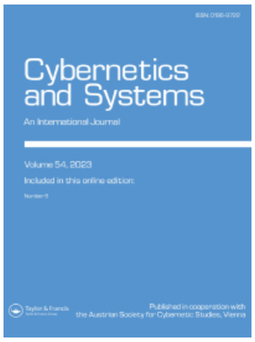


Cybernetics and Systems
An International Journal

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/ucbs20

Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges

Khalifa AL-Dosari, Noora Fetais & Murat Kucukvar

To cite this article: Khalifa AL-Dosari, Noora Fetais & Murat Kucukvar (2022): Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges, Cybernetics and Systems, DOI: 10.1080/01969722.2022.2112539

To link to this article: https://doi.org/10.1080/01969722.2022.2112539

Published online: 23 Aug 2022.

CYBERNETICS AND SYSTEMS
https://doi.org/10.1080/01969722.2022.2112539

Taylor & Francis
Taylor & Francis Group

OPEN ACCESS Check for updates

Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges

Khalifa AL-Dosari, Noora Fetais, and Murat Kucukvar

College of engineering, Qatar University, Doha, Qatar

ABSTRACT

Cyberattacks are becoming more and more intense in the banking industry (Ryzhkova et al. 2020). Banking industry is trying to adopt artificial intelligence to create cyber defence system so that the unauthorized access and cyber attacks would be minimized. Banks in Qatar acknowledge the threat of cybercrimes and the role of cybersecurity in sustainable growth. Meanwhile, the banking industry is experiencing a major technological disruption. It becomes important to understand the implications of such technologies as artificial intelligence (AI) on the cybersecurity of banks. The present paper aims to explore the impacts of AI on the cybersecurity of banks in Qatar. A thematic analysis of interviews of 9 experts in the banking industry of Qatar was conducted. A qualitative thematic analysis was conducted using NVIVO 12 tool. Four key themes were identified: (1) AI is a major tool for enhancing the cybersecurity of banks in Qatar; (2) banks face challenges in using AI for improving cybersecurity; (3) AI can be used destructively and thus poses a threat to cybersecurity in banks of Qatar; (4) employed AI-based tools have vulnerabilities that can be exploited. Overall, Qatar banks can be expected to face new challenges in the future, due to changes in regulatory frameworks and increasing availability of AI-powered malware.

KEYWORDS

AI powered-malware; artificial intelligence; cyberattack patterns; decision-making; fin tech; machine learning

Introduction

Over the past decade, cyberattacks have become more frequent, more impactful, and more sophisticated (Akinbowale, Klingelhöfer, and Zerihun 2020; Kaloudi and Li 2020). The financial sector has become one of the major targets of cyberattacks (Ranjan, Gupta, and Gupta 2020). Meanwhile, artificial intelligence (AI) has been a major disruption in the financial sector (Almutairi and Nobanee 2020). Banks have been investing in AI-powered customer services, such as chat bots and financial management. The use of AI

CONTACT Khalifa AL-Dosari 200704317@qu.edu.qa College of engineering, Qatar University, Doha, Qatar.

for combating cyber threats has also become widespread in the sector (Soni 2019). At the same time, AI-powered cyberattacks have become more common, suggesting that AI can be used for both enhancing and disrupting cybersecurity.

However, using artificial intelligence in vital infrastructures raises several difficulties due to their unpredictable nature (e.g., banking industry, etc.). Most of these worries revolve around safety, accuracy, trustworthiness, and security issues. The degree to which these cyber-security systems are protected against various kinds of cyber-attacks is the primary factor determining their security level. In this way, customer trust and the capability of using banking services can be enhanced by deploying an effective cyber defence system (Chui, Manyika, and Miremadi 2016). Security is related to the lessening of the possibility that accidents will occur, validity is based on conducting the assigned purpose without any flaws or poor decisions, and trust is derived from the capacity of these artificial intelligence systems to precisely perform and replace workers in certain disciplines and activities. Nevertheless, different security concerns, challenges, vulnerabilities, and risks are continually emerging, including the intentional misuse of artificial intelligence technology via cyberattacks that might result in significant injury or even death (Guerrero-Higueras, DeCastro-García, and Matellán 2018; Kirschgens et al. 2018). This is one example of a threat.

Phishing emails, in particular, with harmful attachments, were sent out by cybercriminals. These emails were directed at the upper management of several firms and certain employees working in middle management positions. Phishing emails have been sent out, making it appear as though they originated from the Qatar banking industry (Al-Mhiqani et al. 2018). The emails contain notes that purport to offer some guidance on the payments from the bank. Attached to the message in the email is a SWIFT file that has been infected with malware (Tao et al. 2018). The Qatar government published a report to ensure the safety and security of the banking industry in Qatar (Qatar Banking Perspectives 2021). The report mentioned that Qatar's financial sector should establish and implement a sound system for AI installation and operations to secure Qatar's banking industry from cyber-attacks and crimes. Several technical solutions have been offered in the research in Qatar banking that can identify and fight against email phishing assaults; nevertheless, these methods cannot detect and halt phishing emails that look authentic (Al-Hamar, Kolivand, and Al-Hamar 2019). Phishing via email is not an attack on machines; rather, it is an attack on sensory consciousness, which is difficult to protect against using only technical methods. Nevertheless, awareness training programmes are necessary to limit the success of successful phishing attempts made via email.

"As a result of the response to these incidents, this study concluded that the majority of the attackers—the individuals who are aiming their blaze at the ministries and the banks—are all founded in the same facilities, and they do not alter their methods when they are attempting to attack financial sectors (Perumal 2018). According to al-Marwani, "as a result", the Ministry of Interior had begun issuing recommendations with the banking industry… we work in tandem with clients to effectively halt any form of cybercrime inside the State of Qatar" (Perumal 2018). According to al-Marwani, the cyber defence system may assist in detecting threats, as well as the implementation of detection techniques and the response to various sorts of assaults. These include account compromise, web attacks, data stolen and penetration (Abu-Taieh et al. 2018). Banks in Qatar acknowledge the threat of cybercrimes and the role of cybersecurity in sustainable growth (Perumal 2018). However, little research exists on the use of AI in the security of banks in the country. The present paper aims to explore the impacts of AI on the cybersecurity of Qatar banks. The study contributes to the existing literature by exploring the disruptive effects of AI on the cybersecurity of banks in Qatar. The study significantly contributes to the novel knowledge in implementing AI security system in the Qatar banking industry.

