on cyber investigation and cyber security measures currently in place in Iraq. This study attempted a descriptive and explorative study of the current state of cybersecurity in Iraq and how predictive models can be adopted to investigate cybercrimes in Iraq. Iraq is a land which sees cybersecurity also as a part of national security. Hence, this study first investigated what are the cybersecurity risks prevalent in Iraq; next, it attempted how predictive models can be used to eliminate this great danger to Iraq's national security (Shihan & Radif, 2022). The study analyzed how predictive analytics proved a potential security application and assisted the law enforcement agencies to cope up with cybercrimes most precisely. The rest of the paper has a literature review presenting theoretical views on predictive modelling, types of predictive analytics models, predictive algorithms, specific predictive models used in cybercrime investigation and cyber security situation in Iraq (Yeboah-Ofori et al., 2021). This is followed by sections on, problem statement, research methodology, results, findings and discussions.

Literature Review

- *What is Predictive Modelling: Some examples of Models*

Predictive modeling is more popular as a statistical technique that requires machine learning and data algorithms to predict and forecast likely future outcomes with the help of historical and existing data (Addae et al., 2019; Prabowo & Sinaga, 2021; Schutte, Breetzke, & Edlstein, 2021). The current and historical data are applied by selecting a model suitable to forecast likely outcomes. Such a predictive model is flexible and cannot remain fixed since it is necessary to incorporate changes in the data for the purpose of continuous validation. Other features of predictive models include their speed in computing and making projections (used in banks for calculating risks on online mortgage or credit card application); complexity such as those used in computational biology and quantum computing; and investigative and analytical, such as those used in crime investigations (Jakštaitė-Confortola, 2021; Petrenko & Makoveichuk, 2020; Suhendi & Asmadi, 2022).

Major predictive analytics models are of five types: Classification model, clustering model, Forecast model, Outliers model, and Time series model.

(a) Classification model: Being the simplest model, classification model categorizes data based on query responses. Most queries presented in this model are simple and direct, with closed yes- no type questions. This model helps in making a broad analysis prior to taking a decision.
(b) Clustering model: As the name implies, this model nests data on their common attributes. It prepares clusters of things and people having similar attributes, characteristics or behaviors, and plans decision and analytical strategies for each.
(c) Forecast model: it is the most common and popular model, as it works on any current or historical data with a numerical value. The forecast model makes use of metric and numerical values form historical data for predictions and making estimations about future.
(d) Outliers model: This model is unique model as it works only when it is required to analyze abnormal or outlying data, particularly when an individual or a group behaves abnormally. The outliers model looks for anomalous data entries within a dataset, and analyzes whether the anomaly is individual or combined with other numbers and categories.
(e) Time series model: This model evaluates a sequence of data points based on a time series. It measures and compares single numerical values of data over a span of time and predicts for the next few weeks of data based on that metric.

- *Common Predictive Algorithms*

An algorithm is a process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer (Petrenko & Makoveichuk, 2020). A predictive algorithm primarily uses two subsets of Artificial intelligence operations, machine learning and deep learning. Machine learning, which comprises both linear and nonlinear varieties (Alhayani et al., 2021), uses structured data presented in spreadsheet or machine data in tabular forms. while Deep learning (DL) requires unstructured data such as videos, audios, texts, and social media posts and images (Salih et al., 2021). Based on these two subsets of AI, common predictive algorithms include Random Forest (RF) Generalized Linear Model (GLM), Gradient Boosted Model (GBM), K-Means, and Prophet:

(a) Random Forest (RF)

The RF algorithm is called so as it is derived from a random combination of decision trees. Due to their random selection, none are related, can use both classification and regression data in large volumes. The value of each random vector is sampled independently with the same ratio for all decision trees. The algorithm uses the "boosting" technique to ensure least error possible. The RF model has advantages like: it can accurately and efficiently run on large databases; it is unbiased because there are multiple variables; it resists any kind of overfitting of variables; it is capable to handle thousands of input variables and easily classifying the important ones; and it can also provide accurate estimation for the missing data.

