

# We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,200

Open access books available

168,000

International authors and editors

185M

Downloads

Our authors are among the

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index  
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?  
Contact [book.department@intechopen.com](mailto:book.department@intechopen.com)

Numbers displayed above are based on latest data collected.  
For more information visit [www.intechopen.com](http://www.intechopen.com)



## Chapter

# Detection and Minimization of Malware by Implementing AI in SMEs

*Nisha Rawindaran, Liqaa Nawaf, Vibhushinie Bentotaheva, Edmond Prakash, Ambikesh Jayal, Chaminda Hewage and Daniyal Mohammed N. Alghazzawi*

## Abstract

The malware can threaten personal privacy by opening backdoors for attackers to access user passwords, IP addresses, banking information, and other personal data, whilst some malware extracts personal data and sends them to people unknown to the users. In this chapter, the authors will present recent case studies and discuss the privacy and security threats associated with different types of malwares. The small medium enterprises (SMEs) have a unique working model forming the backbone of the UK economy and malware affects SMEs' organizations. Also, the use of Artificial Intelligence (AI) as both an offense and defense mechanism, for the hacker, and the end user will be investigated further. In conclusion, finding a balance between IT expertise and the costs of products that are able to help SMEs protect and secure their data will benefit the SMEs by using a more intelligent controlled environment with applied machine learning techniques and not compromising on costs will be discussed.

**Keywords:** malware, privacy, cyber defense, ransomware, SME, artificial intelligence, machine learning, big data, GDPR

## 1. Introduction

The people in large numbers continue to keep pace with rapidly evolving technology and that has led to increased use of computers and mobile devices. This trend was clearly visible during the COVID-19 pandemic when traditional businesses resorted to using modern technologies and became dependent on applications such as QR codes and contactless payments. Against that background, the hackers took advantage of the prevailing circumstances to exploit the vulnerabilities of technology and systems, and the level of risks to privacy and national security became a serious concern to the respective authorities.

This environment became hackers' paradise and directly or indirectly provided them with an ideal opportunity to steal personal data and sell them to third parties

in return for financial benefits. They targeted large companies as well as Small and Medium-sized enterprises (SMEs). The SMEs switched to new technologies to maintain their business during the COVID-19 pandemic, but they invariably failed to increase the security aspects of the new systems due to financial constraints. Some researchers have pointed out that well-prepared organizations were able to deal with cyber incidents more efficiently than those that failed to anticipate and plan to address the reality of cyber threats due to the lack of adequate capabilities [1]. Statistically, SMEs represent more than 99% of all businesses in the UK, and given the importance of this commercial sector, the impact of disproportionate financial resources on the operational and reputational of the SMEs is of serious concern [2]. It is therefore crucially important to understand the threats early and act on them to prevent unimaginable repercussions.

SMEs have a unique working model forming the backbone of the UK economy. According to the Federation of Small Businesses (FSB) UK business statistics, there were 5.5 million small businesses at the start of 2021 [3]. The statistics showed SMEs accounted for 99.9% of this business population making up three-fifths of the employment and half of turnover in the UK private sector. These statistics verify how important the SME ecosystem is in providing an important cog to the growth and economy of a developed country. SMEs have an important role to play begging the question of how their usage of emerging technologies is keeping their data and business safe online. A paper by Daniel and Andreas [3], explores these emerging technologies especially the use of Artificial Intelligence (AI) and Machine Learning (ML) as both offense and defense mechanisms, for the hacker, and the end user. Daniel and Andreas identify and evaluate AI-related use cases that have a high impact potential on the cyber security level of SMEs, in particular highlighting the challenges of SME's environment being low in resourcing and challenges in their financial capabilities. AI and ML can be utilized for the defense against cyber threats especially malicious software (Malware). Attacks can easily be obtained from the dark web via malware-as-a-service (MAAS) making the underworld choices easier to conduct. Hackers with limited knowledge are able to use AI technology in order to create chaos and havoc in cyberspace. Traditional signature-based security systems can detect only 75–95% of untargeted mass malware attacks compared to 27% of targeted malware cyber-attacks [4] according to Daniel and Andreas. The detection rates of IT systems that do not use any form of AI cannot be sustained at the same level of security and protection when attackers are also using modern levels of AI methods to attack IT systems.

According to a study by Rawindaran et al. [5], over one million new types of malwares are created each day by malicious hackers. These types of malwares try to infiltrate networks increasing the threat of network attacks, driving the usage and demand for the use of AI and ML-driven intrusion detection protection systems (IDPS) being used throughout the SME market. These systems come with many challenges that include the cost of buying and maintaining the system and resourcing skilled engineers to maintain these systems in order to create a healthy and safe environment within their business [5]. Rawindaran et al. also explored a cost model to understand the outcome of SMEs' decision-making, in getting the right framework in place in securing their data. An experiment was conducted comparing different software vendors in understanding the information captured using AI and ML technology to stop zero-day attacks. The requirements of the UK General Data Protection Regulations Act (GDPR) were also acknowledged as part of the broader framework of the study. ML techniques such as anomaly-based intrusions did show better detection through a commercially subscription-based model for support from Cisco compared

to that of the Open Source model which required internal expertise in ML. Finding a balance between IT expertise and the costs of products that are able to help SMEs protect and secure their data, will benefit the SMEs from using a more intelligent controlled environment with applied ML techniques, whilst not compromising on costs. This research work also focuses on evaluating techniques for managing big data and detecting malware within SMEs.

## **2. Related work**

There is a wealth of literature covering many aspects of malware impact, including data protection and privacy, big data risks, and AI defense mechanisms as discussed in the following subsections. In this chapter, we restrict our attention to the areas relevant to malware detection in SMEs by implementing AI.

### **2.1 Data protection and privacy**

Data protection against malware is the biggest challenge facing the industry, and in general, malware represents a classic example of a confidentiality breach exposing personal data held by a company on its servers [6]. Trojan Horse Virus is a type of malware when downloaded to a computer resembles a legitimate program, the hackers use social engineering to infect computers with it [7]. Most Trojans are designed to take control of a user's computer to steal data and feed more malware in the process, and when once a host computer is infected, they pose significant threats to the business. However, they do not particularly target large organizations, and according to the reports, 29% of cybercrimes affecting SMEs were caused by malware attacks [8]. The Trojan viruses rely on human error [9], and unlike other forms of malware, they do not simply appear on a machine and start damaging the system on their own, and need to be manually opened, when triggered [9] have the capability to delete, block, modify, copy data, and disrupt the performance of the computers [10] by causing damage to the organization's data and personal data collected, processed, and stored in them.

