Chinese Traditional Medicine Journal

ISSN : 2693 6356
2020 | Vol 3 | Issue 5

Methods for Securing Information Systems in the Microfinance Industry

B.Swathi, M.Saritha
Assistant Professor[1,2], Vignan Institute of Technology and Science
GITAM University,Hyderabad,

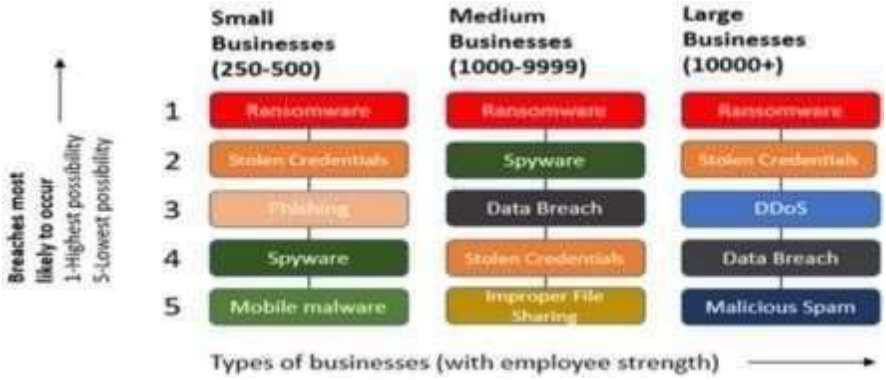
Abstract
The expanding usage of computer networks in commercial and administrative sectors of financial institutions presents a variety of challenges for executives concerned with maintaining the security of sensitive information. This one-of-a-kind case study looked at how the top brass at a modest financial institution countered attempts by malicious actors to get into the firm's computer networks. Data security is an issue that affects all sizes of financial services businesses, and this article looks at those issues and possible solutions. Issues facing financial services companies are the main topic of this article. These results were confirmed by secondary sources. This article provides a comprehensive evaluation of the current market security methods and how well they safeguard private information and other data assets. In addition, it will provide advice on technological solutions that businesses of varying sizes and budgets may use quickly and affordably to protect themselves from a wide range of risks.So far, studies have focused only on either huge corporations or relatively small businesses. This essay makes an effort to provide a thorough analysis that can be used by companies of any size.
Keywords: Small and Medium-Sized Businesses, Cybersecurity, Internet Threats.

Introduction:

Today, no company can afford to ignore the possibility of an online attack. Hackers may get access to systems without proper protections in place. Online data management, such as storing data on cloud-based platforms and transferring crucial files and documents via servers, makes systems more vulnerable to hacking.For this study, we surveyed executives from big and medium-sized businesses to learn about the challenges they face and the steps they've taken to address them. The purpose of this paper is to respond to questions concerning the most pressing cyber risks now confronting businesses, previous examples of cyber threats, the state of the financial industry, the outlook for such challenges, and the possible actions that may be taken to combat them. The financial services sector includes many different types of participants, including consumers, businesses, and governments.Various types of investments are included in the broader category of financial services, which also includes banking, insurance, mutual funds, wealth management, stock markets, and treasury or debt instruments. Cyberthreats may range in severity and form based on a company's resources and the goods or services it offers. In February of 2016, 81 million dollars were stolen in a hacking operation involving the Bank of Bangladesh and moved to accounts in the Philippines and Sri Lanka via the Federal Reserve Bank utilizing some payment messaging system[2]. A data breach may cost an organization an average of $3.86 million, as reported by the Ponemon Institute. Many computers across the world were inaccessible in 2019 due to a ransomware attack. This attack exploited a hole in a Microsoft service in order to spread ransomware over the internet. Each company is scrambling to establish a

foothold in the online world. When businesses of this kind use cutting-edge technology without taking enough precautions to protect themselves from risks like malware, data breaches, and unsecured networks, they make themselves vulnerable to cyberattack. This is in part because of the massive data breach that Capital One experienced. Malware and hacking were responsible for around 75% of the breaches, while accidental exposures were responsible for about 18% of the breaches, according to a comprehensive analysis of the various forms of data breaches. In Figure 1, we see the top cybersecurity threats that companies of all sizes now face. The sheer size of these companies' workforces demonstrates the scope of these challenges. Small businesses invest less than INR 10 crore (USD 1.4 million) and have an annual turnover of more than INR 50 crore (USD 7 million) but less than INR 250 crore (USD 35 million), while medium businesses invest more than INR 10 crore (USD 1.4 million) but less than INR 50 crore (USD 7 million) and have an annual turnover of more than INR 50 crore (USD 7 million) but less than INR 250 crore (USD 35 million). In India, for instance, the definition of a large company is one with Ransomware, a kind of malicious software, encrypts a user's files and then demands payment to decrypt them. The hacker will then demand payment of a ransom from the victim in exchange for the user's restored access to their files and data. Researchers have found[3] that.

