Educational Administration: Theory and Practice
2024, 30(5), 4361-4370
ISSN: 2148-2403
https://kuey.net/

Research Article

A New Method for Detecting Advanced Persistent Threats Utilising Machine Learning

Firas Zawaideh[1]*, Murad Magableh[2], Hassan Al_Wahshat[3], Firas Rashed Wahsheh[4], Said Mohamad Altahat[5], Arkan Walid Al-Smadi[6]

[1]*Assistant professor, Cybersecurity Department, Faculty of Science and Information Technology, Jadara University, Irbid, Jordan, Email: F.zawaideh@jadara.edu.jo
[2]Assistant professor, Department of Computer Science, Faculty of Science and Information Technology, Irbid National University, Irbid, Jordan, Email: m.magableh@inu.edu.jo
[3]Assistant professor, Department of Management Information Systems, Faculty of Business, Ajloun National University, Ajloun, Jordan, Email: hasn.whashat@anu.edu.jo, https://orcid.org/0009-0001-4249-6783
[4]Assistant professor, Department of Management Information Systems, Faculty of Business, Ajloun National University. Ajloun, Jordan, Email: f.wahsheh@anu.edu.jo, https://orcid.org/0009-0009-5728-3738
[5]Assistant professor, Cybersecurity department, Faculty of Science and Information Technology, Irbid National University, Irbid, Jordan, Email: s.tahat@inu.edu.jo
[6]Faculty of Business, Department of Banking and Finance Science, Jearsh University, Jordan, PO.Box 26150, Jearsh, Jordan, Email: Arkan.smadi@jpu.edu.jo, Orchid ID: https://orcid.org/0000-0001-5544-7406

***Corresponding Author:** Firas Zawaideh
*Email: r.alsmadi@aau.edu.jo

Citation: Firas Zawaideh et al. (2024), A New Method for Detecting Advanced Persistent Threats Utilising Machine Learning, *Educational Administration: Theory and Practice*, *30*(5), 4361-4370
Doi: 10.53555/kuey.v30i5.3636

ARTICLE INFO

ABSTRACT

Cyber security is now receiving a great deal of attention owing to the dependency of humans on modern technologies and systems. As a result, defending these systems from cyber attacks has evolved into an absolutely necessary activity in today's world. An advanced persistent threat is a sophisticated cyber-attack in which hostile actors acquire unauthorised network access and stay undetected for a long time. Increasing numbers of sophisticated persistent threats are assaults and risks to enterprises are documented. Machine learning is one way of identifying sophisticated persistent threat assaults. Nevertheless, there is a shortage of datasets that include the whole of an advanced persistent threat assault lifetime, therefore this approach has not been addressed in many earlier types of studies. This research intends to construct a new dataset that spans the whole attack lifecycle of a complex persistent threat assault to identify normal, reconnaissance, and data exfiltration activities. The new empirical dataset will be depending on sophisticated persistent threat assaults utilizing tactics, and strategies. In addition, this paper introduces MLAPT, a new machine learning-based approach that can identify and forecast APT assaults in a systematic manner with high accuracy and speed.

Keywords: Cyber, security, *Information technology*, Machine learning.

1. Introduction

The quantity, complexity, and diversity of cyber assaults continue to rise. Currently, cyberterrorism and the rise of the Internet of Things are driving this trend (Conti et al., 2018; MacDermott et al., 2018). In 2015, cyberattacks cost $3 trillion a year, and by 2021, they are expected to cost more than $6 trillion (Morgan & Hackerpocalypse, 2016). This rising price has generated significant interest and investment in the study and development of novel cyber attack defence systems and strategies (Epiphaniou et al., 2017; Al-Khateeb et al., 2017). Even though virus scanners, firewalls, and intrusion detection and prevention systems (IDPSs) are able to find and stop a large number of cyber attacks, Cybercriminals, on the other hand, have developed increasingly sophisticated ways and strategies to get into the networks of their targets and exploit their resources (Wu et al., 2022). These cybercriminals focus their attention on wireless and wired communications (Salem et al., 2016; Sofotasios et al., 2020; Al-Smadi, 2020). Furthermore, many strategies for defending against cyber assaults take into consideration the possibility that the attacker may give up and move on to a less difficult target if the organization's network is sufficiently secured. Nevertheless, according

to the findings of a research study conducted by Masarweh & ALSaraireh, (2021), this notion is no longer accurate as a result of the proliferation of targeted assaults, also known as Advanced Persistent Threats (APTs), in which cybercriminals and hackers aim their efforts at specific businesses and continue their activity until they have accomplished their objectives. An advanced persistent threat (APT) attack is an ongoing assault that is directed at a particular organisation and is carried out in numerous stages (Xing et al., 2020). The primary objective of APT is espionage, followed by data exfiltration. APT is thus seen as a novel and more complicated kind of multistep assault. Since APTs employ complex methodologies and previously unknown weaknesses, they pose a problem for current detection methods (Wu et al., 2022; Alnsour et al., 2023). Furthermore, the economic impact caused by a comprehensive APT assault would be enormous. Investing in incursion protection systems (Alzahrani & Alenazi, 2021) is primarily motivated by the potential cost of assaults. APTs are now one of the gravest risks to corporations and governments (Ahmed et al., 2021). The majority of studies in the field of APT detection have relied on examining previously identified APTs (Mazraeh et al., 2019) or identifying a single APT that employs a particular piece of malware (Chen et al., 2019). A number of studies have sought to identify new APT assaults. Establishing real time detection (Zhao et al., 2020), identifying all APT attack phases, balancing false negative and false positive values, and relating events across a lengthy time span (Umar & Zhanfang, 2020) are nevertheless very difficult tasks. The current body of study is promising. Nevertheless, reliable and timely APT detection continues to be a difficulty. This study's major objective is to provide a CTI-based dataset to assist in the improvement of the APT model. Furthermore, present a model to identify APTs assaults utilizing machine learning and conduct a comparative evaluation of the methodologies used in the present study to validate the findings. The most important thing that this body of research has contributed is a model that can identify APT assaults based on behaviour by employing ML and making use of a fresh dataset that was built specifically for this study.