Phishing is another variant of cyber-attack used by the hackers to victimize users by unethically persuading the victims to disclose personal and other critical information, and they do this by asking the user to perform standard procedures in personal data handling such as clicking on a connection to download files and applications [11]. The attackers use this technique to transmit malicious links containing viruses as worms, and if the victim followed the given instructions, the attacker would have access to private systems and personal information held in them. The staff can easily be caught unaware of the dangers due to a lack of knowledge and slackness in concentration and leaking personal data to the outside world would cause immense damage to the organization with serious repercussions. In the period between 2013 and 2015, in an extended phishing campaign, the attacker sent faked invoices impersonating Quanta (a Taiwan-based company) as a vendor, to Facebook and Google and both companies were tricked out a sum of \$100 million in payments [12]. Eventually, Facebook and Google discovered the fraud and took legal action through the US legislature [12]. This clearly indicates that large companies are not immune, and the studies reveal that phishing attacks are among the most common cyber incidents that SMEs are likely to be affected and fall victim to [1]. For instance, the cybercriminals made concerted efforts to compromise accounts by using phishing

emails with the subject 'Covid-19' [1], taking advantage of the concerns arising from the pandemic.

According to the National Cyber Security Centre (NCSC), ransomware is one of the most immediate dangers to UK businesses and other organizations [2]. 'Ransomware' is a particular variant of malware that collects data and network devices, and encrypts them, preventing user access [13], and access can be restored only by agreeing to the hacker's demands for paying the ransom. However, it is not always possible to regain access to locked data as the hackers can refuse to unlock the devices until the ransom is paid, or even after making the payment; in such a scenario, the organizations will incur data and financial losses, whilst also ending up with a damaged reputation in the eyes of the public. Hackers have targeted a range of industries, Automotive, Business services, Food and agriculture, Healthcare, Insurance, Law enforcement, Oil and gas, and Tech, demanding ransoms [14], and SMEs have not escaped harassment from the criminals. The reports suggest that many SMEs tend to assume that 'higher value targets' such as critical infrastructure and larger organizations, are likely to be prime targets [2], but the statistics suggest that 82% of Ransomware Attacks also target Small Businesses [15]. The inference drawn from these statistics is that the primary objective of hackers is to obtain data regardless of the size of the organization. The reports also suggest that, in the recent climate of cyber incidents, ransomware attacks have become a menace to organizations as well as to individuals hindering timely access to their personal data [16]. Therefore, any organization collecting, processing, and storing information should stay alert to the threats.

Another malicious software is known as 'Spyware, which is a malicious software/apps (malware) stealthily installed to monitor and track device activity [17]. It allows the attackers remote access to the victim's devices, and it enables the hackers to invade the privacy of the people by reading messages, listening to phone calls, accessing photos, viewing browsing history, capturing, and transferring audio and camera recordings in real-time [18]. According to the statistics, spyware is the third most popular malware used in attacks against organizations in 2021, and it is the second most used in attacks on individuals [19]. In January 2020, a United Nations (UN) investigation discovered that the Amazon CEO's (Jeff Bezos') smartphone was targeted by spyware and several megabytes of data was extracted from it over a considerable period (months) [19]. The UN report identified Pegasus spyware, which was created and sold by Israel-based NSO Group, as the intruder, and another investigation conducted by Amnesty International's cybersecurity team identified the same spyware as the intruder found in the phones of hundreds of people [19]. Therefore, those organizations dealing with personal data need to be aware of the reality of the threats and have preventative mechanisms to deter spyware attacks. The failure to do so will allow hackers to obtain sensitive data and sell captured data through spyware attacks on the Dark Web, and consequences leading to immense damage to personal privacy in the first place, and eventually with threats to national security.

Adware is another (unwelcome) software designed to throw advertisements up on your screen, and they piggyback on another program to trick you into installing it on your PC, tablet, or mobile device [20]. Once the user's device is hijacked by the adware, it detects the location, collects information about the Internet sites visited, and presents advertising pertaining to the types of goods or services searched by the user [20]. There is also a risk of data being shared with third parties, and that amounts to a violation of personal privacy. The threat posed by adware is not limited to large companies, regardless of the size of the organization it affects everyone, and

the consequences can range from threats to personal security as well as to national security.

Malware, in general, represents a classic example of a confidentiality breach extracting and exposing personal data held by a company by hacking and downloading personal data from systems and devices [6]. In the process, malware cause interruptions to the network of the enterprise irrespective of the organization's size. Malware also has the capability to record browsing history, monitor applications being used, and make copies of personal information like user IDs, passwords, and bank account details. That is not all, Malware by hacking the network of an organization can affect the confidentiality and integrity of personal data and delete/edit/steal personal data. In some cases, malware can potentially disable critical services offered by the company, and that will make the services unavailable to the clients with consequences damaging the image of the organization's reputation, affecting trustworthiness, and contributing to financial losses.

Data is valuable to any organization whether it happened to be large or small, and the crucial issue is that it is a sellable item and anyone getting access to it can make money by selling it to the highest bidder on the dark web. Data is wide-ranging and consist of information about the organization, and sensitive personal data about the employees and the clients, and the onus is on the respective organization to ensure the security of that data by having in place adequate data protection mechanism in compliance with data protection regulations applicable at the regional or country level. For example, an organization in the UK collecting, processing, and storing information about their customers, has an obligation to follow data protection mechanisms/guidelines set out in UK GDPR that is on par with the EU regulations. Therefore, it makes any organization outside the EU engaged in commercial activities processing information of the citizens of the EU also bound by EU GDPR.

The application of the GDPR does not depend on the size of the organization. Whether it is an SME or a large organization in the EU or UK, if they collect, process, and store data, they should abide by the GDPR regulations. However, some of the obligations of the GDPR may not apply to all SMEs with less than 250 employees. For example, SMEs do not have to keep records of their processing activities unless the processing of personal data is a regular occurrence, poses a potential threat to individuals' rights and freedom, or includes sensitive data or criminal records [21, 22]. Also, SMEs are required to appoint a Data Protection Officer only if the organization is processing data as part of the main business, and it may also pose threats to an individual's rights and freedoms [22].

A common misconception was that the GDPR would only be looking into the data protection practices of large multinational enterprises. The €50 m fine imposed on Google by Commission Nationale de l'informatique et des libertés (CNIL) or the €204 m fine imposed on British Airways were high in comparison to what had been imposed on smaller enterprises [23]. However, a CNIL had imposed a fine of €400,000 on the real estate firm, SERGIC, whilst the less performing advertising Agency, QuickClickNow, was served with a fine of only €47,000 by the Polish Data Protection Authority [23].

GDPR stipulates that data breach of any kind associated with any variant of malware attack, the data subject, and the relevant authorities should be notified within 72 hours [6], and data breach notification should include the details of the nature of the breach. These are specified as personal data, the name and contact details of the data protection officer, contact point for obtaining additional information, consequences of the personal data breach; description of the measures taken or proposed

to deal with the data breach, and description of the measures taken to mitigate any adverse effects, clear advice on the steps that the individuals should take to protect themselves, and what assistance the organization would be prepared offer them [24] This framework of data protection mechanisms would provide the organizations the knowhow and competences to deal with malware-related data breaches with confidence and to avoid the damage and impact on the reputation and trustworthiness of the organization.

