A Roadmap for SMEs to Adopt an AI Based Cyber Threat Intelligence

Abhilash J. Varma, Nasser Taleb, Raed A. Said, Taher M. Ghazal, Munir Ahmad, Haitham M. Alzoubi, and Muhammad Alshurideh

Abstract Cybersecurity has started to become the most significant concern among organizations as the number of threats and criminal activities in the past decade has increased exponentially. Cybercriminals and their attacking techniques have become increasingly sophisticated over the past couple of years. Conventional security measures will no longer be able to detect and mitigate the propagation of such advanced attacking trends. More and more hackers have started focusing on Small and medium-sized enterprises (SMEs) taking advantage of their limited resources. Therefore, SMEs will have to quickly adopt Artificial Intelligence (AI) based cybersecurity system in their infrastructure to defend themselves effectively and efficiently. It is currently forecasted that by 2021, 75% of all organizations will use AI and Machine learning (ML) applications in their security architecture to protect against all cyber threats. In this paper, the researchers identify the various challenges faced by SMEs in

A. J. Varma · N. Taleb · R. A. Said
Canadian University Dubai, Dubai, UAE

T. M. Ghazal
Faculty of Information Science and Technology, Center for Cyber Security, Universiti Kebansaan Malaysia (UKM), 43600 Bangi, Selangor, Malaysia
e-mail: taher.ghazal@skylineuniversity.ac.ae

School of Information Technology, Skyline University College, Sharjah, UAE

M. Ahmad
School of Computer Science, National College of Business Administration and Economics, Lahore 54000, Pakistan

H. M. Alzoubi (✉)
School of Business, Skyline University College, Sharjah, UAE
e-mail: haitham.alzubi@skylineuniversity.ac.ae

M. Alshurideh
Department of Marketing, School of Business, University of Jordan, Amman, Jordan
e-mail: m.alshurideh@ju.edu.jo; malshurideh@sharjah.ac.ae

Department of Management, College of Business Administration, University of Sharjah, Sharjah, UAE

M. Alshurideh et al. (eds.), *The Effect of Information Technology on Business and Marketing Intelligence Systems*, Studies in Computational Intelligence 1056,
https://doi.org/10.1007/978-3-031-12382-5_105

adopting an AI based cybersecurity due to their knowledge gap and lack of expertise. The researcher intends to provide a good background on AI, Cyber Threat Intelligence (CTI) and highlight some of the significant benefits provided by an AI based CTI system. A simple roadmap is developed using a qualitative research methodology to help SMEs effectively implement an AI based Cyber Threat Intelligent system in their infrastructure.

Keywords Cybersecurity · Artificial intelligence · Machine learning · Cyber threat intelligence · Deep learning · AI · ML

1 Introduction

Cyberattacks have increased exponentially over the globe. The world-famous investor Warren Buffet sees cyber risk as one of the gravest threats to humanity. In the past decade, we have seen some of the largest data breaches, national level hacking activities, political manipulations, and the use of botnets to bring down major telecom industries (Alzoubi et al., 2021a, b). These are compromising our private, professional, and national existence. No industry or organization is now completely safe from a cyber threat and therefore, the security professionals are always expected to stay current and up to date on the latest attack trends and vulnerabilities used by hackers (Kashif et al., 2021). They must detect, analyze and protect the organization in real-time (Alshurideh, 2022; Alshurideh et al., 2022a, b). Alkhalil et al. (2021) mentioned that the global cost of cybercrimes is expected to reach USD 6 trillion by 2021; 43% of the total cyberattacks target small businesses; $3.9 million is the average cost of a data breach for small to medium size businesses; organizations usually take nearly 6 months to detect a breach; the number of connected IoT devices will reach 75 billion by the year 2025 (Alnuaimi et al., 2021a, b).

Cyber threat intelligence is a process that proactively and iteratively searches various systems, databases, networks (Farouk, 2021), and other resources to detect and educate itself about the changing cybersecurity threats that can evade existing security controls. It enables the cybersecurity professionals to quickly recognize indicators of cyberattacks, analyze the attack methods and respond in a timely manner (Ali Alzoubi, 2021a, b). The cyber threat intelligence helps organizations to isolate and remedy these advanced threats before a cyber threat occurs. Even though various cyber threats follow different methods of cyberattack, they have a similar life cycle starting with the victim reconnaissance to performing malicious activities on the victim's network\devices (Mondol, 2021). The primary purpose of Cyber threat intelligence is to detect all weak points in the existing security solution and thereby take the necessary actions to safeguard the organization (Al Ali, 2021).

Over the years, Cyber Threat Intelligence has evolved from small ad-hoc tasks to a much more powerful program with their own dedicated staff, tools and processes that can support the entire organization (Radwan & Farouk, 2021). Most organizations nowadays not only consume cyber threat intelligence but also produce them.

This shows the growing maturity, popularity and professionalization in this field (Lee, 2020). Without the help of advanced data mining techniques, ML and AI, it is practically impossible for cyber analysts to stay on top of the latest attack trends, analyzing the current attack logs, generating intelligent reports that can be used to share and report on cyber security (Al Kurdi et al., 2021; Alhashmi et al., 2020; Salloum et al., 2020). AI and ML systems can significantly support cyber analysts in early detection as well as providing timely recommendations for mitigating various threats (AlShamsi et al., 2021; Nuseir et al., 2021; Yousuf et al., 2021).

In this research, the researcher will be reviewing some of the existing literatures on AI and CTI, discussing their core processes, functions and development lifecycle (Akour et al., 2021; Almaazmi et al., 2020; Alshurideh et al., 2020a, b, c). One of the key issues identified in the literature review is that SMEs are currently lagging in adopting this technology in their infrastructure due to several challenges such as limitations in budget, expertise, knowledge, etc. This problem can be overcome if there is a roadmap that can help SMEs to plan and successfully implement an AI based CTI system (Al Al Suwaidi et al., 2021; Alzoubi et al., 2021a, b; Shebli et al., 2021). Thus, the aim of this research is to develop a simple, effective, customizable roadmap for SMEs. The effectiveness of the roadmap was evaluated using a qualitative analysis and based on this result, an updated, customized, and focused roadmap is finally presented by the researcher (AlHamad et al., 2022). The main advantage of this research would be that it will provide enough knowledge and the confidence for SMEs to go ahead with their investments in AI based cybersecurity and how to use intelligent AI based systems to protect the organization from the vast number of cyber threats in the modern technological environment (Lee et al., 2022a, b). The research also covers some of the main challenges and risks that are usually faced by SMEs as part of their adoption of AI based CTI system (Miller, 2021).

2 Literature Review

In recent years, there has been a significant increase in the number of cyberattacks faced by organizations. Traditional firewall and antivirus based cyber defense tools is now primitive and are no longer able to effectively block cyber threats or keep up with the rapidly developing threat vectors. Cyber attackers are developing new sophisticated AI based smart malwares that can understand the target system, learn their environment, evade detection, and make intelligent decisions making it more and more complex and challenging for the organizations to detect and defend against various cyber threats (Alzoubi, 2021a, b). It is practically impossible for cyber analysts and forensic investigators to keep up with the advanced number of threats, the amount of data to be analyzed and the speed of processes to actively respond to all cyber threats in real-time (Alhamad et al., 2021). Existing literature shows that even though there has been a significant increase in the number of organizations that have started to adopt AI based Cyber (Alzoubi & Aziz, 2021a, b). Threat Intelligence for their cyber defense, a vast majority of cyber security professionals still lack a

deep understanding of Cyber Threat Intelligence, how AI based algorithms work and most importantly how to secure and harden an AI based CTI system (Ali et al., 2021). This is mostly because AI based CTI systems are not mature yet and is still an evolving technology (Alshurideh et al., 2020a, b, c). Large enterprises have the luxury of higher budget to invest in the latest innovative solutions, infrastructure, resources and for acquiring the required knowledge and expertise. Small and Medium sized Enterprises (SMEs) do not have this luxury and often struggle to invest and implement such new technologies in their infrastructure (Alshraideh et al., 2017; AlShurideh et al., 2019; Ghannajeh et al., 2015). SMEs therefore become most vulnerable to these advanced cyber threats as they are not kept up to date with the emerging cyber defense mechanisms (Alzoubi et al., 2021a, b).