Outages due to these kinds of assaults may last longer than 24 hours. Furthermore, hackers utilize stolen credentials to access a company's most sensitive information. Criminals often conduct phishing assaults, in which they trick victims into giving up their login information by sending them emails or linking to websites that seem identical to the real thing. The strategy of deceiving workers works well and is quite inexpensive. Distributed denial of service attacks are more prevalent against SMEs, whereas data breaches are more common against big and medium-sized organizations. An assault known as a distributed denial of service (DDoS) occurs when malicious actors flood an online resource with so much traffic that it crashes.



This served as the motivation for our examination of the current literature, both in terms of its focus and the overlooked areas of SMB research. According to our own experience and the assertions of others, the adoption of cyber security frameworks that provide structure and methodology is the way by which practical and unified execution of cyber security practises in business may be accomplished. The National Institute of Standards and Technology Cyber Security Framework (NIST CSF) is one existing framework that is extensively utilised by small and medium-sized organisations (SMBs).

The purpose of this research is to understand the focus of previous research on cyber security of small and medium-sized companies (SMBs), using the NIST CSF as a baseline, and to identify areas that may be understudied. A secondary goal of this research is to identify the countries or regions of the globe where research on cyber security of small and medium-sized companies (SMBs) is being conducted, as well as the research methodology and data gathering methodologies presently in use. Another goal was to undertake an examination of what researchers identified as the challenges that small and medium-sized firms face, as well as the advised cyber security practises.

Literature survey:

It is being explored if the ecosystem's participants can produce enough value to survive in the market (Head, V., et al., 2022)[4]. To communicate the study's findings, an economic model that analyses the process of value generation as well as the distribution of that value among stakeholders will be employed. This paradigm provides a substantial improvement in terms of better balancing the interests of stakeholders, including utilities and profits. The model's simulation findings reveal that the system's end users are the primary source of value production. A growing installed base of end users creates opportunity for companies that provide cyber security solutions as well as those who spread knowledge about it. Yet, when a market becomes oversaturated, the ecosystem may not be able to exist. This is because the prices paid for cyber security solutions and information do not cover the expenses connected with them. The simulation model and research results may assist corporate executives in making better judgements on long-term viability, pricing plans, and business strategies for cyber security knowledge and solutions. Moreover, for the adoption of cloud computing, particularly edge computing, a robust ecosystem for the exchange of cyber security expertise is essential. It enables the collection, dissemination, and aggregation of reliable and accurate cyber security data from a range of computer platforms and service providers.

Smikle, Lauri, et al. (2022)[5] is still a target of a variety of financial crimes, the most majority of which take place online and include e-fraud, identity theft, credit card forgeries, money laundering, and terrorist operations. Jamaican organisations' cybersecurity is still vulnerable to weaknesses such as spoofing, spamming, virus transmission, spear phishing, buffer overflow, and denial of service attacks. With the growth of cryptocurrencies and digital currencies, Jamaica must embrace intelligence-led policing and data analysis to decrease and prevent financial crimes such as money laundering and the proceeds of corruption. Examine the body of literature, national laws, and current legal proceedings, as well as design and methodological concerns. Conclusions Cybersecurity is no longer only a computer security concern; it is being considered while creating national policy. This is because illegal internet usage may have a big influence on Jamaica's banking economy. Many successful cyberattacks on the financial industry have occurred across the world. Although the majority of efforts and resources are directed on minimising the danger presented by theseassaults, developing economies have received significantly less attention. Since many of these countries, such as Jamaica, have very poor cyber capabilities, their capacity to react to attacks may be limited. But, in order to safeguard their critical financial infrastructure, these governments must respond to these assaults. Originality and worth There aren't many academic works in Jamaica that concentrate on cybersecurity concerns and legislation.

