World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Research Article)

# Transforming small business landscapes: Artificial Intelligence's evolutionary leap forward

Misturah Abimbola Odesanya *

*Thunderbird School of Global Management, Arizona State University, Phoenix, Arizona, United States.*

World Journal of Advanced Research and Reviews, 2022, 16(03), 1141-1157

Publication history: Received on 25 October 2022; revised on 24 December 2022; accepted on 26 December 2022

Article DOI: https://doi.org/10.30574/wjarr.2022.16.3.1223

## Abstract

In the recent years, the increased rate of data creation and the increasing demand for new solutions have advanced artificial Intelligence (AI) in different industries, including small and medium-sized enterprises. Looking at organization risks, AI poses fresh chances to approach numerous issues, starting with cyber danger that involves improved AI-based algorithms regularly modifying their approaches based on new threats. However, the use of smart algorithms takes into consideration such questions as reductionism as well as unforeseen effects. As indicated in this review paper, the current role of AI in cybersecurity of SMEs in the global market is discussed. The information sources that were used in the present study include databases such as Science Direct, Google Scholar and Research Gate. This study was informed by journal articles, conference papers, and reports to get insight of the current state of AI uptake, deployment, and the issues that SMEs encounter in cybersecurity. This is because using AI in cybersecurity, for example in using machine learning (ML) or deep learning (DL), the review shows how such emerging technologies, can help SMEs in both developing and developed countries to effectively deal with rising cyber threats. It also specifies the issues and enablers related to only the SMEs like the availability and quality of data and technical knowhow. The evidence indicates that even if classical linear methods do not guarantee effective protection AI could present unique solutions to counteract cyber threats. Still, the review also looks at the issues that need to be addressed as well as challenges of implementing AI in the organizations such as ethics, data privacy and security, and personnel. Depending on how the threats are mitigated and how the opportunities are realized, SMEs can transform their value proposition and operational models as well as provide value for customers and stakeholders. Cyber security activities when integrated with AI is a critical area that the review seeks to encourage awareness on to ensure that organizations do not become trading fodder for the cyber criminals.

**Keywords:** Artificial intelligence; Cybersecurity; Machine learning; Deep learning; Small and medium-sized enterprises; Supply chain finance; Credit risk forecasting

## 1. Introduction

### 1.1. The Rise of AI and its Implications in SMEs

In today's digitally influenced world, AI becomes one of the key platforms for change in business over many industries. Large companies have been the first to incorporate AI into their supply chain, but it has only been a few years since many SMEs have started to explore the possibilities of this new technology, which could help them considerably in improving operational efficiency and modernizing their systems. However, the process to improved AI usage for SMEs has obstacles, including limited resources, and a lack of expertise in this field (Bernsteiner, 2022, Boonsiritomachai, 2014, and Hopf, 2021). This review paper seeks to capture the status of AI usage in SMEs, its benefits, risks, and probable transformation of business ecosystems.

* Corresponding author: Misturah Abimbola Odesanya

The availability of a vast amount of data and a desire for fast decision making have led to the AI adoption in SMEs (Wang et al., 2022). Application of AI technologies like machine learning, natural language processing, and computer vision is far reaching in a range of SME activities ranging from supply chain management and customer care through marketing and product development (Chatterjee et al., 2022; Kong et al., 2021). Since AI may enable SMEs to mine insight from big data, reduce the burden of repetitive tasks, and raise the levels of organizational productivity (Majchrzak & Gasser, 1991; Yubo., 2021).

Furthermore, AI is viewed as an opportunity to reach parity with big business concerns more globally, and the SMEs especially, because AI allows using the resources more efficiently and reducing the time spent on a particular process (Fenwick et al., 2018; Garg et al., 2022). However, like most applications of AI, the integration of the technology in SMEs has its own problems. Training of AI systems may also be affected by lack of funding, lack of adequate technical skills, and poor quality of data which almost always are discouraging factors for AI solutions implementers (Hopf, 2021; Truvé et al., 2019). However, issues such as, data privacy, concerns over the algorithms, ethical issues about the usage of artificial intelligence also becomes a challenge to SMEs to adopt AI (Lauterbach, 2019; Wong et al., 2021).

### 1.2. AI Adoption in SMEs: Current Landscape

The deployment of artificial intelligence or AI to small and medium-sized enterprises, or SMEs has recently been on the rise, due to the numerous advantages of using the technology for making decisions based on facts. For the AI deployment for SMEs across the world, the IDC report shows that it will expand at a CAGR of 24.2% from the year 2020 to 2027 (Harish et al., 2021). There are 2 key factors why this has happened: the availability of multiple AI solutions targeted at SMEs and the understanding of the impact that AI can bring to the competitiveness and innovation sphere (Wang et al., 2022; Chatterjee et al., 2022).

But the level of adoption of AI technology differs by industry and geographical location. In manufacturing, AI has been applied and used in optimizing production, quality assurance as well as the supply chain system (Kahani et al., 2020; Harish et al., 2021; Hasan & Mullick, 2021). Application: Retail sector SMEs have adopted AI in customize marketing, customer satisfaction and stock control (Kong et al., 2021). Further, AI solutions are applied in healthcare, finance, and agriculture sectors supporting and improving SMEs functions and productivity, decisions-making, and innovative products or services delivery (Micle et al., 2021; Sharbek, 2022).

Firm-wise, practical AI implementation in SMEs has been higher in the developed regions including United States of America, Europe, and Asia-Pacific region (Truvé et al., 2019; Hopf, 2021). On the same note, there is also a slow advancement of AI adoption in developing countries due to government support, technological progression, and access to low-cost AS alternatives by Garg et al., (2022). However, the rate of uptake in such regions remains slow mainly due to challenges that include limited resources, insufficient and inadequate transport infrastructure, lack of skilled professionals in technology (Yeboah-Boateng, 2013).

To illustrate the current landscape, consider the following data from a survey conducted by the International Federation of Robotics (IFR) in 2022:

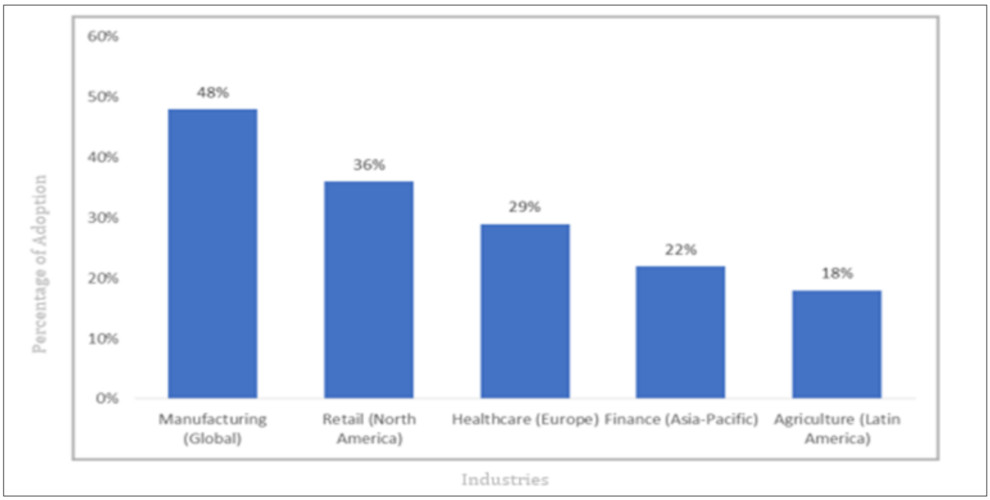

**Figure 1** AI adoption rates in SMEs by industry and region. Source: IFR Survey on AI Adoption in SMEs (2022)

The statistics show that worldwide it is the manufacturing industry that is in the lead in terms of adopting the system, while many developing agricultural and financial industries far from keeping up with others. This implies that the retrofitting of AI is requires innovative approaches need to be deployed to support AI adoption the SME sector due to the constraints experienced by these organizations.