Lee (2020) based on their latest CTI Survey, the biggest challenges faced by most organizations on the successful implementation of CTI are difficulties in integrating CTI with existing systems, the overall cost of implementation and continual improvements, lack of trained cyber security analysts and limited management support. Lidestri (2018) surveyed about 603 IT and IT Security professionals working for various US organizations who have already deployed or are planning to deploy an AI based CTI program in their organization. In this survey, while 71% of AI users voted that the AI technology will increase the speed of analyzing threats and providing a deeper security, only 60% of the current non-AI users believed this to be the primary benefit. 69% of the respondents believe that incorporating AI in Cybersecurity will increase the speed of analyzing threats while 64% believe it will help to quickly contain the infected endpoint (Ghazal et al., 2021). Cyber threat intelligence will increase the requirement for organizations to retain and employ more talented cyber analysts with AI exposure. This will bring a positive cybersecurity posture. Based on the survey, 68% of AI users said AI will improve the productivity of the IT staff while only 60% of non-AI users agreed on this. In one hand, 69% of AI users said that AI and ML technology will significantly improve the effectiveness of various application security activities, while on the other hand, only 59% of the non-AI users believed in this (Alzoubi & Yanamandra, 2020). The AI security experts\users believe that AI adaptation will help reduce the complexities in various security architecture. 56% of AI users responded that the adoption of AI based CTI system will decrease the overall complexity of the organizations security architecture while only 40% of non-AI users shared this view (Lee et al., 2022a, b). As the AI maturity level increases in the organization, the cyber analysts become more capable in understanding and identifying areas where AI implementation would be most beneficial (Aasriya, 2021). The stability, knowledge and expertise of AI based threat detection is drastically expected to improve as more and more organizations start to incorporate it and invest in this technology (Alkalha et al., 2012; Alnuaimi et al., 2021a, b; Altamony et al., 2012; Zu'bi et al., 2012). While non-AI users believe that an AI based CTI system will help them detect 41% of the previously undetected zero-day exploits, the AI users responded that they are able to detect 63% of these exploits with the help of AI (Lidestri, 2018).

With the boom of the Internet of Things (IoT) and cloud computing, the SMEs have become heavily dependent on the cyber world and therefore need to adopt the

latest cyber forensic investigation techniques on exchanged and stored data (Singh & Singh, 2021). The growing attack surface includes amateur threats, such as phishing, sophisticated distributed denial of service attacks and skilled nation-state actors. Prevention is nearly impossible. Advanced persistent threats show that hackers are patient (Lee & Ahmed, 2021). Given enough time, attackers will be able to get in since the cost of an attack is low and automated probing will eventually find a weakness. ML, Data mining and AI can quickly and efficiently detect any network abnormalities, including static and dynamic malware attacks. They can quickly analyze, learn and act intelligently against advanced cyber threats (Hanaysha et al., 2021a, b).

3 Background Information

3.1 Artificial Intelligence (AI)

AI was explained as the science and development of intelligent systems and programs that can understand human intelligence (McCarthy, 2007). Artificial intelligent systems are technologies that can gather or read data from their various inputs, learn from their environment and make autonomous decisions based on the intelligence acquired through their experience and knowledge (Hanaysha et al., 2021a, b). They can adapt to different situations and act independently without any human intervention. AI should be able to automate most of your repeatable tasks and in the long run make intelligent decisions on behalf of the cyber analysts (Ahmed et al., 2021; M. Alshurideh et al., 2020a, b, c; Harahsheh et al., 2021; Naqvi et al., 2021). This will include functions like planning, reasoning, training, problem solving, etc. It's a highly effective tool that can continually learn from internal, as well as external data and become a vital part of the cyber security infrastructure. According to Davies (2020), AI systems can include capabilities like Cognitive computing, ML, DL, Natural Language Processing (NLP), Computer Vision, Speech, RPA, etc. as depicted in Fig. 1.

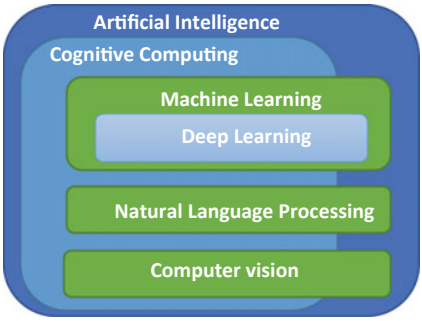

Fig. 1 Artificial intelligence

Cognitive Computing works with multiple subsets of AI such as ML, DL, NLP, Computer vision, etc. to simulate the human thought process and provide recommendations to help humans make better decisions. **Machine Learning** is a subset of AI and it enables machines to interact with data, learn from them and probably make changes to the algorithm in response to the data received without the need to follow explicitly programmed instructions (Alshurideh et al., 2022a, b). It includes deep learning, supervised algorithms and unsupervised algorithms to support predictions, analytics and data mining. These algorithms are used to recognize patterns and anomalies in data. Deep learning is a subset of ML. **Natural Language Processing** is a subset of AI that enables machines to work with text and languages, extracting their meaning and generating texts that are natural and grammatically correct (Ali et al., 2022).

3.2 Cyber Threat Intelligence (CTI)

Cyber threat intelligence is the final product that is disseminated after all cyber information is collected, processed and analyzed through a rigorous procedure called the intelligence cycle. It enables organizations to collect the correct threat intelligence and create a secure plan to detect, respond, prevent and mitigate various types of cyber threats and strengthen the organizations defense (Alzoubi et al., 2020a, b, c, d). The data should provide accurate useable intelligence. Figure 2, shows the various phases in the cycle.

According to Lee (2020), the Intelligence cycle starts with the Planning phase where the requirements are identified. This includes the specific questions and concerns that are to be addressed by the CTI program. Even though the requirements have a generic nature to all organizations, the specifications are unique to each

Fig. 2 The intelligence cycle. *Source* 2020 SANS CTI Survey

organization (Ahmad et al., 2021; AlMehrzi et al., 2020; Alzoubi et al., 2020a, b, c, d; Hayajneh et al., 2021). They are updated in an ad hoc manner based on the past incidents or upcoming trends in the industry. Specify who will be consuming the finished product—will it be used as an input to another system, will it be sent to Cyber analysts with technical expertise or will it be sent to top executives for their broad overview of the current cyber trends (Mehmood, 2021).

These requirements are then passed on to the Collection phase where they identify and evaluate the sources of intelligence that will help answer the requirements in an efficient manner. In addition to the inhouse data that is collected from the different departments\groups, information is also gathered from commercial threat feeds coming from CTI-specific vendors, generic security vendors, open-source threat feeds and forensics data (Alzoubi et al., 2020a, b, c, d). Information should also be periodically evaluated to ensure that it is current, effective and usable (Aburayya et al., 2020; AlShehhi et al., 2020; Svoboda et al., 2021). A data source that may have been critical in the past might no longer be needed, and new data sources might need to be identified as the organization and the threat landscape change (Alzoubi & Aziz, 2021a, b).

This data is then processed in the Processing phase to a format that is usable for the analysis phase (Alzoubi et al., 2022). Thousands of log events are generated every day by each system, these need to be collected, filtered and processed by automated systems to make any sense from the data. In the Analysis phase, the data is synthesized to support the requirements that were defined in the first phase. It searches for any potential security events and alerts the respective teams (Alzoubi & Yanamandra, 2020).

The final step is the Dissemination phase where the intelligence gathered is disseminated to the intended audience outlined in the planning phase. The data should go to the right recipient in the right format so that they are able to use it effectively. Timeliness and relevance are critical to the effectiveness of CTI dissemination. Cyber Threat Intelligence is primarily presented in the form of reports or brief summaries via emails, spreadsheets, power point presentations, etc. It is also used as an input to various security tools to generate alerts in an automated fashion (Alzoubi & Ahmed, 2019).