(b) Generalized Linear Model (GLM)

The GLM is a complex method to narrow down the best fit model from a wide array of continuous variables. The linear regression allows categorical predictors to

interpret and analyze how variables can influence the outcome, making the prediction easier. The advantage of GLM algorithm includes: it can work on relatively large data sets; it is susceptible to outliers; it is fast and speedy.

(c) Gradient Boosted Model (GBM)

The GBM builds a prediction model comprising a group of decision trees (both weak and strong) without generalizing the data. As the name implies, the model uses a "boosted" machine learning technique, different from bagging used in RF model. Its advantages include: it is a classification model which individualizes decisions; it is distinguished type as it builds its decision trees one at a time; each new tree is trained to correct errors made by the previously trained tree; its data is more expressive; and since it builds each tree individually and sequentially, it takes longer time, but its slow performance leads to better generalization.

(d) K-Means

K-Means is the most-used, highly popular and a high-speed algorithm, which classifies data by similarities and therefore often also called a clustering model. It can quickly retrieve personalized details of individuals within a huge group, based on similarities. The advantages of this model includes: it can figure out common characteristics of individuals and groups from large data set; it helps in designing a personalized plan; it can place an individual in separate clusters at the same time; and it can proactively recommend and predict a solution.

(e) Prophet

The Prophet algorithm, mostly used in capacity forecasting, allocating resources and setting goals, is a time series forecast model. It is an open-source algorithm, which even works automatically and with flexibility when applied in inconsistently performing data. Its advantages include: it is flexible and automatic; it can accommodate heuristics amidst numerous arrays of assumptions; it is speedy, reliable and robust when it works on messy data; it always offers alternatives that aids in decision making

- *Predictive Model for cybercrime investigation*

When used in cybercrime investigation and assessing cyber security of a nation or region, various statistical models are operative and applicable. Some major predictive models used include Markov Chain Monte Carlo (MCMC), Hyper-Parameter Optimization, and Sensitivity analysis.

(a) Markov Chain Monte Carlo (MCMC)

MCMC is a statistical method that estimates the probability of a future event given the probability of another event. This is carried out by planning multiple simulations for the best prediction about the future. The MCMC is very effective in analyzing large data sets where the small sample size does not represent the data population. Additionally, it also has the ability to handle missing data, creating a situation of "good fit" for cybersecurity.

(b) Hyper-Parameter Optimization (HPO)

The HPO model helps organizations to optimize security parameters based on data. The objective is to make predictions accurate and precise. Foer example, a user can be trained to click links only in particular scenarios and also to predict what should happen on each click, what websites would open and what would be the consequences.

(c) Sensitivity analysis (SA)

The SA model determines the extent to which an event will affect the revenue of an organization. The model helps in calculating the expected and potential revenue losses and suggest the risk tolerance and risk mitigation techniques. This model also can adjust the predictions in the event of a threat to the business revenue. This model is most challenging to the cybersecurity teams, as it accounts for variables that are not obvious to analysts.

- *Predictive Analytics and Cyber security situation in Iraq*

Iraq is one of those nations that are facing great challenges of cyber security owing to their large presence in the cyberspace, as evident from a large number of electronic gadgets, mobile phones, computers, tablets and over dependence on the Internet (40 million lines, with a telephone density of 107.7 per 100 inhabitants, the number of mobile Internet service lines (19.2) million. In addition, the cybersecurity issues aggravated in Iraq due to laxity shown by the Iraqi government in formulating electronic governance regulations, or establishing a coordination between Iraqi ministries of information communication technologies with judiciary and other decision making bodies. It was evident that they did not realize the importance of cyberspace nor that it could be a threat to the sovereignty of the state.

Predictive analytics (PA) can help Iraqi organizations combat cyberattacks by creating indicators of malicious behavior. For example, if an organization detects a high volume of user logins from a particular region, PA can create a model to predict if users' behavior could lead to some kind of malicious activity, how much time it would take for that activity to happen, and also predicting different outcomes. When Iraqi security agencies have the information in advance when an attack might happen, they can prepare to face it as well as create awareness about the threat, and what action is necessary to take.