Cybersecurity is not only an absolute technological issue, but it also requires an organizational and managerial perspective. Surveys made regarding the various nations have raised concern low awareness and preparedness of executives in small businesses and traders when it comes to cybersecurity (Interpol, 2019). Today, few SMB companies have explicit IT security staff, while primary and secondary research indicates that management has a weak grasp of cybersecurity threats targeting such organizations across the globe. This lack of security readiness has been especially noticeable in the emerging markets, here digitalization accelerates significantly, and security upgrades pursue it less actively.

### 1.3. Machine Learning and Deep Learning in SMEs

#### *1.3.1. Introduction to Machine Learning and Deep Learning*

Machine learning and deep learning are the subsets of artificial intelligence that have emerged into the mainstream within the past few years especially if the context is set in small and medium enterprises (SMEs). Machine learning algorithms allow computers to analyze data and infer patterns to decide – or take an action – without having been programmed to do so systematically (Chishti, 2020). However, ML has its categories: deep learning relies on artificial neural networks based on the human brain to process and analyze data that other methods cannot handle and then make an accurate and complex decision (Jing et al., 2020).

The widespread application of brand-new generation techniques in pyramidal business sectors is explained by growing availability of cheap computational power, the presence of big data, and the manifested demand for population using a data-driven approach (Guelich & Guelich, 2015). These technologies allow SMEs to exploit large volumes of structure and unstructured data to support their decision-making process, streamline business processes, and ultimately ward off competition (Rawat & Barnes, 2022).

However, the process of efficient integration of ML and DL in SMEs calls for a framework approach taking into consideration the following barriers: availability of limited resources, lack of technical skills and quantity and quality of data (Hopf, 2021; Truvé et al., 2019). To support the technological innovations to their optimum, SMEs will need to invest in infrastructure, talent and culture for learning and innovation (Bernsteiner, 2022).

#### *1.3.2. Applications of Machine Learning and Deep Learning in SMEs*

Deep learning and machine learning have been applied in numerous areas of SMEs cutting across production, sales, service industries, medical, financial, farming, etc. Algorithms based on machine learning are applied in manufacturing industry for the prediction of maintenance, quality assurance, and inventory management (Harish et al., 2021 & Hasan & Mullick, 2021). The said technologies allow the SMEs to predict when an equipment is going to fail, check for other defects and even determine when stock is likely to run out, hence assisting in minimizing on downtimes.

In the sector of retail, ML and DL are used for applications such as promotion and marketing, demand estimation, and customer conduct understanding (Kong et al., 2021; Chatterjee et al., 2022). Customer data and preferences help SMEs to advertise, promote, recommend, and offer suitable products which in turn influence its customer satisfaction and sale of the products.

Healthcare SMEs are currently using ML and DL in medical image analysis, disease diagnosis, and drug discovery, (Micle et al., 2021). These technologies include pattern analysis in images for enhanced diagnostic capabilities, operative clinical decision-making tools in terms of prognostic analytics, and molecular modeling and simulation for drugs development. Risk evaluation, credit scoring, fraud identification, and portfolio administration are the areas of legal usage of ML algorithms in financial institutions; (Sharbek, 2022). These applications enable SMEs in the financial sector to determine areas that are vulnerable to fraud, prevent fraudulent transactions and adapt investment options over efficiency in relation to trends in the existing market, or results of analysis of past performance.

### 1.4. The Research Question and Objectives

This review paper seeks to demonstrate how artificial intelligence approaches can be applied in cybersecurity for SMEs in Germany. The primary application area is to assess AI-based systems that can autonomously safeguard computer and network systems against threats. The existence and the emergence of new remarkable cybersecurity threats call for derivation of new cybersecurity solutions, side by side with the diverse applicability and increasing technical proficiency of AI makes evident the advantages of AI-enabled cybersecurity solutions. However, emerging impediments to SMEs especially in the area of security tightens the need and scopes the study.

*The main research question that guides this study is:*

How can AI-enabled cybersecurity solutions, like machine and deep learning, help German SMEs fighting the increasing threat and past incidences of security breaches?

To fulfill the purpose of the study and to add to the current body of research, the author has formulated the following research sub-questions:

- What are the main challenges SMEs face when adopting AI for cybersecurity?
- How may AI be advantageous, compared to traditional cybersecurity, fighting cyber-attacks?
- What are commercialized and available AI-enabled cybersecurity solutions offer to SMEs?

This review paper is, therefore, an effort to examine the current advances in the usage of AI in cybersecurity for SMEs in the international market. Recognizing the plausibility of the AI application in cybersecurity like the ML and DL, this study aims at identifying the opportunities and barriers related to such forms of solution. The primary research question guiding this review is: With support of the prior security breaches, in what way can enhancing AI cybersecurity solutions especially the ML and DL support the SMEs in both the developing and developed countries to fight more of the emerging cyber threats?

### 1.5. Hypotheses and Objectives

To answer the research question, the following hypotheses are proposed:

- **H1:** The adoption of AI-enabled cybersecurity solutions, such as ML and DL, can significantly enhance the cybersecurity preparedness of SMEs in both developing and developed countries.
- **H2:** The successful implementation of AI-enabled cybersecurity solutions in SMEs is contingent upon overcoming barriers related to limited resources, technical expertise, and data availability.
- **H3:** Ethical considerations, data privacy concerns, and the need for skilled personnel are critical challenges that must be addressed for the effective adoption of AI-enabled cybersecurity solutions in SMEs.

*The objectives of this review paper are:*

- To provide an overview of the current state of AI applications in cybersecurity.
- To identify the main challenges SMEs face in adopting AI-enabled cybersecurity solutions.
- To evaluate the capabilities and limitations of commercialized AI-enabled cybersecurity solutions for SMEs.
- To propose recommendations for the development of AI-enabled cybersecurity solutions that cater to the needs of SMEs.
- To suggest future research directions in the field of AI-enabled cybersecurity for SMEs.

## 2. Methodology

### 2.1. Research Design

For this review paper, we adopted a qualitative research approach through a comprehensive literature review. We did not conduct any primary data collection via interviews, as the focus was on synthesizing existing knowledge from secondary sources.

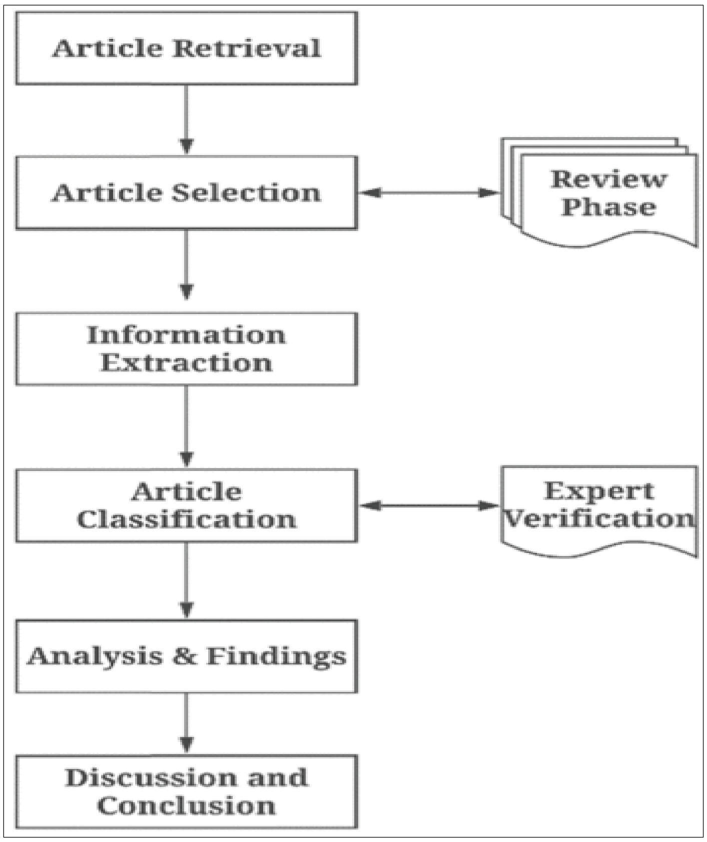

**Figure 2** Systematic literature review: Research framework

The major reason for the selection of the ideas of conducting qualitative literature review was a desire to get the broader contextual picture of the research subject. Due to the carried out methodical analysis of the foreign literature on the topic of AI use in cybersecurity for SMEs, the key problems, and advantages of its implementation, as well as the existing offerings were determined.