3.3 The Benefits of an AI Based CTI

Organizations generate and consume huge amounts of raw CTI data but it's incredibly time consuming and cumbersome to convert into intelligence. Most of these data is used for analyzing the application and its security (Alzoubi et al., 2020a, b, c, d). AI and ML programs can be the most beneficial for such tasks as they can analyze thousands of records\events, learn their behavior and raise an alert to the cyber analyst in case a vulnerability is detected (Alzoubi et al., 2020a, b, c, d). Semi-automation of cyber security tasks and data processing will be the golden standard followed by industries as the AI based CTI program maturity improves (Joghee et al., 2020).

3.4 The Core Functions of an AI Based CTI System

Alnuaimi et al., (2021a, b) proposed the core functions of an AI based cyber threat intelligence as shown in Figure 3. *Identification* of threats and the vulnerabilities is key to understanding the risk a potential attack can have on the organization. AI and ML algorithms can *discover* abnormalities in behavior patterns, flag it immediately and alert the cyber security analyst of a potential breach or threat. AI can use its data sets to *detect* cyber threats by identifying common threat characteristics. It is important to *investigate* events to gather maximum amount of information about the attack, the attack vector, its status, exploits and vulnerabilities (Aziz & Aftab, 2021). *Analysis* would enable the security analyst to identify the vulnerabilities, the devices that were compromised, the elements that failed to prevent the attack and how it happened (Alzoubi & Ahmed, 2019). AI would enable the security analysts to respond in a timely manner and *prevent* any form of progression. AI would be able to immediately *respond* to threats and isolate the infected equipment and stop the threat from progressing any further. Deep learning and ML enable AI to learn the behavior of attacks and thereby *predict* when, how and where the attack will begin. This will enable the security analysts to take appropriate actions to better prevent or mitigate an attack before it happens (Akhtar et al., 2021). AI enables the organization to *continuously monitor* the cyberspace to discover new threats vectors as well as defend against known and unknown threats.

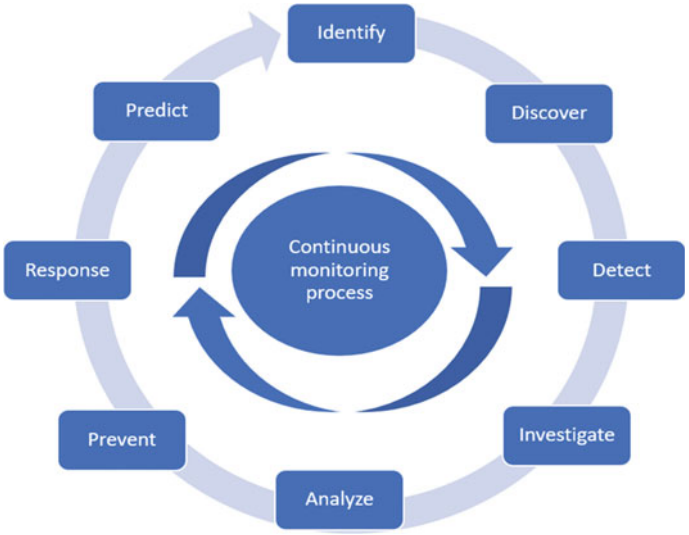

Fig. 3 Core functions of an AI based cyber threat intelligence

3.5 Designing an AI Based CTI system—The AI Development Life Cycle

Darraj et al. (2019) married the traditional SDLC with AI specific design and technology. Figure 4 depicts the 9 phases in the AI development life cycle: Planning, Analysis, Design, Implementation, Training, Optimization & Validation, Testing & Integration, Deployment and Maintenance. In the Planning phase, we need to clearly specify the Cyber threat intelligence requirements, its scope, security, access control, privacy and data encryption along with governance, laws and compliance (Emerita, 2021). In the Analysis phase, various cybersecurity AI tools are analyzed to identify the right tools, algorithms and data sets that are optimal for the organization. Here we will be able to decide which tasks can be automated and which needs a human intervention. In the Design phase, the AI based CTI solution is designed for the organization using the above identified AI tools covering ML, natural language processing, deep neural nets and cognitive computing (Khan, 2021). You will specify what will be the outcome and who will be using the system. In Phase four, the designed AI-CTI solution is implemented. In the Training phase, the designated data sets are used to train the AI-CTI algorithms for building its intelligence that will later be used for automation and taking intelligent decisions (Guergov & Radwan, 2021). In phase six, the cyber security analyst should optimize and validate the AI algorithm and data, ensure the cybersecurity hardening and patching are met and the system is functioning as intended. In phase seven, AI-CTI solution is integrated with the various systems in the organization and tested. The cyber security analyst starts testing the system ensuring all security and privacy requirements are completely met and confirm all PII, PHI, PCI/SOX and FTI data are appropriately protected (Obaid, 2021). In phase eight, the solution is deployed to production environment and becomes completely active. Here the cybersecurity analyst will continue hardening the system, patching and continuously monitor the AI-CTI solution. Phase nine is continual operation and maintenance of the AI-CTI system. The system, as any other application, needs to be continuously monitored and patched to ensure it meets expectations and requirements of the organization. We must make sure the AI system is behaving and functioning as planned. Threat forecasting and risk assessment should be performed at each phase considering the indicators of attack, compromise and interest. All vulnerabilities should be identified and remediated at each phase (Alnazer et al., 2017a, b).

3.6 Incorporating AI into Cyber Threat Intelligence

Learning can be defined as the process of acquiring knowledge or skill sets and when this knowledge is applied in a decision-making process it is called intelligence. An AI system must first learn before it can apply intelligence. To start off, AI systems can be used to perform daily repetitive tasks such as scanning, auditing, analyzing and reviewing huge volumes of data, logs and reports. It can perform

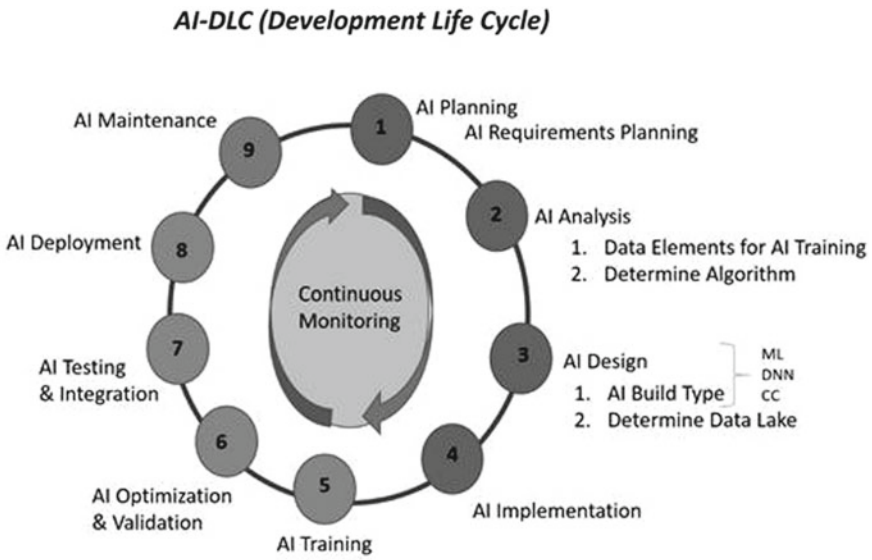

Fig. 4 An AI development life cycle

event correlation and generate intelligent reports which can then be further analyzed by the cyber analysts to strengthen the cyber defense system. AI allows to free up security operators so that they can now focus on more advanced tasks that require deeper thought processes (Alnazer et al., 2017a, b). There are several AI enabled tools and applications such as Neural Networks for intrusion detection, JASK security platform for detecting cyberthreats at its early stage, Cylance's security solution for predictive threat prevention, etc. to support cyber defense (Hamadneh et al., 2021). Adopting an AI based CTI system would improve the cyber resilience of the organization making its cyber defense strategy to be more proactive than reactive. The most significant feature of an AI based CTI system is its ability to adapt and learn. Overtime the system would be able to detect and respond to both known as well as unknown threats. Truong et al. (2020) categorized the most common applications of AI based cybersecurity into: Malware detection, Network intrusion and Phishing/Spam detection as illustrated in Fig. 5.