In 2018, for the first time, the Digital Center in Iraq recognized the penetration of cyber criminals in Iraq and warned that most websites of official government ministries and institutions were not secure and can be easily hacked. In the field of cybersecurity, the vulnerability level of Iraq rose to 107 in 2018 from 158 in 2017 (internationally). In the Arab countries, its vulnerability rose from 19 in 2017 to the rank of 13th in 2018 (Ali & Manickam, 2018). The rise in the vulnerability rank should be seen as a surprise since Iraq had already fought a fateful battle against terrorism which was using cyberspace in its war against Iraq (Cordesman & Khazai, 2014). Iraq was therefore supposed to have all the cybersecurity tools, improved cybersecurity plans and strategies. Yet, Iraq failed to address to the cybersecurity issues and expose its failure to cope up with the cyber risks.

Problem Statement

Several studies have taken initiatives in cybercrime investigations (define, investigate andprosecute cybercrime (Bassett, Bass, & O'Brien, 2006; Cangemi, 2004; Huey & Rosenberg, 2004; Lu et al., 2006; Passas & Vlassis, 2007; Pocar, 2004) but most of these studies are limited to definition of cybercrimes (Pocar, 2004), or determining juris dictional issues and addressing the responsibilities of investigations, (Passas & Vlassis, 2007; Pocar, 2004), and collection of evidence (Bassett et al., 2006; Huey & Rosenberg, 2004). None of these studies has attempted to study the predictive models and their use in the cybercrime investigations in the Iraqi context. No study has attempted to detect cybercrime patterns and evolve prevention strategies prior to investigationand prosecution in Iraq. Hence, there exists a wide research gap in the Iraqi context as far as predictive modeling is concerned.

Recently, cybersecurity in Iraq is facing greater challenges due to the rapid prevalence of internet and communication network system. People have an uninterrupted access to the internet in Iraq. Cases of cybercrime in Iraq are on rise, including Internet cheating, hacking websites, unauthorized online access, cyber piracy, malware and cyber terrorism. Aboud (2012, 2014) shares the records of years between 2006-2011, held by Iraqi Criminal Investigation Bureau, where cybercrime cases were shown increasing at an average yearly rate of 246.2%. In April 2017, in order to prove the vulnerability of the cyber security system, an Iraqi activist hacked the official website of the Iraqi National Security Service, and posted a message criticizing the security system. Though the activist was arrested soon after the breach into security, but several other hackers followed the same course, hacked different websites and posted similar messages, demanding the release of the activist.

Another example which exposes the frailty and vulnerability of cybersecurity in Iraq is its fall in the Global Cyber Security Index (GCI) ranking to 107 in 2018, from 158 in 2017, and down to 13th among Arab countries in the year 2018 from 19 in 2017 (24). The rise in the vulnerability rank should be seen as a surprise since Iraq had already fought a fateful battle against terrorism which was using cyberspace in its war against Iraq. Iraq was therefore supposed to have all the cybersecurity tools, improved cybersecurity plans and strategies. Yet, Iraq failed to address to the cybersecurity issues and exposed its failure in coping up with the cyber risks.

These incidents are signs of warning. The Iraqi government must take initiatives to combat such cybercrime by strengthening its security services and a protective legislation. If the cybersecurity is strong, it can also mitigate larger cybercrimes like the cyber espionage, cyberterrorism and cyberwarfare. There is yet another matter of great concern that Iraq lacks qualified and experienced computer and network security professionals as well as cyber-law legislation professionals. The country also lacks appropriate cyber infrastructure and has failed to establish a centralized cybersecurity monitoring system, to protect the people's "right to personal privacy", which the Iraqi Constitution of 2005 had guaranteed to all its citizens. Even Iraq has failed to enact a robust data protection legislation and privacy protection under the Civil or Criminal Code. Hence there is need to examine how such AI assisted predictive analytics models can help to cope up with the cybercrimes.

