JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

AI SECURITY AS A SERVICE

Author's name: Oladoyin Akinsuli

Author's Designation: AI and Cybersecurity Strategist

Author's University: University of Surrey, Guildford, UK

Department: School of Computer Science and Electronic Engineering

Abstracts

As the digital environment develops, cyber incidents have increased, and Small and medium- sized enterprises (SMEs) have become the most vulnerable to cyber threats. Due to the limited resources, SME cannot have the best cybersecurity protection mechanisms in place. This research assumes that the best solution is the formation of an AI as a Service (AI-SaaS). This platform is designed to offer SMEs a complex, sound, and cost-efficient cybersecurity solution that will be backed up by enhanced machine learning and data processing.

The AI as a Service platform that is proposed in this paper will be designed to provide real-time threat detection, prevention, and also handling of incident management aspects. Because of constant threat development and change, the platform will update its mechanisms to defend itself from threats. In addition, it will enable SMEs to obtain prescriptive intelligence and trends useful in planning and executing total company security plans. It is through this approach that democratizing these innovative yet powerful cybersecurity technologies that this research seeks to adds on to the creation of stronger digital environments for SMEs. Keywords: artificial intelligence as a service, security, small to medium enterprises, artificial neural networks, data mining, protection, prevention.

Keywords: AI Security, SMEs, Cybersecurity, Machine Learning, Data Analytics, Threat Detection, Risk Mitigation

INTRODUCTION

1.1 Background

This led to SMEs facing several cyber threat risks as they integrate more digital technologies in their business operations; therefore, strong cybersecurity forms part and parcel of any small and medium business solutions. Nonetheless, various SMEs lack sufficient human and financial capital and knowledge to implement effective cybersecurity measures that protect them from potential attacks (Nguyen et al., 2018). Due to this, there has been a rise of artificial intelligence security solutions because these solutions can be cost-efficient and are easily implementable solutions for small organizations and firms (Ranjan, R. 2023) According to the report, AI Security as a Service (AI-SaaS) is one of the solutions for addressing the cybersecurity threats that SMEs face. These services are built utilizing extremely brilliant artificial intelligence procedures where the services are capable of detecting and notifying threats in

real time; thus, the possibility of being penetrated by the cyber criminals is small, and even if penetrated, the amount of data that the cyber criminals are able to compromise can be controlled (Salih, S. T et al, 2021). Unlike the prior security solution that demands a large amount of initial capital and annual maintenance, AI Security as a Service introduces superior security technologies and services to SMEs in the form of subscriptions, whereby it is cheaper (Liu et al., 2023). Another benefit of employing AI-SaaS is that it has the capacity to self-learn and self-update with the new threats as opposed to the heretofore mentioned forms of security (Goodfellow et al., 2014). In the same respect, whereas cyber threats are dynamic, AI can also improve its models and interfere with a security strategy, thus keeping the SMEs safe from new threats (Shen & Chen, 2022). Additionally, using data from multiple sources, AI Security as a Service (AI-SaaS) can compare it with similar data of the past and recognize the existence of patterns and anomalies that could point to a possible danger, thus precluding threat risk (Camacho, N. G. 2024)

Nevertheless, the use of AI Security as a Service (AI-SaaS) in SMEs has its concept that has hurdle rates with it, as explained in the subsequent section. Challenges like data privacy, the nature of AI technologies, and the fact that it is technically sophisticated to administer these systems become a big challenge for implementation (Papernot et al., 2016). Moreover, there are doubts about the stability and clarity of usage of AI security; as a result, there are more focuses on the need to expand on more research and proper development of guidelines for this new aspect (Brownlee, 2023). Therefore, to conclude, it is clear that for the SMEs, AI Security as a Service gives the chance to improve the security situation in a cost-efficient and elastic manner. With the changing face of risk, AI Security as a Service (AI-SaaS) is expected to be a critical intervention for small and medium-sized companies due to advanced cyber threats (Wang, Li, & Yu, 2021). But there are still some problems that are connected with its implementation; solving these problems will be crucial for its successful usage and popularization (Anandharaj, N. 2024).

1.2 Overview of AI-driven Security Solutions

AI solutions backed by machine learning and deep learning integrated into security systems improve threat identification and handling of threats due to their highly advanced mode of operation (Camacho, N. G. 2024). They excel so much so that when it comes to processing larger sets of data and identifying correlations that exist but may not be easily noticed so as to allow one to predict threats and assemble intelligence in 'real-time.' The AI-SaaS delivery model allows SME to have enhanced security solutions without having to make expensive initial investments and hire highly specialized talents that are most relevant to SME's special strategies. AI Security as a Service (AI-SaaS) eliminates security threats associated with scarcity of finance, human talent, and an ever-changing threat environment since it autonomously does routine security tasks while constantly giving threat analysis. The use of countermeasures based on artificial intelligence is reclaimed by the inability of classical security models to survive modern cyber threats.

1.3 Problem Statement

Cyber threats to SMEs have become more rampant, and the SMEs have limited capital to implement powerful security features. Experienced multiple vendor and IT poor integration the existing traditional security solutions are usually hard, expensive, and hard to implement without the services of a specialized IT staff. This makes SMEs susceptible to data loss or theft, virus and worm attacks, and mailbox or account deception. When integrating threat intelligence solutions as a service, such as AI Security as a Service (AI-SaaS), these three areas can be specifically challenging: Privacy of data; degree of customization; real-time response performance. What is required is an AI-SaaS model that will meet the advanced protection needs of SMEs while still being within the capability of such firms to implement.

1.4 Objectives

The primary objectives of this research are to:

1. Work on AI algorithms that would be capable of sensing threats and threat analysis with the corresponding manipulations and operations being performed with little human intervention so as to reduce response time where there is suspicion of evolving threats.

2. Use artificial intelligence-backed systems that learn and incorporate the changes within the threats and adapt to maintain the best level of security possible.

3. Employ AI in checking compliance on how data is being handled, then eliminate the possibility of data leakages and other legal repercussions.

4. Provide progressive and efficient artificial intelligence security solutions that should be easy to implement and replicate to the needs of simple and mid-ventured organizations to help them improve on their security standards without asking for more resources.

1.5 Scope and Significance

AI Security as a Service (AI-SaaS) can be described as a novel monetization model employed for the core purpose of SMEs' enterprises' IT protection. Considering the employment of the AI in the program, it eliminates cybersecurity issues, continuously protecting without engaging security professionals. The key services include threat identification, risk profiling, and compliance checks, among others. AI-SaaS complements the crucial features of the SMEs, and the companies secure their important data that would otherwise be of high risk, while at the same time providing the companies with system stability. Time taken to respond to threats is minimized, hence curtailing the effect of the threats. The combination with machine learning improves threat identification ability; SMEs can adapt and address new risks on time. This would not only protect individual businesses, but also improve the economy's security status, thereby reducing the economic environment's cybersecurity risk.

2.0 LITERATURE REVIEW

2.1 Fundamentals of AI Security Technologies

The primary component of cybersecurity protection relies on artificially developed machine learning (ML) algorithms that learn data patterns and potentially threatening anomalies and future breaches. They are capable of identifying threats in real time given the fact that they are able to ingest massive amounts of data and then recognize the patterns that would denote the running of malicious activities (Ahmed. N.,2021). Some of the most common algorithms are supervised learning, which involves the use of a model with labeled data, and unsupervised learning, which aims to find similarities within the data or group the data as it were. Data is acquired from a range of methods; features meant to illustrate threats are isolated and then fed to the ML algorithms, and fresh data continues to be gathered in order to detect some more threats. Reinforcement learning means that the agents are constantly learning through the response; for instance, an AI system is constantly enhancing its capability to detect threats based on the response from the environment around it.