4 Research Design and Methodology

To address the research problem, the researcher has come up with a simple roadmap for SMEs that can help them to easily and effectively incorporate an AI based CTI system in their cyber security architecture. This roadmap was shared with some of the subject matter experts who are currently working in the cyber security team for various reputable organizations. This research is limited to the development of a

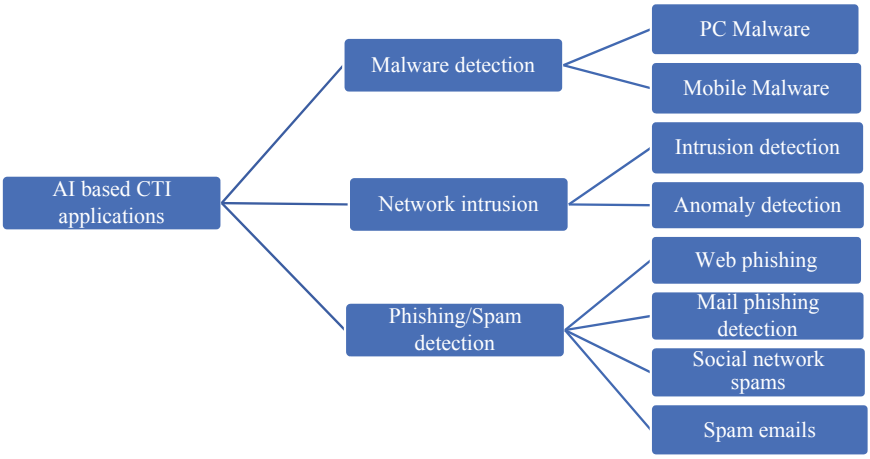

Fig. 5 Common AI based CTI applications

roadmap for SMEs for the successful adoption of an AI based CTI system as part of their cyber defense.

A qualitative research primarily deals with data which is verbal in the participants own written or spoken words based on his beliefs and understanding of the phenomenon (Bless et al., 2000). It tries to identify the problems that might be experienced by the participants with respect to the subject. The qualitative approach is appropriate for this study because the data collected and used focuses on the participants' subjective experiences in the field of organizational cyber security and the way they interpret them.

To evaluate the effectiveness of this roadmap we will be using a qualitative research method where the newly developed framework, as shown in Fig. 6 will be shared with various IT professionals. These participating IT professionals would be requested to evaluate the effectiveness, efficiency and the simplicity of the roadmap. The feedbacks from each of the participants are noted and used to develop our final roadmap for SMEs for the successful adoption of an AI based CTI system.

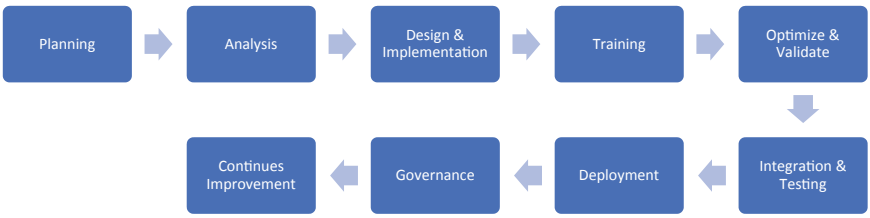

Fig. 6 A roadmap for SMEs for adopting an AI based CTI

1. Planning
    a. Setting up the requirements, scope, goals, security, access control, privacy, data protection, compliance.
    b. List of systems to be integrated.
    c. Create a team of experts with in-depth technical and process knowledge. Include SMEs from third party partners.
2. Analysis
    a. Identify the data platform.
    b. Evaluate data quality.
    c. Data collection (inhouse + external).
    d. Analyze various AI tools, algorithms, data sets.
    e. What tasks to automate.
    f. Tasks that need human interaction.
    g. Selecting the use cases that is easy to implement, provides a significant benefit, high impact to the cyber defense, high quality, complete, up-to-date data set that is readily available, has a with a very high impact.
    h. Look at some of the common use cases like malware detection, network intrusion detections and Spam\phishing detection.
3. Design and implement
    a. Designing the AI solution using the selected AI tools, algms, data sets identified from step 2.
    b. Specify what will be the outcome, who will be using it.
    c. Implement the solution in development environment.
4. Training
    a. Use pre-defined data sets to train AI to build intelligence.
    b. Exchanging and collaborating with other threat researchers and security professionals through various open-source threat intelligence platforms like Open threat exchange, Facebook threat exchange or IBM X-Force exchange is very critical for improving the efficiency and effectiveness of the AI algorithm in detecting new threats. Such collaborations help the AI solution to keep up to speed with the latest attack trends and vulnerabilities.
    c. Train cyber analyst for AI by upskilling their employees and improving their knowledge in the logic underpinning the AI algorithms and its behavior. Create proper interfaces that can enable them to interact with the AI tools and incident alerts.
5. Optimize and validate
    a. Fine tune the AI CTI for maximum efficiency and effectiveness.
    b. Ensure the AI CTI is functioning as intended.
    c. Continue patching and hardening.
    d. Assess the performance wrt initial requirements.

6. Integration and Testing
    a. Deploy Security orchestration, automation and response (SOAR) technologies to improve incident alert triage quality, defining a standardized incident response workflow, improving the security and operations management as well as reducing the onboarding time for a cyber analyst.
    b. Use SIEM to integrate the silos.
    c. Security and privacy requirements are met.
    d. Data is properly protected.
    e. Test the system thoroughly.
7. Deployment
    a. Deploy to production.
    b. Continue patching and hardening.
    c. Ensure the AI CTI is functioning as intended.
    d. Begin continues monitoring.
8. Governance
    a. A clear, transparent governance process needs to be implemented and adhered to monitor the performance of the AI-CTI solution. The controls should include checks on the roles and responsibilities, AI algorithm behavior abnormalities, risk tolerance, output verification and key performance indicators to measure the success of the program.
    b. Control processes to monitor the performance of AI CTI.
    c. BCP if the AI CTI stops working or goes rogue.
    d. It gives you the information you need to reduce Mean Time to Detect and Mean Time to Respond (MTTD and MTTR)—with a quicker, more decisive escalation process.
    e. It enables SOCs to assess and refine their IR processes, continually.
9. Continues Improvement
    a. Look at adding other tasks into the AI CTI.

The roadmap was sent via email to:

a. Senior Cyber Advisor working for a manufacturing company.
b. SIEM—Subject Matter Expert working for a reputed Information Technology and Service provider.
c. Director of Network, Infrastructure and Security working in the hospitality industry.

5 Findings and Results

5.1 Comments Received from the Senior Cyber Advisor

The road plan looks fab. It is really very impressive and efficient from what I understand. Great Job. I have some suggestions hoping they will be of some help.

Continual Improvement: I was expecting it from the planning phase itself. I was happy to see a heading in the end. I would recommend that every phase should have a clause of continual improvement. For instance, the processes defined need to be changed and improved with changing time. Our design needs to continuously evolve to better our product and its security. In the heading 9 itself we can say something of this sort in a couple of lines maybe?

Reviews and Approvals: Can we add some reviews and approvals? For instance, I would be more comfortable saying "reviewed and approved pre-defined data set" than 'pre-defined data set'.

One subheading, maybe a one liner somewhere about 'Segregation of Duties'?

5.2 Comments Received from the SIEM—Subject Matter Expert

Vulnerability assessment and Penetration testing should be used in the Planning phase for a better understanding of the current security infrastructure. This can be used to customize the solution for the customer. Getting to know the type of industry and customizing the solution accordingly for EG: Bank (SWIFT, PCIDSS), Healthcare (HIPPA etc.). Knowing the Number of users in an organization is important for the right sizing of Tools and devices. Use cases have to be custom tailored as per industry type of the organization. eg: create use cases for SWIFT application for banks etc. Providing Analyst with a Database for them to input information based on customer feedback after an incident is raised. Creating automated Templates in SOAR based on the incident triggered and for low-risk incidents automating the action using SOAR. For eg: IP is blacklisted, automatic action of blocking IP. Data should always be encrypted and make sure the main hardware is not connected to internet. Testing of the system should include PT or VA activity and detection of the threat. Tasks based on customer requirements and required less analysis by the Engineer needs to be automated. Further automation can be achieved but should have a final approval from Analyst before performing the actions.