2. Related works

Current Intrusion Detection Systems (IDS) have difficulty detecting APTs, and study has been performed to combat this sort of multi stage assault. The limitations of existing APT detection methods (Xing et al., 2020). The detector employs dataflow monitoring to identify the connections between basic assaults launched throughout the APT life-cycle. TerminAPTor relies on an user, which may be a regular system for intrusion detection, to identify these basic assaults (Brogi & Tong, 2016). By modelling just two APT situations, the researchers stated that the APT detector must be enhanced by reducing false positives. Chen et al., (2019) introduces an APT detection technique depending on C&C domain detection. The study analyses C&C communication and identifies a novel characteristic in which entry to C&C domains is unrelated whereas entry to lawful domains is connected. Concerning the technique of detection that performed well when tested on a public dataset, the scientists claim that detection may be readily evaded when infected PCs connect to C&C domains when Internet users are browsing the web. In addition, failure to identify C&C domains results in the failure of APT detection, as this system relies on detecting just one phase of the APT life-cycle. Xing et al., (2020) explores a technique for APT detection that relies on spear phishing detection. To filter spam emails, this method relies on computational and mathematical investigation. To distinguish between legal and spam emails, the detection algorithm must construct tokens, which are groups of characters including replica, here, click, Viagra and free.

Nevertheless, the spear-phishing emails might not always include any of the essential tokens for the algorithm. As a consequence, a system that relies on a single step for APT detection fails when that step is absent. Similar to TerminAPT or detector (Xing et al., 2020; Al-Smadi and Malkawi, 2020) develops a statistical APT detector. The approach assumes that an APT experiences five phases, namely delivery, exploitation, installation, command and control, and actions, and that each state contains several activities. The created events in each state are statistically connected. The system demands extensive specialist expertise for installation and maintenance. Nissim et al., (2015) proposes an active learning based methodology for detecting fraudulent PDF. The above malicious PDF could be utilised in the initial stages of an APT attack to gain access to the target system. The "known files module," which is reliant on white lists, reputation systems, and an antivirus signature database, then screens all known benign and malicious files. Continuing this, the compatibility of the remaining "unknown files" with PDF files is evaluated. This method only identifies one phase of the APT life cycle. Chen et al., (2019) proposes a technique related to Data Leakage Prevention (DLP). The method concentrates on discovering the previous phase of APT, which is database moving. The information flow is processed by a DLP algorithm to identify cyberattacks and produce "fingerprints" based on the characteristics of the leak. The suggested system makes use of external Cyber Counter Intelligence (CCI) sensors to trace the place or course of leaked data. This method can only identify the data exfiltration phase of an APT attack. Additionally, it is unable to perform real time detection since the CCI analysis unit must wait for sensor data. Moreover, there is no assurance that CCI sensors could offer the needed information on data fingerprints that have been compromised. However, this approach also creates privacy problems since actors inside the CCI may access the information that is stored and transmitted by all individuals who use the system. In Balduzzi et al., (2017), a functional prototype of SPuNge is demonstrated. This suggested method relies on host-side data collection and tries to identify potential APT assaults. In the first of SPuNge's two major stages, identified dangerous URLs are analysed. These URLs may be accessed

through HTTP(S) using a web browser installed on affected PCs. The computers that exhibit comparable behaviour are then identified. This method relies on identifying a single APT behaviour, namely a malicious URL connection, and disregards the other APT activities. In other words, If the detection method fails to identify the malicious URL connect, the whole APT scenario cannot be recognised. Moreover, the technology is incapable of detecting in real time. The document Chen et al., (2019) explains a context based methodology for APT detection. The approach is built on the model of APT as an attack pyramid, with the apex representing the assault objective and the lateral planes representing the surroundings associated with the APT life-cycle. The model for detection demands extensive specialist expertise for installation and maintenance. Existing APT detection systems have significant problems with real-time detection, a balance between false positive and false negative rates, and the long-term correlation of events. This research provides a novel technique for APT detection and prediction in order to overcome these flaws.

2.1. Machine learning

The primary objective of machine learning is to allow computers to learn without user intervention and to alter their behaviours and conclusions accordingly. The two most common types of learning algorithms are supervised and unsupervised (Sofotasios et al., 2020). Two parts comprise the machine learning (ML) process: training and categorization. The objective of the training stage is to create a framework for estimating or identifying hidden data properties and attributes. In the second step, classification, the framework optimised during training is used with fresh datapoints to complete a specific job, such as clustering (Epiphaniou et al., 2017). This study addresses a multiclass-classification issue; the most common machine learning (ML) algorithms utilised for this type of issue utilising supervised learning method, including eXtreme Gradient Boosting (XGB), Decision Tree (DT), Support Vector Machine (SVM), Nave Bayes, Random Forest (RF) and K-Nearest Neighbor (KNN).

3. Methodology

This part explains how the suggested APT framework is built, how it will be used to reach future goals, and what its key stages are. The suggested detection method involves many steps. The first step is the collection and preprocessing of information, and the next is the categorization of datasets. Lastly, an M-L detection framework is applied to the data for testing. The following are the key approaches and routes for APT detection: Collect the information, Persisting pre-processing, Extrapolate the attributes and make use of the feature selection, as well as divide the information into the components of training and testing. Construct a framework, then assess it. The approaches of machine learning emphasise the development of explicit or implicit models that permit the categorization of data changes. could employ ML approaches for standalone, hybrid, or ensemble classifiers. The classification framework used can be divided into three procedure categories: supervised, unsupervised, and semisupervised. Generally, the supervised approach is superior to the alternatives. In intrusion detection systems, DT, Naive Bayes, Genetic Algorithm, SVM, and Logistic Regression are ML algorithms. Four phases comprise the ML model creation procedure: data collection and acquisition, data preprocessing, framework training and variety, and framework evaluation. There are various jobs that may be performed in the pre-processing data stage; feature selection and normalisation are the two essential concepts of this job (Kalbouneh et al., 2023; Umar & Zhanfang, 2020).