Tam, Tracy, et al (2021)[6] highlight some features of small enterprises that make them well- suited for implementing cyber-security measures. Until date, small business cybersecurity talks have been limited in scope and lack flexibility for

use in a variety of settings. For our analyses, we rely on data collected from organisations in business, government, and science all across the world. We examine the non-technical and technical aspects that have a detrimental influence on a small corporation's capacity to defend itself, such as resource limits, organisational process maturity, and legal frameworks. The findings of our research suggest that various features of small businesses, such as agility, high cohort sizes, and scattered IT architecture, may assist to increase cyber security. Our findings indicate that there is a knowledge gap in the field of small business cyber security. Further work in the legal and policy domains is also necessary to assist small firms in becoming cyber- resilient.Two factors have been addressed, according to the results of Netwrix's 2021 IT Risks Report. The first is a comparison of the cyber security risks presented by large firms against those posed by small and medium-sized enterprises, and the second is a review of the most serious cyber security dangers confronting the financial sector. As we look closer at the first component, we notice a comparison in numerous other areas. For example, just 33% of major organisations do not have a distinct IT team, however around 73% of small and medium-sized enterprises do not have a separate IT team; this is a considerable percentage. Moreover, 65% of large enterprises prioritise data security, while 60% of small and medium- sized businesses prioritise endpoint protection. Moreover, only around a quarter of all small, medium, and large businesses are effectively prepared to protect themselves against cybercrime. The remaining parts are unprotected. When it comes to financial commitment, around 72% of large organisations and 42% of SMEs are willing to invest in cyber security solutions. The second component covers the banking industry's threats. A specialised information security team is present in around 64% of all financial institutions. Moreover, 91 percent of financial services firms have complete visibility into their consumer data. The security team's major focus is on the endpoints database and virtual infrastructure. Insiders with legitimate access are seen as a severe threat to information security by 82% of financialbusinesses. This is due to the fact that these persons already have access to the information. The three most major obstacles that financial organisations confront are a lack of cash, the complexity of the IT infrastructure, and a lack of time.

Methodology:

The researcher employed a qualitative research approach in combination with the case study research method to analyse cyber security solutions used by small, medium, and large organisations to guard against serious cyber risks for the goal of the research paper. The sample technique utilised in this instance was "Purposive Sampling." This is a strategy in which a small group of people may potentially represent a much bigger population. The goal was to gather first-hand stories from experts who have dealt with cyber security-related difficulties. Figure 2 and table 1 show the overall number of responders as well as information about them. The qualitative research technique has been shown by researchers to be one of the major tools that gives substantial insights. This method is used by researchers to get a better grasp of the participants' experiences and cognitive processes. The themes generated by this technique are useful in the process of developing the framework for the article. It is vital to take the time to define the study subject precisely. The following is an example of a fundamental research question related to the idea[7]: What tools and strategies can small, medium, and large companies employ to reduce the amount of data breaches that occur?