5.3 Comments Received from the Director of Network, Infrastructure and Security

In the Planning phase, the company's mission, vision and executive management directions has to be analyzed. Based on these directions, the current security infrastructure must be reviewed and their setbacks to be noted. The AI based enhancements should be able to overcome these setbacks to gain the confidence and buy-in from the executive management.

Future research on various AI based cyberattacks by nefarious actors, their prevention and mitigation methods can further bridge the knowledge gap and secure the defense against such cyberattacks. The application of AI is a relatively new trend in combating cybercrimes and is still evolving. Further research should be conducted to improve the maturity of AI based cyber threat intelligence, their design, architecture and implementation. International Government bodies should also research and study how best they can legally cooperate and fight cybercrimes. The roadmap was evaluated and developed specifically for an SME; therefore, larger organizations might have added requirements to be addressed in the roadmap.

Considering the generic audience with backgrounds from different industries and having their unique requirement, we have restricted ourselves from discussing any vendor application or solution in detail. This gives us the opportunity to create a general guideline for SMEs that want to develop their own AI based CTI application as well as helping them negotiate with third-party service providers to make an educated and detailed blueprint to support their strategic decision on how they want to implement an AI based CTI system in their infrastructure.

6 Conclusion

Cybercrimes are increasing day by day and the attackers are using technologically advanced, complex and sophisticated threat models to evade detection. Adaptation of the various AI technologies have several benefits and can be used to detect and prevent attacks before it takes place. It is imperative that cybersecurity analysts have a deep and clear understanding of the AI algorithms, their functions and various possible applications to make the most of the cyber threat intelligence. The cyber analysts should ensure the AI systems are secured, hardened and continuously monitored to check and confirm they are behaving as expected, meeting all security/privacy requirements. More and more SMEs are acknowledging the need for an AI based Cyber Threat Intelligence to provide a secure and reliable cyberspace. It is critical that SMEs work together with larger organizations, Government, and other not-for-profit organizations to improve the current overall maturity of AI programs so that they become more dependable and less prone to going rogue.

The researcher believes that SMEs should start investing and adopting the latest AI based cyber security systems in their infrastructure so that they are all well prepared

and understand the nuances of future AI-powered exploitations and other attacking trends. This will also help in the continued research, development and maturing of the AI technology. With the help of this article, cyber security leaders would have gained the knowledge and confidence required for the successful implementation of an AI based cybersecurity system as part of its cyber defense and resilience program. Organizations can start off with the basic automation of daily repetitive tasks such as analyzing security logs, errors and reports for the Cyber analyst. Eventually, the AI applications scope can be increased to a broader set of more complicated cases to significantly increase the speed, efficiency, and effectiveness of their cyber defense.

7 Recommendation and Future Research

Even though there are several benefits in incorporating AI in CTI, very few SMEs have successfully implemented this in their infrastructure. There are several factors contributing to this, such as lack of expertise, lack of thorough knowledge about the algorithm behavior, its stability, cost of implementation, lack of awareness about the evolving cybercrimes, false positives, marketing hypes, etc. Due to these, SMEs often struggle to come up with a strong roadmap that would enable them to implement an efficient AI based CTI system. With the help of the qualitative analysis that was completed in this research, the researcher proposes the final roadmap, Fig. 7, for SMEs to develop their own customized AI based cybersecurity in their current security infrastructure.

Planning—In the Planning phase, based on the company's mission, vision and executive management direction, analyze the security infrastructure of the company using vulnerability assessment and penetration testing to understand the current risks. The AI based CTI system should be an enabler for the SME to achieve their strategic goals and should be able to mitigate the identified risks to gain the confidence and buy-in from the executive management. create a team of subject matter experts that include inhouse members with technical expertise, deep process knowledge as well as third-party partners. The third-party partners should be well experienced working with SMEs so that they can provide innovative solutions that are effective, optimized for SME requirements and are budget friendly. Specify the list of requirements, objectives and scope of the AI based CTI system. The specifications should also include information regarding the security, access control, privacy, data protection, encryption and compliance requirements. You should also list out all existing applications

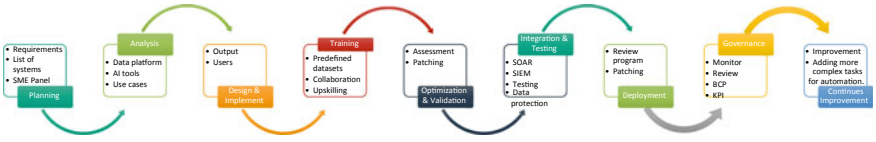

Fig. 7 Roadmap for AI implementation

and systems in the organization so that we do not miss out any critical application during rollout.

Analysis—In this phase, you need to analyze the data sets, data platform, AI tools and algorithms available in the market to identify the best ones that meet your organizations requirements. AI systems are heavily depended on the data that is fed to the system and is popularly publicized to be Garbage in garbage out systems. Identify the datasets that will be used by the AI based CTI system and evaluate them. The data sets used should be of the highest quality, up-to-date and complete. Specify which tasks should be automated by the AI based CTI system and which processes require human intervention. By the end of this phase, you should have selected the use cases that is easy to implement, provides significant benefits, has a high impact in the organizations cyber defense strategy. Select use cases that already have a high quality, complete, up-to-date data set that is readily available. The use cases have to be custom tailored based on the industry type of the SME. Some of the popular use cases are:

- Use of ML for analyzing huge amounts of data and identifying threats before it is exploited. ML can observe anomalies much quicker and with lot more accuracy than humans can and thereby enabling us to predict future threats.
- AI and ML can be used to track and detect any phishing attempts and remediate much faster than humans can. AI-ML can scan through every email in its network to detect phishing campaigns, block them or tag them immediately.
- AI-CTI systems can effectively combine threat intelligence received from various external sources such as discussion boards in the dark web, hacking patterns used, zero-day vulnerabilities, latest attacking trends, etc. This information can be used by the system to proactively determine when and how a cyber-attack might make its way to the organization. This will give the cyber advisors enough lead time to close the vulnerability or mitigate the risk.
- AI can be used to automatically learn the network topology, the traffic pattern and suggest security improvements. AI algorithms can be used to scour through large volumes of data, analyze them and identify anomalies. The AI algorithm can be trained to take some predefined steps in the event of an attack through inputs from the subject matter experts and overtime it will learn these response pattern and make its own decisions.
- ML can be used to learn and create a behavior pattern for your devices. AI can use this pattern to detect any anomalies on the behavior from these devices such as unusual amounts of downloads, uploads, financial transactions, shipments, data access, sudden change in typing speed, etc. Such activities will then trigger the AI algorithm to immediately flag those devices and block them. Al based antivirus software's can detect unusual behavior from programs rather than depending on traditional methods such as matching signatures of known malwares.

Design & Implementation—Design the AI solution using the selected data sets, platform, AI algorithms and tools. Specify what is the expected output from the system and who will be using the system. The solution is then implemented in a development environment.

AI Training—Start building the AI intelligence using reviewed and approved data sets that were pre-defined as per our algorithm requirements. Exchanging and collaborating with other threat researchers and security professionals through various open-source threat intelligence platforms like Open threat exchange, Facebook threat exchange or IBM X-Force exchange is very critical for improving the efficiency and effectiveness of the AI algorithm in detecting new threats. Such collaborations help the AI solution to keep up to speed with the latest attack trends and vulnerabilities. Train cyber analyst for AI by upskilling their employees and improving their knowledge in the logic underpinning the AI algorithms and its behavior. Create proper interfaces that can enable them to interact with the AI tools and incident alerts. Provide the cyber analyst with a database for them to input information based on the customer feedback after an incident is raised.

Optimize & Validate—Optimize the AI based CTI system through fine tuning, patching and hardening to maximize the effectiveness and efficiency of the system. Deploy Security orchestration, automation and response (SOAR) technologies to improve incident alert triage quality, defining a standardized incident response workflow as well as improving the security and operations management. Create automated templates in SOAR for low-risk incidents with the actions to be taken such blacklisting IP, blocking IP, etc. Access and validate the performance of the system with respect to the initial requirements that were specified, ensuring they are functioning as intended.