Methodology

This study employed the Literature review and documentation research as the main data collection instrument. Literature review has emerged as a popular means of academic research. Jesson and Lacey (2006) assert that critical literature reviews enhance the academic community's knowledge about previous research, particularly those which are systematic or meta-analytical reviews with a scientific approach On the contrary, general literature reviews are narrated through short summary statements (Jesson & Lacey, 2006). The current study adopted the methodology of critical literature review to develop insights about previous research and to collect scientific information about the topic under view. Snyder (2019) observes that a critical literature review always has a purpose and an objective, particularly the objective of assessing, critiquing, and synthesizing the relevant literature. In some cases, literature review also helps in framing new theoretical frameworks and perspectives

Cybercrime data is obtained from crime investigations and reports, and is available in a wide range of formats. Much of it is available over periods of time. The quality of the data is varied, often with large pieces missing. This has given impetus to data mining techniques that can deal with time-series data, in different formats, and of varied quality. Researchers have thus examined issues related to the tools that can be used for different types of crime data (Chen et al., 2004) and the manner in which data can be aggregated for analysis (Ritschard et al., 2008).

Results and Discussion

Cybersecurity can best be understood by knowing more about Artificial intelligence (AI). In its evolution, AI witnessed three phases called evolutionary waves: The first wave was based on codes written by programmers wherein the collected data was distributed with historical baselines. This wave used primitive methods to detect anomalies and was comparatively very slow as it took months to create baselines, which also caused many inaccuracies. The second wave was more advanced than the first as the unsupervised and supervised machines were being used that could create their own rules through statistical methods, which made predictions possible however, this phase could not detect anomalies without network access or during network changes. The third wave of AI evolution demonstrated self-learning capabilities to derive own conclusions from new observations. It is also known as Predictive Artificial Intelligence (PAI), which is utilized to generate most advanced types of cybersecurity solutions. The AI system in this phase is self-supervised and its analysis can be applicable even in rapidly-changing situations. A close study of the archives resulted in two broad data fields: one, the uses and benefits of PAI models and second, classification of predictive models aiming to harness the cybercrimes and online frauds.

- *Use and benefits of Predictive Artificial Intelligence*

There are various benefits of Predictive Artificial Intelligence (PAI) that need to be mentioned in the context of the Iraqi security system, as most of these benefits can be applied in Iraq. First and foremost, PAI enables Automotive Threat Monitoring in a network very effectively, despite the presence of unstructured data. When the data is

automated and threats are monitored predictively for their occurrence, there is a least possibility of human errors, besides being more cost-effective than doing the same task manually. Additionally, the automatic and effective monitoring system facilitates a company's risk management and reduces the possibility of cyber-attacks and ransomware attacks. Predictive artificial intelligence can also make available high volumes of gathered data in order to reach rational decisions in the event of impending threats. It can make accessible greater data-anchored choices and valuable cybersecurity solutions that can effectively help in making strategic decisions and preventing data breaches. With the help of AI algorithms, it is possible to devise consistent preventive techniques for data and revenue security. According to IBM's 2021 report, a data breach can be due to compromised credentials, business email compromise (BEC), phishing, social engineering, and malicious insiders and it can cost a company around $4.24 million.

One of the benefits of using Predictive AI models is the efficiency and dexterity by which cyber security models work in sensing the risk and quickly initiating the prediction and preventive process with their restrictive algorithms. These algorithms make the cyber security system highly-efficient, as they are equipped with predictive self-learning capacities which enable the security system to identify anomalies and assess the current risks as well as predict future risks. One of the numerous benefits, the most significant and effective is the Predictive Analytics platform (See Figure 1) recommended as an efficient and effective fraud detection solution. This Predictive Analytics Platform comprises batch data and real-time analytics, both assisting the predictive analytics platform to carry out various transaction from its domain knowledge such as detecting fraud, utilizing predictive models and data clustering through an interactive dashboard used for data querying and visualizations.