Literature Review

Use of AI in the Banking Sector

AI is an umbrella term comprising a range of techniques and methods aiming to reproduce complex capabilities, such as autonomous decision-making and language use (Truby, Brown, and Dahdal 2020). Machine learning (ML) is a subset of AI aimed at discovering patterns in data and making decisions appropriately. ML can be divided into supervised and unsupervised learning, based on whether the system is explicitly told the correct answers (Caldwell et al. 2020). Deep learning (DL) uses neural networks to perform highly complex information processing. AI allows for the use of advanced analytical tools and innovative business solutions in the banking sector. AI-powered systems make it possible for banks to develop multichannel customer access, gain insight into customer preferences, and tailor services to customer needs (Kochhar, Purohit, and Chutani 2019; Shmuratko and Sheludko 2019).

The financial sector has become more competitive with the rise of FinTech companies (Truby, Brown, and Dahdal 2020). Banks are expected to implement innovative solutions and appropriate security measures for ensuring the privacy of their customers' information and meeting the needs of their customers (Lukonga 2018). However, incumbent banks are at an inherent disadvantage compared to new FinTech firms when it comes to using new technologies (Shmuratko and Sheludko 2019). Banks may struggle to adapt, due to the established practices impairing the implementation of new technologies (Financial Stability Board 2017). This may create additional security risks, due to legacy financial and security software systems being incompatible with innovative solutions.

A major issue surrounding the use of AI in the banking sector is data privacy (Financial Stability Board 2017). As related regulatory frameworks are still in development, it may not be clear whether the bank should rely on third-party service providers to ensure data privacy (Truby, Brown, and Dahdal 2020). Using AI-powered tools, such as natural language processing (NLP), for analyzing employee and customer communication or chat bots for communicating with clients may infringe upon individuals' privacy (Caldwell et al. 2020; Lai, Leu, and Lin 2018). The regulatory environment is still changing. This uncertainty may impede the banks' ability to address cybersecurity threats.

While many AI-powered tools used by banks are related to backend systems, certain AI capabilities are explicitly presented to end users. In the context of cyber security, this implies that the security measures adopted by banks should account for the customers' familiarity with the technology. This ties into the technology acceptance model (TAM), which describes why users may accept new technologies (Alghazo, Kazmi, and Latif 2017). The model posits that the two major factors behind technology acceptance are usefulness and ease of using. As such, the cybersecurity of AI-powered systems should account for the users' behavior and security vulnerabilities arising from such behavior. In particular, users of Internet banking services may unknowingly share their login credentials with others, which would lead to security breaches. Extensions, such as the theory of reasoned action (TRA) and the theory of acceptance and use of technology (UTAUT), introduce additional factors, including cultural differences, perceived risks, mass media, skepticism, and family influence (Alghazo, Kazmi, and Latif 2017).

AI and Cybercrime

AI may offer banks powerful tools for combating cybercrime threats. Such methods as artificial neural networks (ANNs), artificial immune systems, fuzzy logic, and genetic algorithms have been successfully used for preventing and detecting cybercrime (Dilek, Çakı r, and Aydı n 2015; Mosteanu 2020; Ortiz, Marin, and Gualdron 2016). In particular, ANNs can be used to process distributed information in order to detect irregularities and propose countermeasures (Elzamly et al. 2017). ANNs are robust to noise and sufficiently flexible for handling complex dynamic phenomena (Dilek, Çakır, and Aydın 2015). More generally, AI has been used by businesses to detect threats and stop attacks, to analyze mobile end points, and to enhance human analysis (Geluvaraj, Satwik, and Ashok Kumar 2019). In the banking sector, the AI can be applied at three levels, namely protection, detection, and response (Goosen et al. 2018; Ling et al. 2019).

Losses suffered by banks following cyberattacks can be classified into two groups, namely direct losses and indirect losses (Akinbowale, Klingelhöfer, and Zerihun 2020). Direct losses correspond to actual money theft and data breaches. Indirect losses are presented by poor public relations and increased customer frustration and dissatisfaction. The analysis of the extent of cybercrimes in the banking industry of developing economies (Akinbowale, Klingelhöfer, and Zerihun 2020) suggests that cybercrimes adversely affect banks integrity, efficiency, and reputation. Similar results were reported by (Lai, Leu, and Lin 2018), who examined cybersecurity in the Internet banking services of Saudi Arabia, India, and Pakistan. Notably, the scholars found that the login webpage of a substantial number of banks had no security risk information about phishing, social engineering, public networks, Secure Sockets Layer (SSL), and password policy. A related study (Lukonga 2018) reported that regulatory gaps exist in the data protection laws in MENA countries.

Adversarial machine learning is an ML area aimed at influencing the output of a trained system by feeding it specific inputs (Kaloudi and Li 2020). Considering the number of AI-powered systems employed in the banking industry, adversarial ML could become a major threat (Geluvaraj, Satwik, and Ashok Kumar 2019). A generative adversarial network (GAN) is an ML configuration where an ML system is trained to find flaws in the output generated by another ML system. The development of GANs has improved the capabilities of AI to generate convincing artificial content, or "deep fakes" (Caldwell et al. 2020). A related ML method of adversarial perturbation aims to exploit the decision boundaries of existing ML systems. This allows for forcing the existing system to produce a wrong output by slightly changing the inputs (Kaloudi and Li 2020).

The existence of adversarial ML implies that AI-powered systems have inherent vulnerabilities that should be addressed when using such systems in cybersecurity (Geluvaraj, Satwik, and Ashok Kumar 2019). It follows that AI-based cybercrimes can be grouped into two categories (Caldwell et al. 2020). Firstly, AI can be used as a tool facilitating crime. For example, hackers might employ AI algorithms to discover vulnerabilities in banks' security systems (Kaloudi and Li 2020). Secondly, an AI system can itself be the target of a crime. This corresponds to adversarial ML and may be represented by hackers making banks' security systems behave erratically in order to cause damage.