Integration & Testing—Start integrating the system with the various applications that are part of the scope of this project. Applications such as SIEM can be used to integrate various security systems in the organization working in silos and then SIEM can be integrated to our AI based CTI to automate the tasks. The main hardware should not be connected to the internet. Test the system thoroughly to ensure the security and privacy requirements are met and data is appropriately protected with encryption. Use penetration testing and vulnerability assessment to detect the threats.

Deployment—The AI based CTI solution is deployed in the production environment. Continuously monitor the performance of the system, patching and hardening the system as and when required.

Governance—A clear, transparent governance process needs to be implemented and adhered to monitor the performance of the AI-CTI solution. The controls should include checks on the roles and responsibilities, segregation of duties (Mehmood et al. 2019), AI algorithm behavior abnormalities, risk tolerance, output verification and key performance indicators to measure the success of the program. It should allow the cyber analysts to assess and refine their Incident Response processes, Mean Time to Detect and Mean Time to Respond (MTTD and MTTR) matrix. The data sets and the initial requirements specified in the planning phase must be periodically re-evaluated to ensure the quality and effectiveness of implemented AI based CTI system. We should also look at documenting a business continuity plan (BCP) in case the algorithm goes rogue.

Continues Improvement—Once the organization and the cyber advisors are confident with the performance and the logic controlling the AI based CTI system, we should start looking at expanding the scope of tasks to be automated and include

more complex tasks to maximize the productivity of the program. Moreover, SMEs should continuously monitor and review each process so that the products efficiently and effectiveness improves over time.

Future research on various AI based cyberattacks by nefarious actors, their prevention and mitigation methods can further bridge the knowledge gap and secure the defense against such cyberattacks. The application of AI is a relatively new trend in combating cybercrimes and is still evolving. Further research should be conducted to improve the maturity of AI based cyber threat intelligence, their design, architecture and implementation. International Government bodies should also research and study how best they can legally cooperate and fight cybercrimes. The roadmap was evaluated and developed specifically for an SME; therefore larger organizations might have added requirements to be addressed in the roadmap.

Considering the generic audience with backgrounds from different industries and having their unique requirement, we have restricted ourselves from discussing any vendor application or solution in detail. This gives us the opportunity to create a general guideline for SMEs that want to develop their own AI based CTI application as well as helping them negotiate with third-party service providers to make an educated and detailed blueprint to support their strategic decision on how they want to implement an AI based CTI system in their infrastructure.

References

Aasriya, N. Al. (2021). *International Journal of Technology, Innovation and Management (IJTIM), 1*(Special Issue 1), 90–104.

Aburayya, A., Alshurideh, M., Al Marzouqi, A., Al Diabat, O., Alfarsi, A., Suson, R., Salloum, S. A., Alawadhi, D., & Alzarouni, A. (2020). Critical success factors affecting the implementation of tqm in public hospitals: A case study in UAE Hospitals. *Systematic Reviews in Pharmacy*, *11*(10). https://doi.org/10.31838/srp.2020.10.39.

Ahmad, A., Alshurideh, M. T., Al Kurdi, B. H., & Salloum, S. A. (2021). Factors impacts organization digital transformation and organization decision making during Covid19 Pandemic. In *Studies in Systems, Decision and Control* (Vol. 334). https://doi.org/10.1007/978-3-030-67151-8_6.

Ahmed, A., Alshurideh, M., Al Kurdi, B., & Salloum, S. A. (2021). Digital transformation and organizational operational decision making: A systematic review. In *Advances in Intelligent Systems and Computing: Vol. 1261 AISC* (Issue September). Springer International Publishing. https://doi.org/10.1007/978-3-030-58669-0_63.

Akhtar, A., Akhtar, S., Bakhtawar, B., Kashif, A. A., Aziz, N., & Javeid, M. S. (2021). COVID-19 detection from CBC using machine learning techniques. *International Journal of Technology, Innovation and Management (IJTIM)*, *1*(2), 65–78. https://doi.org/10.54489/ijtim.v1i2.22.

Akour, I., Alshurideh, M., Al Kurdi, B., Al Ali, A., & Salloum, S. (2021). Using machine learning algorithms to predict people's intention to use mobile learning platforms during the COVID-19 pandemic: machine learning approach. *JMIR Medical Education, 7*(1), 1–17.

Al Ali, A. (2021). The impact of information sharing and quality assurance on customer service at UAE banking sector. *International Journal of Technology, Innovation and Management (IJTIM)*, *1*(1), 1–17. https://doi.org/10.54489/ijtim.v1i1.10.

Al Kurdi, B., Alshurideh, M., Nuseir, M., Aburayya, A., & Salloum, S. A. (2021). The effects of subjective norm on the intention to use social media networks: An exploratory study using

PLS-SEM and machine learning approach. *Advanced Machine Learning Technologies and Applications: Proceedings of AMLTA, 2021*, 581–592.

Al Shebli, K., Said, R. A., Taleb, N., Ghazal, T. M., Alshurideh, M. T., & Alzoubi, H. M. (2021). RTA's Employees' perceptions toward the efficiency of artificial intelligence and big data utilization in providing smart services to the residents of Dubai. *The International Conference on Artificial Intelligence and Computer Vision*, 573–585.

Al Suwaidi, F., Alshurideh, M., Al Kurdi, B., & Salloum, S. A. (2021). The impact of innovation management in SMEs performance: A systematic review. In *Advances in Intelligent Systems and Computing*, Vol. 1261 AISC. https://doi.org/10.1007/978-3-030-58669-0_64.

AlHamad, A., Alshurideh, M., Alomari, K., Kurdi, B. A., Alzoubi, H., Hamouche, S., & Al-Hawary, S. (2022). The effect of electronic human resources management on organizational health of telecommunications companies in Jordan. *International Journal of Data and Network Science, 6*(2), 429–438. https://doi.org/10.5267/j.ijdns.2021.12.011.

Alhamad, A. Q. M., Akour, I., Alshurideh, M., Al-Hamad, A. Q., Kurdi, B. A., & Alzoubi, H. (2021). Predicting the intention to use google glass: A comparative approach using machine learning models and PLS-SEM. *International Journal of Data and Network Science, 5*(3), 311–320. https://doi.org/10.5267/j.ijdns.2021.6.002.

Alhashmi, S. F. S., Alshurideh, M., Al Kurdi, B., & Salloum, S. A. (2020). A systematic review of the factors affecting the artificial intelligence implementation in the health care sector. In *Advances in Intelligent Systems and Computing*, Vol. 1153 AISC. https://doi.org/10.1007/978-3-030-44289-7_4.

Ali, N., Ahmed, A., Anum, L., Ghazal, T. M., Abbas, S., Khan, M. A., … & Ahmad, M. (2021). Modelling supply chain information collaboration empowered with machine learning technique. *Intelligent Automation and Soft Computing*, *30*(1), 243–257.

Ali, N., M. Ghazal, T., Ahmed, A., Abbas, S., A. Khan, M., Alzoubi, H., Farooq, U., Ahmad, M., & Adnan Khan, M. (2022). Fusion-based supply chain collaboration using machine learning techniques. *Intelligent Automation & Soft Computing*, *31*(3), 1671–1687. https://doi.org/10.32604/iasc.2022.019892.

Alkalha, Z., Al-Zu'bi, Z., Al-Dmour, H., Alshurideh, M., & Masa'deh, R. (2012). Investigating the effects of human resource policies on organizational performance: An empirical study on commercial banks operating in Jordan. *European Journal of Economics, Finance and Administrative Sciences*, *51*(1), 44–64.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science, 3*, 6.

Almaazmi, J., Alshurideh, M., Al Kurdi, B., & Salloum, S. A. (2020). The effect of digital transformation on product innovation: A critical review. *International Conference on Advanced Intelligent Systems and Informatics*, 731–741.

AlMehrzi, A., Alshurideh, M., & Al Kurdi, B. (2020). Investigation of the key internal factors influencing knowledge management, employment, and Organisational performance: A qualitative study of the UAE hospitality sector. *International Journal of Innovation, Creativity and Change, 14*(1), 1369–1394.

Alnazer, N. N., Alnuaimi, M. A., & Alzoubi, H. M. (2017a). Analysing the appropriate cognitive styles and its effect on strategic innovation in Jordanian universities. *International Journal of Business Excellence, 13*(1), 127–140.