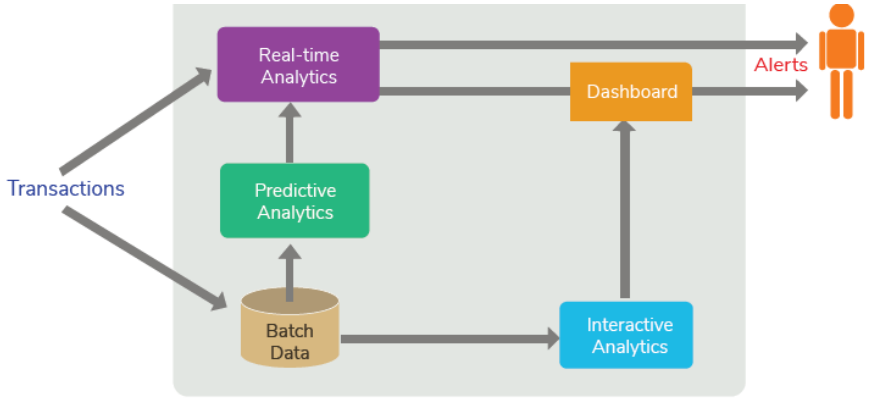

Figure 1 Application of the Markov Model carried out through real-time analytics engine,

Figure 1 depicts the application of the Markov Model through transactions carried out through real-time analytics engine, while the data in each batch is seen being used by Predictive Analytics to create data clusters to be used as operators. In this model, the feature of Interactive Analytics provides meaningful visualizations as a response to the alerts generated by the real-time analytics rules.

There are many predictive analytics techniques that can be used to understand, investigate and counter cyber threats. These techniques relate their 'abnormal' or 'fraudulent' behavior with a machine algorithm, which help an individual to self-learn and self-adjust the most legitimate and fraudulent activity patterns in real time. A major technique is known as Markov modelling. Markov models are stochastic models that randomly model the changes in the systems. These models assume that future states depend only on the present state and not on the sequence of events that preceded it. A three step process is required to build a Markov model to detect any cybercrime, namely State Classification, Probability Calculation, and Metric Comparison.

The first step of state classification classifies each event based on the qualities of the event such as the low, normal or high risk, or time and duration between crimes committed, etc. the second step of probability calculation requires a further classification of each crime event or transaction into transition probabilities. The final step of metric comparison first prepares a sequence of all transactions in real time, and then metrics based on transition probabilities of that sequence are compared with the probable cybercrimes or cyber frauds. These three steps are taken in a single sequence until a remedy is found.

Machine Learning algorithms are adopted to understand the 'normal' behavior of events and detect deviations from the modelled 'normal' behavior in real time data. Such a model is unsupervised since the classification algorithm is embedded with the quality to detect the fraudulent events from the legitimate ones. However, due to a very big disparity in the ratio between the fraudulent data and legitimate data, most classification algorithms fail to detect the anomaly. In such a case, 'clustering' mechanisms are used which model the 'normal' behavior as clusters, and anomalies (fraud) as deviations from those clusters. Figure 2 presents examples of clustering algorithm, wherein clusters hold normal or legitimate events. Any incoming event entering into these clusters from outside is flagged as anomalous or fraudulent while any preexisting activity within the cluster would be considered as legitimate. The cybercriminal, a hacker or a fraudster., cannot have access to any of these clusters since they will not be able to decode the detection mechanisms, which is complex due to the combination of historical and real time data. Besides, each cluster is capable of self-learning and can adjust according to both legitimate and fraudulent activity trends (Figure 2).