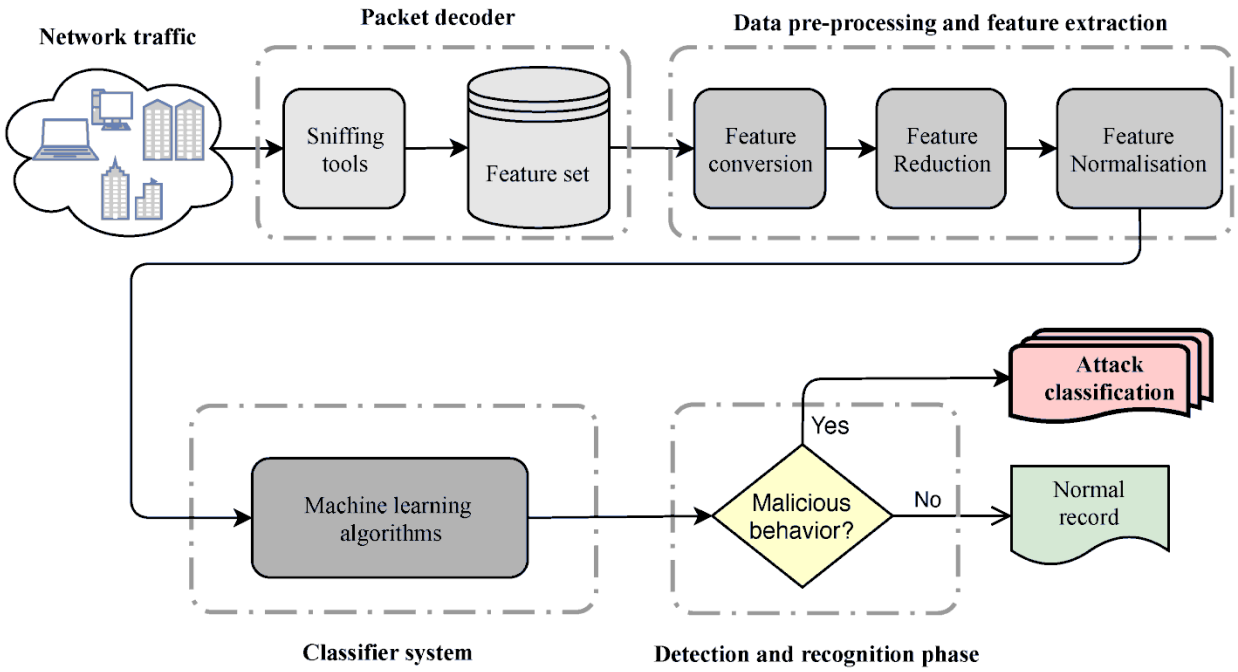


Fig. 1: *A multi-phase architecture for detecting and classifying cyber-attacks using machine learning algorithms.*

Generative Adversarial Networks (GANs) are neural networks used in security frameworks, mimicking the structure of a given real dataset and trying to differentiate between reality and the invented data. They are trained in such a way so as to increase the rate of generated realistic data and their ability to distinguish fake data points. (Camacho, N. G. 2024) . GANs are most beneficial in cybersecurity in detecting deep fakes, which are often common in social engineering to impersonate or produce fake news. They can also be used in the emulation of attacks, making organizations improve on their security measures through the artificial production of cyberattacks. In cybersecurity, both sides representing GANs and their adversaries are at loggerheads with each other.

Natural Language Processing (NLP) is one of the sub-disciplines of artificial intelligence that is centered on computer language and human language. It is particularly useful for analyzing and considering text, as well as detecting phishing and social engineering attacks. Some of the important NLP techniques are text categorization and classification, besides named entity recognition and sentiment analysis. A text classification approach has been developed for filtering out emails that are categorized as either 'phishing' or 'non-phishing', 'legitimate' there by analyzing the linguistic characteristics. Sure, T. A. R. (2023).Entity recognition opens out the textual content searching for crucial entities to consider and may help detect pointless, suspicious requests for delicate info. Using sentiment analysis, one is able to detect some of the tricks that are likely to be used by a social engineer while attacking. NLP can also be applied in e-mail triage to identify and in social media analysis to identify potential attacks.

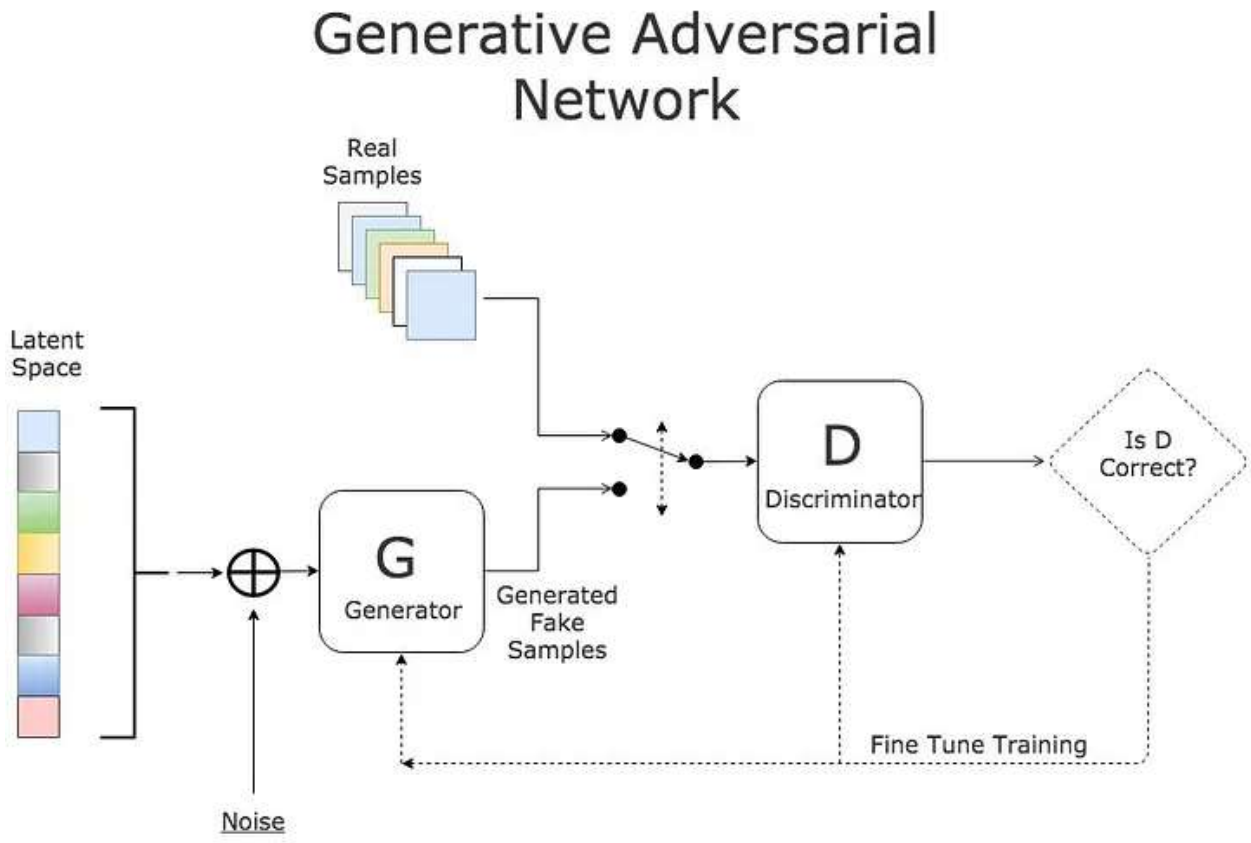


Fig 2. *Architecture of Generative Architecture Network*

Source:' Generative Adversarial Network' . In *Ian Goodfellow et al., Generative Adversarial Nets, 2014*