## **2.2 Malware impacts on SMEs**

Every year a survey of the UK Cyber Security Breach Survey 2022 [25] is conducted by the Department of Digital, Culture, Media, and Sports (DCMS) in line with the UK National Cyber Strategy, detailing the cost and impact of cyber-attacks on UK businesses. The year 2022 showed that 39% of UK businesses have been a victim of cyber-attacks. The most common attacks were phishing which accounted for 83 and 21% were attack types such as a denial of service, malware, or ransomware attack. Despite having a lower percentage of attacks, businesses cited ransomware as a major threat, with 56% having a policy not to pay the ransom as quoted by this survey. The report gave insight on SMEs and the culture of not believing ransomware will pose a threat to their business, and that it was unlikely to happen, as SMEs assumed that they did not hold anything of value the hackers would be interested in. In the event of a cyber-attack, the SMEs in this survey tended to resort to traditional methods of recovery, such as shutting down systems and re-booting with backed-up data. SMEs also sought advice from external IT providers for assistance in the event of an attack and some had no plans at all. However, SMEs who took cyber-attacks seriously viewed ransomware such as malware as a serious threat and often had a strict plan in place in the event of an attack. The survey particularly raised points such as SMEs not necessarily engaging in industry standards to help protect their business such as Cyber Essentials and how the uptake for this standard was still exceptionally low as they felt they did not meet the criteria. SMEs who felt they did not have the technical understanding was clearly observed in this survey to suggest that the role of external IT companies is particularly important in the supply chain model. This is so SMEs can access the benefits of a larger and more resourced specialist. The survey also highlighted the importance of how the supply chain poses a threat as an entry point for attackers and the business can only be as strong as the weakest link of the supply chain. The survey indicated that fewer than one in ten organizations actively monitor the risks within their supply chain and so this presents a clear risk for the future. This DCMS survey is particularly important as it is a window into the activities year on year on how trends of cyber-attacks affect businesses in the UK and how our behavioral patterns have a consequence towards risk and its management of it.

A study conducted by Tirumala et al. [26], explored that ransomware (malware) attacks have forced businesses to think about the security of their resources due to SMEs not having the right cyber defense mechanisms in place. This research explores implementing a “Raspberry Pi” based intelligent cyber defense system (iCDS) for SME networks and Smart-homes and how these devices are used to filter malicious contents from incoming traffic and be able to detect malware using AI. The paper concluded that the “Raspberry Pi” device is feasible to use to develop a low-cost iCDS as an alternative to the traditional rule based IDSs in use. Tirumala’s study reinforces the study of Rawindaran et al. [5] on the uses of open-source IDS versus commercial IDS, and the challenges faced when introducing ML and AI technologies versus traditional

IDS to promote better hygiene within the cyber interface. Rawindaran et al. took requirements from the UK General Data Protection Regulations Act (GDPR) as part of the broader framework of the study and further explored the techniques of ML to show better detection through a commercially subscription-based model for support from Cisco compared to that of the Open-Source model which required internal expertise in ML. The study went on to discuss the challenges between IT expertise and costs of products to help SMEs protect and secure their data and the benefits of moving to an intelligently controlled environment and not compromising on costs. Kshetri [27] added that.

*“Cybersecurity company Blue Voyant’s survey found that 97% of firms had been impacted by a cybersecurity breach in their supply chain, and 93% had suffered a direct cybersecurity breach due to their supply chains’ weaknesses.” [27].*

There are various points in an SME business whereby malware can make its presence, and Kshetri’s study performs an exploration into the various elements that contribute to the health of SMEs. Part of the vulnerability lies in the much-used supply chain partners to SMEs. These are in the form of third-party software, managed service providers (MSPs), IT vendors and other providers of software and its content, vendors in a physical capacity, and non-IT contracting vendors. For third-party software, the vulnerability lies in the “implanting” of malicious codes within this software. Understanding where this software come from and how they are managed within the supply chain can be a challenge and barrier. For MSPs, it is the reliance of these MSPs pushing out updates that could contain malicious code from their supply chain, in providing their own service of performing remote monitoring on managed computers. When it comes to IT vendors and partners, both virtual and physical, understanding the vulnerabilities of installing or injection of malicious codes by the attack on these vendors before products get shipped or provided to businesses. Lastly non-IT contracting vendors are using this platform to gain access to privileged resources to target the business. On each story of this supply chain, Kshetri gave examples, such as the attack on Equifax in 2017, showing a compromise of 146.6 million social security numbers and personal data. In the attack on Kaseya in 2021, victims were from 17 countries targeting nearly 1500 businesses. SolarWinds breached in 2020, showing an impact to 18,000 of their customers in the installation and injection of malicious codes. Most recently in the August of 2022, Advanced, a company that provides software for the NHS, experienced a ransomware attack causing patient data to be the target. Advanced as a supply chain provided NHS with services that included patient referrals, ambulance dispatch, out-of-hours appointment bookings, mental health services, and emergency prescriptions as reported by The Guardian [28].

Research is consistently showing ways in which to overcome malware attacks from various angles of business management, technology management, and of course human awareness within the SME. A paper by Cruzado et al. [29], suggested SMEs develop a “HOGO” reference framework based on two regulations, ISO 27002, and ISO 27032 for cybersecurity. The “HOGO” framework in this study applies good practices relating to internet security, critical infrastructures for information, network security, and information security, covering all aspects of the SME business [29]. Cruzado explains the framework being a combination of ISO 27002, which provides good controls for information security, and ISO 27032, providing good practices and recommendations. Both take into account the risks of the context for the security of the company’s information. Using regulations can help identify supply chain partners



with high cybersecurity risks (e.g., the U.K.'s Cyber Essentials) and reduce vulnerability in third-party software through frameworks such as "HOGO."

### **2.3 Big data risks**

This section of the research is related to the essentials of the big data collection process through several resources from Wireless Sensors Networks (WSN) and other IoT sensors. Data collection is a procedure of collecting significant information to evaluate the outcome process and it becomes gradually significant since the burst of big data and the new development of technologies. SMEs collect an increasingly large amount of data, with information following into departments from many directions. For the data that SMEs collect to be meaningful and actionable, it needs to be provided in real-time so policy makers or managers can make decisions based on understanding the situation as it is, and not as it was. Thus, what technology is needed to make the most up-to-the-moment besides developing and modifying the policies to make the most of up-to-date data?

Big data refer to collecting and managing data in three forms High Volume, High Velocity, and Wide Variety. Big data management refers to the effective procedure that focuses on the management and usage of structured and unstructured data and its main purpose is to attain great data quality and accessibility for big data applications that certainly influence the performance of the organization [30]. The appropriate oversight of data throughout its life cycle is important to optimize its utility and minimize potential errors.

The most crucial purpose of big data is to guarantee that the data is captured and stored securely from resources, so it includes good data protection to avoid cyber risks. Big data management is challenging, and it has a vital role in managing the organization's data, it's a useful technique companies follow to maintain or preserve the data. The critical role in exploring and analyzing a big quantity of data is to discover effective patterns for big data. The business organization/SME aims to generate products and provide insight from this big data to improve its product achievements.

Recent technological developments in the field of communication struggle with internet connectivity issues that have led to the development of Wireless Mesh Networks (WMN). WMN is a wireless form of communication that works on the multi-hop concept for connecting multiple devices in the same grid area [31].