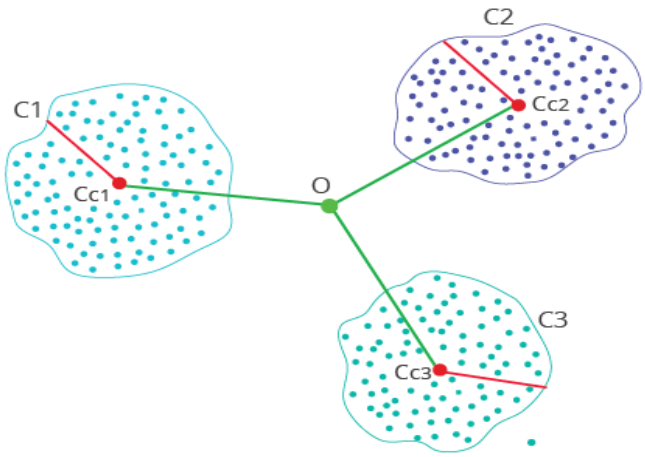

Figure 2: Examples of clustering algorithms

A great concern has been shown by the Digital Center in Iraq over the penetration of cybercriminals in the cyberspace of Iraq, which is demonstrated in frequent hacking and intercepting incidents of the websites of official government ministries and trading organizations in Iraq (Al-Awadi, 2016). This concern was also seen at the international level, when Iraq's Global Cyber Security Index (GCI) ranking fell down to 107 in 2018, from 158 in 2017, down to 13th among Arab countries in the year 2018 from 19 in 2017 (Al-Awadi, 2016). This was seen as a result of poor coordination between the Iraqi Ministry of Communications and other ministries and the judiciary, which made the Iraqi cyberspace vulnerable to cybercrimes. The fall in the ranking came as a surprise since Iraq was already equipped with all types of cybersecurity tools that it had used to fight with the terrorist organizations in the recent past.

Cyber analysts, therefore, have felt that Iraq needed to strengthen its cybersecurity plans and programs, create stronger pillars of cyber security and build legal measures related to cybersecurity. Additionally, Iraq also needs to deal with technical and organizational aspects, capacity building, training and coordination, and establish an institution specialized in cybersecurity in Iraq. Currently, the cybersecurity related issues in Iraq are addressed by small departments and ministries at local level, which lack coordination and professional cooperation (Al-Awadi, 2016).

Analysts also recommend that since Iraq is equipped with sufficient financial and scientific resources, it should work fast toward a renaissance of its cyber security. The National Security Adviser in Iraq although initiated a cybersecurity strategy, as found on the Internet, but it has several drawbacks. First, every strategy targets a specific period, restricting it to a fixed time interval, and invalidating it after the expiry of that period. Secondly, the context of every strategy is ambiguously theoretical and formal, suggesting that the authors of these strategies lacked awareness about the Arab scenario and what relevant solutions are required to achieve cybersecurity in Iraq. Moreover, the cybersecurity scenario in Iraq is different as it depends more on data science training and education, implementation of data-driven projects, and demonstration and communication of the results in the public domain. A good example can be cited of iDATA (Iraqi Data Analysis to Action), a non-profit initiative that works towards continuous activation of data and collecting data enthusiasts across whole Iraq. The iDATA works towards finding the right data or guiding how to procure the data. It is not business oriented nor it has any commercial or profit making agenda. Its main goal is to equip the Iraqi young graduates with data analytics skills, making them useful in technical fields. Such initiatives also raised awareness about the significance of data and building analytical mindsets for effective decision-making.

Conclusion

Though cyber security is not an easy process, and more than the technical resources, trained team, infrastructure and a robust network, it also needs the necessary political will, a political strategy, and a governance comprising digital infrastructure, cybersecurity management personnel and a full-fledged supreme body or a council dedicated to cybersecurity, directly linked to the Council of Ministers, which should be empowered to take decisions in multidisciplinary directions with ready solutions. Iraq has a functional Iraqi Cyber Incident Response Team (CERT), a body that should take charge of cyberspace in Iraq, and protect it

from any breach and provide the necessary support. The CERT however needs empowerment including the right to monitor and analyze any dubious activity outside the context, investigate any kind of cyber risks and vulnerabilities and disseminate information related to cyber hazards, with a view to educate and alert the Iraqi citizens, stakeholders, Internet users and government departments.

However, all traditional security efforts in Iraq have failed as there is an increased vulnerability caused by the unrestrictive use of the Internet and cyberspace. What Iraq needs is an early warning system that can address to the cybercrime issues, reducing vulnerabilities and potential problems, disseminating general cybersecurity best practices and guidelines for incident response and prevention (Al-Awadi, 2016). Iraq also needs to optimize its technical resources allocation decisions and ensure the protection of its key corporate assets against cybercriminals. Moreover, cybersecurity is closely related to Iraq's national security, and any security breach may destroy its infrastructure and expose it to risks.

It is therefore necessary to enact new cyber security laws to highlight the Iraqi cyber legal status internationally and make amendments in the existing laws like Telecommunications and Information Security Law and the Privacy Act. Iraq needs to develop a defense mechanism and a security network in the cyber security domain. This defense system must have the feature of predictability about future when it comes to cybercrimes and identifying beforehand security gaps in the network. This study attempted to determine how predictive analytics models can best suit these needs of Iraq. It has been note significantly that each PA model is strong enough to optimize itself according to the required needs.