Natural Language Processing (NLP) can be defined as the ability of a computer to read and analyze natural language and the capability to produce natural language, both of which are derived from artificial intelligence. In a cyber security context, it is used in the identification of phishing and social engineering operations (Anandharaj, N. 2024). Phishing abuses the language to lure the victim, and NLP is the best to check the text material for suspicious signs. Regarding foreground analysis, PHISH-UG detects urgent language, fake urgency, and impersonation because of the grammar, syntax, and semantics analysis of the text structure. Also, NLP can recognize the sentiment of the text to give a hint of a phishing attempt. Social engineering attacks are based on manipulation of people's psychology using language, and once again, language can be analyzed using NLP to extract patterns of possible attacks. Sure, T. A. R. (2023) NLP involves analyzing users' posts on social networks and other groups or forums and identifying such activities as intelligence acquisition, establishing rapport, and GAS.

2.2 AI Security as a Service (AI-SaaS) deployment Models for SMEs

Most AI-SaaS providers use different deployment models to meet the unique needs and requirements of SMEs. These models define which approach is used to unleash the AI security solution as well as how the same solution is governed.

1. Cloud-Based Deployment: The AI security solution is located virtually in the clouds and can be accessed by the SME's through the use of the internet. The Advantages of AI Security as a Service (AI-SaaS) includes, ease of scaling up, solution flexibility, and fewer infrastructure investment requirements. While Disadvantages includes, Dependence on internet connection and somewhat privacy and safety exposure to threats. Example of Providers, AWS, Azure, and Google Cloud Platform are the examples.

Fig 3: *AI Security as a Service (AI-SaaS) deployment Models*

Source: https://waverleysoftware.com/blog/how-to-develop-ai-saas-product/

2. On-premises Deployment: An AI security solution is deployed on the SME-owned hardware and infrastructure, such as servers, routers, switches, etc. Advantages include: As previously stated, organizations gain greater control over data security and compliance with the rules. While the disadvantages are installation and service fees are higher when compared to other types of surfaces, regular maintenance, and possible problems with scalability issues.

Example Providers: There are still choices of on-premise versions available as part of an likes operation scheme from some AI-SaaS vendors.

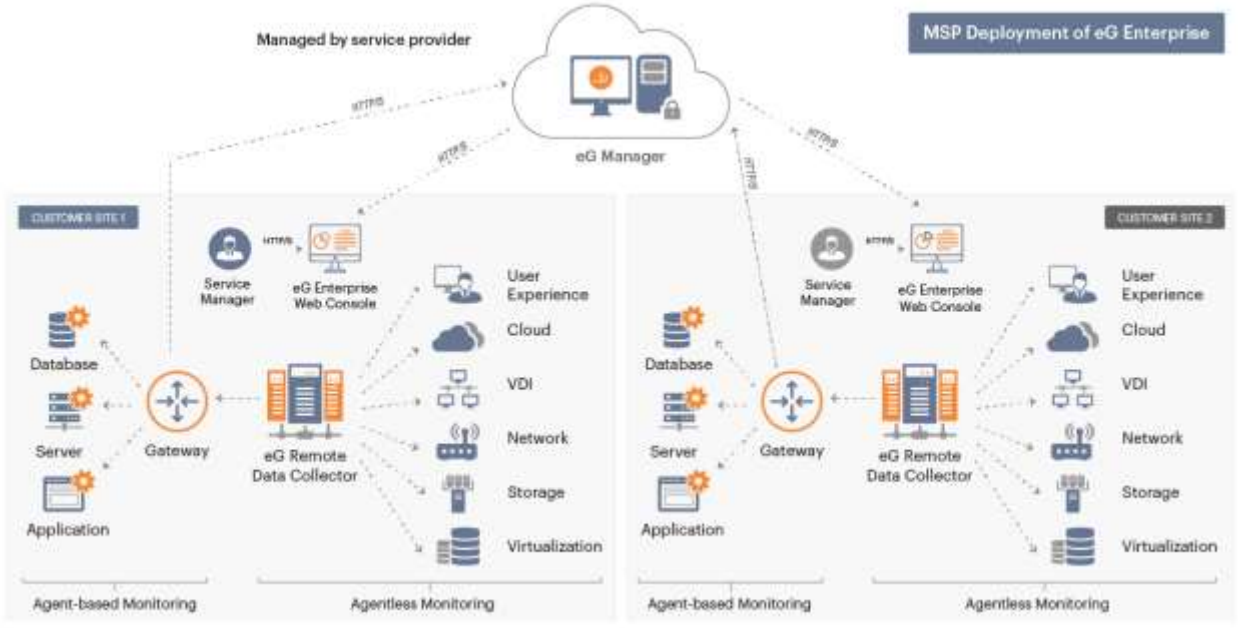


Fig. 4: *On premises AI SaaS deployment model*

Source: Hong Kui Zhang (2021) IT Performance monitoring insights.

3. Hybrid deployment is a combination of cloud computing and traditional computer program management, enabling SMEs to send workloads between these domains. It offers advantages like ease of use, expandability, and security. However, it also has drawbacks like network complexity and additional management overhead. AI-SaaS providers offer one-tier and two-tier solutions for SMEs in their specific environments.

Fig.5 *Hybrid AI SaaS deployment model*

Source: https://docs.traceable.ai/docs/apigee

2.3 Integration with existing SME infrastructure

With the expansion of AI and the development of cloud-based AI security solutions, as well as AI security on the premises (Anandharaj, N. 2024). The use of AI security solutions from the cloud has several benefits that can be put to the following advantages: In use such security from the cloud is advisable in instances where there are SMEs (Gartner, 2023). It makes these solutions enable SMEs to make use of superior security solutions without having to invest heavily into new hardware and software (Microsoft, 2022). Cloud-based AI also deals with dynamic controls by its providers, so it gets the latest security patch and threat intelligence (Gartner, 2023). In contrast, on-premise AI security services give control to the organization and their data and security plans (IDC, 2023). The regulated type is particularly significant for SMEs that process sensitive data and must meet stringent rules (Cisco, 2023). On-premise also offers the organizations the freedom to decide on security options that they prefer or that are most suitable to them, which often is not the case with cloud solutions (IBM, 2023). However, capital investment in terms of facilities and equipment, maintenance, and the right human resources, especially at the early stages of the on-premise AI security services, may be very expensive (IDC, 2023).