AI-powered crimes include audio and video impersonation, tailored phishing, disruption of AI-controlled systems, large-scale blackmail, and data poisoning (Caldwell et al. 2020). Audio and video impersonation could be used by hackers to request access to the secure systems of a bank (Kaloudi and Li 2020). Phishing is a major social engineering threat to both customers and employees in the banking industry (Deep and Sharma 2018). Tailored phishing could use AI-powered systems to exploit data from social networks in order to improve the success rate of the attack (Geluvaraj, Satwik, and Ashok Kumar 2019). Hackers may also use AI to disrupt banks' AI-powered security systems. AI might facilitate large-scale web-based attacks, which could make banks prone to blackmail (Kaloudi and Li 2020). Considering that annual global economy losses due to cyber-crimes are estimated at US $400 billion, it becomes especially important to investigate the AI disruption in cybersecurity in the banking industry.

Methods

The present study employs thematic analysis of interviews for assessing the use of AI for cybersecurity in the banking sector of Qatar. This allows for exploring the established AI practices in the country based on the views and experiences of experts in the industry. The interview protocol has been prepared and checked by the two professional researchers (university faculty members) and one cybersecurity professional so that the reliability and validity of the interview questions can be justified and managed. However, the professionals recommended some changes to the questions, and the researcher made changes and made them according to the professional recommendations. Finally, the study ensures the validity and reliability of the interview questions.

Data Collection

The interview questions were developed based on the relevant literature. The interview comprised a total of 30 questions. The following is an example of a question from the interview: "Are there any obstacles for using AI for monitoring and analysing employee communication in Qatari banks?" The questions can be grouped into two categories. The first category included questions on the use of AI for enhancing the cybersecurity of banks in Qatar. These questions covered web-based attacks, external and internal fraud, and know-your-customer (KYC) processes. The second category included questions on the threats and vulnerabilities associated with AI-powered systems. These questions covered chat bots, fake data, regulations and compliance, data privacy, and AI-powered attacks, including adversarial ML. The interviews were collected from a total of 9 experts from the banking industry of Qatar. The sample size is in line with the sample size recommendations of 6-15 interviews of (Braun and Clarke 2013) for a professional doctorate project. Another recommendation by Dworkin (2012) has been given for qualitative research sampling. Dworkin suggested that at least 5 interviews are adequate to reach the conclusion of the qualitative study. Galvin (2015) has a same intention to go for at least 5 qualitative interviews so the study conducted 9 interviews to conclude the findings.

Data Analysis

The present paper uses experiential thematic analysis (Appendix 1). This type of analysis is based on the realist ontology and the assumption that language reflects reality and focuses on what participants think and say. The study uses a flexible approach to coding and theme development, as suggested by (Terry et al. 2017). It is often recommended that interview questions guide themes (Braun and Clarke 2013). A similar method is employed in the present analysis. The interview questions are formed based on existing theories and relevant literature. The questions are expected to at least partly determine the major themes. However, coding and final development of themes are performed independently of the interview structure, to reduce subjectivity bias and enhance analysis. Codes are developed inductively, which corresponds to using data as the main starting point. Semantic coding is used, which allows for capturing explicit meaning and limits the impact of researcher's subjectivity. The analysis was performed in several phases based on the framework of (Terry et al. 2017): familiarizing with the data, generating codes, constructing themes, reviewing potential themes, and defining themes. The NVIVO 12 software was used to organize the data according to developed codes. The study employed six steps of qualitative analysis by Braun and Clarke (2013). Each step and related information is given below:

1. **Familiarization with the data:** The first step is to completely immerse oneself in the data and become thoroughly acquainted with it by studying and rereading it multiple times.
2. **Coding:** In the next step, brief labels (coding) are created that identify essential data elements that may be utilized to answer research questions. The entire dataset must be coded, and then all the coding and relevant data extracts must be combined for further research.
3. **Generating initial themes:** The codes and data collected during this stage are studied to develop early themes. The next step is to acquire

relevant information about each conceivable theme so that you can analyze its viability and engage with it.

4. **Reviewing themes:** These prospective themes are contrasted with the data, and if they fit the data and respond to the research questions, they move on to the next stage. In this phase, themes can be improved by splitting, merging, or removing them. A theme is a collection of shared meanings underpinned by a particular discipline or concept in this approach.
5. **Defining and naming themes:** The next step is thoroughly examining each subject, determining its scope and purpose, and creating a "narrative" for it. It also requires that each sub-topic be given a descriptive name.
6. **Writing up:** During this phase, you'll combine your analytic narratives with your data extraction and then interpret your findings in light of past work.

Coding of the Nodes

After completing the focus groups, the data was transcribed to further code it and generate the nodes projected to analyze. Following queries were applied to find the results while using NVIVO 12 software:

(a) Draw word tree
(b) Text search Query
(c) Word Frequency Query
(d) Coding Query
(e) Word cloud
(f) Tag cloud