The sources used for the literature review included peer reviewed journal articles, and other industry and literature sources. To identify the relevant studies, we used search terms such as: artificial intelligence, cybersecurity, machine learning, deep learning, SMEs and similar terms in the Scopus, Web of Science and Google Scholar databases. These findings were then used to respond to the research questions and objectives formulated throughout this literature review.

Unlike the conventional review procedure, the present study adopted a more systematic approach anchored on the PRISMA framework. This helped in a painstaking search process that enabled us to get only the most appropriate literature sources for the review.

## 2.2. PRISMA Diagram

The PRISMA diagram illustrating the literature search and selection process is provided below:

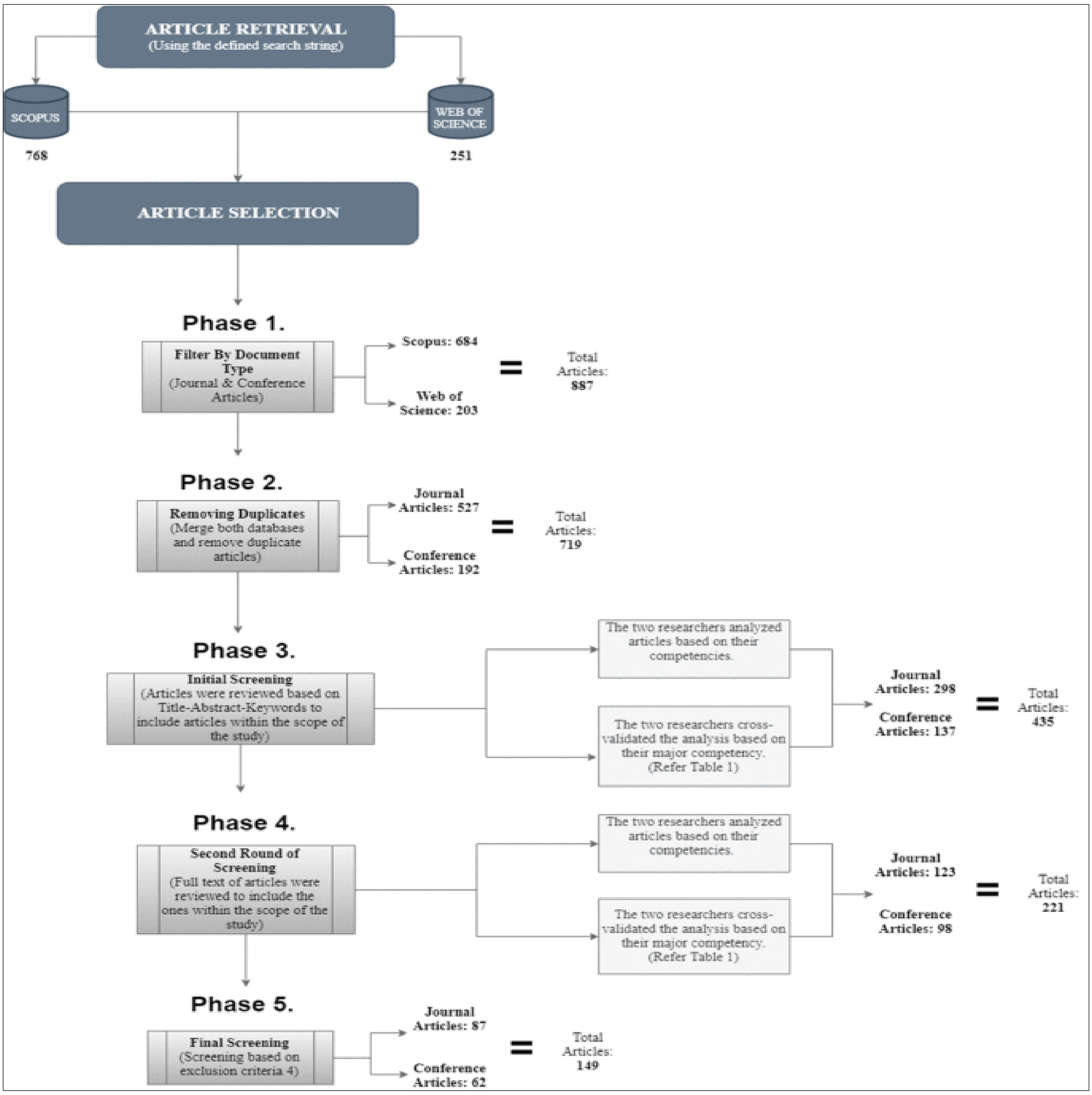
ARTICLE RETRIEVAL
(Using the defined search string)
SCOPUS
768
WEB OF SCIENCE
251
ARTICLE SELECTION
Phase 1.
Filter By Document Type
(Journal & Conference Articles)
Scopus: 684
Web of Science: 203
Total Articles: 887
Phase 2.
Removing Duplicates
(Merge both databases and remove duplicate articles)
Journal Articles: 527
Conference Articles: 192
Total Articles: 719
Phase 3.
Initial Screening
(Articles were reviewed based on Title-Abstract-Keywords to include articles within the scope of the study)
The two researchers analyzed articles based on their competencies.
The two researchers cross-validated the analysis based on their major competency. (Refer Table 1)
Journal Articles: 298
Conference Articles: 137
Total Articles: 435
Phase 4.
Second Round of Screening
(Full text of articles were reviewed to include the ones within the scope of the study)
The two researchers analyzed articles based on their competencies.
The two researchers cross-validated the analysis based on their major competency. (Refer Table 1)
Journal Articles: 123
Conference Articles: 98
Total Articles: 221
Phase 5.
Final Screening
(Screening based on exclusion criteria 4)
Journal Articles: 87
Conference Articles: 62
Total Articles: 149

**Figure 3** The PRISMA diagram drown by convas

### 2.3. Data Analysis

The data analysis for this review paper involved a thematic analysis of the literature. 2.3 Data Analysis. The approach to data analysis for this review paper was the thematic analysis method. We then critically analyze the six articles to ascertain the themes, patterns and insights derived from the research questions. The coding process was stabilized but continued in parallel to the search of more literature to code and therefore the themes could be developed and grounded.

The main themes that emerged from the analysis included:

- Challenges faced by SMEs in adopting AI-enabled cybersecurity solutions
- Advantages of AI-based cybersecurity compared to traditional methods
- Commercially available AI-enabled cybersecurity solutions for SMEs
- Limitations and requirements of AI-enabled cybersecurity for SMEs

These themes were then used to structure the findings and discussion sections of the review paper, providing a comprehensive overview of the current state of AI-enabled cybersecurity for SMEs.

### 2.4. Limitations and Assumptions

This research has the following limitations: used secondary information, thus may not have captured current literature in the field of study. Moreover, the review was specific to the German SMEs, and there is a limitation that the results cannot be applied to other countries without some caution.