References

Aboud, S. J. (2012). An overview of cybercrime in Iraq. *The Research Bulletin of Jordan ACM, 2*(2), 31-34. https://www.researchgate.net/publication/261876935

Aboud, S. J. (2014). Cybercrime in Iraq. *International Journal of Scientific & Engineering Research, 5*(3), 422-425. https://www.ijser.org/paper/Cybercrime-in-Iraq.html

Addae, J. H., Sun, X., Towey, D., & Radenkovic, M. (2019). Exploring user behavioral data for adaptive cybersecurity. *User Modeling and User-Adapted Interaction, 29*(3), 701-750. https://doi.org/10.1007/s11257-019-09236-5

Al-Awadi, A. M. G. (2016). Cyber Information. *Security, Series of Publications, Al-Bayan Center for Studies and Planning*, 30-31.

Al Duhaidahawi, H. M. K., Zhang, J., Abdulreza, M. S., Sebai, M., & Harjan, S. A. (2020). Analysing the effects of FinTech variables on cybersecurity: Evidence form Iraqi Banks. *International Journal of Research in Business and Social Science, 9*(6), 123-133. https://doi.org/10.20525/ijrbs.v9i6.914

Alem Al-Deen, B. (2019). The risks of cyberattacks and their economic effects: A case study: Gulf Cooperation Council countries. *Journal of Development Studies, Arab Planning Institute, Kuwait,* (63), 9-10. https://www.researchgate.net/publication/332866225

Alhayani, B., Mohammed, H. J., Chaloob, I. Z., & Ahmed, J. S. (2021). Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2021.02.531

Ali, M., & Manickam, S. (2018). *A Brief Review of Cybersecurity Issues in Iraq*. Technical Report, Palau Pinang: Universiti Sains Malaysia. http://dx.doi.org/10.13140/RG.2.2.23975.04006

Bassett, R., Bass, L., & O'Brien, P. (2006). Computer forensics: An essential ingredient for cyber security. *Journal of Information Science & Technology, 3*(1), 22–32. https://www.academia.edu/download/51933007/10.1.1.126.2719.pdf

Cangemi, D. (2004). Procedural law provisions of the council of Europe convention on cybercrime. *International Review of Law, Computers & Technology, 18*(2), 165-171. https://doi.org/10.1080/1360086042000223472

Chen, H., Chung, W., Xu, J. J., Wang, G., Qin, Y., & Chau, M. (2004). Crime data mining: a general framework and some examples. *computer, 37*(4), 50-56. https://doi.org/10.1109/MC.2004.1297301

Cordesman, A. H., & Khazai, S. (2014). *Iraq in crisis*. Rowman & Littlefield. https://ciaotest.cc.columbia.edu/wps/csis/0029991/f_0029991_24273.pdf

Grimes, R. A. (2020). *11 types of hackers and how they will harm you*. CSO. https://www.csoonline.com/article/3573780/11-types-of-hackers-and-how-they-will-harm-you.html

Harjan, S. A., Thabit, T. H., & Faaeq, M. K. (2015). Technology Innovation Usage in Public Services Among Employees in Republic of Iraq. In *7th International Conference on Information Technology, Al-Zaytoonah University of Jordan, Amman, Jordan* (pp. 42-49). The Applications of E-Systems in Developing Countries. https://www.researchgate.net/publication/274251925

Huey, L., & Rosenberg, R. (2004). Watching the web: Thoughts on expanding police surveillance opportunities under the cyber-crime convention. *Canadian Journal of Criminology and Criminal Justice, 46*(5), 597-606. https://doi.org/10.3138/cjccj.46.5.597

Jakštaitė-Confortola, G. (2021). Russia's 'sharp Power' Manifestations in Lithuania's Mass Media. *Baltic Journal of Law & Politics, 14*(1), 73-102. https://doi.org/10.2478/bjlp-2021-0004

Jesson, J. K., & Lacey, F. M. (2006). How to do (or not to do) a critical literature review. *Pharmacy education, 6*(2), 139-148. https://doi.org/10.1080/15602210600616218