The multi-hop nature of WMN tied with fewer security mechanisms being employed makes it mandatory to make WMN secure from foreign attacks and malware. It's clear that security needs more attention in the characteristic of WMN. The Wireless Sensors Networks (WSN) enable the communication between devices and Radio Frequency Identification (RFID) allows the category of devices to collect the data. The amount of data collected from WSN puts entities at risk as they become more easily recognized with unauthorized processing, which can disrupt data protection laws, for instance, General Data Protection Regulation (GDPR), any data breaches, the data controlled will pay fines under GDPR (4% of annual turnover or 20 million) or evolving data protection laws [32]. There are many security concerns related to wireless communication, network transmission, information processing, and privacy. Also, two types of security parameters must be upgraded such as encryption and authentication.

The perception of business organizations/SMEs believes that more data is collected to gain visions and offer greater knowledge and greater benefit to the organizations, and data minimizations will limit the success of some specific applications.

Also, big data has a big impact on security performance and should be evaluated. Apparently, gathering mass amounts of data using WSN can be acceptable only if the benefits outweigh the privacy and security of personal data. Therefore, securing personal data has become a significant challenge in contradiction to the growing malware and data risks [33]. There is more to be done in this aspect of the collected data addressing privacy and security concerns as explained in the previous Section 2.1.

Technology development is predicted based on the collected data from a particular application, so examining the collected data and detecting any deviations to report the error is significant by applying artificial intelligence, such as the machine learning algorithm that will help to perform and detect malware. Prediction is made by different data mining approaches using the data set through the networks. Sophisticated algorithms are mainly used to predict and detect malware. Further investigation of the potential malware risk is recommended to optimize security in SMEs.

## **2.4 Artificial intelligence for defense mechanism**

There are high risks with big data in SMEs and it is crucial and significant to preserve by determining the security and utilizing a secure protocol that could be the contributing factor prevent various types of attacks. A novel method by applying a metaheuristic algorithm would be suggested for security and protection. Metaheuristic algorithms are general-purpose algorithms that can be applied to a wide range of optimization problems, with only minor alterations and modifications to the basic algorithm definition. Most metaheuristic techniques attempt to mimic biological, physical, and natural phenomena. Many heuristic and metaheuristic algorithms have been applied to improve solutions quality and solve large complex network optimization problems of maintaining QoS and have been shown to be important tools in a variety of disciplines. Metaheuristic methods can be developed to determine the best location to place the infrastructure and data to optimize security and reduce risks arising [34, 35].

The conversations and collaboration have taken place around making sure the necessary infrastructure is put in a secure place to help these SMEs succeed. The world is becoming smaller and smaller, so we need to bet on these digital innovations and help SMEs to reach out to secure markets where there is no longer a traditional definition. It is also important to consider the environmentally sustainable financial issues that are built to support these sectors. The overall vision is to optimize security and reduce malware risk in SMEs based on the recent technological revolution using AI approaches.

## **3. Technical methodology**

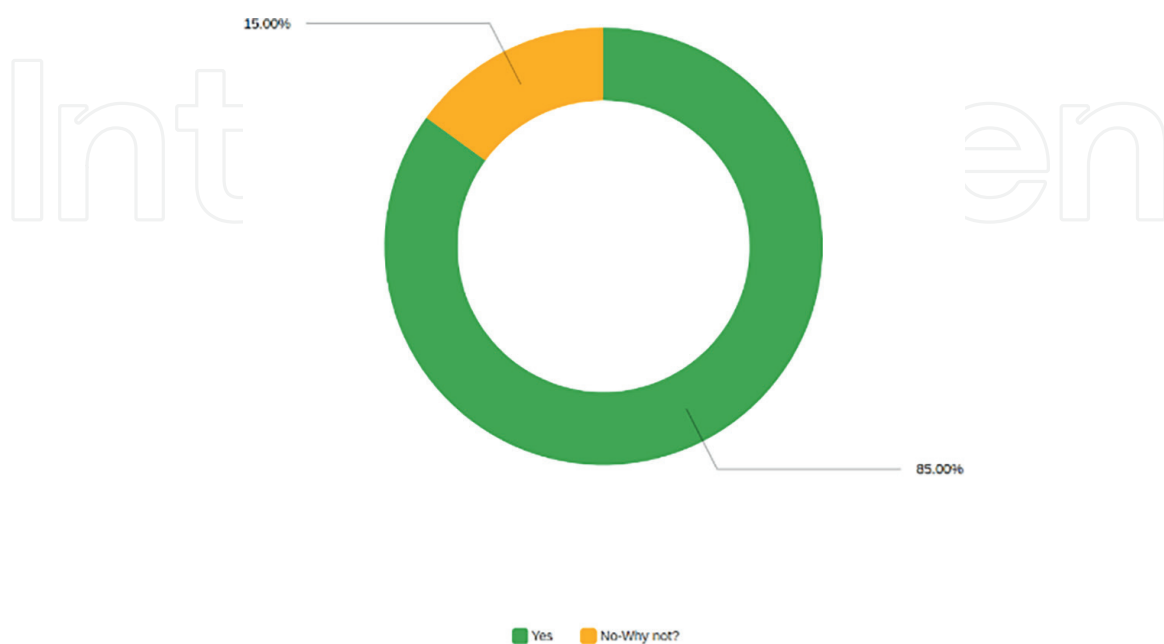
The research methodology describes the methods used to collect and analyze data. The selection of the data collection method depends on the nature, scope, aims, and objectives of the research. In this research, the authors collected the data using secondary and primary data collection methods and analyzed the data to answer the research question. The outcome of this research aims to add new knowledge to the existing literature. The authors used published data in books, government publications, newspapers, magazines, and journals. These sources provided factual data related to the research scope. Finding secondary data with 100 percent applicability to one particular research scope is difficult; therefore, the primary data

collection method has also been used in this research. However, the data collected from secondary resources have credibility and contribute to the validity of the research study.