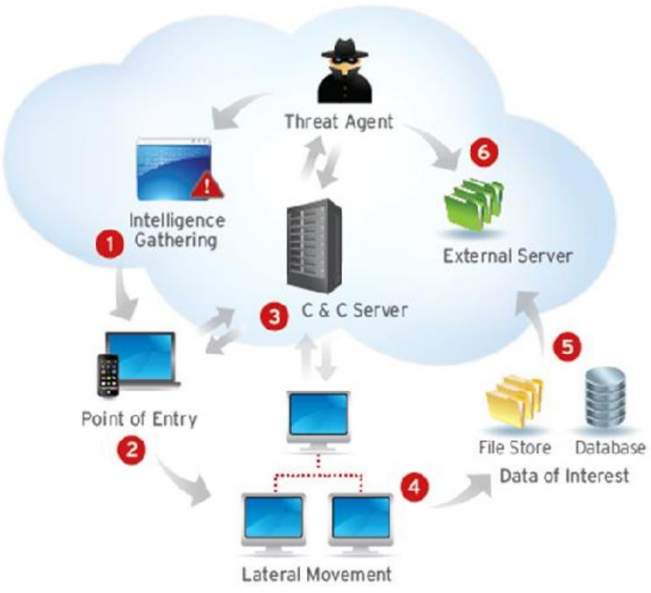

Fig. 1. APT Model Design.

Figure 1 displays the suggested model architecture for APT detection. The objective of the suggested strategy is to solve a multiclass classification issue in which the model receives pure data labelled as "data exfiltration," "reconnaissance, and "normal." The goal is to categorise typical traffic as normal, while all other classifications would be considered assaults. The assaults signify the stage reached in the attacker's attack. If the log is regarded as a slide, for instance, the attacker is in the third phase of the assault. The study employs a data collection method depinding on packet capture. Applying the TTP and IOC, APT undertakes attacks to compile such a dataset. APT's group tactics would also aid academics in their analysis and comprehension. It took ten weeks for this study to collect data on the design of real-world cyber networks. And early on in the data collection phase, we gave a base of people user and admin credentials so that we could replicate regular and routine traffic. Throughout this period, business operations continued as normal at the firm. A network administrator might, for instance, reorganise data, directories, and individuals, or change the data on a website. There has been no malicious data on the internet to serve as a baseline for the usual traffic. Once the network traffic baseline has been determined, specific data collection activities are conducted to collect it. Several APT category assaults on the internet were launched. Each assault was conducted independently over-time. The objectives of each assault vary. Each assault had the objectives of reconnaissance and exfiltration of information.

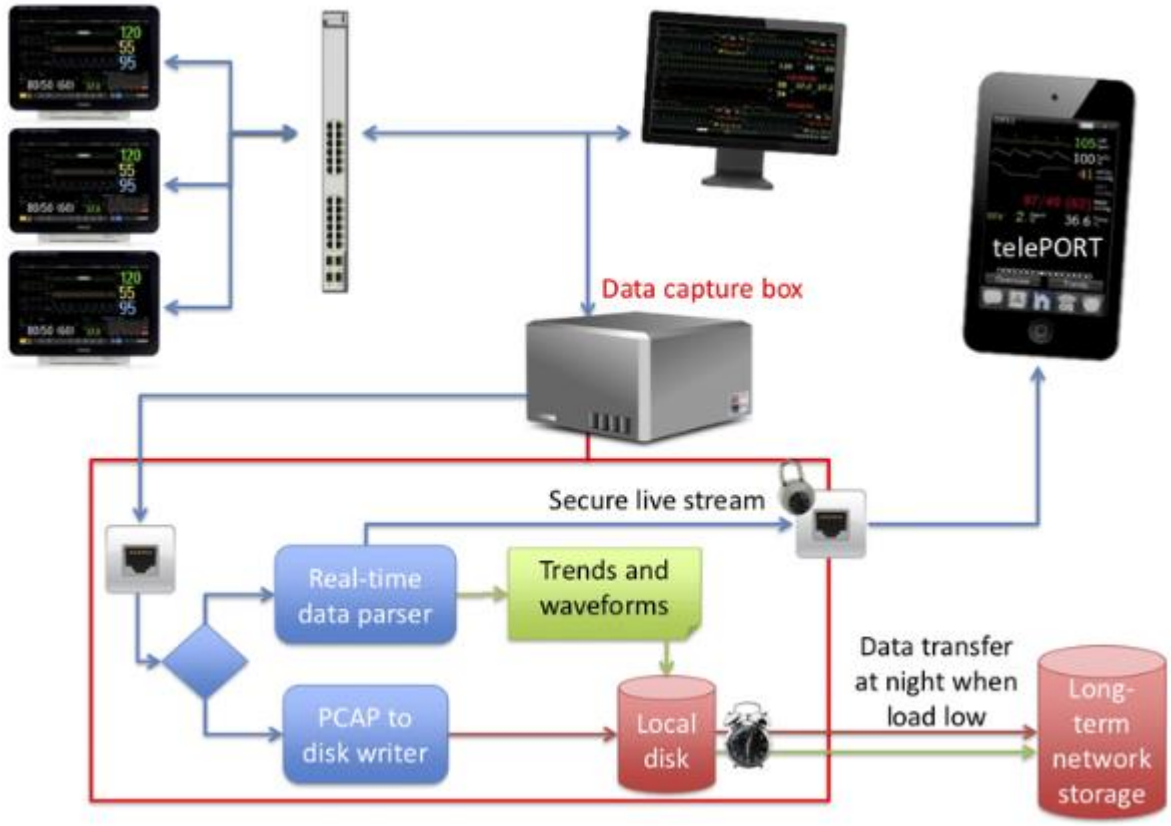

Fig. 2. Systems for Data Collection.

Figure 2 displays the data collection systems employed for this investigation. The diagram above depicts several data collection systems. The network is subjected to APT assaults by the attacker (tester), and each machine records each attack or manoeuvre. Using Logstash, the API Internet gathers the internet's logs. Additionally, it enables incompatible apps to function together. Numerous methods were employed to collect data. Initially, both free and paid CTI elements were utilised. CTI offers exceptional knowledge of current APT assaults, TTP, and IOC. Next, SIEM systems were employed to link APTs data and behavioural patterns. This level makes use of Moloch and SIEM (Arkime). The Moloch and SIEM shall gather information on genuine APT assaults. They have carried out assaults during the threat driven APT method phases (Chen et al., 2019) that APT categories monitor. The assaults utilized many methods to collect information about APT threats. The gathering procedure focused on regular traffic in order to build a network baseline and get an understanding of how normal traffic appears. Then several APT attacks were launched, resulting in increased network traffic. Each assault should reflect the mission stage of the attacker and the strategies used at each level: Various attack and regular operation traffic records were gathered. In all, 25,000 traffic records were collected and categorised according to their normalcy or assault situation.