Results

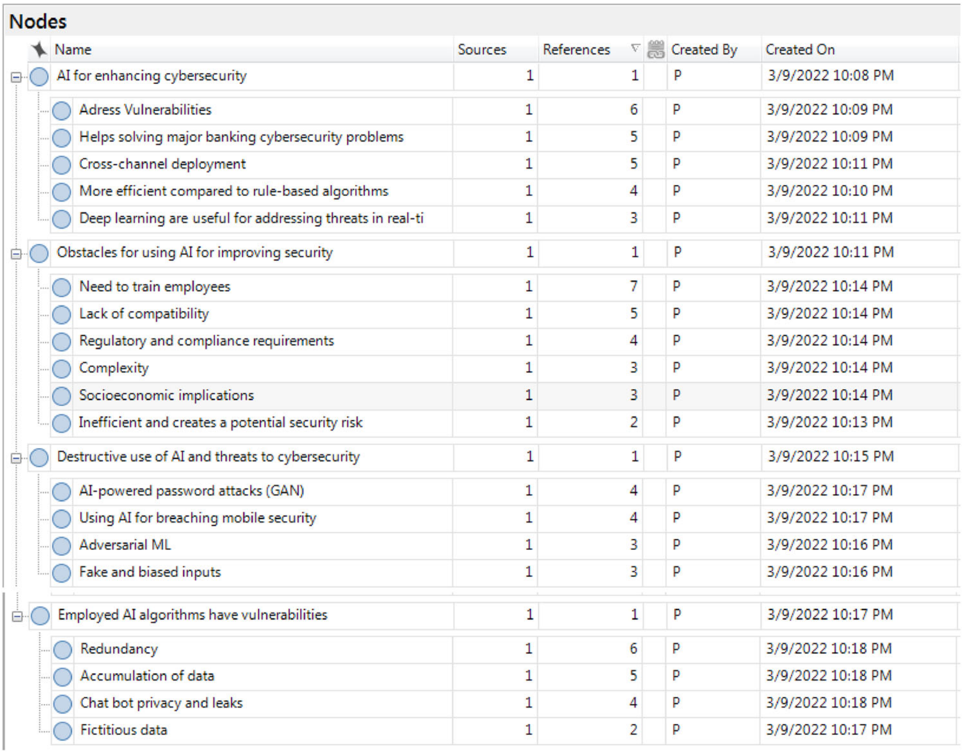
Data Coding and Generating Themes/Nodes

After transforming audio-recorded focus groups into English, different contextual factors (themes) were extracted from textual data. The next step is organized to develop different “Nodes” from these themes of the present study. Each theme of a particular group represented a “Node.” This qualitative study aimed to identify the contextual factors affecting cybersecurity system of Qatar banking sector. Each theme was developed from each contextual factor divided into different factors according to participants’ textual data (Appendix 2). The present study extracted several challenges for cybersecurity and implementation of artificial intelligence (Figure 1).

Figure 1 shows the coding from both (1) Source (S) and (2) Reference (R) against generated each theme. Sources and References are explained below:

- It indicates the number (frequency) of participants contributing data on a specific topic (factor).
- It shows the total number of themes classified in a specific factor about a specific participant. It is possible that a single person brought up a given topic more than once, which results in more References (R) than Sources (R). It signifies that a previous study coded participant conversation on a single theme twice as a reference (R) and the participant source as a reference (S).

Figure 1 demonstrated the themes extracted from the interviews. The study mainly identified four basic themes; AI for enhancing cybersecurity, Obstacles for using AI for improving security, Destructive use of AI and threats to cybersecurity, and Employed AI algorithms have vulnerabilities. These parents' nodes have further child nodes that demonstrate the discussion of parent nodes. So, sources mean total one document is based on



Nodes

Name	Sources	References	Created By	Created On
AI for enhancing cybersecurity	1	1	P	3/9/2022 10:08 PM
Adress Vulnerabilities	1	6	P	3/9/2022 10:09 PM
Helps solving major banking cybersecurity problems	1	5	P	3/9/2022 10:09 PM
Cross-channel deployment	1	5	P	3/9/2022 10:11 PM
More efficient compared to rule-based algorithms	1	4	P	3/9/2022 10:10 PM
Deep learning are useful for addressing threats in real-ti	1	3	P	3/9/2022 10:11 PM
Obstacles for using AI for improving security	1	1	P	3/9/2022 10:11 PM
Need to train employees	1	7	P	3/9/2022 10:14 PM
Lack of compatibility	1	5	P	3/9/2022 10:14 PM
Regulatory and compliance requirements	1	4	P	3/9/2022 10:14 PM
Complexity	1	3	P	3/9/2022 10:14 PM
Socioeconomic implications	1	3	P	3/9/2022 10:14 PM
Inefficient and creates a potential security risk	1	2	P	3/9/2022 10:13 PM
Destructive use of AI and threats to cybersecurity	1	1	P	3/9/2022 10:15 PM
AI-powered password attacks (GAN)	1	4	P	3/9/2022 10:17 PM
Using AI for breaching mobile security	1	4	P	3/9/2022 10:17 PM
Adversarial ML	1	3	P	3/9/2022 10:16 PM
Fake and biased inputs	1	3	P	3/9/2022 10:16 PM
Employed AI algorithms have vulnerabilities	1	1	P	3/9/2022 10:17 PM
Redundancy	1	6	P	3/9/2022 10:18 PM
Accumulation of data	1	5	P	3/9/2022 10:18 PM
Chat bot privacy and leaks	1	4	P	3/9/2022 10:18 PM
Fictitious data	1	2	P	3/9/2022 10:17 PM

Figure 1. Nodes.

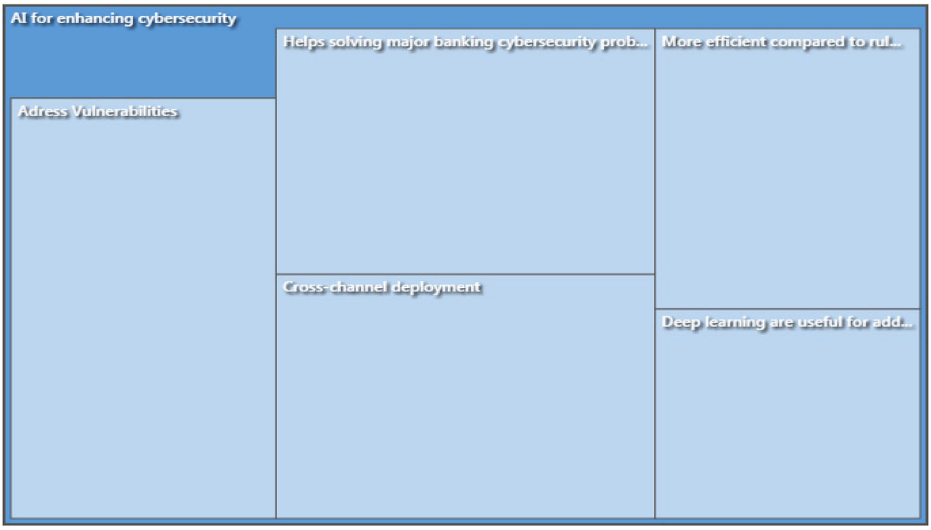
interview transcription and references mean how many times an interviewee talks about a particular theme/node.

Hierarchy Chart

Visualizing coding patterns and assigning values to situations and sources is easier with hierarchical charts (McNiff 2016; Zamawe 2015). Hierarchical charts are an excellent tool when a reader wants to learn more about the numerous points of view represented by the data. Hierarchy charts and Treemaps are two types of diagrams (Richards 2002). Regarding data aspects, TreeMap compares the hierarchies based on their sizes. In addition, the hierarchy chart's rectangular design makes it simple to compare to curved shapes. As a result, the reader can see in the figure below that the respondents mostly claimed the threats and the application of AI for cyber-security. Following is a description of how the major issues and subthemes were discussed:

Theme 1: AI is a Major Tool for Enhancing Cybersecurity of Banks in Qatar

The majority of respondents expressed that AI-based solutions for distributed denial of service (DDoS) attacks have been commonly employed in Qatar banks. The responses suggest that banks employ deep learning and artificial neural networks to identify and prevent web-based attacks. AI-based algorithms were characterized by the experts as being more efficient at defending against DDoS attacks compared to traditional mitigation systems, due to higher flexibility and robustness. One expert mentioned that a genetic algorithm was used for scalable analysis of traffic in one of the banks in Qatar. The researchers (Al-Mhiqani et al. 2018; Rubio et al. 2019) also argued that There are primarily two ways that AI is helping to strengthen cybersecurity. To begin, AI has the potential to assist in the automation of many operations that a professional analyst would typically undertake manually. This category includes automatically discovering unidentified workstations, computers, code repositories, and other hardware components and applications on a network. When combined with some degree of human oversight, AI applications in cybersecurity tend to produce the greatest results (Tao et al. 2018). AI solutions such as machine learning assist security professionals in detecting and preventing malicious conduct, lowering the chance of a security breach and the amount of data that is compromised.