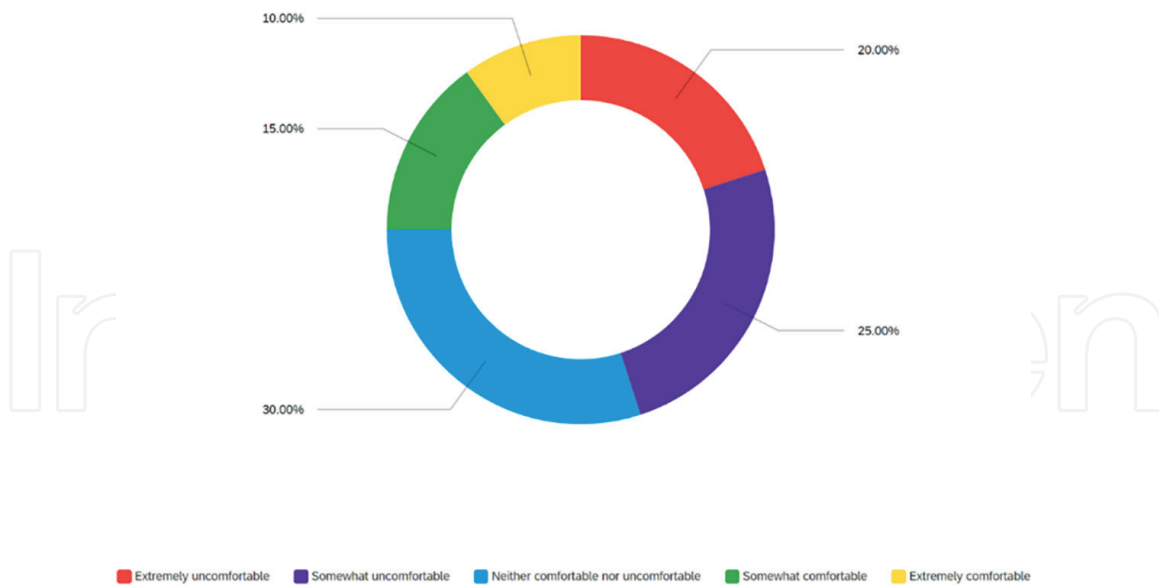
The technical methodology took the form of a survey questionnaire. In order for the authors to deeper understand how SMEs, manage the detection and minimization of malware, the implementation of AI over standard traditional methods are discussed in this paper. The aim of this paper is to understand SMEs' awareness of Machine Learning Cyber Security (MLCS) software packages in SMEs; hence a survey was conducted to observe the uses of MLCS in the protection of data within the SME, against cyber threats as part of the SME cyber security implementations. A survey questionnaire was conducted through market research to a targeted SME audience in Wales. The survey was sent to 600 registered members of the Cyber Resilient Centre (CRC) of Wales. The survey was sent via email. The results showed that 40 people completed the survey with completed answers. The majority of the questions were answered by SME management between the ages of 46–55 and being decision-makers within the business. As part of GDPR, participation was voluntary, and all responses were kept anonymous. Consent was obtained and participants were given the right to withdraw and cancel participation at any one time. Various questions were asked to the SME population members of CRC.

#### 4. Discussion and implemented techniques

The results from the survey are discussed further and analyzed to give feedback accordingly. **Figure 1** below showed that 85% of the respondents came back stating that they have the right cyber security software package in place to protect their business from cyber threats. The percentage who did not have any software in place was 15% of the respondents as shown below in the pie chart.



**Figure 1.**  
*SMEs having the right cyber security software package.*

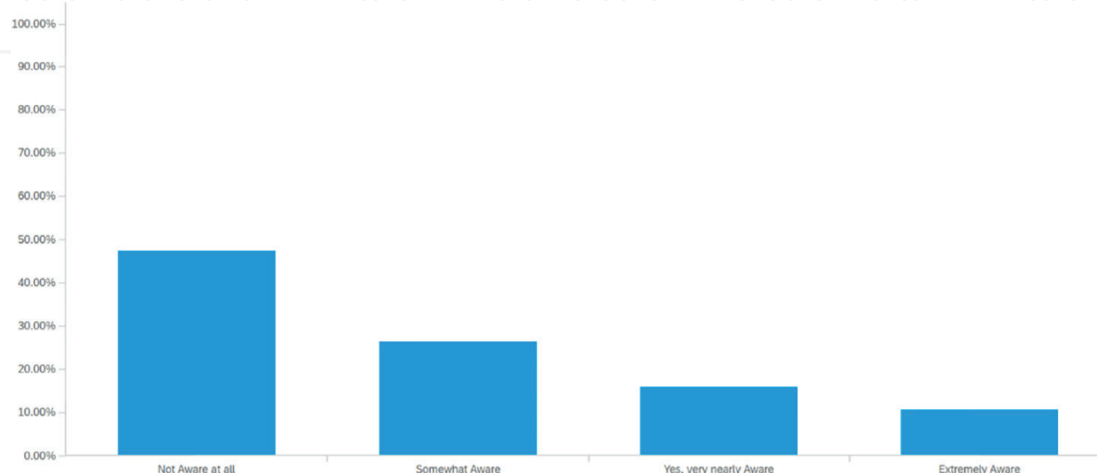


**Figure 2.**  
 SMEs understanding of ML.

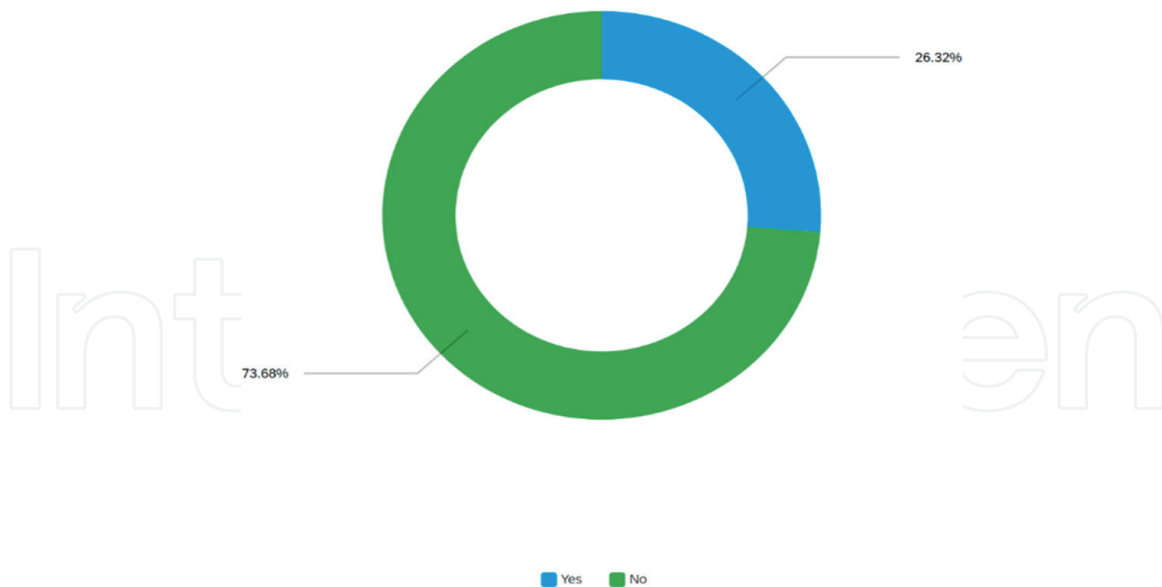
From the 85% of respondents that said “Yes” in **Figure 1**, used a combination of commercial, non-commercial, and open-source software to protect their business. The next question looked at how comfortable SMEs were with the understanding of ML. **Figure 2** shows this breakdown with 10% being “Extremely comfortable” with ML, 15% being “Somewhat comfortable” and 30% being “Neither comfortable nor uncomfortable” with the understanding of ML.

**Figure 2** went on to explain how 25% of SMEs were “Somewhat uncomfortable” with ML and 20% were “Extremely uncomfortable” with the understanding of ML. **Figure 3** answered the question on the awareness of MLCS and its application within the SME business. Nearly 11% were “Extremely Aware” of MLCS software packages within the business, 15% were “Yes, very nearly Aware” and 26% were “Somewhat Aware”.