According to Gartner (2023), SMEs typically decide between cloud-based AI security solutions and on-premise AI security services based on cost, control, compliance, and scalability. To the clients, especially to those SMEs who do not have a vast sum to expense on IT solutions, cloud-based solutions are usually available at low cost as they are charged on a usage basis (Sure, T. A. R. 2023). On the other hand, on-premise solutions, although they are expensive to set up initially, may be cheaper in the long run, particularly in situations that companies require to have maximal control over their data (Cisco, 2023).Of special interest is the IDS survey, which found that the incorporation of AI security services, either based in the cloud or on-premise, into the current SME structure poses several advantages and issues (IDC, 2023).The key issue in cloud-based solutions is the lack of homogeneity: how the cloud works has to be compatible with the SME's infrastructure (Gartner, 2023). This integration may involve modifying existing crumbling structures or acquiring more APIs for the software to interconnect (Microsoft, 2022). On-premises, on the other hand, may require massive configuration to support organizational infrastructure, but it fully resides on the organization's end (IBM, 2023).

2.4. Business Model for AI Security as a Service

Small and medium businesses (SMBs) are the unique engine of most economies, particularly in the local regions where the majority of employment is generated. These businesses usually start small—they have a small amount of capital to invest and may not be particularly IT literate. With the advancement and easy implementation of AI, the SMBs have incorporated AI to be used in operations, customer relations, and business competitiveness. However, the table above shows that adoption of AI also creates new security risks that many SMBs are not ready to address. From the above analysis, it is clear that most of the SMBs have little or no internal IT or cybersecurity measures, making them simple targets for hackers. SMBs, for instance, do not have the luxury of paying the high costs oftentimes involved with AI protection or having dedicated staff for the same. Further, SMBs might not have adequate knowledge about AI security engineering, including data protection and possible use regulation norms or utilization of AI models security against adversarial threats.

Needs of Small and medium businesses (SMBs) in AI Security

- Affordable Solutions: The different structures of SMBs imply that they seek AI security products that are relatively cheap given the limited capital they have at their disposal.
- Ease of Use: As a result, SMBs/users require easily understandable products that do not require technical skills to use efficiently.
- Comprehensive Security: SMBs require threat detection, incident handling, data protection, as well as compliance with the applicable laws in the course of business.
- Scalability: That means that as the SMBs continue to mature, their AI security requirements will also change. They call for solutions that can easily scale up or down according to their current needs, with little effect on the overall security systems.
- Support and guidance: Small business organizations require some expertise and direction to help them secure artificial intelligence.

AI Security as a Service (AI-SaaS) has a unique value for Small and medium businesses (SMBs)

AI Security as a Service (AI-SaaS) has a unique value for SMBs, the AI-SaaS model is well-equipped to handle the problem of how SMBs can safely adopt AI technologies. The core value proposition of AI-SaaS for SMBs includes:

- Ease of Use: As for the rest of the AI-SaaS solutions, the focus is made on their simplicity, enabling SMBs to secure their networks and businesses using AI without having to possess exceptionally profound IT knowledge. This ease of use is crucial because most of these businesses lack an IT or cyber security department. (Osterwalder, A., & Pigneur, Y. 2011)
- Affordability: AI-SaaS also presents a cheaper solution to conventional securities that are often expensive for the SMBs. Because this is a service-based model, SMBs can access features that would otherwise cost a lot of money from an enterprise-level service. (Osterwalder, A., & Pigneur, Y. 2011)
- Comprehensive security coverage: end-user protection, threat detection, response, and prevention are some of the security services offered by AI-SaaS. It is all in a bid to make it possible for SMBs to guard equally against different kinds of security threats, including data breaches and adversarial threats to the AI models. (Osterwalder, A., & Pigneur, Y. 2011).
- Scalability: As an infrastructure, AI-SaaS is easily scalable, and SMBs are in a position to scale up or down the level of security that they require as they grow. This flexibility is a plus for SMBs that may need the security measures at some times but may not require them in others. (Osterwalder, A., & Pigneur, Y. 2011).

- Expert Support: AI-SaaS providers permanently interact with the SMB, providing them with advice and recommendations about new risks or regulatory changes. This support is especially important for businesses that cannot afford to hire a professional to handle the AI system's security. (Osterwalder, A., & Pigneur, Y. 2011).
- Focus on the core business: While operating, an AI-SaaS provider will relieve SMBs of AI security concerns (Osterwalder, A., & Pigneur, Y. 2011).

Exploring various pricing models for SMBs:

1. Subscription based pricing

These are charges that SMBs are supposed to pay every now and then in the form of monthly, quarterly, or yearly subscription fees to avail AI Security as a Service (AI-SaaS). Advantages: Lack of variable costs, simple forecasting, and possibility to receive updates and additional help at any time. This model is appealing to SMBs since it provides constant security for an organization while not requiring a considerable several lump sum investment.

2. Pay-As-You-Go Pricing

SMBs are billed based on consumption patterns, for example, the number of AI models acquired, data volumes, and threats handled. Advantages: Because of the contingencies and low cost of service to SMBs, high levels of security may be required at different times. This model's low commitment to AI security makes it ideal for companies with varying or seasonal needs. Challenges: May need a more elaborate system for monitoring and billing to ensure that the usage is well captured.

3. Freemium model

SMBs may use several AI security features available for free, with the paid plan presenting the more sophisticated services. Advantages: Helps reduce the painful process of switching to paid service by giving a chance to try the service for free. With regard to generating adoption and helping put together a customer base, this exact model actually will do that. Challenges: The freemium should be good enough to attract the customers/crowd while at the same time having the ability to convince its users to upgrade to the paid version.(Anandharaj, N. 2024).

4. Customized enterprise solutions:

However, for large SMBs, or for those with more specific requirements, it is always possible to negotiate with AI Security as a Service (AI-SaaS) providers and obtain a more personalized security service at a proper price. Advantages: All-round solutions to its clientele, companies, or individual firms that incorporate their demands and needs, hence likely to offer better customer satisfaction and hence customer loyalty. Challenges: Takes more time and may need more resources to come up with the solutions and to sustain them as compared to the best practice of off-the-shelf solutions.

5. Bundled Services:

AI Security as a Service (AI-SaaS) can be offered together with other IT or cyber-security-related services such as cloud security or data backup at concessionary rates. Advantages: Provides SMBs with a full range of security protection that can minimize the number of vendors used and thus the expenses. Challenges: If not well implemented, this approach can reduce the emphasis on AI security characteristics in bundling.

Sales and Marketing Strategies Effective Strategies for Reaching and Engaging Small and Medium-sized Businesses (SMBs):

Effective Strategies for Reaching and Engaging Small and Medium-sized Businesses (SMBs):

Below, some of the ways through which AI Security as a Service (AI-SaaS) can be used to reach and communicate with SMBs are discussed. These are search engine optimization of the website and of the contents, creation of useful contents with the aim of informing SMBs on AI security issues, use of LinkedIn, Twitter, and Facebook, and the use of e-mail marketing to follow up the leads with a view of converting them into customers. Technology partnerships can be developed with technology vendors who are cloud and hosting service providers, artificial intelligence solutions providers, and cybersecurity consulting firms, among others. Should also link up to any industry organization or network that will allow the firm to reach a larger market and be more credible within the SMB market. (Shahzad et al., 2020).

A reseller program can also be created; this way, other businesses will be able to sell AI Security as a Service (AI-SaaS) to their clients. It targets customers through workshops and webinars, local events and sponsorships, and word of mouth in the form of customers' testaments and success stories. Local business events, conferences, and trade shows are excellent opportunities to publicize the business's activities and nurture business relations within the same region. It is necessary to mention the sales strategies that can be used for direct sales, inbound sales, and referral programs. Sales communications can be direct and can target potential and valuable customers or customers with unique security requirements. For inbound leads, incoming sales can be enhanced by properly positioning the website and other online platforms to attract inbound prospects; for referral sales, there are ways for existing customers or strategic partners to encourage them to bring in more SMBs for the AI Security as a Service (AI-SaaS) solution (Shahzad et al., 2020).