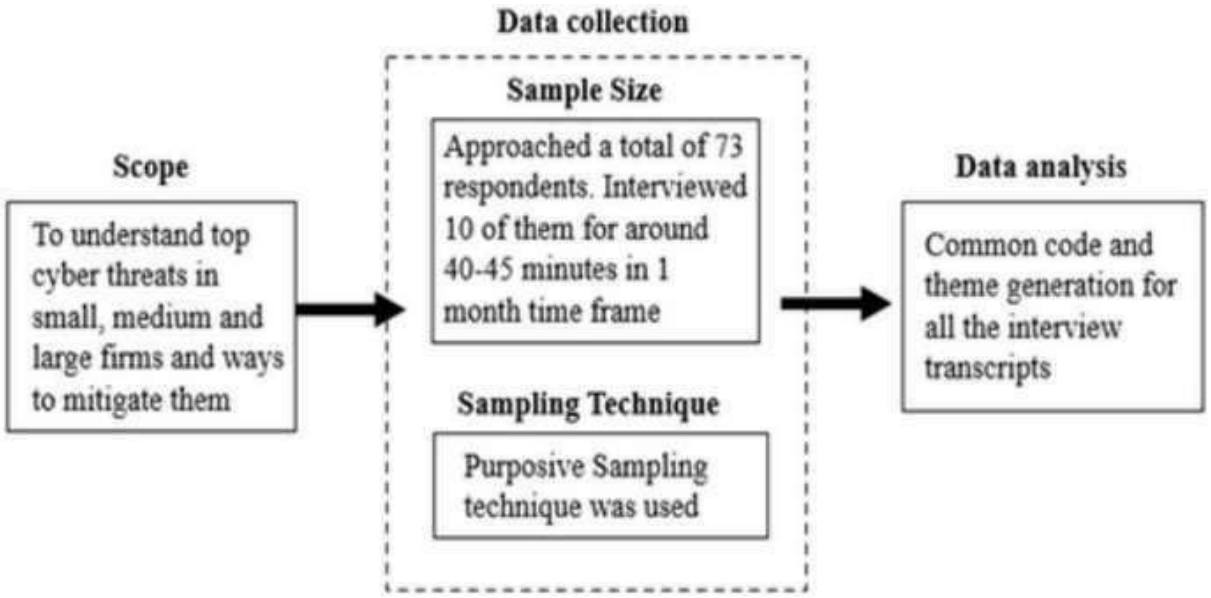


Figure 2:Research Framework

i)Collection of data:
The data collection process requires two phases. The initial step was to send out interview requests to various Chief Information Security Officers, Chief Information Officers, and Directors of Information Security working for small, medium, and large firm units. Through sending emails, messaging on LinkedIn, and establishing personal connections, the researcher reached out to 73 different respondents situated in various geographical locations and working for various financial organisations. The next step was to schedule an online interview using a suitable platform such as Zoom, Google Meet, or Cisco Webex. The interview really took place here. Ten persons out of a total of seventy-three who were contacted agreed to an online meeting. During the interviews, these respondents were asked a number of in-depth questions. A approach based on interviews was employed alone to study the following topics:
Among the most serious threats that a range of companies confront;
- The protection practises in place for their company;
- Plan modifications that take into consideration the company's size;
- The function that cyber security firms
- play in corporate protection;
- Performing risk assessments and penetration testing to identify weaknesses

· The employees' involvement in the security violation.
During the interview, they were each asked around nine open-ended questions as part of the exploratory inquiry. The majority of interviews lasted between 40 and 45 minutes. The individual's present position, the amount of years of experience they have, and whether or not they work or have worked in the financial services industry were the key variables examined when selecting a response. The privacy of individuals was protected, and no private or personal information was acquired. Each respondent is represented by a distinct set of alphabetic and numeric codes (R1, R2,.....R12). They were quite kind and helpful in taking the time to engage in the interview and respond to the topics posed to them[8]. ii)Assumptions:
The initial idea was that conducting interviews with 10 respondents and combining the findings of those interviews with secondary data would be sufficient to achieve data saturation. The second hypothesis was that the interviewees offered accurate answers to the questions presented to them and that they suggested that interviewers often provide truthful
answers during phone and in-person

interviews since doing so helps to the interview's credibility.

iii) Analysis of data

The analysis of qualitative data is divided into three stages: data reduction, data presentation, and data interpretation.

Data interpretation. All of these stages are linked in some manner, establishing what is known as an iterative process. The interview transcripts were placed into a spreadsheet, and numerous themes and patterns were extracted from them. Each transcript, which included a wide range of words and phrases,The statements that did not overlap were constructed from the phrases that were examined. Researchersshould provide a link between the study's findings and the conceptual framework, as well as any gaps.

iv) Demographics: a breakdown of responses based on several demographic variables.

produced using data that was gathered and analysed during the process. The nine core research questions that emerged from the open-ended questions guided our thinking throughout the questioning process.

During the study, the following research questions served as the study's focus point:

Q1: In their perspective, what are the biggest hazards, as well as the measures they haveemployed for their organisation and how they have coped with these challenges?

Instruct current employees.

Question 2 discusses the differences in business tactics adopted by small, medium, and largeorganisations.

Question 3: What role do cybersecurity corporations play, and how significant are thetechnology developed by such firms?

The first study question focuses on the main hazards, the strategies they picked for their organisation, and how they educate their internal staff.