Kudhair, A. T., & Shihab, H. K. (2018). Review to the Levels of Cybersecurity of Information Systems in Iraq. In *Mind technologies: Step to the future* (pp. 71-73). European Association of Educators and Psychologists "Science". https://www.elibrary.ru/item.asp?id=36361669

Lu, C., Jen, W., Chang, W., & Chou, S. (2006). Cybercrime & cybercriminals: An overview of the Taiwan experience. *Journal of Computers, 1*(6), 11-18. http://www.jcomputers.us/vol1/jcp0106-02.pdf

Nehme, T. (2020). Impasse of Cyber laws: Iraqi Case. *Defence Magazine,* (112). https://www.lebarmy.gov.lb/en/content/impasse-cyber-laws-iraqi-case

Passas, N., & Vlassis, D. (2007). Background and outline of the 2nd world summit of attorneys general, prosecutors general, chief prosecutors, prosecutors and ministers of justice. *Crime, Law and Social Change, 47*(4), 193-200. https://doi.org/10.1007/s10611-007-9074-4

Petrenko, S., & Makoveichuk, K. (2020). Development of BI-Platforms for cybersecurity predictive analytics. In *International Conference on Convergent Cognitive Information Technologies* (pp. 273-288). Springer. https://doi.org/10.1007/978-3-030-37436-5_25

Pocar, F. (2004). New challenges for international rules against cyber-crime. *European Journal on Criminal Policy and Research, 10*(1), 27-37. https://doi.org/10.1023/B:CRIM.0000037565.32355.10

Prabowo, H., & Sinaga, O. (2021). The Effect of Information and Communication Technology on Competitive Advantage of International Business in Indonesia. *Croatian International Relations Review, 27*(88), 205-222. https://www.cirrj.org/index.php/cirrj/article/view/562

Ritschard, G., Gabadinho, A., Muller, N. S., & Studer, M. (2008). Mining event histories: A social science perspective. *International Journal of Data Mining, Modelling and Management, 1*(1), 68-90. https://doi.org/10.1504/IJDMMM.2008.022538

Salih, A., Zeebaree, S. T., Ameen, S., Alkhyyat, A., & Shukur, H. M. (2021). A survey on the role of artificial intelligence, machine learning and deep learning for cybersecurity attack detection. In *2021 7th International Engineering Conference "Research & Innovation amid Global Pandemic"(IEC)* (pp. 61-66). IEEE. https://doi.org/10.1109/IEC52205.2021.9476132

Schutte, F. H., Breetzke, G. D., & Edlstein, I. (2021). The Relationship Between Temperature and Crime on the Cape Flats of South Africa. *International Journal of Criminal Justice Sciences, 16*(1), 127-145. https://ijcjs.com/menuscript/index.php/ijcjs/article/view/296/233

Shihan, K. H., & Radif, M. J. (2022). Internal and External Factors to Adopt a Cyber Security Strategy in Iraqi Organisations. *Webology, 19*(1), 5181-5198. https://doi.org/10.14704/WEB/V19I1/WEB19349

Shires, J. (2022). *The Politics of Cybersecurity in the Middle East*. Oxford University Press. https://global.oup.com/academic/product/9780197619964

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of business research, 104*, 333-339. https://doi.org/10.1016/j.jbusres.2019.07.039

Suhendi, D., & Asmadi, E. (2022). Cyber laws Related to Prevention of Theft of Information Related to Acquisition of Land and Infrastructure Resources in Indonesia. *International Journal of Cyber Criminology, 15*(2), 135-143. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/35

Sukhija, N., Sevin, S., Bautista, E., & Dampier, D. (2019). Prescriptive and predictive analytics techniques for enabling cybersecurity. In *Smart Data* (pp. 113-132). Chapman and Hall/CRC. https://www.taylorfrancis.com/chapters/edit/10.1201/9780429507670-6

Yeboah-Ofori, A., Islam, S., Lee, S. W., Shamszaman, Z. U., Muhammad, K., Altaf, M., & Al-Rakhami, M. S. (2021). Cyber threat predictive analytics for improving cyber supply chain security. *IEEE Access, 9*, 94318-94337. https://doi.org/10.1109/ACCESS.2021.3087109