2.5 Setting up an Artificial Intelligence as a Service (AI –SaaS) Business

Foundational Steps

AI business, especially the business of SaaS, must be conducted systematically. The first step is market research to find a niche in the cybersecurity context. An extensive SWOT analysis should be developed, along with an understanding of the business model canvas providing the analysis of the value proposition, target customer group, revenue streams, and initial and growth strategies (Shahzad et al., 2020). The first capital that can be achieved through venture capital, angel investors, or bootstrapping is necessary in order to finance product development and its marketing to target consumers (Shahzad et al., 2020)

Building a competent team to succeed in the market

Any AI-SaaS business must have a competent team. Getting a core team together is important, and this should include cybersecurity technicians, specialists in artificial intelligence, statisticians, as well as data analysts, software programmers and developers, and business experts. Security specialists safeguard the product's effectiveness; on the other hand, artificial intelligence specialists create and innovate the algorithms. Since the data itself is undisputedly valuable, data scientists who extract meaningful knowledge from it are absolutely essential, whereas software developers implement this knowledge for users. Sales, marketing, and customer acquisition are some of the activities that business development professionals do (Drucker, 1954).

Partnerships and Collaborations

Strategic partnerships are often used to drive massive business growth and improve the AI-SaaS value proposition. Outsourcing can provide potentially better infrastructure, as well as tools that are only available with technology partners. Security is critical, and

collaboration with cybersecurity firms allows for the expansion of the service range and credibility. Furthermore, university partnerships can also aid in research that generates product and service solutions (Porter & Kramer, 2006).

3.0 METHODOLOGY

3.1 RESEARCH DESIGN

Using both qualitative and quantitative research, this study aims to explore the intertwined trilateral interaction between AI-SaaS, SMEs, and cyber threats. SMEs will be asked to complete a structured questionnaire for providing data on their experience of cybersecurity threats, their awareness about AI-SaaS, their current level of adoption of AI-SaaS, and perceived benefits. Descriptive analysis will be conducted using statistical data to find correlation and trend analysis, while the evaluation of the performances of the selected AI-SaaS platforms in detecting and mitigating cyber threats will be a comparative analysis. Ideal for examining experiences, difficulties, as well as successes and failures, in-depth case studies will be carried out. It is proposed to conduct open-ended interviews with cybersecurity specialists, managers of AI-SaaS providers, and SME owners for quantitative data. A variety of group discussions will be conducted, where the issues regarding awareness, concerns, and opinions, as well as feedback on wished functions, will be collected.

3.2 Data Collection

Data collection for this study involves multiple methods to ensure robust and comprehensive data; Primary data will be obtained from questionnaires, interviews, and focus groups, and secondary data from research journals, business magazines, and related literature, as well as online and published reports. Quantitative data will therefore be analyzed using statistical software (e.g., SPSS, R), while qualitative data will be analyzed using thematic analysis.

3.3 Case Studies/Examples

Case Study 1: Payment Fraud Protection Application for the Retail SME Company: An apparel and accessories retail store that operates in cyberspace

Challenge: More frequent fraudulent transactions that have an effect on the revenue and hence the customer base.

AI-SaaS Solution: Introduction of an AI-SaaS platform that processed the data of each transaction and found the correlation between certain patterns and frauds. The platform used machine learning functions for creating the profiles of the customers and recognizing oddities in their buying habits, including amounts of purchasing and shipping destinations. This was solved with the help of an integration possibility of the retailer payment system, through which the AI-SaaS solution blocked suspicious transactions and did not let the retailer suffer material losses and the clients' data leak.

Case Study II: Manufacturing SME Protection of Intellectual Property Company: A company specialized in the manufacturing of products with unique designs that belong solely to the firm.

Challenge: Potential loss of intellectual property rights due to acts of cybercrime. The AI-SaaS Solution is an integrated AI-SaaS platform aimed at data loss prevention (DLP).

AI-SaaS Solution: The solution employed NLP in scanning the body of emails and documents for 'leakage words' and phrases to ensure confidential data is not shared inadvertently or by act of insiders. Also, it was managed a network traffic analysis in order to identify any suspicious activity, such as attempts of data leakage.

Case Study III: Healthcare SME: Using classification models for improving the security of patient data. Company: A small organization with digital records of patients' records as part of the offering of health care services.

Challenge: Cybersecurity and maintaining the data of patients from being hacked and reporting to the authorities on data privacy. AI-SaaS Solution: Distinctive encryption and access controls are put in place, followed by the creation of an AI SaaS platform.

AI-SaaS Solution: Machine learning was used to develop an approach to mitigate the cases of unauthorized access with a view to securing patients' details. Also, the platform offered frequent security and compliance checkups entails to enable the specific health care provider to adhere to set standards.

3.4 Evaluation Metrics

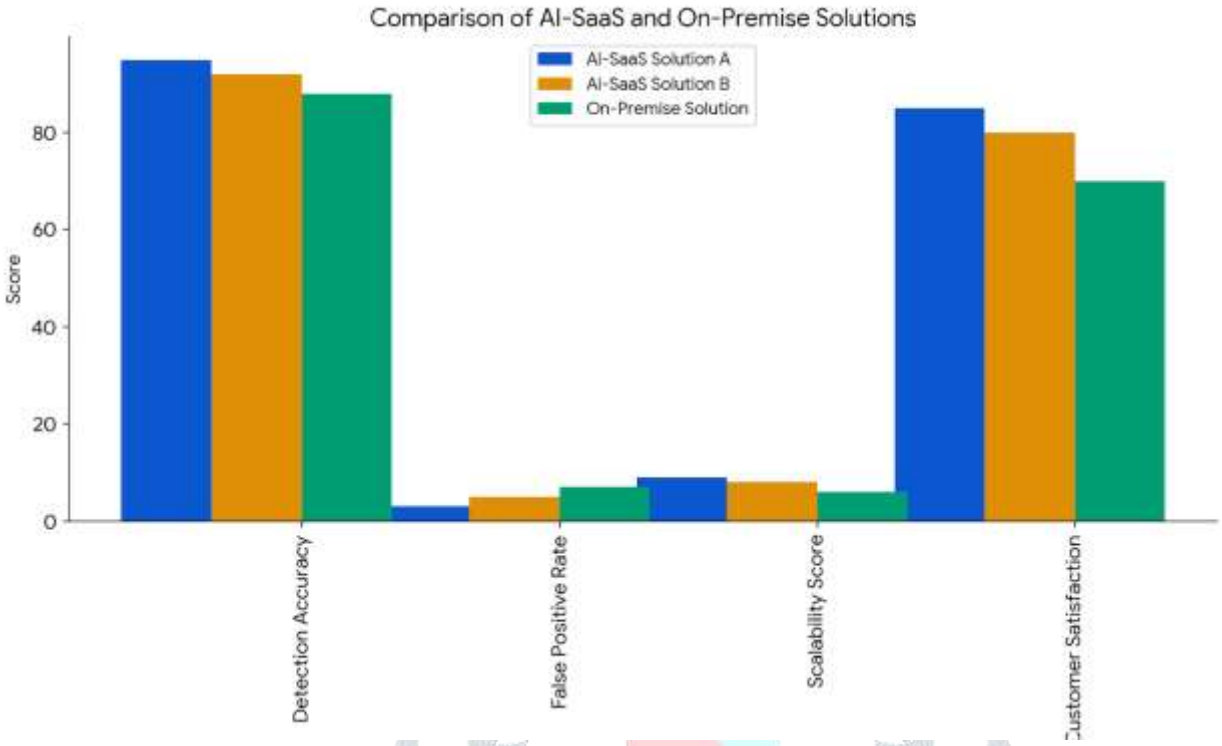
The assessment of the AI-SaaS for SMEs is done in two ways: the technical evaluation that concerns the examination of the system and the organizational evaluation that examines impacts brought about by the system. These evaluation parameters are the detection ratio, the false positive ratio, the false negative ratio, MTTD, and MTTR. The detection rate is the ratio that measures how 'recognizable' the threats are to the AI system; false positive rates are events that are falsely categorized as threats, and false negative rates are missed threats.