Respondent	Firm Size	Current Position	Years at current position
R1	Medium	CISO & DPO	1
R2	Medium	CISO	1
R3	Small	Senior Manager, Information Security	1
R4	Large	Cybersecurity Advisory Director	1
R5	Large	Director, Cybersecurity & Risk Services	1
R6	Large	CISO	5
R7	Medium	Project Manager & CISO	4
R8	Large	CISO	2
R9	Small	VP/CISO	1
R10	Small	CISO	2

Table 1:Current positions of different respomdent

Results&Discussion:

Based on the data that was gathered and analysed during the process, the researcher produced several themes that cut through all of the replies that we obtained when interviewing the respondents. These themes were

Theme: Phishing and ransomware are two sorts of internet assaults that may be very damaging. Strategies may require either an internal setup or outside aid.

Seven out of ten respondents cited phishing and ransomware as the two most prevalent forms of cyberattacks. Because of the increased professionalism of hackers, all respondents felt that the

frequency of such attacks is increasing at an alarming pace each year. Before you can start planning your strategy, you must first understand your digital presence. We will be able to establish the most significant areas that need to be fixed once we have a better grasp of the online presence.

"Understanding the IT footprint plays a significant role in terms of strategy formulation," according to R7, and the importance of this statement is defined by the quantity of data- intensive work being done.

Three respondents raised the point that the methodology differs depending on the industry. When you become a reseller, your website becomes a valuable asset that must be protected. A financial organisation must safeguard the sensitive information linked with its clients' credit cards. On the other hand, a manufacturing organization's main goal must be the preservation of data related with the supply chain.

"In some circumstances, employees may be the most important contributor in terms of data breach," according to R5.

Consistent assistance and teaching may go a long way. "Two respondents stated that accidentally clicking on a link may take someone to a phoney website that looks exactly like the real one. When the data is entered, it will display an error, and then it will take the user back to the page they were previously on, at which point the original data has already been compromised due to cyber crimes. Phishing attacks operate on this general premise.

The second study question inquires about differences in organisational strategy across small,medium, and large enterprises.

The notion here is that regardless of the size of the firm, a multi-layered approach to securityshould be implemented.

Eight out of ten respondents agreed that a layer-based security approach should be explored. That seems to make sense.

Cybersecurity plans for small, medium, and large enterprises willchange based on aspects such as the firm's revenue, IT budget, and IT employees. The approach we are describing here is one that consists of three levels.

First layer (Applicable Primarily to Small Businesses): Since smaller firms have a limited or nonexistent toolset or skill set, as well as a limited budget and resources, they must be choosy in order to get the most value for their money.

According to R4, it is critical that we understand the components that comprise our IT infrastructure, since this will be valuable in the future.

significantly improved data security for SMEs "Six respondents said that small businesses must utilise data encryption technology as a first step. Due of the limitations imposed on available resources, another task that must be completed is the installation of an antivirus solution. Endpoint security solutions, such as the creation of a complex password or multifactor authentication, may also be incorporated in the first security layer solution.

Second Layer (Medium-Sized Businesses May Pick This): This option is available to both small and medium-sized organisations.

Technology that constitutes the second layer of security, which is put on top of the first. Four responders recommended baselining servers, creating a firewall around the network layer replete with lock management for firewalls, and implementing an approval system for internal proxies.

According to R9, EDR is one of the most successful methods for identifying early warning indicators of dangers. Even though it is still in its infancy, more established firms are seeing it as a possible answer.

The third tier, which is frequently designated for huge corporations, is achieved when a company grows in size and starts to use digital data. The complexity of the surrounding environment for cyber security grows in this setting.

According to Statement 6, the majority of large corporations make an attempt to establish their own internal security

systems. They have the cash as well as a budget, which allows them to meet their individual needs.

According to four of the respondents, zero-trust should be incorporated as a component of the third layer of security solutions.

Security systems, improved detection capabilities, and mitigation tools, such as log management and response time estimations, are also available.

3. What role do cyber security organisations play, and how significant are the capabilities these businesses provide?

How do businesses grow?

The primary concept is that they serve as a strategic partner in terms of digital asset security. Seven out of 10 respondents in the poll said cyber security firms were significant.

Companies like CyberArk, FireEye, and Fortinet that invest heavily in research and development to build cyber security technology to prevent data breaches definitely provide considerable value. A firm cannot even contemplate continuing in business if they do not have them. Hackers create new tools for building new types of malware, each of which has the potential to do more damage. "Companies like CyberArk and Crowdstrike have very fantastic solutions, but they are complex to operate and need some experience to install it correctly," according to R5, indicating that they do, in fact, play an important role. This is where we (the chief information security officers) come in.