3.2. Data pre-processing

To reach a better output, the full dataset should be standardised before data mining techniques are used. In database pre-processing, errors, incomplete data, and database standardisation are deleted. The present

study employed full case analysis to account for missing variables. In a data with a broad numeric values range, normalisation brings the numbers to a common scale. Normalizing data optimises various qualities. Normalization accelerates the model training phase for classification algorithms utilising neural networks or nearest neighbours. Some prominent normalising approaches such as decimal scaling. To normalise the dataset, we use Min-Max normalisation to normalise all of the numeric characteristics within the range from 0 to 1 determined by employing the equation (Ahmed et al., 2021). Feature extraction describes techniques that opt for or combine parts to form features, thus reducing the amount of data that must be processed while accurately defining the real dataset. The data will be labelled after the extraction of characteristics and generation of the CSV folder. Identify the dataset for each flow with the attack scenario's timing, the source and destination IP addresses, and the protocols employed. The gathered dataset includes 25,000 items. The dataset consists of several stages or classes, including Standard, Reconnaissance, and Exfiltration of Data. There were 83 internet traffic characteristics retrieved. Before the feature selection process, a feature heat map is made so that people can get to know the major characteristics and get a visual overview of them. The total feature relevance was plotted to help people understand and use the heat map better. Feature significance defines a collection of methodologies for evaluating characteristics of a categorization framework, expressing the relative significance of each feature for creating a classification. The classification algorithm is regarded as one of the most crucial processes in ML since it may have a substantial impact on the efficacy and performance of an ML model [20]. Nevertheless, prior to adopting any attribute selection approaches, an additional data cleansing step is required. Flow ID, source IP, destination IP, and timestamp have been deleted. The characteristics may influence the categorization procedure by creation the classifier biassed towards them and the cardinality of the data. In prior studies, the destination port was likewise eliminated from the data. However, as this study focuses on exfiltration of data and APT attacks, this component is required.

4. Results and discussion

In the present study, an APT detection method employing machine learning and a freshly produced dataset is presented. To determine the efficacy of the suggested framework and the novel dataset, a comparison was done with numerous m-learning techniques. Furthermore, the constructed dataset was utilised to assess the validity of a previously employed methodology. Initially, the suggested model was compared to two established classifiers: DT, and KNN. For a similarity measure, each classifier will employ the same number of characteristics. Employing the ANOVA feature selection approach, the XGB was equipped to attain the greatest outcomes with the smallest fewest characteristics. Hence, for all of this assessment, 9 characteristics would be utilised to compare each of the other classifiers. By using the confusion matrix for precision, F-measure, recall, and accuracy, the measures are assessed. Next, put the new dataset into a model from a prior study (Abass et al., 2017; Bekhet, and Al-Smadi, 2016). They constructed a framework using an XGB classifier on the KDD data. The full dataset, including all 45 characteristics, was included in their model. This examination yielded the following results: 98.7 percent accuracy, 97.4 percent precision, 97 percent recall, and 97.1 percent F1 measure. These findings clearly demonstrate that the produced data is genuine and may be utilised to identify APT attacks. Significant assessment criteria are established in order to get an intuitive understanding of the proposed model's primary concerns; for evaluating the effectiveness of the provided framework, accuracy, precision, recall, and the F1 measure (Abass et al., 2017) are employed. Accuracy is the accuracy rate of the model or the proportion of examples correctly classified by the classifiers. Precision is the number of examples that a classifier accurately categorises. The recall is the ratio of the number of relevant examples retrieved to the total number of significant situations. The F-measure is a statistic used to determine a test's precision. In harmonic form, it is the sum of memory and accuracy. The PyCM was used to acquire all metrics, measures, and assessment criteria. PyCM is a library for multiclass confusion matrices built in Python (Min et al., 2018). Applying the confusion matrix to the measurements yields four potential outcomes: TP, FP, TN, and FN. Figure 4 is an example of a confusion matrix for multiclass classification. In machine learning, a multiple regression is a breakdown of simulation results for a multiclass classification issue. It shows the result of a classifier's output on any dataset. It provides easy and apparent methods for measuring the precision and effectiveness of a model. It is employed to tackle classification issues with outputs that may be separated into two or more groups. This diagonal elements comprise proper or acceptable categorization, whereas the other elements indicate that the categorization framework has misclassified some items. Consequently, the classification model becomes more accurate and effective as the diagonal members of the confusion matrix increase in value. For the suggested framework, a comparison was conducted to assess the efficacy of all algorithms. Using the same data, eight characteristics have been derived. The suggested model's confusion matrix. Regarding the confusion matrix, it is evident that the suggested framework worked successfully in categorising each event into the right stage, with only a small number of examples being incorrectly classified. A TP prediction is the detection of a situation that already exists. Every time a TN test result is achieved, the absence of the condition is not identified. FP happens anytime a condition is identified, even if it is not present. FN refers to the failure of a model to identify a condition. These measures may be used to determine the TPR, FPR, TNR, and FNR.

5. Conclusion and future work

A technique for detecting APT assaults was described in this body of study, and it made use of a dataset on APT attacks that had just been constructed. The dataset was used to train a machine learning model that was suggested to identify advanced persistent threats depending on several sorts of assaults. There were a total of three different categories of data that were gathered: normal, reconnaissance, and exfiltration of data. Every type of data stands for a different level that the attacker may have reached throughout their assault. The suggested machine learning model for the identification of APT attacks was constructed on top of the XGB classifier using ANOVA attribute selection algorithm. Only 9 out of the total 45 features in the dataset were used in order to accomplish an impressive level of performance, which resulted in a detection accuracy of 98.92%. The suggested model was evaluated against other well-established ML classifiers, and it was shown to perform much better than the competition when the findings were taken into account. According to the plans for the future work, more research will be carried out to enhance this stage of the process by including multi-label categorization into the model. In light of this, upgrading the suggested APT detection approach to incorporate an inter technique will give additional insight into potential internet assaults.