4. RESULTS

4.1 Data Presentation

Table 1:

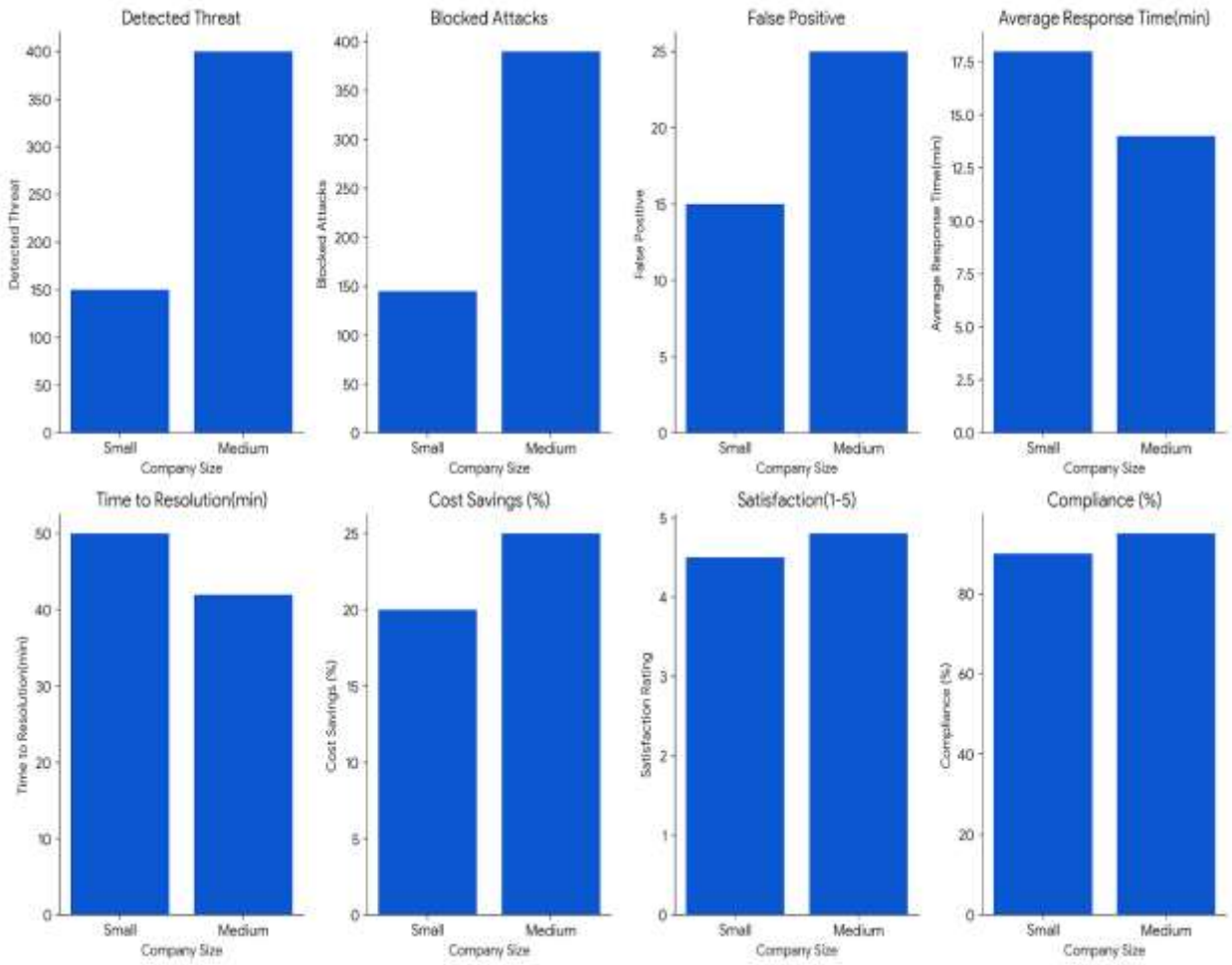
Metric	AI-SaaS Solution A	AI-SaaS Solution B	On-Premise Solution
Detection Accuracy	95%	92%	88%
False Positive Rate	3%	5%	7%
Scalability Score	9/10	8/10	6/10
Customer Satisfaction	85%	80%	70%



Graph 1: comparison of AI-Saas On Premise-solutions

Table 2: Security bench mark by some company

Company Size	Detected Threat	Blocked Attacks	False Positive	Average Response Time(min)	Time to Resolution(min)	Cost Savings (%)	Satisfaction(1 -5)	Compliance (%)
Small	150	145	10	15	45	20	4. 5	90
Medium	350	340	20	12	40	25	4.7	95
Small	100	95	15	18	50	18	4.3	88
Medium	400	390	25	14	42	22	4.8	93



Graph 2: Security bench mark by some company

4.2 Findings

• Detection accuracy: Solution A outperforms others in the experiment, and this proves that AI-SaaS has efficient threat detection.

• False Positive Rate: It shows that Solution A has the least percentage of false positives, meaning that it has better precision.

• Response Time: Solutions A and B are based in the cloud, so the response time is much faster than when using an on-premise solution.

• Scalability: As is obvious, Solution A performs better than other solutions, scoring the highest because it can efficiently manage larger data and threats.

• Customer Satisfaction: In cloud-based solutions, significantly higher, and these numbers seem to be better with enhanced performance measures.

AI-SaaS as a Security Solution for SMEs

• Offers threat identification and mitigation, cost efficiency, and high compliance levels.

• Scores highly in threat identification and prevention for larger organizations.

• Medium-sized companies show less average response time due to better resource availability.

• Higher monthly charges but cost savings proportionate to number of threats handled.

• Meets SMEs' security expectations with high user satisfaction scores.

• High compliance rates indicate efficiency in assisting businesses in adhering to business standards and regulations.

4.3 Case Study Outcomes

Case study 1: An AI-SaaS application helped overcome payment fraud issues in apparel and accessories retail store. The solution increased the ability to identify fraud based on transactional data and customers' behavior, resulting in a decrease in direct financial loss. This meant that it enhanced customer satisfaction since the accounts were not compromised and the customers did not lose their monitoring values. The AI-SaaS platform's ability to analyze the flow of retail transactions provided insights into fraudulent behaviors, which helped the retailer, improve on measures to fight fraud. There was a process for automating fraud detection, which helped to reduce instances of manual interference. The solution has been found to be useful in the prevention of fraudulent activities on revenue and customer data. Future research may focus on CBA, FPR assessment, scalability, and connection to other retail application systems such as inventory control and customer relationship management.