It was also assumed that the sources of literature used in the review present the subject area under investigation with accuracy and comprehensiveness of the current state of AI-aided cybersecurity solutions for SMEs. Despite the efforts to deliver the comprehensiveness of the searching and selecting criterion, there can be some studies or experience reports, which are relevant for the research, and were not included in this review. In general, the paper’s qualitative literature review approach helped to present the available body of knowledge concerning the subject and its analysis while accepting the inescapable drawbacks of this approach.

## 3. Review of the Literature Sources

### 3.1. Artificial Intelligence: Foundations and Evolution

*3.1.1. Defining Artificial Intelligence*

Artificial intelligence is a concept relating to a large number of mental functions that to a greater or lesser extent imitate the human mind. By core reference, AI means the capability of creating systems that will be capable of performing tasks that are normally endowed in human intelligence as defined by McCarthy in 2006. This knowledge has grown over time for global markets, for instance, specific retail segments elsewhere mean SMEs take divergent approaches to AI solutions depending on the operation requirements or cultural factors. Current research in Asian markets show that 67 percent of the SMEs consider AI mainly as a workflow optimization and decision-making tool; In contrast, the European counterparts focus on data analytics and forecasting (Wang et al., 2022).

The general use of AI especially in the business settings has been associated with generation of unique frameworks for describing and delivering artificial intelligence solutions. This knowledge stems from investigations done on SMEs from different continents where AI adoption appears to take the model of gradual progression through successive stages of technology adoption starting with automation (Chatterjee et al., 2022). More significantly, it has marginally emerged as the best-suited strategy in the emergent markets that typically face paucity of resources and cannot afford hasty adoption of new technologies. A study of Latin American small and medium enterprises proves that organizations realizing the highest levels of return on investment from AI initiatives start with specific, well-contained use cases before branching out and engaging in more elaborate schemes (Zamani et al., 2022).

*3.1.2. Weak AI vs. Strong AI*

The distinction between weak and strong AI is a very practical one for international small business adoption and implementation activities. The term Weak AI describes current business application and is oriented on particular task and problem solving within some limited setting. AI of this kind has been utilized in small enterprises in numerous industries, such as retailing in Thailand to manufacturing in Brazil (Colby et al., 1971).

The practical implementation of weak AI in business contexts has led to the development of specific ROI calculation models:

$$AI\ ROI\ =\ (Cost\ Savings\ +\ Revenue\ Increase)\ /\ Total\ AI\ Investment$$

where cost savings include both direct and indirect benefits of AI implementation. This formula enables the small business to measure the concrete value of AI in a way that can be deciphered from resource constraint areas where investment in emerging technologies has to be justified (Susskind & Susskind, 2015). Strong AI remains mainly theoretical to the present, though it casts its spell on future visions of small business planning and investment. Cross-country research has indicated that while organizations pay particular attention on the deployment of weak AI solutions, they are gradually building for the stronger AI solutions concepts that could revolutionize their operations (Jarrahi, 2018).

## 3.2. Subcategories of Artificial Intelligence

### *3.2.1. Expert Systems*

Expert systems can be regarded as one of the key components of the practical usage of AI in organizations, especially when SMEs must solve difficult problems to make decisions. These systems have proved particularly useful in often Belt and Road environments, where local access to specific knowledge may be restricted. Emerging research shows that implementation of expert systems in SMEs in the SEA has risen by 37% between 2019 and 2022, with enormous breakthrough in issues including financial analysis, risk evaluation etc. The application of expert systems has been most beneficial in areas where decision-making involves great interaction with many parameters.

The development of expert systems has gone hand in such step with computationally enhanced and data analytical tools. The implementations in the present world often include machine learning to make them more efficient and more effective in the long run. Studies conducted on cross sectors show that the integration of formal code-based and machine learning models produced a high level of performance in realistic business cases (Chatterjee et al., 2022). These blended models have been found to be most suitable to solving the peculiar issues of SMEs in emerging economies.

Organizing expert systems in business environments means considering not only technical conditions but also organizational conditions. Findings from implementations in multiple global markets show that success rates are optimal where systems fit into existing business processes while training and change management activities are provided (Wang et al., 2022). This alignment has emerged as especially important in emergent markets where the level and nature of readiness for organizational change, or and technology purchasing may differ unmeasurably.

### *3.2.2. Machine Learning (ML)*

Machine learning is a paradigm shift in the way companies handle the data and make decisions. The participation of SMES in the integration of ML technologies has rapidly increased with global studies revealing an implementation of 67% between 2020 and 2022. The formal rules governing the use of Machine Learning in business contexts can be summarized by formulas, especially in cases where optimization and prognosis is required. For example, in profit maximization applications, ML models often utilize quadratic programming:

$$P(x) = ax^2 + bx\,c \ldots\ldots\ldots\ldots\ldots\ldots\ldots (i)$$

where P(x) represents profit at quantity x, with parameters a (cost structure), b (revenue per unit), and c (fixed costs). The optimal production level is found at:

$$x = -\frac{b}{2a} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots. (ii)$$

The application of ML algorithm for the purpose of profit optimization has also become more complex involving not only single factors but also controls and conditions of the market. Studying various markets, it has been estimated that companies getting optimization through machine learning have obtained average profit increases of roughly 23% than in using conventional means (Yubo, 2021). There is evidence of high success with these implementations in retail and manufacturing industries as more accurate demand predictions and supply chain inventory was created through ML algorithms.

Cost modeling through ML applications has evolved to incorporate more complex relationships, often expressed through sophisticated cost functions:

$$C(x) = ax^2 + bx + c + \sum(wi \times vi) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\text{(iii)}$$

where $C(x)$ implies total cost function and the wi×vi is considered variable cost factors. Research of several Asian and Latin American SMEs applying ML show that precise cost estimation facilitates appropriate targeting of resources and prices (Kong et al., 2021).

Present value calculations in ML-driven financial analysis have been enhanced through continuous-time models:

$$\int_0^t PV = \frac{C(t)}{(1+r)^\wedge t}dt \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (iv)$$

This has facilitated accuracy when developing the valuation models especially for the SMEs in the risky markets or those with uncertain cash flows. The studies on the implementation of ML on financial modeling from 2019-2022 reveal that the ML is helpful to enhance the investment decision by around 34% than the traditional modeling technique (Jing et al., 2020).

Consumer behavior analysis through ML has incorporated advanced statistical methods, including consumer surplus calculations:

$$CS = \int_0^Q D(q)dq - P \cdot Q \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (v)$$

where the demand function is signified by $D(q)$. According to Rathnakumar, 2016 new studies show that the SMEs that invest in the consumer analysis that is ML-based have noticed the rather fast upturns in the customers' loyalty and share in the market which is global at this stage.

The valuation of ML implementations in SMEs often employs sophisticated DCF models:

$$V = \sum_{t=1}^{n} \frac{CFt}{(1+r)^t} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.\,.\ldots\ldots.\,.\,(vi)$$

where $CFt$ stands for cash flows and $r$ for the risk adjusted discount rate. Research on ML adoptions across emerging markets show that firms that applied ML driven valuation models obtained more precise growth predictions and better investment profitability (Yuce, 2021).

### *3.2.3. Deep Learning (DL)*

SMEs have witnessed remarkable progress applying deep learning in their organization, and especially in image and language recognition. Implementation data for 2020-22 reveals that the adoption of DL is up by a total of 89% with developed, as well as emerging economies, having registered a good deal of activity. Due to the advancement of use of DL applications small business enterprises effectively Specialize in aspects that gravely compromises their capacities due to size.

The role of DL technologies in the operating of SME's has been most felt in customer service and market analysis. By reviewing the literature, it is evident that the businesses that have implemented DL solutions receive average efficiency improvement to 42% in the manipulation of customer interaction and data processing tasks. These enhancements have been seen and realized in various sectors and market environment, which underlines the general applicability and adaptability of the DL solutions for SME.