References

1. Abass, A., Xiao, O., Mandayam, B., & Gajic, Z. (2017). Evolutionary Game Theoretic Analysis of Advanced Persistent Threats Against Cloud Storage," IEEE Access, doi:.
2. Abusaimeh, H. (2020). Distributed denial of service attacks in cloud computing. International Journal of Advanced Computer Science and Applications, 11(6).
3. Abusaimeh, H., Shkoukani, M., & Alshrouf, F. (2014). Balancing the network clusters for the lifetime enhancement in dense wireless sensor networks. Arabian Journal for Science and Engineering, 39, 3771-3779.
4. Ahmad, A. Y. B., Kumari, D. K., Shukla, A., Deepak, A., Chandnani, M., Pundir, S., & Shrivastava, A. (2024). Framework for Cloud Based Document Management System with Institutional Schema of Database. International Journal of Intelligent Systems and Applications in Engineering, 12(3s), 672-678.
5. Ahmad, A. Y. B., Tiwari, A., Nayeem, M. A., Biswal, B. K., Satapathy, D. P., Kulshreshtha, K., & Bordoloi, D. (2024). Artificial Intelligence Perspective Framework of the Smart Finance and Accounting Management Model. International Journal of Intelligent Systems and Applications in Engineering, 12(4s), 586-594.
6. Ahmad, A., Abusaimeh, H., Rababah, A., Alqsass, M., Al-Olima, N., & Hamdan, M. (2024). Assessment of effects in advances of accounting technologies on quality financial reports in Jordanian public sector. Uncertain Supply Chain Management, 12(1), 133-142.
7. Ahmad, A. (2024). Ethical implications of artificial intelligence in accounting: A framework for responsible ai adoption in multinational corporations in Jordan. International Journal of Data and Network Science, 8(1), 401-414.
8. Ahmad Y. A. Bani Ahmad, "Firm Determinants that Influences Implementation of Accounting Technologies in Business Organizations," WSEAS Transactions on Business and Economics, vol. 21, pp. 1-11, 2024
9. Ahmad, A. Y. B., William, P., Uike, D., Murgai, A., Bajaj, K. K., Deepak, A., & Shrivastava, A. (2024). Framework for Sustainable Energy Management using Smart Grid Panels Integrated with Machine Learning and IOT based Approach. International Journal of Intelligent Systems and Applications in Engineering, 12(2s), 581-590.
10. Ahmad, A. B., Atta, A. A. B., Asma'a Al-Amarneh, M. S., & Dahbour, S. A. (2023). Fund Family Selectivity Skills and Market Timing Ability: Comparison Study
11. Ahmad, A. Y. Bani ahmad , (2019). Empirical Analysis on Accounting Information System Usage in Banking Sector in Jordan. Academy of Accounting and Financial Studies Journal, 23(5), 1-9.
12. Ahmad, A. Y. B., Gongada, T. N., Shrivastava, G., Gabbi, R. S., Islam, S., & Nagaraju, K. (2023). E-Commerce Trend Analysis and Management for Industry 5.0 using User Data Analysis. International Journal of Intelligent Systems and Applications in Engineering, 11(11s), 135-150.
13. Alhawamdeh, H., Al-Saad, S. A., Almasarweh, M. S., Al-Hamad, A. A.-S. A., Bani Ahmad, A. Y. A. B., & Ayasrah, F. T. M. (2023). The Role of Energy Management Practices in Sustainable Tourism Development: A Case Study of Jerash, Jordan. International Journal of Energy Economics and Policy, 13(6), 321–333. https://doi.org/10.32479/ijeep.14724
14. Ahmed, Y., Asyhari, A., & Rahman, M. (2021). A Cyber Kill Chain Approach for Detecting Advanced Persistent Threats. Comput. Mater. Contin.67(2):2497–513.doi: https://doi.org/10.32604/cmc.2021.014223.
15. Al-Smadi, R. W. (2020). Financial Development, Energy Consumption And Economic Growth In Jordan: New Evidence From Time Series Analysis. International Journal Of Advanced Science And Technology, 29(3), 1558-1567
16. Al-Khateeb, H., Epiphaniou, G., & Alhaboby, J. (2017). Investigating formal intervention and the role of corporate social responsibility, Telemat. Inform. 34 (4) 339–349.