Alnuaimi, M., Alzoubi, H. M., Ajelat, D., & Alzoubi, A. A. (2021a). Towards intelligent organisations: An empirical investigation of learning orientation's role in technical innovation. *International Journal of Innovation and Learning, 29*(2), 207–221.

AlShamsi, M., Salloum, S. A., Alshurideh, M., & Abdallah, S. (2021). Artificial intelligence and blockchain for transparency in governance. In *Artificial Intelligence for Sustainable Development: Theory, Practice and Future Applications* (pp. 219–230). Springer.

AlShehhi, H., Alshurideh, M., Al Kurdi, B., & Salloum, S. A. (2020). The impact of ethical leadership on employees performance: A systematic review. *International Conference on Advanced Intelligent Systems and Informatics*, 417–426.

Alshraideh, A., Al-Lozi, M., & Alshurideh, M. (2017). The impact of training strategy on organizational loyalty via the mediating variables of organizational satisfaction and organizational performance: An empirical study on Jordanian agricultural credit corporation staff. *Journal of Social Sciences (COES&RJ-JSS)*, *6*, 383–394.

Alshurideh, M. T., Al Kurdi, B., Alzoubi, H. M., Sahawneh, N., & Al-kassem, A. H. (2022a). Fuzzy assisted human resource management for supply chain management issues. *Annals of Operations Research, 24*(1), 1–19.

Alshurideh, M. (2022). Does electronic customer relationship management (E-CRM) affect service quality at private hospitals in Jordan? *Uncertain Supply Chain Management, 10*(2), 1–8.

AlShurideh, M., Alsharari, N. M., & Al Kurdi, B. (2019). Supply chain integration and customer relationship management in the airline logistics. *Theoretical Economics Letters, 9*(02), 392–414.

Alshurideh, M., Gasaymeh, A., Ahmed, G., Alzoubi, H., & Kurd, B. A. (2020a). Loyalty program effectiveness: Theoretical reviews and practical proofs. *Uncertain Supply Chain Management*, *8*(3). https://doi.org/10.5267/j.uscm.2020a.2.003.

Alshurideh, M, Al Kurdi, B., Alzoubi, H., Ghazal, T., Said, R., AlHamad, A., Hamadneh, S., Sahawneh, N., & Al-kassem, A. (2022b). Fuzzy assisted human resource management for supply chain management issues. *Annals of Operations Research*, 1–19.

Alshurideh, Muhammad, Al Kurdi, B., Salloum, S. A., Arpaci, I., & Al-Emran, M. (2020b). Predicting the actual use of m-learning systems: A comparative approach using PLS-SEM and machine learning algorithms. *Interactive Learning Environments*, 1–15.

Alshurideh, M., Gasaymeh, A., Ahmed, G., Alzoubi, H., & Kurd, B. A. (2020c). Loyalty program effectiveness: Theoretical reviews and practical proofs. *Uncertain Supply Chain Management, 8*(3), 599–612. https://doi.org/10.5267/j.uscm.2020.2.003.

Altamony, H., Masa'deh, R. M. T., Alshurideh, M., & Obeidat, B. Y. (2012). Information systems for competitive advantage: Implementation of an organisational strategic management process. *Innovation and Sustainable Competitive Advantage: From Regional Development to World Economies—Proceedings of the 18th International Business Information Management Association Conference*, *1*.

Alzoubi, H., & Ahmed, G. (2019). Do total quality management (TQM) practices Improve Organisational success? A case study of electronics industry in the UAE. *International Journal of Economics and Business Research, 17*(4), 459–472.

Alzoubi, Ali. (2021a). The impact of process quality and quality control on organizational competitiveness at 5-star hotels in Dubai. *International Journal of Technology, Innovation and Management (IJTIM)*, *1*(1), 54–68. https://doi.org/10.54489/ijtim.v1i1.14.

Alzoubi, Asem. (2021b). Renewable Green hydrogen energy impact on sustainability performance. *International Journal of Computations, Information and Manufacturing (IJCIM)*, *1*(1), 94–110. https://doi.org/10.54489/ijcim.v1i1.46.

Alzoubi, H., Alshurideh, M., Kurdi, B. A., & Inairat, M. (2020a). Do perceived service value, quality, price fairness and service recovery shape customer satisfaction and delight? A practical study in the service telecommunication context. *Uncertain Supply Chain Management*, *8*(3). https://doi.org/10.5267/j.uscm.2020a.2.005.

Alzoubi, H., & Yanamandra, R. (2020). Investigating the mediating role of information sharing strategy on agile supply chain in supply chain performance. *Uncertain Supply Chain Management*, *8*(2), 273–284.

Alzoubi, H. M., Vij, M., Vij, A., & Hanaysha, J. R. (2021a). What leads guests to satisfaction and Loyalty in UAE Five-Star Hotels? AHP analysis to service quality dimensions. *enlightening tourism. A Pathmaking Journal, 11*(1), 102–135.

Alzoubi, H., Ahmed, G., Al-Gasaymeh, A., & Kurdi, B. (2020b). Empirical study on sustainable supply chain strategies and its impact on competitive priorities: The mediating role of supply chain collaboration. *Management Science Letters, 10*(3), 703–708.

Alzoubi, H., Alshurideh, M., Kurdi, B. A., Akour, I., & Azi, R. (2022). Does BLE technology contribute towards improving marketing strategies, customers' satisfaction and loyalty? The role

of open innovation. *International Journal of Data and Network Science, 6*(2), 449–460. https://doi.org/10.5267/j.ijdns.2021.12.009.

Alzoubi, H., Alshurideh, M., Kurdi, B. A., & Inairat, M. (2020c). Do perceived service value, quality, price fairness and service recovery shape customer satisfaction and delight? A practical study in the service telecommunication context. *Uncertain Supply Chain Management, 8*(3), 579–588. https://doi.org/10.5267/j.uscm.2020.2.005.

Alzoubi, H. M., Ahmed, G., Al-Gasaymeh, A., & Al Kurdi, B. (2020d). Empirical study on sustainable supply chain strategies and its impact on competitive priorities: The mediating role of supply chain collaboration. *Management Science Letters, 10*(3), 703–708. https://doi.org/10.5267/j.msl.2019.9.008.

Alzoubi, H. M., & Aziz, R. (2021a). Does emotional intelligence contribute to quality of strategic decisions? The mediating role of open innovation. *Journal of Open Innovation: Technology, Market, and Complexity, 7*(2), 130. https://doi.org/10.3390/joitmc7020130.

Alzoubi, H. M., & Yanamandra, R. (2020). Investigating the mediating role of information sharing strategy on agile supply chain. *Uncertain Supply Chain Management, 8*(2), 273–284. https://doi.org/10.5267/j.uscm.2019.12.004.

Alzoubi, H. M., Alshurideh, M., & Ghazal, T. M. (2021b). Integrating BLE beacon technology with intelligent information systems IIS for operations' performance: A managerial perspective. *The International Conference on Artificial Intelligence and Computer Vision*, 527–538.

Alzoubi, H. M., & Aziz, R. (2021b). Does emotional intelligence contribute to quality of strategic decisions? *The Mediating Role of Open Innovation.*

Aziz, N., & Aftab, S. (2021). Data mining framework for nutrition ranking Nauman Aziz. *International Journal of Technology, Innovation and Management, 1*(1), 90–100.

Bless, C., Higson-Smith, C., & Kagee, A. (2000). Fundamentals of social research methods. *An African Perspective*, *3.*

Darraj, E., Sample, C., & Justice, C. (2019). Artificial intelligence cybersecurity framework: Preparing for the here and now with ai. *ECCWS 2019 18th European Conference on Cyber Warfare and Security*, 132.

Davies, A. (2020). *AI Software Development life cycle: Explained*. DevTeam.Space.

Emerita, A. (2021). Convergence between blockchain and the internet of things Alma Emerita. *International Journal of Technology, Innovation and Management (IJTIM)*, *1*(1), 35–56.

Farouk, M. (2021). The universal artificial intelligence efforts to face coronavirus COVID-19. *International Journal of Computations, Information and Manufacturing (IJCIM)*, *1*(1), 77–93. https://doi.org/10.54489/ijcim.v1i1.47.