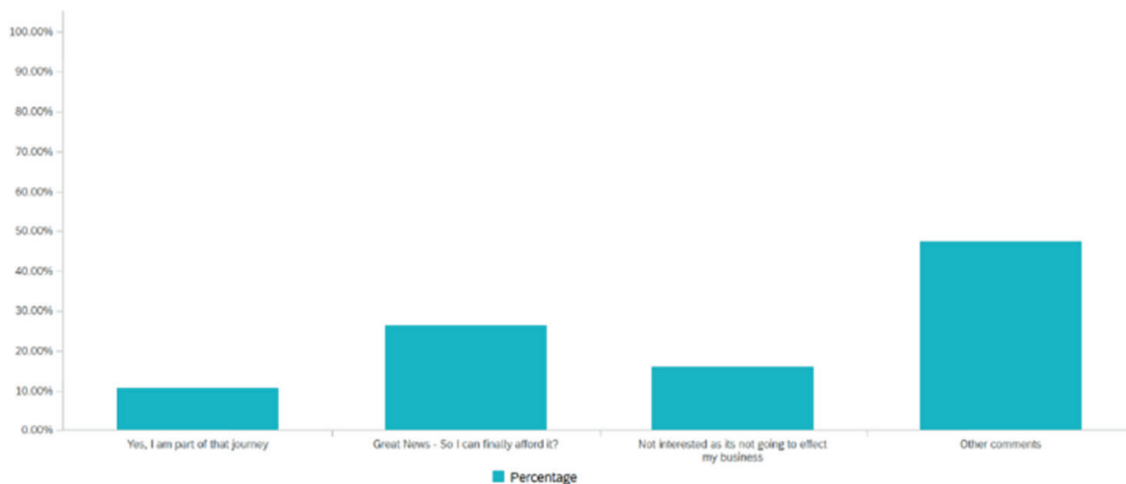
**Figure 3** resulted in 47% of the SMEs “Not Aware at all” of MLCS software packages within their business. The next survey question asked these SMEs if their



**Figure 3.**  
 Awareness of MLCS software packages within the business.



**Figure 4.**  
SMEs recognizing existing software having ML to detect cyber attacks.



**Figure 5.**  
SMEs thoughts on AI and ML usage and its affordability.

existing cyber security software packages supported ML to detect cyber-attacks as shown in **Figure 4**.

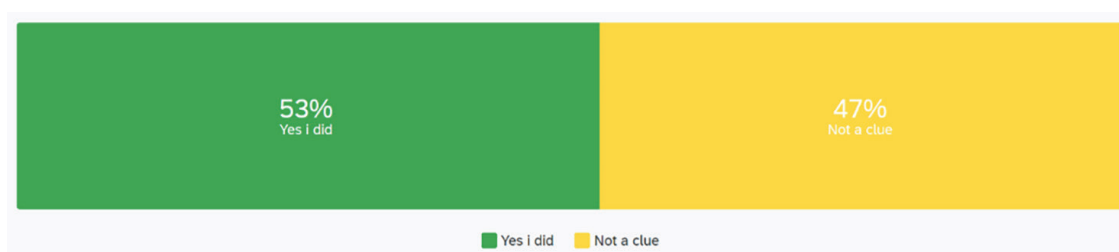
**Figure 4** showed that 73.7% of SMEs said they were aware of their cyber security software packages supported ML to detect cyber-attacks. Out of those who said “No” were 26.3% of the respondents. The SMEs reasons were “due to costs” and the fact that they “Did not think that ML will be effective in cyber security and hence did not use or need this feature”. The survey then asked SMEs if they knew of the recent Intuit research study in collaboration with the 2019 Gartner CIO survey that showed findings of SMEs already adopting next-generation AI and ML technology for many parts of their business already to combat the increase in cyber-attacks and that these costs were now affordable. **Figure 5** below visualized the results showing that 10% said they were “part of the journey” in attaining this intelligent software and 25% of the respondents were shocked that they could finally afford it.

**Figure 5** showed 15% of SMEs saying they were “Not interested as it’s not going to affect their business”. A large percentage of 47% had other comments such as “having

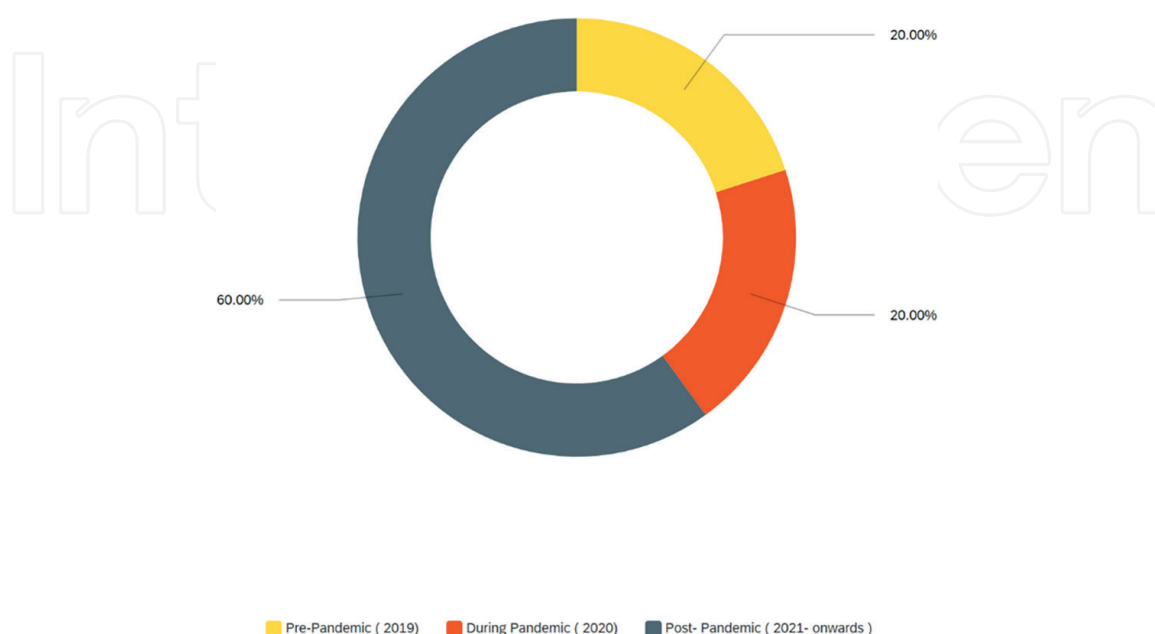
no idea about ML software”, “Only just become aware that Defender used machine learning” and some saying, “Never heard about it” and some “wanting to need time to understand the benefits”. The survey pointed out the average ransomware attack payout was now \$177,000 according to Gartner 2020. Based on the fact explained, the survey went on to ask SMEs about their strategic planning in adopting ML to implement within business. **Table 1** showed 42% of SMEs were already talking to experts in this field, whilst 16% would rather concentrate on sales and marketing than cyber security, and still debating the perspective of costs.