17. Alzahrani, & Alenazi, A. (2021). Designing a network intrusion detection system based on machine learning for software defined networks. Futur. Internet;13(5):1–18. doi: https://doi.org/10.3390/fi13050111.
18. Al-Smadi, R. W., & Malkawi, E. (2020). Determinants of Jordanian economic growth: time series approach. J Crit Rev, 7(2), 534-541.
19. Balduzzi, M., Ciangaglini, A., & McArdle, R. (2017). Targeted attacks detection with spunge.
20. Brogi, G., & Tong, V. (2016). Terminaptor: Highlighting advanced persistent threats through information flow tracking, in: New Technologies, Mobility and Security NTMS, 2016 8th IFIP International Conference on, IEEE, pp. 1–5.
21. Bekhet, H. A., & Al-Smadi, R. W. (2016). The dynamic causality between FDI inflow and its determinants in Jordan. International Journal of Economics and Business Research, 11(1), 26-47.
22. Chen, R., Zhang, W., Niu, & Lan, Y. (2019). A Research on Architecture of APT Attack Detection and Countering Technology, Dianzi Keji Daxue Xuebao/Journal Univ. Electron. Sci. Technol. China, vol. 48, no. 6, pp. 870–879, 2019, doi: 10.3969/j.issn.1001-0548.06.011.
23. Alnsour, I., Alghadi, M., Ahmad, A., Alibraheem, M., Altahat, S., Al-Smadi, R., & Alshboul, K. (2023). Islamic financial technology acceptance: An empirical study in Jordan. International Journal of Data and Network Science, 7(4), 1659-1668.
24. Conti, M., Dehghantanha, A., Franke, K., & Watson, ,. S. (2018). Internet of things security and forensics: Challenges and opportunities.
25. Epiphaniou, G., Karadimas, P., Ismail, A., & Al-Khateeb, A. (2017). Dehghantanha, K.-K.R. Choo, Non-reciprocity compensation combined with turbo codes forsecret key generation in vehicular ad hoc social iot networks, IEEE Internet of Things Journal.
26. MacDermott, A., Baker, S., Shi, Q., & forensics, A. (2018). Challenges for the ioa era,in: New Technologies, Mobility and Security, NTMS, 2018 9th IFIP International Conference on, IEEE, pp. 1–5.
27. Bani Atta, A. A., Ali Mustafa, J., Al-Qudah, S. S., Massad, E., & Ahmad, A. B. (2023). The effect of macroprudential regulation on banks' profitability during financial crises [Specialissue]. Corporate Governance and Organizational Behavior Review, 7(2), 245-258.
28. Cheng, Congbin, Sayed Fayaz Ahmad, Muhammad Irshad, Ghadeer Alsanie, Yasser Khan, Ahmad Y. A. Bani Ahmad (Ayassrah), and Abdu Rahman Aleemi. 2023. "Impact of Green Process Innovation and Productivity on Sustainability: The Moderating Role of Environmental Awareness" Sustainability 15, no. 17: 12945. https://doi.org/10.3390/su151712945
29. Atta, A., Baniata, H., Othman, O., Ali, B., Abughaush, S., Aljundi, N., & Ahmad, A. (2024). The impact of computer assisted auditing techniques in the audit process: an assessment of performance and effort expectancy. International Journal of Data and Network Science, 8(2), 977-988.
30. ALLAHHAM, M., SHARABATI, A. A. A., HATAMLAH, H., AHMAD, A. Y. B., SABRA, S., & DAOUD, M. K. Big Data Analytics and AI for Green Supply Chain Integration and Sustainability in Hospitals.Magboul, I., Jebreel, M., Dweiri, M., Qabajeh, M., Al-Shorafa, A., & Ahmad, A. (2024). Antecedents and outcomes of green information technology Adoption: Insights from an oil industry. International Journal of Data and Network Science, 8(2), 921-934.
31. Daoud, M. K., Al-Qeed, M., Ahmad, A. Y. B., & Al-Gasawneh, J. A. (2023). Mobile Marketing: Exploring the Efficacy of User-Centric Strategies for Enhanced Consumer Engagement and Conversion Rates. International Journal of Membrane Science and Technology, 10(2), 1252-1262.
32. Daoud, M., Taha, S., Al-Qeed, M., Alsafadi, Y., Ahmad, A., & Allahham, M. (2024). EcoConnect: Guiding environmental awareness via digital marketing approaches. International Journal of Data and Network Science, 8(1), 235-242.
33. Fraihat, B. A. M., Ahmad, A. Y. B., Alaa, A. A., Alhawamdeh, A. M., Soumadi, M. M., Aln'emi, E. A. S., & Alkhawaldeh, B. Y. S. (2023). Evaluating Technology Improvement in Sustainable Development Goals by Analysing Financial Development and Energy Consumption in Jordan. International Journal of Energy Economics and Policy, 13(4), 348
34. Almestarihi, R., Ahmad, A., Frangieh, R., Abu-AlSondos, I., Nser, K., & Ziani, A. (2024). Measuring the ROI of paid advertising campaigns in digital marketing and its effect on business profitability. Uncertain Supply Chain Management, 12(2), 1275-1284.
35. Al-Dweiri, M., Ramadan, B., Rawshdeh, A., Nassoura, A., Al-Hamad, A., & Ahmad, A. (2024). The mediating role of lean operations on the relationship between supply chain integration and operational performance. Uncertain Supply Chain Management, 12(2), 1163-1174.
36. Lin, C., Ahmad, S. F., Ayassrah, A. Y. B. A., Irshad, M., Telba, A. A., Awwad, E. M., & Majid, M. I. (2023). Green production and green technology for sustainability: The mediating role of waste reduction and energy use. Heliyon, e22496.
37. K. Daoud, D. . Alqudah, M. . Al-Qeed, B. A. . Al Qaied, and A. Y. A. B. . Ahmad, "The Relationship Between Mobile Marketing and Customer Perceptions in Jordanian Commercial Banks: The Electronic Quality as A Mediator Variable", ijmst, vol. 10, no. 2, pp. 1360-1371, Jun. 2023
38. Mohammad Jebreel, Mohammad Alnaimat, Amjad Al-Shorafa, Majed Qabajeh, Mohammad Alqsass, & Ahmad Bani Ahmad. (2023). The Impact of Activity Ratios on Change in Earnings (Case Study:Based on