Several experts noted that Qatar banks are forced to employ sophisticated DDoS prevention methods, as the banks are blackmailed by hackers to pay in order to avoid DDoS attacks:

> *"These days' hackers are blackmailing the financial institutions to pay them handsome amount to avoid any type of attacks. DoS <…> can be prevented by using the AI that can distinguish between the legitimate requests and DDoS attacks" (Expert 4).*

> *"AI based solutions are used to handle DoS in Qatari banks because hackers are blackmailing the banks to pay them" (Expert 5).*

Thus, AI appears to have become a crucial tool for combating web-based attacks. Another recurring subtheme was the use of third-party AI-based software, such as IBM AI, to prevent external fraud. Several experts reported that Qatar banks use the IBM Safer Payment service. It was stated that the service provided tools for analyzing fraudulent patterns, alerting the bank of emerging fraud threats, and proposing suitable countermeasures. According to the respondents, such AI-based tools are widely used in Qatar banks to address credit card fraud.

The KYC procedures and compliance constitute another area where AI may enhance security in Qatar's banking sector. The majority of participants acknowledged the use of AI-powered systems in KYC checks. One expert stated the following:

> *"KYC compliance <…> has been made more dynamic and effective through AI-enabled systems. The financial sector produces huge amounts of data, which is what AI works best with. It can mine high volumes of data within seconds and produce risk-*

> *analysis of clients, that would otherwise prolong to take days or even weeks for the combatting staff to produce" (Expert 3).*

At the same time, two out of nine experts reported that Qatari banks do not use AI for identifying customers. These ambiguous results suggest that there is some heterogeneity across banks with respect to automating KYC tasks. Nevertheless, several experts provided examples for the use of AI systems in the KYC process. This includes employing deep-learning optical character recognition (OCR) for scanning documents in real time, as well as sorting and tagging documents based on an AI engine.

Another major topic covered by the responses is internal fraud. Phishing is recognized as a major cyber security threat in Qatar banks by the majority of the experts. Several participants noted the increasing use of AI-based systems for internal monitoring:

> *"Tessian and Expert System are being employed more often in Qatari banks. The reason is due to the increase in cyber-attacks via email" (Expert 1).*

> *"Employee monitoring is the best way to prevent insider threat and is widely being used nowadays in most of the FSI sector" (Expert 9).*

One expert reported that the use of NLP for detecting phishing attempts is not widespread in Qatar banks. Another respondent noted that Qatar banks are investing in NLP-based tools to detect phishing attempts. Some of the responses linked the limited use of AI-based tools to potential privacy issues and the development of personal data regulatory frameworks, including the European Union General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

In addition to solving specific security problems, AI was suggested to have advantages over traditional methods. A recurring subtheme was that AI-powered systems are more flexible and robust compared to rule-based algorithms:

> *"There have been numerous intrusion detection systems (IDS) proposed that include AI-based solutions. Use of neural networks that are trainable, instead of designed to follow specific rules are becoming more wide-spread in use" (Expert 1).*

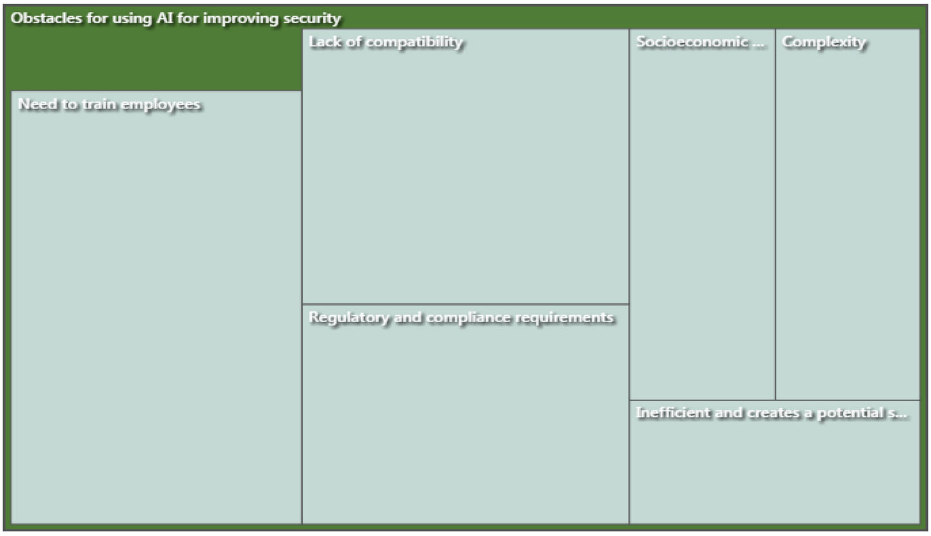
Considering that modern cyberattacks may also be AI-based, flexibility becomes a major strength of AI-powered tools for Qatar banks. Another advantage is the ability to more easily deploy ML technology across several channels, such as transactions and loan applications because, to uncover new types of assaults, AI in cybersecurity analyses the relationships between dangers in your entity's information systems. People teams now have access to new degrees of cybersecurity intelligence, such as IT asset inventories, threat exposures and safeguards, breach threat prediction and information security, and increased internal communication about cyber security (Perumal 2018). AI technology can help security professionals lower the threat of a breach and enhance their overall security more quickly and efficiently. In particular, one expert stated the following:

> *"Machine learning technology can be deployed across multiple channels <… > in the banking industry. <… > As a result, AI can be used to detect fraud in more than one channel simultaneously simply by improving the way it finds anomalies in data over time" (Expert 9).*

This response is in line with other experts acknowledging that the banking industry covers numerous products and features and thus requires multi-channel monitoring.