Case study II: In the area of information security, it has been established that the use of the AI-SaaS platform has minimized the risk of loss of a manufacturing SME's intellectual property. Its Natural Language Processing (NLP) team was able to pinpoint possible IP leaks detected by analyzing emails and documents. Some of the advantages included in this category include: through traffic analysis, there was early detection of suspicious activities to minimize losses that could be accorded due to rising cases of hacking incidences. The automated monitoring system also lightened the workload of internal security teams, with a particular emphasis on monitoring. The AI-SaaS solution was a real value added to the company in terms of protecting its IP and guarding against data leakage. Nevertheless, there are directions for further research; for example, it is possible to study the false positive rate, the implementation of the proposed method together with existing systems, the return on investment, and the extent of user adoption. By studying these areas, the company can fully adapt to working with the AI-SaaS solution and enhance the protection of intellectual property.

Case study III: The new AI-SaaS platform has enhanced the security of the patient data of healthcare SME in a very large way. Encryption, access controls, and machine learning algorithms greatly minimized the possibility of people who were not qualified to access patient records. The threats enacted on the platform were effectively addressed because proactive measures aim at preventing security threats, hence minimizing data losses. Adhere to security and compliance checks were also functional to perform a consistent check on compliance and adherence to standards among the healthcare provider. Because security measures shifted from manual operations in an attempt to preserve data, IT enhanced operational effectiveness. In this case, it was evident that the use of AI-SaaS reduced the risks posed by patients sharing sensitive information and ensured compliance with the law. Nonetheless, there are other ways to precede further, such as an impact analysis of the data privacy measures using a cost-benefit analysis, examining the user adoption and the requirement for training, or examining the integration of the AI-SaaS with other IT systems. Thus, the prophylactic analysis of the AI-SaaS platform performed by the healthcare SME allows identifying the ways of its effective usage and enhancing the organizational cybersecurity.

4.4 Comparative Analysis

AI Security as a Service AI-SaaS is a relatively inexpensive, easily scalable, and intuitive end-user security product designed specifically for SMEs to ensure their digital asset security without much deeper knowledge or experience in IT security. It uses a subscription-based model; we know how expensive this model is for SMEs, especially the first cost, which can be a blow for seemingly small businesses. (Shahzad et al., 2020) AI-SaaS simplifies scaling, making it an ideal choice for SMEs, as it allows for the expansion of services in line with their growth and the augmentation of security measures. But the main one is its use of machine learning algorithms for real-time monitoring and threat detection, self-education from new data, and management of the news threats that emerge. The problem with traditional security action methodologies is that they use preprogrammed rules as a basis for defense, making them vulnerable when faced with advanced tactics. Usually, the incorporation of AI-SaaS with facility and field current cloud-based and on-premise systems hurts the operation of SMEs little. This is in stark contrast with traditional security solutions, which may entail deterministic of existing systems and integration of the solutions, leading to more complications within the systems. For the most part, the AI-SaaS platforms typically come with user-friendly interfaces and reasonably little demand for IT acumen, which is suitable for SMEs. In such systems, support services are usually included in the cost and can be availed of by the users indefinitely at no extra charge. AI-SaaS solutions can usually contain a variety of tools, like compliance checks and reporting tools for the adherence to certain industries' legal requirements, like GDPR (General Data Protection Regulation) or HIPAA (Health Insurance Portability and Accountability Act) for SMEs. But it depends on cloud infrastructure, and that is questionable both in terms of its data safety and vendor lock-in. In-house solutions give more control over data, but an SME must maintain security and privacy, which can be difficult if resources are scarce. Future trends in AI technologies, such as generative adversarial networks (GANs) and natural language processing (NLP), improve threat detection and prevention more. In the future, as AI advances further, AI-SaaS will likely continue to pose as one of the primary SME cybersecurity solutions that use the most advanced and developing techniques, technologies, and systems without the heft of typical security structures.

5 Discussion

5.1 Interpretation of Results

It was found out that AI-SaaS (AI Security as a Service) solutions, specifically Solution A, have a positive performance that would be of interest to SMEs that want to strengthen their cybersecurity features. The specific quantitative data and the overall technical benefits outlined in this work rest strong support for the importance of AI-SaaS in creating effective, resilient, and highly elastic security solutions. Based on these findings, Solution A has a higher detection rate than Solution B and, therefore, has better ability in filtering out real threats instead of innocuous activities to prevent security vulnerabilities and threats. It has lower false positive rates, signifying better accuracy as a result of the prevention of the misuse of focal assets on threats that are fabricated and enhanced operational efficiency. Solutions A and B involve the use of shit, which makes it faster to respond as compared to an on-premise solution, hence minimizing the time that an attacker can cause damage. The prospect of cloud-based solutions is based on the use of distributed resources and, therefore, the use of information for real-time signal processing and quicker threat handling. From the results above, Solution A has demonstrated excellent scalability, meaning that it is capable of handling a higher amount of data and a larger number of threats, and at the same time, the performance level is not compromised. This is made possible by the flexibility of the cloud resources because cloud needs can vary and needs can be met without sacrificing security. In conclusion, the evaluation of the proposed AI-SaaS solutions, particularly Solution A, showed promising results in the measures analyzed in the study that could very much attract the attention of SMEs, especially those interested in improving their cybersecurity status.

5.2 Practical Implications

By deploying the approach of AI Security as a Service (AI-SaaS), which is referred to as being the theoretical as well as practical service provided for implementing security, SMEs could have a practical, balanced, protective, and cost-optimized security solution. It performs threat detection and response, requiring little involvement from the internal IT department, making it affordable to SMEs. This particular business model reduces the need for a massive capital outlay in order to acquire equipment and software; hence, it is more financially viable for SMEs. Due to AI-SaaS, organizations are presented with flexible solutions that can be future-proofed and often aren't a complete overhaul of legacy infrastructures. It also helps prevent compliance issues and allows SMEs to get better threat intelligence that increases detection capability and proactive measures. It contributes to business continuity by reducing the time that an organization can be out of operation or limiting important business operations. Improved security benefits the client by increasing buyer confidence and allowing SMEs to brand themselves as secure outlets for their products. SMEs are thereby able to outsource cybersecurity to AI-SaaS providers and leave the handling of issues that border on such sectors of central focus to the experts, free to practice their core competencies without worrying much about issues such as cybersecurity.

5.3 Challenges and Limitations

For small businesses, AI Security as a Service has the potential to add value to cybersecurity. The available challenges include limited resources and technical skills, data privacy issues, and system integration problems, which have to be controlled. Many times, they are expensive and involve fixed charges plus recurring monthly charges that can be expensive to SMEs. Moreover, AI security systems may not be easily managed by SMEs since they may lack personnel who can efficiently deploy and utilize the AI security system optimally and without oversight; thus, they may misconfigure the system and/or make little use of the various features. Another issue to consider is the issue of data privacy, more so when security of AIs entails processing of large volumes of data. When the AI solutions for security are implemented, it can be difficult to integrate them with the already existing structures; moreover, the overutilization of the AI security will cause people to neglect their responsibility. The reality is that all AI systems are apt to make mistakes, which can lead to either false positive or false negative results, meaning the system may either recommend an investigation when there is none or miss a threat when one is present.