SMEs thoughts on ML adaptation for cyber security	Percentage
None—I would rather just concentrate on the budget for Sales and Marketing than Cyber Security	16
Yes—I am trying to figure this out from a cost perspective	16
Yes—already talking to experts in this field	42
Any other comments to add	26

**Table 1.**  
 SMEs thoughts on ML adaptation for cyber security.



**Figure 6.**  
 SMEs knowledge of MLCS in predicting malware.



**Figure 7.**  
 SMEs being victims of cyber attacks.

Interestingly 26% of SMEs had varied strategic plans such as “*Cloud back up*”, “*advice taken from Cyber Resilience Centre for Wales*”, “*Investing in training to adopt a robust ISMS that will be conform with ISO 27001*”, “*Make backups*” and “*Ransomware is something we deal with as with any other business outage*”. The survey continued to ask SMEs if they knew MLCS software packages (compared to regular detection software) are trained in detecting a range of malware and can proactively detect, foresee breaches, and predict the types of malwares that might infiltrate the network.

**Figure 6** showed that 53% said “Yes” to the statement above and 47% of SMEs did not have a clue.

The survey then asked the question to SMEs if their business was a victim of cyber-attacks (pre and post-pandemic). **Figure 7** below shows that 20% of SMEs surveyed were victims of cyber-attacks pre-pandemic (2019) and during the pandemic (2020).

This then left 60% of SMEs being victims of cyber-attacks post-pandemic (2021-onwards). One SME victim in the case study said, “*We had not secured our server with the latest updates. We took the server offline and had most of our files available on our computers still so lost a small portion. No customer data held on the server.*” Another SME victim said that “*We employed a Social Media company who sadly clicked an email message which got our Instagram account hacked. We lost 30,000 followers. That’s it really, we no longer use them and have learnt while hacking is not nice, it happens and the companies you bring in to help need to be registered to confirm they understand the damages they can cause to small business by not following a simple set of do’s & don’ts.*”

## 5. Conclusion

Any organization, regardless of the size, could be susceptible to malware threats and risk becoming victims of cybercrime, unless proper defense mechanisms are put in place. The failure to do so will pose threats to personal privacy and national security. The threats posed by malware are not a new phenomenon for large organizations in comparison to that SMEs. Also, large companies are equipped with resources both in terms of financial and technical capabilities, with policy defense mechanisms in place, whereas SMEs have limited resources, face budget constraints, and often lack in-house technical skills. That makes SMEs an attractive target for cyber-criminals, and breaches of personal data will have immediate consequences on the organizations and will impact the company finances, corporate image, and trustworthiness of the organization. Therefore, the onus is on the large organization to support SMEs with the provision of technical and policy know-how to protect SMEs from malware attacks.

The overarching focus must be to understand the different variants of malware, act on them promptly, manage the impact of the data breaches ensure the security of personal data, avoid recurrence by adherence to guidelines and regulations set out in the GDPR, to protect the interests of the data subjects, employees, the organization, and not forgetting the impact of bad publicity on the organization itself regardless of the size or the brand name of the enterprise.

Whilst the research is strong on the benefits of emerging technologies such as AI and ML in the detection of malware and intelligent cyber-attacks, MLCS software packages do take on an important role in the SME ecosystem in combatting these threats. Collaboration between technology, organization, and the understanding of

human awareness, might still need some catching up to do. Through various methods of engagement within the industry coupled with education and training of the workforce, regularly conducted SME surveys such as the one in this paper, will give better meaning and understanding to the structure of how SMEs are having to cope and keep up with technology evolving in keeping their data safe and secure. Whilst AI and ML are emerging technologies that are maturing in their capabilities to protect intelligent cyber warfare, life in general for SMEs at the moment is trying to keep the balance between running their business running and prioritizing financially between sales, marketing, and now cyber. Support from decision makers and business owners taking on this responsibility will still be a long and windy road, where technology will finally try and meet the demands and affordability of the uses of MLCS within the SME business. Allowing for the costs to become affordable will rely on the supply and demand of the supply chain driving the affordability economically for all SMEs to get on the bandwagon of using intelligent software without breaking the bank when trading online to continuously keep their data safe and secure in line with GDPR within the context of the UK.

The novelty is to apply metaheuristic algorithms for detecting and predicting malware in SMEs and to optimize the problem. Also, more investigation of the likely malware is proposed to optimize security in SMEs.

## **6. Recommendations**

All the software applications used must have integrated protection by design and default. That is an important precautionary measure to avoid incidents of breaches and to mitigate risk vulnerabilities associated with the security of sensitive data thus safeguarding the rights of the data subject. Also, risk impact assessment must be undertaken to evaluate the susceptibility to risks and to take measures to mitigate the risks.

The implementation of a consolidated uniform global level data protection mechanism is an imperative requirement to protect user information collected by small, medium, and large enterprises, and meaningful, robust provisions must be embedded in it to bring prosecutions against the perpetrators.

Within the SME market, decision-makers play an important role in keeping their business safe. With the onset of GDPR, the role of the data controller should allow for better understanding and safekeeping of the types of protection the SME business will use in order to keep their data safe. Having the right technology in place does have its advantages, however, whilst many SMEs still play the game of having “no protection”, many still use traditional methods that are getting out of date. With the intelligence of the underworld growing, AI and ML software are becoming highly sought after at a cost to combat these threats. SME organizations are being advised to keep their level of security higher and use the right technology to help. This balance in getting the right IT expertise, coupled with the right costs of products, will inevitably help SMEs protect and secure their data. SMEs will surely benefit from using more intelligent controlled environments with applied machine learning techniques thus this demand will hopefully favor on costs. That said, the human engagement within this cycle is room for improvement, and the need to be trained and awareness raised in the workforce. This still remains a gap that will need to be managed by SMEs to stay ahead of the cyber warfare upon us already!



## Acknowledgements

This paper has been supported by the British Council, KESS2—Knowledge Economy Skills Scholarships, Cardiff School of Technologies—Cardiff Metropolitan University, Cyber Resilience Wales, and Aytel Systems Ltd., Cardiff, UK.

## Conflict of interest

The authors declare no conflict of interest.

## Author details

Nisha Rawindaran<sup>1</sup>, Liqaa Nawaf<sup>1\*</sup>, Vibhushinie Bentotahewa<sup>1</sup>, Edmond Prakash<sup>2</sup>, Ambikesh Jayal<sup>3</sup>, Chaminda Hewage<sup>1</sup> and Daniyal Mohammed N. Alghazzawi<sup>4</sup>

1 Cardiff Metropolitan University, Cardiff, UK


2 University of Creative Arts, Farnham, Surrey, UK

3 University of Canberra, Bruce, Australia

4 King Abdulaziz University, Jeddah, Saudi Arabia

\*Address all correspondence to: [llnawaf@cardiffmet.ac.uk](mailto:llnawaf@cardiffmet.ac.uk)