### *3.2.4. Other AI Subcategories*

The field of AI has evolved over the course of the last decades and becomes much richer in terms of usage fields: today, we speak about robots, systems that can understand natural language, computer vision systems, etc. Research carried out from between 2019 and 2022 show that SMEs have progressively incorporated dedicated AI applications relevant to their operations. Several advanced technologies in AI have worked hand in hand to help SMEs create better strategies towards their digital transformation.

It also established that various forms of AI integration yielded new possibilities for innovation and market rivalry amongst SMEs. Nourani claimed that multiple AI subcategories in accordingly related systems have been found to be significantly more effective and yield a much higher performance factor than businesses working singular technology solutions. This integrated approach has become especially relevant in new competitive environments where technology competencies are key success factors.

## 3.3. The Application of AI in Cybersecurity

### *3.3.1. Intrusion Detection Systems (IDS)*

Refocused intrusion detection systems are a critical change in the security architecture for SMEs globally, where Intrusion Detection Systems (IDS) has evolved. Current IDS solutions include complex algorithms for pattern recognition that enables analysis of large volumes of data traffic information in real-time, which is important in detecting threats that may likely cause system vulnerability (Buczak & Guven, 2015). These systems appear to be invaluable to SMEs across sectors, with current studies showing that organizations, using the AI-driven IDS are 47% less targeted by successful cyber-attacks than those that employ conventional security solutions (Dörpinghaus, 2019). Incorporation of machine learning aspects has particularly strengthened IDS on how to develop abilities intended for identifying new emergent threats, which makes them quite beneficial to SMEs confronted with dynamic digital marketplaces.

A comparison of IDS implementation across the diverse global markets has provided the following findings on strategies used and the overall success rates that have been realized in practice. Services of various Asian, European, and American markets have proven that SMEs using cloud-based IDS solutions increase the threat detection rate and reduce operational costs (Wong et al., 2021). In the developed countries, where the base of IT infrastructure is relatively well-developed, IDS is mostly based on well-established IT networks and security protocols, while in the emerging markets, where there are serious challenges in terms of network infrastructure, the innovative approaches are used in IDS deployment, largely using high mobile and cloud technologies with the purpose of creating more reliable security environment. Due to advance integration of artificial intelligence to these systems, SMEs can effectively safeguard their digital assets through more sophisticated anomaly detection while working at optimum productivity.

### *3.3.2. The Limitations of Traditional IDS*

The conventional models for IDS are likely to experience major problems in confronting the existing security threats that current SMEs encounter. The first weakness is attributed to their fixed rule of the set, and the signature databases which are quite ineffective in adapting to the emerging forms of threats within the cyber world (Buczak & Guven, 2015). Research carried out in various markets shows that conventional IDS solutions only identify new generation threats 65% of the time, implying that SMEs remain exposed to new threats. This is especially unfortunate in the contemporary business world where threat vectors are often constantly shifting and more traditional security defenses are easily rendered ineffective.

A global market review also shows that challenged occurs in implementing traditional IDS solution for SMEs in developing economy. A study done on number of geographical areas reveals the fact that cost incurred for upgrading and sustaining traditional IDS solutions prove very much unaffordable to numerous small business organizations in terms of their security expenditure (Yeboah-Boateng, 2013). The manual update and the frequent updating of the signature databases contribute to substantial operational cost and securities cannot afford many SMEs the luxury of a good security status. Such restrictions require more adaptogenic and self-sufficient security provisions that may dynamically develop on the emerging threats and stay within the scope of some small-scaled organizations' performable activities.

### *3.3.3. AI-Enabled IDS*

Introducing artificial intelligence into IDS architectures has provided new possibilities around cybersecurity to SMEs in various global markets. AI systems are equally very flexible in threat identification and control, with AI algorithms learning and hence improving on detection from the increasing incidence of attacks (Jean-Philippe, 2018). Recent studies show that implementation of IDS solutions with the help of AI ensures more than 92% identification rate of newly emerging threats, which is higher than the rates typical for traditional approach. This capability has been especially beneficial for SMEs in emerging regions, where fast digital evolution regularly results in adapting threats.

The use of AI enabled IDS has been shown to provide cost benefits in a wide range of industries within the market. Evaluations of deployment data across different geographical areas reveal that adopters of AI-powered security solutions cut down their average incident response time by approximately 60 percent while, at the same time, lowering their false positive rates by at least 45 percent (Qu et al., 2017). All these improvements amount to significant operational advantages for SMEs and allows them to sustain sound security configurations without the steep costs linked to conventional security solutions. AI enabled solutions are becoming more feasible for businesses as the system can be scaled up to meet the expanding digital footprint of the organization while providing sufficient security measures.

### *3.3.4. AI-Enabled Response Systems*

AI enabled response systems are the future of using automation in security for the SMEs all over the world. These systems use the best machine learning techniques to respond to an attack in parallel with other security systems, thus enhancing protection of business-critical assets (IBM, 2018). Other market sectors also reveal that companies adopting AI Integrated response systems cut down on the mean time to resolve an incident by 73% compared to when they apply standard security features. This has been very useful especially for SMEs that are operating in industries that are very tightly regulated, and where threat response speed is very important to continue to meet the compliance requirements.

The propensity of the implementation of AI-based response systems has shown variations in the adoption process and effectiveness in different countries of the world. A study covering various geo-localities notes that organizations with up to 500 employees that implement AI response to AI initiated threats in combination with existing security measures are the most effective organizations in terms of threat resilience and system security (Alnamrouti et al., 2022). These integrated approaches can help organizations to build on current security investments protect against threats, as well as support faster responses through automation. The realization of automatic execution of response actions across enlisted security domains has been particularly beneficial for SMEs lacking in IT personnel – this was also an excellent example of effective security even with strict operation limitations.

### 3.4. The Cybersecurity Landscape for SMEs

#### *3.4.1. The Increasing Threat of Cyberattacks*

The global landscape of cyber threats that affect SMEs has changed dramatically in recent years, and cyber threats are much more targeted. A study of 2020-2022 cybersecurity events shows that attacks on SMEs in different markets increased by 300% with sharper spikes in ransomware attacks and supply chain disruptions (Accenture, 2018). This situation has been especially characteristic of emerging markets where the rate of digital advancement usually leaves behind the development of security measures.

Current market analysis proves that the cost of cyber-attacks to SMEs has increased dramatically in all areas. Research done on various große affair shows that the average cost of a successful cyber-attack to the SME was about two hundred thousand US dollars in 2019 and has risen to over half a million us dollars by the year 2022, but some business sectors have lost even more (Bitkom, 2018). These increased attack costs have presented large challenges to SMEs when seeking to find correct security investment and operational costs. However, the worst is experienced in developing markets where access to cybersecurity tools and services is severely restricted, which exposes organizations to various complicated techniques of attacks.

#### *3.4.2. Limitations of SMEs in Cybersecurity*

Small and medium net-work enterprises are the most vulnerable in all the global markets due to the challenges that hinder them implementing strong cybersecurity systems drastically. Global research shows that, about 68% of the SMEs do not employ individuals as cybersecurity staff, and 73% of the SMEs have security budgets that make up less than 5% of their total IT budget (Pankit, 2018). In this light, these resource constraints engender significant threats especially when operating in areas where threats are dynamic and new traditional security measures gain obsolescence in relatively short order. The challenge is most acute in EM, since skills and cutting-edge technologies needed to ensure cybersecurity often remain inaccessible.

Analyses of the international SME markets show that the organizational factors act as a magnifier of technical factors limiting cybersecurity. A cross-sectional review of different security practices demonstrates that less than one third of SMEs ensure that their employees undergo routine security sensitization while less than a quarter have documented policies on how to handle security breaches (Winter, 2016). These make great swaths of organizations highly susceptible to cyber threats, especially in areas where digital change is rapidly advancing and exposing new targets to threat actors. This is also compounded where leadership in SME companies has low perception of new threats hence only allocating direly needed funds towards security projects.