Theme 2: Banks Face Challenges in Using AI for Improving Cybersecurity

While all experts agreed on the increasing importance of AI in enhancing banks' cybersecurity in Qatar, the participants noted that banks face many challenges when implementing AI-powered systems. One of the recurring topics was in-house development of security systems. The researchers also pointed out the challenges by banking industry in the implementation of AI such as The absence of a well-defined plan for artificial intelligence is, by far, the most common barrier that prevents banks from achieving their goals (Ranjan, Gupta, and Gupta 2020). First, a weak underlying technology and data foundation is one extra difficulty that many banks face. Second, banks face two more challenges an antiquated operations strategy and securing a job. Cybercriminals can train artificial intelligence systems or inject fraudulent information into data sets that AI utilizes. They will be able to build more realistic and complex attacks as a result of this (Thowfeek, Samsudeen, and Sanjeetha 2020). Ethical hacking is one of the most significant dangers to the banking and financial industries. People are frequently the weakest cause of data breaches because they might be persuaded to reveal confidential information and credentials when duped. Both bank personnel and clients could be adversely affected by this situation. The history of artificial intelligence is replete with unethical behavior, including violations of users' privacy, manifestations of bias, and decision-making by AI that could not be contested. It is also vital to detect and reduce ethical hazards during the design and development phase of artificial intelligence (AI) and continuously once it has been implemented (Ryzhkova et al. 2020). Overall, the experts acknowledged that developing AI software locally is not efficient:



> *"An AI solution can be developed in-house if the IT team is large and experienced enough. It is time-consuming and can disrupt operations when a third-party vendor is not brought in. Delegating the development of your AI solutions will save time and is also more cost-effective. A third-party vendor is also better equipped to spot vulnerabilities that an in-house IT team may miss" (Expert 1).*

Thus, banks in Qatar appear to be ill-equipped to develop and maintain system-wide AI solutions from the ground up. The experts' responses on key challenges provide more insight on the reasons behind this. For one, there may be a shortage of high-skilled workers on the Qatari labor market. Several participants mentioned that training employees is a major obstacle for using AI-powered systems:

> *"Employee training is another problem, along with knowing how to respond when the AI system indicates it has neutralized a potential or real threat" (Expert 1).*

> *"[The problems faced by Qatari banks when integrating AI-based security systems include] lack of technical staff and system complexity" (Expert 2).*

> *"Some of the issues faced during AI integrating [include] training of people" (Expert 6).*

> *"The integration of IT with AI causes some issues such as the training of employees" (Expert 8).*

As such, training is a recurring subtheme in the experts' responses. Another challenge faced by banks when developing software in-house is a potential security risk. One expert suggested that criminals may be privy to important security information:

> *"Local Qatar banks still have security issues due to employee involved in crime activities and them being given access to third parties who worked in banking systems development" (Expert 2).*

Not only may developing AI software locally create security risks due to leakage, it can also complicate the integration of such software with third-party tools in the future. Several experts reported that Qatar banks often faced integration obstacles when moving from in-house solutions:

> *"The bank software is developed internally/locally and some developers worked with contract so there was lack of documentation of system implementation by control flow programming which causes problem in integrating and information encapsulation when information sharing with third-party AI-based solution" (Expert 2).*

In general, the participants seem to agree that banks in Qatar have been struggling to adopt new AI solutions due to compatibility issues with legacy financial software:

> *"The primary problem banks in Qatar face when integrating AI technology is a lack of compatibility with older existing systems and networks" (Expert 1).*
>
> *"For the past 2 year banks in Qatar have been adopting AI solutions but those are still lacking in implementation because the banks' financial software systems are developed locally and it is not easy to convert the whole bank with AI as soon as possible" (Expert 2).*

Overall, the use of third-party software and integration is a major recurring subtheme in experts' responses. In addition, banks seem to be limited in how they may use AI-powered solutions for analyzing communication. Several participants noted that privacy of both customers and employees is an important consideration when implementing AI systems:

> *"The employee personal information is becoming a major issue" (Expert 5).*
>
> *"Chat bot with AI features may infringe customer security and personal privacy" (Expert 4).*

It can be expected that the development of regulatory frameworks, such as GDPR and CCPA, may be impairing the banks' ability to maximize the effectiveness of their AI-powered systems. This is supported by the responses of several experts who voiced concerns over privacy regulations impacting the use of AI in Qatar banks:

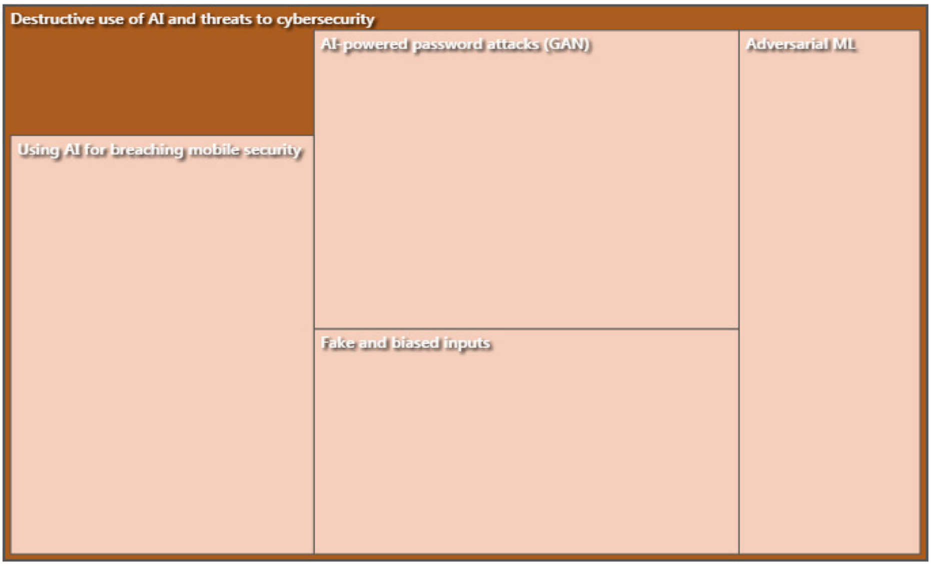
> *"The future regulation of AI may cause some legal issues regarding customer security" (Expert 8).*
>
> *"[Existing AI regulations in other countries] impede the use of AI in banks in Qatar" (Expert 7).*