According to R1, there is no such thing as 100% protection. When it comes to security, experience is more important than the tools themselves.

Five respondents responded that, although cyber security organisations make recommendations, the system is managed by the organization's IT employees. As a result, the business now owns the property. Their connection is comparable to that of a strategic collaboration. Companies like CyberArk, whose exclusive concentration is the creation of security products, must have their activities reviewed by the company's information security team. The IT team is in charge of handling things like zero trust and security technology. Before implementing these cyber security solutions, it is vital to do an analysis of them. As a result, the company must do a risk assessment before adequately scaling the solution to the issue. Since the company cannot afford even a minute of interruption, even basic procedures like backing up data on the cloud server should be performed on the organization's end. Deals of billions of dollars are feasible at that time.

Conclusion:

Doing qualitative research is likely to make it much easier to understand a person's path throughout their professional life. The qualitative exploratory study was utilised by the researcher to conduct an analysis in order to get a better knowledge of the data breach

protection measures accessible to organisations of all sizes (small, medium, and large).The remarks of the ten participants helped us understand how different techniques are employed, what purpose cyber security businesses perform, and how various investments are made.He successfully discovered five distinct themes, each of which was subsumed by a separate research question generated as part of the study method. Each course focuses on a different part of the overall cyber security strategy that may be utilised to help academics and businesses. It has been shown that phishing and ransomware are regarded as severe concerns in the banking industry.

Particularly, as well as all other industries as a whole. It also highlighted how, depending on the amount of available investment funds, utilising a system-based approach to stacking security might be a prudent option. When a company grows, it may add an extra layer of protection to its system. Moreover, the researcher was well-versed in the strategic function that cyber security firms play in securing the company. Yet, the firm must be present and actively

monitoring the responses supplied by other organisations. Moreover, the data we obtained indicated that a minimum investment in a cyber security system should be between 10% and 15% of the whole budget.This was another of our discoveries. If it does happen, it will do the least amount of harmhappens, and the time it takes to respond to it should be minimal. Finally, workers have a key role in the countless data breaches that occur. People should be extra careful when replying to emails and clicking on links to prevent accidentally assisting hackers in collecting personal information.In terms of advice, it is highly encouraged to do research on the total amount of data breaches.Consider what is now happening and the major events that have occurred so far. Throughout the course of this study report, research into different company sectors, such as manufacturing or eCommerce, may be highly beneficial. Utilizing these technologies correctly and in line with a plan may help the organization's reputational credibility while also improving its financial data assets. Future researchers may aim to broaden the scope of this study to include other sectors and conduct in-depth studies using surveys to analyse and verify the model.

References:

[1] Ahmad, T., Zhang, D., Huang, C., Zhang, H., Dai, N., Song, Y., and Chen, H., 2021. Artificial intelligence in sustainable energy industry: Status Quo, challenges and opportunities. Journal of Cleaner Production, 289, p.125834.

[2] Bag, S., Gupta, S., Kumar, A. and Sivarajah, U., 2021. An integrated artificial intelligence framework for knowledge creation and B2B marketing rational decision making for improving firm performance. Industrial Marketing Management, 92, pp.178-189.

[3] Rosário, A.T. and Raimundo, R., 2021. The impact of Artificial Intelligence on Data System
Security: A Literature Review

[4] Head, V & Zine, Rasika. (2022). THE ECOSYSTEM OF BUSINESS AND ECONOMY; CHALLENGES AND OPPORTUNITIES: THE ANALYSIS OF CYBER SECURITY ASPECTS AND ITS IMPACT ON CYBER CRIME AUTHOR.

[5] Smikle, Lauri. (2022). The impact of cybersecurity on the financial sector in Jamaica. Journal of Financial Crime. ahead-of-print. 10.1108/JFC-12-2021-0259.

[6] Tam, Tracy & Rao, Asha & Hall, Joanne. (2021). The Good, The Bad and The Missing: A Narrative Review of Cyber-security Implications for Australian Small Businesses. Computers & Security. 109. 102385. 10.1016/j.cose.2021.102385.

[7] Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F. and Choo, K.K.R., 2021. Artificial intelligence in cyber security: research advances, challenges, and opportunities. Artificial Intelligence Review, pp.1-25.

[8] Chehri, A., Fofana, I. and Yang, X., 2021. Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence. Sustainability, 13(6), p.3196.