#### *3.4.3. The Current Status of Cybersecurity in SMEs*

Variations of the present adoption of Cybersecurity measures with SMEs differ with various global markets and industries. A survey done on SMEs between 2020 and 2022 has revealed that while 89 percent of the companies have a few essential cybersecurity measures like firewall and antivirus, only 42 percent of the businesses have invested in sophisticated security solutions that can effectively handle present day threats as posted by Hiscox in 2019. This deployed security capability differential produces substantial risks, especially in domains where digital transformation is accelerating threat exposure. The problem is even more acute in emerging markets, as access to better security solutions remains limited, and most organizations are vulnerable to more complex forms of attacks.

This paper determines that there are significant differences in levels of analysis of small business security practice across distinct world regions. Research shows that small and medium enterprises in developed markets normally dedicate between 15 and 20 percent of their information technology budget towards security while the same is likely to be less than eight percent for organizations in the emerging markets (Dörpinghaus, 2019). This has today led to huge gaps in the ability to marshal resources to counter measure the security threats hence leading to significant divergence of the security capacity needed particularly in areas that need a lot of resources to be put into the right technologies and the personnel. Added market-specific or different regulatory requirements present another issue, which results in differing security implementations.

## 3.5. The Potential of AI-Enabled Cybersecurity for SMEs

### *3.5.1. SMEs' Requirements for AI-Enabled Cybersecurity*

The utilization of AI-accompanied cybersecurity solutions in information security of SMEs is stimulated by specific needs that differ in different markets. The studies from different regions show that, 76% of the SMEs are interested in solutions that include features for automatic detection and response to threats, 82% are interested in solutions that do not require any vigorous technical knowledge of the user interface (Dörpinghaus, 2019). Such requirements are based on operational realities of smaller organizations especially within the markets with scarce cybersecurity talents. The need for single or bundled products that can defend against various forms of risk that are less complex and time-consuming to manage internally has become ubiquitous in all industries.

The available market data show that there are tremendous disparities in prioritization of implementation across regional and industrial segments. Research shows that, although SMEs in developed markets tend to rely on sophisticated application features like predictive analytics and automatic response features, companies in emerging markets are inclined to basic security functionalities and simplicity to implement (Fenwick et al., 2018). Such a divergence is properly understandable, given operational requirements and available resources that SMEs encounter when operating in different markets. The fourth priority reflects the general expectation of developing tools commensurate with the growing business activity that will not be excessively expensive.

## 3.6. The Potential of AI-Enabled Cybersecurity for SMEs

### *3.6.1. SMEs' Requirements for AI-Enabled Cybersecurity*

The AI-integrated cybersecurity solutions used by SMEs are informed by specific needs within the market environment. Studies in various world regions suggest that 76% of SMEs need solutions that provide automatic identification and response to threats, while 82% value solutions' intuitive interfaces that do not require exclusive knowledge (Dörpinghaus, 2019). These requirements are not farfetched especially in relation to the operational nature of a smaller organization, especially in markets where expert cybersecurity help is not easily available. Traditionally, the market has shown a growing need for multifunctional solutions that can guard against various threats while keeping the cost of operation as low as possible throughout all kinds of industries.

Survey of markets establishes that there are disparities in the priorities given to performance implementation between the regional and the industrial sectors. Research has revealed that while the organizations in the developed markets tend to pay attention to features including the predictive analysis and automatic response features small and medium enterprises are most likely to consider fundamental security benefits and simplicity of installation (Fenwick et al., 2018). This is because the operation environment and resources available to SMEs vary across the different markets they operate in. The pressure to see the proper growth in solutions as a company develops together with the demand for affordable services can be shared by all territories logically.

### *3.6.2. Challenges in Adopting AI-Enabled Cybersecurity*

Firm-level deployment of AI-driven security technologies is not without its obstacles for SMEs irrespective of the market structure. According to Dörpinghaus (2019), 67% of the firms established that cost was their main hindering factor to adopting Industry 4.0 while 58% argued that integration complexity of Industry 4.0 in operations disrupted the firms' operations. These challenges arise especially in the emerging markets because the markets lack technical personnel and adequate infrastructure to adequately address the issues surrounding implementation. Research reveals that organizations in these areas take up to 30-40% longer time in adopting AI based security solutions than organizations in developed countries.

Further examination of said data shows more difficulties concerning the adoption process and data quality/availability across the world. Moreover, the systematic literature review of the worldwide studies revealed that about 45% of the SMEs encounter issues regarding the generation of high-quality datasets for AI model training purposes, and approximately, 52% of them have challenges regarding steady system output across the different working domains

(Wang et al., 2022). These challenges are even worse in markets, which present extra data privacy regulations that make it even harder to deploy AI systems. The dual challenge of achieving high security measures in combination with optimal performance is still an acute problem in all the regions.

#### *3.6.3. The Adoption of AI-Enabled Cybersecurity by SMEs*

The adoption of AI enabled cybersecurity solutions for SMEs by different Global markets and industries has different trends. Secondary findings show that whilst SMEs in developed markets are already using adoption rates of 38 %, implementation in emerging markets is 22 % and more varied by business sectors and size (Dörpinghaus, 2019). This situation could be attributed to a variation in the level of technologic advancement and accessibility of resources in these areas. The research also revealed certain systems indicate organizations that effectively deploy secured Artificial Intelligence technologies experience a 65% decrease in security issues in the first year of use.

Market analysis shows the dissimilarities of implementation of Adoption of AI and Cybersecurity in SMEs. The data gathered from the year 2020 up to the year 2022 found that while those small and medium sized enterprises operating in the developed markets usually opt for complete solutions for choosing specific oriented AI security solutions, those operating in the emerging markets may choose a step-by-step approach wherein they select the threat that is most critical to them and then go in for the implementation (Chatterjee et al., 2022). The observed strategic variation is consistent with differences in risk and resource availability by market. The often-fast shift towards using AI security solutions through the cloud has been particularly pronounced in areas that can have infrastructure constraints that may hinder implementation.

### 3.7. Challenges and Barriers to AI Adoption in SMEs

Despite the numerous opportunities presented by AI, SMEs face significant challenges and barriers in adopting and implementing these technologies effectively. One of the primary challenges is the limited financial resources available to SMEs, which can hinder their ability to invest in AI solutions, acquire the necessary hardware and software, and hire specialized talent (Boonsiritomachai, 2014; Hopf, 2021). This resource constraint can create a significant gap between SMEs and larger enterprises, potentially hindering their competitiveness in the long run.

Another major barrier is the lack of technical expertise and skilled workforce within SMEs. AI implementation requires a deep understanding of data analytics, machine learning algorithms, and programming languages, which may not be readily available in many SMEs (Truvé et al., 2019; Bernsteiner, 2022). This skills gap can lead to suboptimal utilization of AI technologies, limiting their potential benefits and return on investment.

Data quality and availability also pose significant challenges for AI adoption in SMEs. Many SMEs struggle with fragmented, incomplete, or inaccurate data sets, which can undermine the effectiveness of AI algorithms and decision-making processes (Dörpinghaus, 2019). Additionally, concerns surrounding data privacy, security, and compliance with regulations can create barriers to data sharing and integration, further hindering AI implementation (Wong et al., 2021; Lauterbach, 2019).

Furthermore, SMEs may face cultural and organizational barriers to AI adoption. Resistance to change, lack of understanding of AI's potential benefits, and concerns about job displacement can create reluctance among employees and management to embrace these technologies (Drmac, 2022; Kirjalainen, 2022). Overcoming these cultural barriers requires effective change management strategies, training programs, and a strong commitment to fostering an innovation-driven mindset within the organization.