## IntechOpen

© 2022 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

## References

- [1] European Union Agency for Cyber Security. Phishing Most Common Cyber Incident Faced by SMEs. 2021. Available from: <https://www.enisa.europa.eu/news/enisa-news/phishing-most-common-cyber-incidents-faced-by-smes>
- [2] Huq S. Ransomware: the number one cyber threat for enterprises and SMEs. 2022. Available from: <https://www.ncsc.gov.uk/blog-post/ransomware-the-number-one-cyber-threat-for-enterprises-and-sme>
- [3] Daniel K, Andreas J. Evaluation of AI-based use cases for enhancing the cyber security defense of small and medium-sized companies (SMEs). *Electronic Imaging*. 2022;**34**:1-8
- [4] Pohlmann N. Cyber Security. The Textbook for Concepts, Principles, Mechanisms, Architectures, and Properties of Cyber Security Systems in Digitalization (transl. from German). 2019. Available from: [https://doi.org/10.1007/978-3-658-25398-1\\_15](https://doi.org/10.1007/978-3-658-25398-1_15). [Accessed: August 26, 2021]
- [5] Rawindaran N, Jayal A, Prakash E, Hewage C. Cost benefits of using machine learning features in NIDS for cyber security in UK small medium enterprises (SME). *Future Internet*. 2021;**13**:186. DOI: 10.3390/fi13080186
- [6] Valdetero J. Do All Malware Attacks Need to be Reported under the GDPR?. 2021. Available from: <https://www.gtlaw-dataprivacydish.com/2021/02/do-all-malware-attacks-need-to-be-reported-under-the-gdpr/>
- [7] Towergate. Cyber Attacks and Security Threats—The Impacts of Cyber Attacks and How SMEs Can Help Prevent Them. 2020. Available from: <https://www.towergateinsurance.co.uk/liability-insurance/smes-and-cyber-attacks>
- [8] NortonLifeLock Employee. What is a Trojan?. (N.D). Available from: <https://uk.norton.com/internetsecurity-malware-what-is-a-trojan.html>
- [9] Get Support IT Services. What Is a Trojan Horse? The Essential Guide for Small Business. 2020. Available from: <https://www.getsupport.co.uk/blog/2020-12/what-is-a-trojan-horse-the-essential-guide-for-small-business/>
- [10] Kaspersky. What is a Trojan Horse and What Damage Can It Do?. (N.D). Available from: <https://www.kaspersky.co.uk/resource-center/threats/trojans>
- [11] Zainab A et al. Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*. 2021;**3**:563060. DOI: 10.3389/fcomp.2021.563060
- [12] Checkpoint. The 5 Most Expensive Phishing Scams of all Time. (N.D). Available from: <https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/the-top-5-phishing-scams-of-all-times/>
- [13] Kaspersky. Ransomware Attacks and Types—How Encryption Trojans Differ. (N.D). Available from: <https://www.kaspersky.co.uk/resource-center/threats/ransomware-attacks-and-types>
- [14] Pavilion. The Biggest Ransomware Attacks of 2021. 2021. Available from: <https://www.pav.co.uk/blog/the-biggest-ransomware-attacks-of-2021/>
- [15] Drapkin A. 82% of ransomware attacks target small businesses, Report

Reveals. 2022. Available from: <https://tech.co/news/82-of-ransomware-attacks-target-small-businesses-report-reveals#:~:text=twitter-,82%25%20of%20Ransomware%20Attacks%20Target%20Small%20Businesses%2C%20Report%20Reveals,employees%20are%20most%20at%20risk.&text=Small%20businesses%20are%20increasingly%20targeted,by%20ransomware%20recovery%20specialists%20Coveware>

[16] ICO. Ransomware and Data Protection Compliance. (N.D). Available from: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/ransomware-and-data-protection-compliance/>

[17] Kaspersky. What is Spyware? (N.D). Available from: <https://www.kaspersky.co.uk/resource-center/threats/spyware>

[18] Phillips G. How to Protect Yourself From Unethical or Illegal Spying. 2019. Available from: <https://www.makeuseof.com/tag/how-to-protect-yourself-from-unethical-or-illegal-spying/>

[19] Ahaskar A. Spyware: How They Impact Enterprises and How to Spot an Infection. 2021. Available from: <https://www.spiceworks.com/it-security/cyber-risk-management/articles/spyware-threat-against-enterprises/>

[20] Malwarebytes. Adware. (N.D). Available from: <https://www.malwarebytes.com/adware>

[21] ICO. Who Needs to Document Their Processing Activities?. (N.D). Available from: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/>

who-needs-to-document-their-processing-activities/

[22] European Commission. Do the Rules Apply to SMEs?. (N.D). Available from: [https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-rules-apply-smes\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-rules-apply-smes_en)

[23] PrivacyPerfect. GDPR for SMEs: Benefit or Burden?. 2019. Available from: <https://blog.privacyperfect.com/gdpr-for-smes-key-points>

[24] Intersoft Consulting. Art. 33 GDPR- Notification of a Personal Data Breach to the Supervisory Authority. (N.D). Available from: <https://gdpr-info.eu/art-33-gdpr/>

[25] GOV.UK. Cyber Security Breaches Survey 2022. (N.D). Available from: <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022>

[26] Tirumala SS, Nepal N, Ray SK. Raspberry pi-based intelligent cyber defense systems for SMEs and smart-homes: An exploratory study. EAI Endorsed Transactions on Smart Cities. 2022;**6**(18):e4-e4

[27] Kshetri N. Economics of supply chain cyberattacks. IT Professional. 2022;**24**(3):96-100

[28] The Guardian. NHS Ransomware Attack: What Happened and How Bad is it?. 2022. Available from: <https://www.theguardian.com/technology/2022/aug/11/nhs-ransomware-attack-what-happened-and-how-bad-is-it>. [Accessed: August 25, 2022]

[29] Cruzado CF, Rodriguez-Baca LS, Huanca-López LG, Acuña-Salinas EI. Reference framework “HOGO” for

cybersecurity in SMEs based on ISO 27002 and 27032. In: 2022 12th International Conference on Cloud Computing, Data Science & Engineering (Confluence). IEEE Xplore Digital Library; 2022. pp. 35-40

International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2018. New York, NY, USA: IEEE; 2019

[30] Ugli MIB. The importance of data mining In retail industry. *International Journal of Progressive Sciences and Technologies*. 2021;28(1):216-223

[31] Sayad L, Bouallouche-Medjkoune L, Aissani D. An electromagnetism-like mechanism algorithm for the router node placement in wireless mesh networks. *Soft Computing*. 2019;23(12):4407-4419. DOI: 10.1007/s00500-018-3096-y

[32] Gruschka N, Mavroeidis V, Vishi K, Jensen M. Privacy issues and data protection in big data: a case study analysis under GDPR. In: 2018 IEEE International Conference on Big Data (Big Data). IEEE Xplore; 2018. pp. 5027-5033

[33] New Technologies and Challenges for Personal Identity—The Digital Health Society. Feb 2021. Available from: <https://thedigitalhealthsociety.com/new-technologies-and-challenges-for-personal-identity/>. [Accessed: August 5, 2022]

[34] Nawaf L. Optimizing IoT Security by Implementing Artificial Intelligence—Infosecurity Magazine. May 2020. Available from: <https://www.infosecurity-magazine.com/next-gen-infosec/optimizing-iot-ai/>. [Accessed: August 1, 2022]

[35] Nawaf LF, Allen SM, Rana O. Optimizing infrastructure placement in wireless mesh networks using NSGA-II. In: 20th International Conference on High Performance Computing and Communications, 16th International Conference on Smart City and 4th