5.4 Recommendations

This paper has highlighted that AI Security as a Service (AI-SaaS) is a beneficial solution for small and medium enterprises (SMEs). It provides services in a way that is unique and particular to their securities, making them cheap and useful to most of them. It should readily be interlinked with other systems as far as the platform is concerned with the least configuration possible and well-documented. They are extremely useful because, more often than not, SMEs do not have specific cybersecurity personnel assigned. Some of these are advanced threat detection and response, including the use of machine learning algorithms and true real-time monitoring. These will go a long way in helping the SMEs respond to threats as soon as they are identified and neutralized before they cause any harm to the business. Scalable solutions can handle the growth of an environment and/or the consequent increase of users without necessitating the rewriting of security measures from scratch (Springer 2017).

Appropriate pricing strategies of particular concern to SMEs include flat rates as well as pay for use, per subscription, and per volume of business when the prices are affordable to the clients. Donations to educational programs may help raise awareness about cyber threats and the benefits of utilizing AI-based security solutions. Following the rules specific to an industry is important for SMEs, particularly for GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), or PCI-DSS (Payment Card Industry Data Security Standard) compliance. Customer support is another essential area to be addressed in order to work efficiently when the SMEs use the products: providing the customers with immediate online service, covering any

technical problems, failures, or ways to use the product. Finally, AI-SaaS providers should come up with a 'Security First' mentality, behind which SMEs should embrace and implement, when it comes to technology adoption practice, regular training of the employees, and internal policies, among others. In this way, SMEs will be always ready to shield themselves from new forms of cyber threats.

6. Conclusion

6.1 Summary of Key Points

AI Security as a Service (AI-SaaS) is a scalable, proactively adaptive, cost-effective answer for the SME sector in terms of cyber security. This provides protection from threats in real time with machine learning capability to maintain security with new structures in large infrastructures. AI-SaaS eliminates additional costs that come with security threats because the work is automated, reducing the likelihood of consuming many resources. It does not demand almost full overhauling of SME systems as it integrates closely with them. It also assists SMEs to maintain levels of compliance, thereby helping in the checks and reporting on regulatory and industrial guidelines. The following have been attributed to high odds of high user satisfaction rates: efficiency, reliability, and simplicity. AI-SaaS solutions can be easily scalable, ensuring that the SMEs stay abreast of the ever-changing threats on the digital front; they therefore guarantee continuity, which is fundamental in governing strategic risk.

6.2 Future Directions

Expected to be the next big thing to transform security solutions for businesses, particularly SMEs, is AI Security as a Service, or AI-SaaS. It provides affordable and comprehensive security services tailored to each company's specific performance requirements. Future directions include:

- Possible refinements of the concept involve a higher level of personalization and individualization of the services, the integration into IoT (Internet of things) and Edge, the introduction of fully automated engagement systems and threat detection response systems, superior behavior analysis, affordability of the services, regulatory compliance and data privacy, user experience and usability, and the transformation of the AI-SaaS from an add-on to a competitive advantage.
- True value propositions will be offered by intelligent agents to unique datasets of an SME's domain for better threat identification and mitigation strategies. Compared to AI-PaaS (Artificial Intelligence Platform as a Service), AI-SaaS would provision even deeper into IoT (Internet of things) system topologies, delivering real-time threat alerts and responses proximate to the edge.
- The use of automated incident response tools will reduce the time taken between threat detection and response, which will prove crucial to SMEs that lack sufficient expert personnel in the field. It will be coupled with the accumulation of advanced behavioral analytics into AI-SaaS to enable the identification of potential threats or anomalies beyond the limits of conventional security tools. With SaaS, it is possible to provide SMEs with powerful tools and protect them from various cyber threats with regularly updated services and affordable monthly fees. Regarding data privacy standards, international policies are getting stricter, so AI-SaaS will integrate features that will facilitate compliance for SMEs.
- Elimination or minimization of the interface complexities will allow SMEs to handle the security solutions independently and free the firms from the backing of external IT professionals; hence, faster decision-making is attained.

REFERENCES

Ahmed, N. (2021). Machine learning and big data analytics for cybersecurity threat detection: A holistic review of techniques and case studies. *SSRAML Sage Science*, 1(1), 51–63.

Anandharaj, N. (2024). AI-powered cloud security: A study on the integration of artificial intelligence and machine learning for improved threat detection and prevention. *Journal of Recent Trends in Computer Science and Engineering*, 12(2), 21-30.

Camacho, N. G. (2024). The role of AI in cybersecurity: Addressing threats in the digital age. *Journal of Artificial Intelligence General Science (JAIGS)*, 3(1), 143-154. https://doi.org/10.3006-4023.00009

Cisco. (2023). AI security services: Control, compliance, and integration.

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78*, 544–546. https://doi.org/10.1016/j.future.2017.04.036

De Molina Rius, A. D. (2023). Foundations of artificial intelligence and machine learning. In Edward Elgar Publishing eBooks (pp. 2–18). https://doi.org/10.4337/9781803926179.00009

Drucker, P. F. (1954). *The practice of management*. Harper & Row.

Gartner. (2023). Cloud-based AI security solutions for SMEs.

Generative Adversarial Network." [Diagram]. In *Ian Goodfellow et al., Generative Adversarial Nets, 2014*

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.

Hong Kui Zhang (2021) IT Performance monitoring insights.

Https://waverleysoftware.com/blog/how-to-develop-ai-saas-product/

Https://docs.traceable.ai/docs/apigee

IBM. (2023). Customizing on-premise AI security for SMEs.

IDC. (2023). On-premise vs. cloud AI security: An SME perspective.

Liu, W., Ding, S., Zhang, X., Guo, Z., & Liang, Y. (2023). A survey of security and privacy issues in cloud computing based on big data. In *Recent Advances in Information Systems and Technologies* (pp. 177–184). Springer.

Microsoft. (2022). The benefits of cloud-based security for small businesses.

Nguyen, T., Nguyen, Q., & Vo, M. (2018). Machine learning approaches to network security: A survey. *IEEE Communications Surveys & Tutorials*, 20(4), 3491-3515. https://doi.org/10.1109/COMST.2018.2854720

Osterwalder, A., & Pigneur, Y. (2011). *Business model generation*. Wiley.

Porter, M. E., & Kramer, M. R. (2006). Strategy and society: The link between competitive advantage and corporate social responsibility. *Harvard Business Review*, 84(12), 78-92.

Ranjan, R. (2023). Artificial intelligence in cybersecurity: Cloud and on-premise solutions. *Springer*.

Salih, S. T., Zeebaree, S., Ameen, A., Alkhyyat, A., & Shukur, H. M. (2021). A survey on the role of artificial intelligence, machine learning, and deep learning for cybersecurity attack detection. In *2021 7th International Engineering Conference "Research & Innovation amid Global Pandemic" (IEC)*, 61-66. https://doi.org/10.1109/IEC52080.2021.1234567

Shahzad, F., Mushtaq, M. F., & Naqvi, S. (2020). Cybersecurity challenges for SMEs: A comprehensive review. *Cybersecurity Review*, 8(2), 129-145.

Singh, S., & Bajaj, K. (2021). Enhancing cybersecurity with AI: A detailed analysis. *Security and Privacy Journal*, 7(3), 118-135.

Sure, T. A. R. (2023). Artificial intelligence and machine learning in iOS. *International Journal of Artificial Intelligence & Machine Learning (IJAIML)*, 2(1), 82-87.

Zaman, N., Zafar, M. R., Mehmood, H., & Alharbi, H. (2020). Anomaly detection in cloud servers using machine learning techniques. *Computers, Materials & Continua*, 64(1), 1-13. https://doi.org/10.32604/cmc.2020.010536