Ghannajeh, A. M., AlShurideh, M., Zu'bi, M. F., Abuhamad, A., Rumman, G. A., Suifan, T., & Akhorshaideh, A. H. O. (2015). A qualitative analysis of product innovation in Jordan's pharmaceutical sector. *European Scientific Journal*, *11*(4), 474–503.

Ghazal, T. M., Hasan, M. K., Alshurideh, M. T., Alzoubi, H. M., Ahmad, M., Akbar, S. S., Al Kurdi, B., & Akour, I. A. (2021). IoT for smart cities: Machine learning approaches in smart healthcare—a review. *Future Internet, 13*(8), 218. https://doi.org/10.3390/fi13080218.

Guergov, S., & Radwan, N. (2021). Blockchain convergence: Analysis of issues affecting IoT, AI and blockchain. *International Journal of Computations, Information and Manufacturing (IJCIM)*, *1*(1), 1–17. https://doi.org/10.54489/ijcim.v1i1.48.

Hamadneh, S., Pedersen, O., Alshurideh, M., Kurdi, B. Al, & Alzoubi, H. (2021). An investigation of the role of supply chain visibility into the scottish blood supply chain. *Journal of Legal, Ethical and Regulatory Issues*, *24*(Special Issue 1), 1–12.

Hanaysha, J. R., Al Shaikh, M. E., & Alzoubi, H. M. (2021a). Importance of marketing mix elements in determining consumer purchase decision in the retail market. *Internation Journal of Service Science, 12*(6), 56–72.

Hanaysha, J. R., Al-Shaikh, M. E., Joghee, S., & Alzoubi, H. (2021b). Impact of innovation capabilities on business sustainability in small and medium enterprises. *FIIB Business Review*, 1–12.https://doi.org/10.1177/23197145211042232.

Harahsheh, A. A., Houssien, A. M. A., & Alshurideh, M. T. (2021). The effect of transformational leadership on achieving effective decisions in the presence of psychological capital as an intermediate variable in Private Jordanian. In *The Effect of Coronavirus Disease (COVID-19) on Business Intelligence* (pp. 243–221). Springer Nature.

Hayajneh, N., Suifan, T., Obeidat, B., Abuhashesh, M., Alshurideh, M., & Masa'deh, R. (2021). The relationship between organizational changes and job satisfaction through the mediating role of job stress in the Jordanian telecommunication sector. *Management Science Letters*, *11*(1), 315–326.

Joghee, S., Alzoubi, H. M., & Dubey, A. R. (2020). Decisions effectiveness of FDI investment biases at real estate industry: Empirical evidence from Dubai smart city projects. *International Journal of Scientific and Technology Research, 9*(3), 3499–3503.

Kashif, A. A., Bakhtawar, B., Akhtar, A., Akhtar, S., Aziz, N., & Javeid, M. S. (2021). Treatment response prediction in hepatitis C Patients using machine learning techniques. *International Journal of Technology, Innovation and Management (IJTIM)*, *1*(2), 79–89. https://doi.org/10.54489/ijtim.v1i2.24.

Khan, M. A. (2021). Challenges facing the application of iot in medicine and healthcare. *International Journal of Computations, Information and Manufacturing (IJCIM)*, *1*(1), 39–55. https://doi.org/10.54489/ijcim.v1i1.32.

Lee, C., & Ahmed, G. (2021). Improving IoT privacy, data protection and security concerns. *International Journal of Technology, Innovation and Management (IJTIM)*, *1*(1), 18–33. https://doi.org/10.54489/ijtim.v1i1.12.

Lee, K. L., Azmi, N. A. N., Hanaysha, J. R., Alzoubi, H. M., & Alshurideh, M. T. (2022a). The effect of digital supply chain on organizational performance: An empirical study in Malaysia manufacturing industry. *Uncertain Supply Chain Management, 10*(2), 495–510. https://doi.org/10.5267/j.uscm.2021.12.002.

Lee, K. L., Romzi, P. N., Hanaysha, J. R., Alzoubi, H. M., & Alshurideh, M. (2022b). Investigating the impact of benefits and challenges of IOT adoption on supply chain performance and organizational performance: An empirical study in Malaysia. *Uncertain Supply Chain Management, 10*(2), 537–550. https://doi.org/10.5267/j.uscm.2021.11.009.

Lee, R. M. (2020). *2020 SANS cyber threat intelligence (CTI) survey*. Sans.Org.

Lidestri, N. (2018). The impact of artificial intelligence in cybersecurity. *ProQuest Dissertations and Theses, 6*(2), 709–717.

McCarthy, J. (2007). *What is artificial intelligence?* (pp. 1–15). Stanford University. http://faculty.otterbein.edu/dstucki/inst4200/whatisai.pdf.

Mehmood, T. (2021). Does information technology competencies and fleet management. *International Journal of Technology, Innovation and Management, 1*(1), 14–41.

Mehmood, T., Alzoubi, H. M., Alshurideh, M., Al-Gasaymeh, A., & Ahmed, G. (2019). Schumpeterian entrepreneurship theory: Evolution and relevance. *Academy of Entrepreneurship Journal, 25*(4), 1–10.

Miller, D. (2021). The best practice of teach computer science students to use paper prototyping. *International Journal of Technology, Innovation and Management (IJTIM)*, *1*(2), 42–63. https://doi.org/10.54489/ijtim.v1i2.17.

Mondol, E. P. (2021). The impact of block chain and smart inventory system on supply chain performance at retail industry. *International Journal of Computations, Information and Manufacturing (IJCIM)*, *1*(1), 56–76. https://doi.org/10.54489/ijcim.v1i1.30.

Naqvi, R., Soomro, T. R., Alzoubi, H. M., Ghazal, T. M., & Alshurideh, M. T. (2021). The nexus between big data and decision-making: a study of big data techniques and technologies. *The International Conference on Artificial Intelligence and Computer Vision*, 838–853.

Nuseir, M. T., Al Kurdi, B. H., Alshurideh, M. T., & Alzoubi, H. M. (2021). Gender discrimination at workplace: Do artificial intelligence (AI) and machine learning (ML) have opinions about it. *The International Conference on Artificial Intelligence and Computer Vision*, 301–316.

Obaid, A. J. (2021). Assessment of smart home assistants as an IoT. *International Journal of Computations, Information and Manufacturing (IJCIM)*, *1*(1), 18–36. https://doi.org/10.54489/ijcim.v1i1.34.

Radwan, N., & Farouk, M. (2021). The growth of internet of things (IoT) in the management of healthcare issues and healthcare policy development. *International Journal of Technology, Innovation and Management (IJTIM)*, *1*(1), 69–84. https://doi.org/10.54489/ijtim.v1i1.8.

Salloum, S. A., Alshurideh, M., Elnagar, A., & Shaalan, K. (2020). Machine learning and deep learning techniques for cybersecurity: A review. *Joint European-US Workshop on Applications of Invariance in Computer Vision*, 50–57.

Singh, R., & Singh, P. K. (2021). Integrating blockchain technology with IoT. *CEUR Workshop Proceedings, 2786*(1), 81–82.

Svoboda, P., Ghazal, T. M., Afifi, M. A. M., Kalra, D., Alshurideh, M. T., & Alzoubi, H. M. (2021). Information systems integration to enhance operational customer relationship management in the pharmaceutical industry. *The International Conference on Artificial Intelligence and Computer Vision*, 553–572.

Truong, T. C., Diep, Q. B., & Zelinka, I. (2020). Artificial intelligence in the cyber domain: Offense and defense. *Symmetry, 12*(3), 410.

Yousuf, H., Zainal, A. Y., Alshurideh, M., & Salloum, S. A. (2021). Artificial intelligence models in power system analysis. In *Artificial Intelligence for Sustainable Development: Theory, Practice and Future Applications* (pp. 231–242). Springer.

Zu'bi, Z., Al-Lozi, M., Dahiyat, S., Alshurideh, M., & Al Majali, A. (2012). Examining the effects of quality management practices on product variety. *European Journal of Economics, Finance and Administrative Sciences*, *51*(1), 123–139.