Jordanian Food Companies). Kurdish Studies, 11(2), 4551–4560. Retrieved from https://kurdishstudies.net/menu-script/index.php/KS/article/view/1044
39. Mohammad Alqsass, Munir Al-Hakim, Qais Al Kilani, Lina Warrad, Majed Qabajeh, Ahmad Y. A.Bani Ahmad, & Adnan qubbaja. (2023). The Impact of Operating Cash Flow on Earnings Per Share (Case Study Based on Jordanian Banks). Kurdish Studies, 11(2), 2718–2729. Retrieved from https://kurdishstudies.net/menu-script/index.php/KS/article/view/831
40. Mohammad Alqsass, Munir Al-Haki, Mohammad Dweiri, Majed Qabajeh, Dmaithan almajali, Ahmad Bani Ahmad, & Adnan Qubbaja. (2023). The Impact of Current Ratio on Net Profit Margin (Case Study: Based on Jordanian Banks). Kurdish Studies, 11(2), 2894–2903. Retrieved from https://kurdishstudies.net/menu-script/index.php/KS/article/view/834
41. Mustafa, J. A., ATTA, A. A. B., AHMAD, A. Y. B., SHEHADEH, M., & Agustina, R. (2023). Spillover Effect in Islamic and Conventional Fund Family: Evidence from Emerging Countries. WSEAS Transactions on Business and Economics, 20, 1042-1058.
42. Mohsin, H. J., Hani, L. Y. B., Atta, A. A. B., Al-Alawnh, N. A. K., Ahmad, A. B., & Samara, H. H. (2023). THE IMPACT OF DIGITAL FINANCIAL TECHNOLOGIES ON THE DEVELOPMENT OF ENTREPRENEURSHIP: EVIDENCE FROM COMMERCIAL BANKS IN THE EMERGING MARKETS.
43. Ni, L., Ahmad, S. F., Alshammari, T. O., Liang, H., Alsanie, G., Irshad, M., ... & Ayassrah, A. Y. B. A. (2023). The role of environmental regulation and green human capital towards sustainable development: The mediating role of green innovation and industry upgradation. Journal of Cleaner Production, 138497.
44. Peng, Yixuan, Sayed Fayaz Ahmad, Ahmad Y. A. Bani Ahmad, Mustafa S. Al Shaikh, Mohammad Khalaf Daoud, and Fuad Mohammed Hussein Alhamdi. 2023. "Riding the Waves of Artificial Intelligence in Advancing Accounting and Its Implications for Sustainable Development Goals" Sustainability 15, no. 19: 14165. https://doi.org/10.3390/su151914165
45. Peiran Liang, Yulu Guo, Sohaib Tahir Chauhdary, Manoj Kumar Agrawal, Sayed Fayaz Ahmad, Ahmad Yahiya ,Ahmad Bani Ahmad, Ahmad A. Ifseisi, Tiancheng Ji,2024”Sustainable development and multi-aspect analysis of a novel polygeneration system using biogas upgrading and LNG regasification processes, producing power, heating, ,fresh water and liquid CO2”,Process Safety and Environmental Protection
46. Peiran Liang, Yulu Guo, Tirumala Uday Kumar Nutakki, Manoj Kumar Agrawal, Taseer Muhammad, Sayed Fayaz ,Ahmad, Ahmad Yahiya Ahmad Bani Ahmad, Muxing Qin 2024. “Comprehensive assessment and sustainability improvement of a natural gas power plant utilizing an environmentally friendly combined cooling heating and power-desalination arrangement”,Journal of Cleaner Production,Volume 436,,,140387
47. A. Y. A. Bani Ahmad, Y. M. A. Tarshany, F. T. M. Ayasrah, F. S. Mohamad, S. I. A. Saany and B. Pandey, "The Role of Cybersecurity in E-Commerce to Achieve the Maqasid of Money," 2023 International Conference on Computer Science and Emerging Technologies (CSET), Bangalore, India, 2023, pp. 1-8, doi: 10.1109/CSET58993.2023.10346972.
48. Rumman, G., Alkhazali, A., Barnat, S., Alzoubi, S., AlZagheer, H., Dalbouh, M., ... & Darawsheh, S. (2024). The contemporary management accounting practices adoption in the public industry: Evidence from Jordan. International Journal of Data and Network Science, 8(2), 1237-1246.
49. Singh, R., Gupta, N. R., & Ahmad, A. Y. (2024). An Empirical Study on Challenges of Working From Home During COVID-19 on Work-Life Domains in the Education Sector in Bengaluru. In S. Singh, S. Rajest, S. Hadoussa, A. Obaid, & R. Regin (Eds.), Data-Driven Intelligent Business Sustainability (pp. 111-121). IGI Global. https://doi.org/10.4018/979-8-3693-0049-7.ch008
50. William, P., Ahmad, A. Y. B., Deepak, A., Gupta, R., Bajaj, K. K., & Deshmukh, R. (2024). Sustainable Implementation of Artificial Intelligence Based Decision Support System for Irrigation Projects in the Development of Rural Settlements. International Journal of Intelligent Systems and Applications in Engineering, 12(3s), 48-56.
51. Wang, C., Ahmad, S. F., Ayassrah, A. Y. B. A., Awwad, E. M., Irshad, M., Ali, Y. A., ... & Han, H. (2023). An empirical evaluation of technology acceptance model for Artificial Intelligence in E-commerce. Heliyon, 9(8).
52. Yahiya Ahmad Bani Ahmad (Ayassrah), Ahmad; Ahmad Mahmoud Bani Atta, Anas; Ali Alawawdeh, Hanan; Abdallah Aljundi, Nawaf; Morshed, Amer; and Amin Dahbour, Saleh (2023) "The Effect of System Quality and User Quality of Information Technology on Internal Audit Effectiveness in Jordan, And the Moderating Effect of Management Support," Applied Mathematics & Information Sciences: Vol. 17: Iss. 5, Article 12. DOI: https://dx.doi.org/10.18576/amis/170512
53. Zhan, Y., Ahmad, S. F., Irshad, M., Al-Razgan, M., Awwad, E. M., Ali, Y. A., & Ayassrah, A. Y. B. A. (2024). Investigating the role of Cybersecurity's perceived threats in the adoption of health information systems. Heliyon, 10(1).
54. Alhawamdeh, H. M., & Alsmairat, M. A. (2019). Strategic decision making and organization performance: A literature review. International review of management and marketing, 9(4), 95.