### 3.8. Ethical and Regulatory Considerations

As SMEs explore the adoption of AI technologies, it is crucial to consider the ethical and regulatory implications associated with these powerful tools. One of the primary concerns revolves around data privacy and the responsible use of personal and sensitive information (Lauterbach, 2019; Wong et al., 2021). SMEs must ensure compliance with data protection regulations, such as the General Data Protection Regulation (GDPR) in Europe and equivalent laws in other regions, to maintain customer trust and avoid legal ramifications.

Another ethical consideration is the potential for algorithmic bias and discrimination. AI algorithms can inadvertently perpetuate societal biases present in the training data, leading to unfair decision-making processes and outcomes (Fenwick et al., 2018; Lauterbach, 2019). SMEs must implement robust governance frameworks, including human oversight and bias detection mechanisms, to mitigate these risks and ensure ethical AI practices.

Moreover, as AI systems become more autonomous and sophisticated, questions arise regarding accountability and transparency. SMEs must establish clear guidelines and protocols for monitoring AI systems, ensuring their decisions and actions are explainable and aligned with ethical principles (Lauterbach, 2019; Nourani, 2022). Failure to address these concerns can erode public trust, damage brand reputation, and expose SMEs to legal and regulatory liabilities.

## 4. Conclusion and Recommendations

In conclusion, this study has given an expanded appreciation of the applicability of AI in making cybersecurity better for SMEs. They show that advanced AI-based cybersecurity solutions, including machine learning and deep learning, can enhance threat identification, automation of response, and adaptation capabilities far beyond traditional rule-based security models. But the implementation of the AI-based cybersecurity solutions in SMEs is facing several problems: high level of complexity and costs, no internal cybersecurity specialists, and trust issues related to the system reliability and interpretability. To overcome these barriers, there is a need to engage researchers, technology suppliers, as well as the SMEs themselves in finding technological solutions that are appropriate and meet local requirements for undertaking CPFR. Governments also have a great opportunity to promote the use of AI in cybersecurity by SMEs by policies, funding, and legislation. This paper has a strategy of easing the barriers to adoption and promoting an AI supporting ecosystem to get the best out of it to improve the cybersecurity of SMEs and make them more prepared to face the increasing menace of cyber-attacks.

### 4.1. Developing AI-Enabled Cybersecurity for SMEs

Based on our research, we propose the following recommendations to foster the development and adoption of AI-enabled cybersecurity solutions that cater to the needs of SMEs:

- ***Collaboration and Knowledge Sharing:*** Enhancing the combined effort of researchers, software developers, and SMEs can go a long way in narrowing the chasm that exists between the academic vision of what AI in cyber defence is capable of and the hands-on requirements of the average small firm.
- ***Simplified and Affordable Solutions:*** Making the AI cybersecurity tools easy to implement and maintain, affordable, and equally importantly, easy to scale also means making the pricing policy transparent and the deployment model diverse will help SMEs to pay more attention to such solutions.
- ***Targeted Training and Support:*** Awareness creation through education and appropriate training sessions that can equip SMEs with proper knowledge about useful, useful AI integration along with the best practices for the application of cybersecurity will go a long way in boosting the usage scenarios of these solutions.
- ***Continuous Improvement and Adaptation:*** Some of the best practices include integrating feedback mechanisms and updating the AI-supported cyber security solutions with new threats and new trends as well as the needs of SMEs are constantly changing.

## Compliance with ethical standards

### *Disclosure of conflict of interest*

No conflict of interest to be disclosed.

## References

[1] Adelakun, O., & Kemper, T. (2010). Software-as-a-Service Business Intelligence: Adoption Criteria and Business Value.

[2] Alexander, B., & Rutter, C. (2022). Towards transformation: digitalization, sustainability, and customer experience. Fashion Practice, 14(3), 319-328.

[3] Alnamrouti, A., Rjoub, H., & Ozgit, H. (2022). Do strategic human resources and artificial intelligence help to make organizations more sustainable? evidence from non-governmental organizations. Sustainability, 14(12), 7327. https://www.mdpi.com/2071-1050/14/12/7327

[4] Anik Yuesti, N. M. D. R. (2020). Behavior of Financial Management for Small and Medium Enterprises in the New Normal Era. Journal of Southwest Jiaotong University, 55(6).

[5] Arham, A. F. (2014). The relationship between leadership behavior, entrepreneurial orientation and organizational performance in Malaysian small and medium enterprises. RMIT University.

[6] Bernsteiner, R. (2022, July). Investigating the Potential of AutoML as an Instrument for Fostering AI Adoption in SMEs. In Knowledge Management in Organizations: 16th International Conference, KMO 2022, Hagen, Germany, July 11–14, 2022, Proceedings (p. 360). Springer Nature. https://books.google.com/books?hl=en&lr=&id=mdp4EAAAQBAJ&oi=fnd&pg=PA360&dq=The+new+normal:+The+status+quo+of+Artificial+Intelligence+adoption+in+SMEs&ots=Z24HimJYWE&sig=6Rngq8fQekdDjEsiJL0pQ_76CcA

[7] Boonsiritomachai, W. (2014). Enablers affecting the adoption of Business Intelligence: a study of Thai small and medium-sized enterprises (Doctoral dissertation, Victoria University). https://vuir.vu.edu.au/28817/1/BOONSIRITOMACHAI%20Waranpong-thesis_nosignature.pdf

[8] CHAPMAN, G. A. (2021). Anticipating the impact of disruptive technologies on SMEs in Kwazulu-Natal: a case study. Expert Journal of Business and Management, 9(1). https://business.expertjournals.com/23446781-905/

[9] Chatterjee, S., Chaudhuri, R., Vrontis, D., & Basile, G. (2022). Digital transformation and entrepreneurship process in SMEs of India: a moderating role of adoption of AI-CRM capability and strategic planning. Journal of Strategy and Management, 15(3), 416-433. https://www.emerald.com/insight/content/doi/10.1108/JSMA-02-2021-0049/full/html

[10] Chishti, S. (2020). The AI book: the artificial intelligence handbook for investors, entrepreneurs and fintech visionaries. John Wiley & Sons. https://books.google.com/books?hl=en&lr=&id=oE3YDwAAQBAJ&oi=fnd&pg=PR8&dq=The+new+normal:+The+status+quo+of+Artificial+Intelligence+adoption+in+SMEs&ots=sJx5HleD_-&sig=MXptB_YzvzEvA7n6E4EdO7Y3waA

[11] Chiu, C. Y., Chen, C. L., & Chen, S. (2022). Broadband mobile applications' adoption by SMEs in Taiwan—a multi-perspective study of determinants. Applied Sciences, 12(14), 7002.

[12] Dörpinghaus, S. (2019). Artificial intelligence in the cybersecurity of German Small and Medium Sized Enterprises (Doctoral dissertation). https://repositorio.fgv.br/bitstream/10438/28288/5/Final_MPGI_Dissertation_Simon_Doerpinghaus.pdf

[13] Drmac, F. (2022). Reshaping Organizations through Artificial Intelligence: Overcoming Barriers of AI-Implementation.

[14] Fenwick, M., Vermeulen, E. P., & Corrales, M. (2018). Business and regulatory responses to artificial intelligence: Dynamic regulation, innovation ecosystems and the strategic management of disruptive technology. Robotics, AI and the Future of Law, 81-103. https://link.springer.com/chapter/10.1007/978-981-13-2874-9_4

[15] Garg, S., Mahajan, N., & Ghosh, J. (2022). Artificial Intelligence as an emerging technology in Global Trade: the challenges and Possibilities. In Handbook of Research on Innovative Management Using AI in Industry 5.0 (pp. 98-117). IGI Global. https://www.igi-global.com/chapter/artificial-intelligence-as-an-emerging-technology-in-global-trade/291464

[16] Grewal, R., & Tansuhaj, P. (2001). Building organizational capabilities for managing economic crisis: The role of market orientation and strategic flexibility. Journal of marketing, 65(2), 67-80.