One expert touched upon communication efficiency implications of privacy legislation

> *"AI causes obstacles between the communication of the employees as employees are restricted to share sensitive information" (Expert 8).*

Theme 3: AI Can Be Used Destructively and Thus Poses a Threat to Cybersecurity in Banks of Qatar

Just as banks are using AI-powered technology to enhance cybersecurity, hackers may also employ AI-based tools. Generally, experts acknowledged the threat of adversarial ML, as such attacks are flexible and are less likely to be detected by security systems:



> *"AI-based malware is hard to detect because it is a deep learner and acts normally; antivirus cannot detect it because antiviruses are designed to catch malware by signature from binaries" (Expert 2).*

One expert suggested that that destructive use of AI algorithms will only become more widespread with the increasing availability of AI-powered solutions on the dark web:

> *"Attackers have easy access to more tools as the lines between state actors and criminal gangs fade. Malware and identity theft kits are easy to find and inexpensive to buy on dark web exchanges. AI-enabled attack kits are on the way, and we can expect that they will be readily available at commodity prices in the next few years" (Expert 6).*

Password-based attacks can also be made more effective using AI tools such as Recurrent Neural Networks (RNN) and GAN. Some experts reported that Qatari banks used AI-based systems for addressing such threats:

> *"Qatar banks are using trained and deep learner AI systems to prevent from cyber threats because attackers are also using AI-based malicious tools" (Expert 2).*

However, the majority of responses suggested that password-based attacks were prevented using traditional methods, such as refreshing passwords, locking accounts, forcing captchas, and mailing customers in the case of multiple failed login attempts:

> *"Traditionally system lock the account for some time period or mail the respective customer in which wrong login attempts are mentioned and requesting them to change the password to make your account more secure" (Expert 5).*

Hackers could also use AI capabilities for circumventing mobile security systems. The majority of experts agreed that mobile systems are highly vulnerable to backdoor attacks, which is only exacerbated by the existence of AI-powered tools:

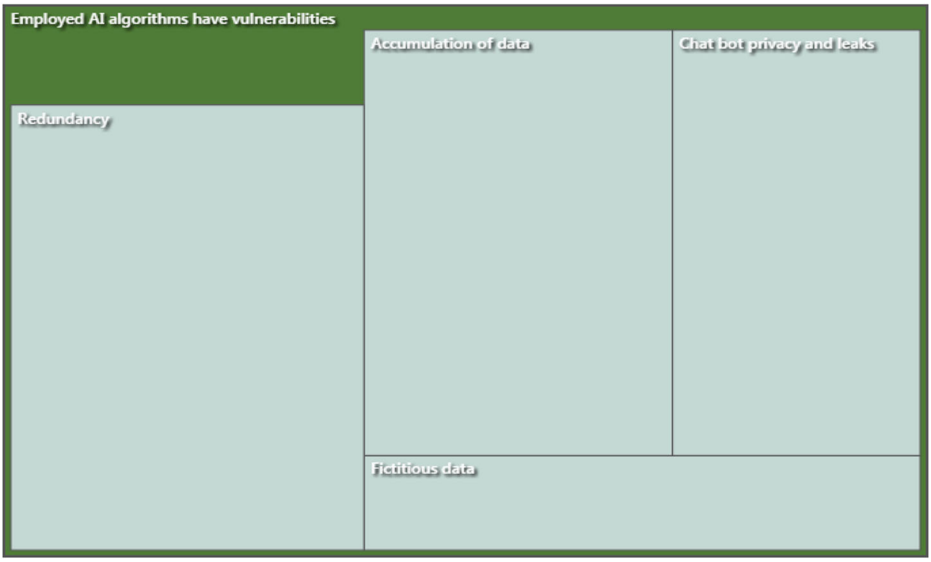
> *"While the technology is improving and banks are upgrading their systems, mobile platforms are still a weak spot that is being looked at in industry compliance laws" (Expert 1).*

> *"Mobile platforms are highly vulnerable to serve as backdoor through voice assistant software (Expert 3)."*

One expert mentioned that mobile threats are addressed by web server monitoring and web application firewall (WAF) systems. In general, it seems that banks in Qatar use a combination of traditional and AI-based tools for preventing AI-powered attacks.

Theme 4: Employed AI-Based Tools Have Vulnerabilities That Can Be Exploited

Another recurring theme is the vulnerabilities of AI-based security systems. In particular, some experts voiced their concern over the widespread use of chat bots in the banking industry:


Employed AI algorithms have vulnerabilities
Redundancy
Accumulation of data
Chat bot privacy and leaks
Fictitious data

> *"Its new and people are not much familiar with chat bots in Qatar banks" (Expert 2).*

> *"Banking chatbots can put consumers' money at risk" (Expert 3).*

Chat bots may create privacy risks and result in data leakage. The respondents reported that Qatar banks use traditional methods, such as SSL encryption and two-factor authentication, to combat this threat. SSL ensures that the information exchanged through the connection is private. Two-factor authentication requires the user to verify their identity by retrieving a code sent to another device.

While the threat associated with chat bots stems from the web-based implementation of an AI-powered system, such systems are also associated with inherent vulnerabilities. A major concern is that hackers may embed fraudulent mechanics in AI engines by feeding them fake data. The respondents mentioned several AI solutions that have been used in Qatari banks, including Teradata, Feedzai, and DataVisor. The responses suggest that banks are addressing these inherent vulnerabilities of AI-powered systems:

> *"Fake data is quickly identified using AI based systems" (Expert 3).*

> *"AI is used < … > to mitigate wrong inputs" (Expert 7).*

> *"Can be mitigated by using technologies like network APT or ATP to prevent fake data's getting collected within the AI platform" (Expert 9).*

Another concern mentioned by the experts is the insufficient redundancy systems associated with AI-powered security:

> *"Currently, bank systems are not employing redundant systems for them to be able to check on each other" (Expert 3).*

One expert mentioned that Qatar banks use RDBMS and the DataGrip tool for managing SQL databases. However, it is not clear whether the established management practices take into the account the data access patterns of AI-based systems. Another participant reported that the use of Security Orchestration, Automation, and Response (SOAR) software for automation would address these concerns.