55. Alhawamdeh, H., Al-Saad, S. A., Almasarweh, M. S., Al-Hamad, A. A. S., Ahmad, A. Y., & Ayasrah, F. T. M. (2023). The role of energy management practices in sustainable tourism development: a case study of Jerash, Jordan. International Journal of Energy Economics and Policy, 13(6), 321-333.
56. Alkhawaldeh, B., Alhawamdeh, H., Al-Afeef, M., Al-Smadi, A., Almarshad, M., Fraihat, B., ... & Alaa, A. (2023). The effect of financial technology on financial performance in Jordanian SMEs: The role of financial satisfaction. Uncertain Supply Chain Management, 11(3), 1019-1030.
57. Ali, O., Al-Duleemi, K., Al-Afeef, D. J., & Al-hawamdah, D. H. (2019). The Impact of the Decisions of the COBIT 5 Committee on the Effectiveness of the Internal Control Systems in the Jordanian Industrial Joint Stock Companies. The Journal of Social Sciences Research, 5(11), 1587-1599.
58. Ali, O. A. M., Matarneh, A. J., Almalkawi, A., & Mohamed, H. (2020). The impact of cyber governance in reducing the risk of cloud accounting in Jordanian commercial banks-from the perspective of Jordanian auditing firms. Modern Applied Science, 14(3), 75-89.
59. Al-Hawamdeh, H. M. (2020). The Intermediate Role of Organizational Flexibility in the Impact of Using Information Technology on the Efficiency of the Application of IT Governance in Jordanian Industrial Companies. Modern Applied Science, 14(7).
60. Fraihat, B. A. M., Alhawamdeh, H., Younis, B., Alkhawaldeh, A. M. A., & Al Shaban, A. (2023). The Effect of Organizational Structure on Employee Creativity: The Moderating Role of Communication Flow: A Survey Study.
61. Al-gharaibeh, S. M., Al-Zoubi, D. M., Hijazi, H. A., Al-Sakarneh, A., Alhawamdeh, H. M., Abdel, M., & Al-Afeef, M. (2021). The Relationship Between E-learning During Coronavirus Pandemic and Job Burnout Alkhawaldeh, B. Y. S., Alhawamdeh, H., Almarshad, M., Fraihat, B. A. M., Abu-Alhija, S. M. M., Alhawamdeh, A. M., & Ismaeel, B. (2023). The effect of macroeconomic policy uncertainty on environmental quality in Jordan: Evidence from the novel dynamic simulations approach. Jordan Journal of Economic Sciences, 10(2), 116-131.among Faculty Members in Public and Private Universities in Jordan
62. SALIH, A. A., & NASEREDDIN, A. Y. The Role of Strategic Awareness in Developing the Practice of Strategic Foresight in Business Organizations-Epistemological Perspective.
63. Nasereddin, A. (2023). Exploring the effect of corporate environmental management responsibility on firm performance. Uncertain Supply Chain Management, 11(2), 625-636.
64. Salih, A., Mousa, Z., & Nasereddin, A. (2023). The impact of career capital on sustainable competitive advantage: The mediating role of human resource management capabilities. Uncertain Supply Chain Management, 11(2), 489-502.
65. Raza, A., Al Nasar, M. R., Hanandeh, E. S., Zitar, R. A., Nasereddin, A. Y., & Abualigah, L. (2023). A Novel Methodology for Human Kinematics Motion Detection Based on Smartphones Sensor Data Using Artificial Intelligence. Technologies, 11(2), 55.
66. Nasereddin, A. Y. (2023). Impact of the Blue Ocean Strategy Dimensions in Achieving Competitive Advantage from the Perspective of Faculty Members.
67. Nasereddin, A. Y. (2023). A Business Analytics Approach to Strategic Management using Uncovering Corporate Challenges through Topic Modeling.
68. Yacoub Nasereddin, Ahmad (2023) "The Impact of Lean Thinking on Strategic Planning in Industrial Companies in Jordan from the Upper and Middle Management: A Perspective Study," Information Sciences Letters: Vol. 12 : Iss. 6 , PP -
69. Al-Afeef, M., Fraihat, B., Alhawamdeh, H., Hijazi, H., AL-Afeef, M., Nawasr, M., & Rabi, A. (2023). Factors affecting middle eastern countries' intention to use financial technology. International Journal of Data and Network Science, 7(3), 1179-1192.
70. Al-Waely, D., Fraihat, B. A. M., Al Hawamdeh, H., Al-Taee, H., & Al-Kadhimi, A. M. M. N. (2021). Competitive Intelligence Dimensions as a Tool for Reducing the Business Environment Gaps: An Empirical Study on the Travel Agencies in Jordan. Journal of Hunan University Natural Sciences, 48(11).
71. Masarweh, A., & ALSaraireh, J. (2021). Threat Led Advanced Persistent Threat Penetration Test. Int. Jourmal Secur. Networks;16(4):239–57.
72. Mazraeh, S., Ghanavati, S., & Neysi, Q. (2019). Intrusion detection system with decision tree and combine method algorithm. Int. Acad. J. Sci. Eng. Jun. 06 (01):167–77. doi: https://doi.org/10.9756/IAJSE/V6I1/1910016.
73. Min, Xiao, Xie, Hajimirsadeghi, & Mandayam. (2018). Defense Against Advanced Persistent Threats in Dynamic Cloud Storage: A Colonel Blotto Game Approach, IEEE Internet Things J., doi: 10.1109/JIOT.2018.2844878.
74. Morgan, S., & Hackerpocalypse. (2016). A Cybercrime Revelation, Cybercrime Report, Cybersecurity Ventures.
75. Nissim, N., Cohen, A., Glezer, G., & Elovic, ,. Y. (2015). Detection of malicious pdf files and directions for enhancements: a state-of-the art survey, Comput. Secur. 48 246–266.
76. O, B., Sofotasios, P., & Muhaidat, S. (2020). On the secrecy capacity of fisher-snedecor f fading Nasereddin, A. Y. (2023). Impact of the Blue Ocean Strategy Dimensions in Achieving Competitive Advantage from the Perspective of Faculty Members.

77. Nasereddin, A. Y. (2023). A Business Analytics Approach to Strategic Management using Uncovering Corporate Challenges through Topic Modeling.
78. Peng, Yixuan, Sayed Fayaz Ahmad, Ahmad Y. A. Bani Ahmad, Mustafa S. Al Shaikh, Mohammad Khalaf Daoud, and Fuad Mohammed Hussein Alhamdi. 2023. "Riding the Waves of Artificial Intelligence in Advancing Accounting and Its Implications for Sustainable Development Goals" Sustainability 15, no. 19: 14165. https://doi.org/10.3390/su151914165
79. Singh, R., Gupta, N. R., & Ahmad, A. Y. (2024). An Empirical Study on Challenges of Working From Home During COVID-19 on Work-Life Domains in the Education Sector in Bengaluru. In S. Singh, S. Rajest, S. Hadoussa, A. Obaid, & R. Regin (Eds.), Data-Driven Intelligent Business Sustainability (pp. 111-121). IGI Global. https://doi.org/10.4018/979-8-3693-0049-7.ch008
80. channels, arXiv preprint arXiv:1805.09260.
81. Salem, A., Hamdi, F., & Rabie, M. (2016). Physical layer security with rf energy harvesting in af multi-antenna relaying networks, IEEE Trans. Commun. 64 (7) 3025–3038.
82. Umar, A., & Zhanfang, C. (2020). Effects of Feature Selection and Normalization on Network Intrusion Detection, no. June, pp. 1–25, doi: 10.36227/.
83. Kalbouneh, N., Bataineh, K., Al-Hamad, A., Dwakat, M., Abualoush, S., Almasarweh, M., & Al-Smadi, R. (2023). The effects of the blockchain technology and big data analytics on supply chain performance: The mediating effect supply chain risk management. Uncertain Supply Chain Management, 11(3), 903-914.
84. Wu, Q., Li, Q., Guo, W., & Meng, D. (2022). Exploring the vulnerability in the inference phase of advanced persistent threats. International Journal of Distributed Sensor Networks, 8(2), 1-13.
85. Xing, K., Aiping, L., Rong, I., & Yan, J. (2020). A Review of APT Attack Detection Methods and Defense Strategies. IEEE Fifth International Conference on Data Science in Cyberspace, (pp. 67-70).
86. Xing, K., Li, W., JiangA, & Jia, Y. (2020). A review of APT attack detection methods and defense strategies, Proc. – IEEE 5th Int. Conf. Data Sci. Cyberspace, DSC 2020, pp. 67–70, Jul. 2020, doi: 10.1109/DSC50466.2020.00018.
87. Zhao, X., Jia, Y., Li, R., Jiang, & Song, E. (2020). Multi-source knowledge fusion: a survey, World Wide Web, no. March, pp. 2567–2592,doi: 10.1007/s11280-020-00811-0.