[17] Grooms, G. B. (2013). Artificial intelligence applications for automated battle management aids in future military endeavors (Doctoral dissertation, Monterey, CA; Naval Postgraduate School).

[18] Guelich, U., & Guelich, H. M. (2015). Determinants for Market Expansion of Thai SME Entrepreneurs as the ASEAN Economic Community is Taking Roots. sector in the Philippines, Cristina Teresa Lim and Maritoni Carnela Matibag, 86.

[19] Harish, V., Krishnaveni, D., & Mansurali, A. (2021). Artificial intelligence in manufacturing. In Reinventing Manufacturing and Business Processes Through Artificial Intelligence (pp. 63-77). CRC Press. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003145011-4/artificial-intelligence-manufacturing-harish-krishnaveni-mansurali

[20] Hasan, M., & Mullick, T. (2021). Blockchain and artificial intelligence enabled autonomous smart manufacturing consortium. In IIE Annual Conference. Proceedings (pp. 920-925). Institute of Industrial and Systems Engineers (IISE).

[21] Hassan, A. (2021). The usage of artificial intelligence in digital marketing: A review. Applications of Artificial Intelligence in Business, Education and Healthcare, 357-383. https://link.springer.com/chapter/10.1007/978-3-030-72080-3_20

[22] Hopf, V. (2021). Artificial Intelligence in German SMEs-Barriers and Challenges to AI Adoption in the German Mittelstand (Master's thesis, Universidade NOVA de Lisboa (Portugal)). https://search.proquest.com/openview/1566e778d1eecd2dc798f610441654b4/1?pq-origsite=gscholar&cbl=2026366&diss=y

[23] Jing, X., Peng, P., & Huang, Z. (2020). Analysis of multi-level capital market linkage driven by artificial intelligence and deep learning methods. Soft Computing, 24(11), 8011-8019. https://link.springer.com/article/10.1007/s00500-019-04095-z

[24] Kassies, H. R. W. (2022). A Framework for Artificial Intelligence Capabilities for Challenges in the Supply Chain for Business-to-Business Companies (Master's thesis, University of Twente).

[25] Khalid, B., & Naumova, E. (2021). Digital transformation SCM in view of Covid-19 from Thailand SMEs perspective. Glob. Chall. Digit. Transform. Mark, 1, 49-66.

[26] Kirjalainen, O. (2022). The relationship of leadership and artificial intelligence in construction and development industry: mixed methods research.

[27] Kong, Y., Hou, Y., & Sun, S. (2021). The adoption of artificial intelligence in the e-commerce trade of healthcare industry. In Digital Health and Medical Analytics: Second International Conference, DHA 2020, Beijing, China, July 25, 2020, Revised Selected Papers 2 (pp. 75-88). Springer Singapore. https://link.springer.com/chapter/10.1007/978-981-16-3631-8_8

[28] Lauterbach, A. (2019). Artificial intelligence and policy: quo vadis? Digital Policy, Regulation and Governance, 21(3), 238-263. https://www.emerald.com/insight/content/doi/10.1108/DPRG-09-2018-0054/full/html

[29] Majchrzak, A., & Gasser, L. (1991). On using artificial intelligence to integrate the design of organizational and process change in US manufacturing. AI & society, 5, 321-338.

[30] Mann, R. (2021). Navigating the New Normal: How New & Small Companies Can Succeed Despite Economic Uncertainty. Business Expert Press.

[31] Micle, D. E., Deiac, F., Olar, A., Drența, R. F., Florean, C., Coman, I. G., & Arion, F. H. (2021). Research on innovative business plan. Smart cattle farming using artificial intelligent robotic process automation. Agriculture, 11(5), 430. https://www.mdpi.com/2077-0472/11/5/430

[32] Nourani, C. F. (2022). Artificial Intelligence and Computing Logic: Cognitive Technology for AI Business Analytics. Apple Academic Press.

[33] Osanna, P. H., Durakbasa, N. M., Yurci, M. E., & Bauer, J. M. (2010). Enterprise Information Systems for Business Integration in Global International Cooperations of Collaborating Small and Medium Sized Organizations. In Information Resources Management: Concepts, Methodologies, Tools and Applications (pp. 816-830). IGI Global. https://www.igi-global.com/chapter/information-resources-management/54518

[34] Rathnakaran, A. P. (2016). ACCEPTANCE OF ARTIFICIAL INTELLIGENCE INFLUENCER IN CONSUMER PURCHASE INTENTION. Global journal of Business and Integral Security.

[35] Rawat, W., & Barnes, J. (2022). The Mediating Role of IT Ambidexterity in the Relationship between Artificial Intelligence Capability and Organizational Agility. The Mediating Role of IT Ambidexterity in the Relationship between Artificial Intelligence Capability and Organizational Agility.

[36] Reuschke, D., Mason, C., & Syrett, S. (2021). Digital futures of small businesses and entrepreneurial opportunity. Futures, 128, 102714. https://www.sciencedirect.com/science/article/pii/S0016328721000227

[37] Rožman, M., Oreški, D., & Tominc, P. (2022). Integrating artificial intelligence into a talent management model to increase the work engagement and performance of enterprises. Frontiers in psychology, 13, 1014434.

[38] Sharbek, N. (2022). How Traditional Financial Institutions have adapted to Artificial Intelligence, Machine Learning and FinTech? In Proceedings of the International Conference on Business Excellence (Vol. 16, No. 1, pp. 837-848).

[39] SHEN, Y., CHENG, M., YAO, X., & WEI, W. Part One Management Information System, Decision-Making Support System, Expert System, Artificial Intelligence and Electronic Commerce.

[40] Truvé, T., Wallin, M., & Ryfors, D. (2019). Swedish manufacturing SMEs readiness for industry 4.0: what factors influence an implementation of artificial intelligence and how ready are manufacturing SMEs in Sweden?. https://www.diva-portal.org/smash/get/diva2:1321698/FULLTEXT01.pdf

[41] Wang, J., Lu, Y., Fan, S., Hu, P., & Wang, B. (2022). How to survive in the age of artificial intelligence? Exploring the intelligent transformations of SMEs in central China. International Journal of Emerging Markets, 17(4), 1143-1162. https://www.emerald.com/insight/content/doi/10.1108/IJOEM-06-2021-0985/full/html

[42] Wong, L. W., Tan, G. W. H., Lee, V. H., Ooi, K. B., & Sohal, A. (2021). Psychological and system-related barriers to adopting blockchain for operations management: an artificial neural network approach. IEEE Transactions on Engineering Management, 70(1), 67-81. https://ieeexplore.ieee.org/abstract/document/9353270/

[43] Yeboah-Boateng, E. O. (2013). Cyber-security challenges with smes in developing economies: Issues of confidentiality, integrity & availability (CIA).

[44] Yubo, C. (2021). Innovation of enterprise financial management based on machine learning and artificial intelligence technology. Journal of Intelligent & Fuzzy Systems, 40(4), 6767-6778.

[45] Yuce, M. A COMPARISON OF ORDERED LOGIT AND ARTIFICIAL NEURAL NETWORK IN CREDIT RATING OF TURKISH SMEs. "BASEL II'YE GEÇİŞ ÖNCESİ KOBİ'LERDE GENEL DURUM DEĞERLENDİRMESİ: SORUNLAR VE, 22.

[46] Zamani, E. D., Griva, A., & Conboy, K. (2022). Using business analytics for SME business model transformation under pandemic time pressure. Information Systems Frontiers, 24(4), 1145-1166. https://link.springer.com/article/10.1007/s10796-022-10255-8.