A major vulnerability associated with AI is accumulation of data. The majority of the experts acknowledge that it is a major threat in the banking industry in Qatar:

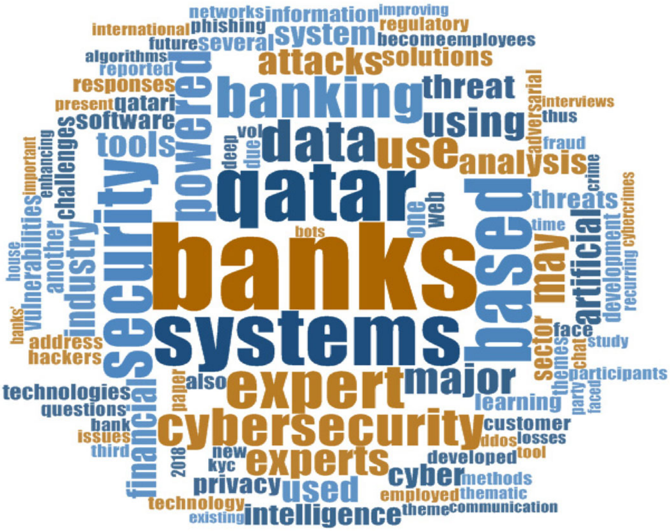
> *"Accumulation of data is considered a threat in Qatari banks and those around the world" (Expert 1).*

> *"Accumulation of data on single system is surely a threat in Qatari banks" (Expert 3).*

In general, the experts' responses suggest that Qatar banks use redundant systems and quantification methods to address this issue. This raises concerns since businesses that integrate Internet of Things equipment and services should conduct a self-assessment of the IoT cyber country's security that their organization maintains (Radanliev et al. 2021). There are currently no self-assessment methodologies available for evaluating the cyber risk posture of the internet of things (IoT). It is believed that the Internet of Things (IoT) represents a complicated system with an excessive number of risk states that cannot be controlled to quantify risk. To facilitate the quantitative risk assessment of uncontrollable risk phases in complicated Internet of Things (IoT) systems, a new design has been developed and validated with the help of comparative research. This approach allows for evaluating uncontrollable risk jurisdictions in complex Internet of Things (IoT) systems that start to imitate AI. It is suitable for a quantifiable self-assessment of the Internet of Things cyber risk stance (Cerrudo and Apa 2017). This can be accomplished with the assistance of algorithms for deep learning and neural networks (Radanliev and De Roure 2021).

Word Clouds

Applying a query based on word frequencies also results in the presentation of the findings in the form of a word cloud (McNiff 2016; Richards 2002). Word clouds display the most frequently occurring words throughout the thematic analysis (Zamawe 2015). According to the findings of the present study's thematic assessments, the word "Banks" is the one that was mentioned most frequently by cybersecurity experts. On the other hand, the words "qatar data" and "security systems" were the words that were mentioned the second most frequently in the interviews. The magnitude of the talk reflects the number of times it was brought up in the focus groups. Consequently, "banking in Qatar" emerged as the primary topic of discussion during the interviews. It is the last and most common term in the study and serves as the focal point for the entire investigation.



Discussion

All participants acknowledged that the AI plays an important role in addressing modern cybersecurity threats in Qatar banks. Based on the experts' replies, these threats include web-based and DDoS attacks, KYC procedures and security, external fraud, internal security risks, and email-based phishing. In addition, the respondents emphasized that AI-based technologies allow for detecting threats more easily compared to rule-based tools, and that such technologies can be deployed across multiple channels. These results are in line with the existing literature on the disruptive effects of AI in the financial industry (Appendix 3) (Dilek, Çakı r, and Aydı n 2015; Goosen et al. 2018; Mosteanu 2020; Ling et al. 2019).

Many experts noted that banks face numerous challenges when implementing AI-powered systems. A major recurring topic was in-house development of AI-based security systems. The responses suggested that developing AI software locally is not feasible, in part due to the shortage of high-skilled workers. Several participants reported that training employees was a major obstacle for using AI-powered systems. Furthermore, criminals may be privy to important security information. Another problem faced by banks in Qatar is integrating innovative AI-powered solutions with legacy systems. These challenges are in agreement with the literature on AI adoption and the Technology Acceptance Model (Alghazo, Kazmi, and Latif 2017).

It appears that banks in Qatar largely use traditional security methods, such as SSL encryption and password resets, for combating AI-based attacks. Considering that one of the experts expressed concern over the increasing availability of AI-powered malware on the dark web, it could be argued that Qatari banks should consider using AI-based security systems to prevent more sophisticated attacks in the future. Nevertheless, banks should ensure that all basic security features are in place, including SSL certificates, device registration, system-based alarms, group policy settings, multifactor authentication, inbound and outbound access rules, data encryption, and private keys with passwords (Alghazo, Kazmi, and Latif 2017). Failing to properly address adversarial ML attacks may adversely impact the bank's operations. In particular, this could lead to false information about market events, corrupted training data for risk models, and suboptimal decision-making in automated financial management. Overall, these results agree with the AI itself being a major target for hackers (Caldwell et al. 2020; Kaloudi and Li 2020). Failing to address this issue may cause significant financial disruption.

Almost all experts agreed that accumulation of data presents a major threat in the banking industry of Qatar. Redundant system structures are used to alleviate this problem. As some banks are only starting to adopt

AI-based technologies, collecting data in a single system for security monitoring and event management can become a serious issue. Thus, IT security regulations should address the data being stored in one place. Data can be distributed and decentralized. Decentralized blockchain systems can be used to address this problem. Data collection should be deployed into multiple servers with multiple search heads.

Another recurring topic covered challenges posed by regulatory frameworks. Most notably, several experts expressed concern over regulations, such as GDPR and CCPA, impeding the implementation of AI solutions in the banking industry. These concerns are in line with the uncertainty surrounding AI, as regulatory frameworks are still being developed (Financial Stability Board 2017; 2019). Notably, MENA countries have substantial gaps regarding data privacy in the context of innovative technologies (Lukonga 2018). Some concerns have been raised over AI technologies leading to job losses, reduction in customer loyalty, and misuse of data (Kochhar, Purohit, and Chutani 2019). Thus, it can be expected that banks in Qatar will face new challenges in the future, as new legislation is developed.

Cyberattacks are increasingly frequent across all industries but are particularly prevalent in the financial services sector. According to the most recent research from security agencies, the banking and insurance industry is the most targeted industry (Ryzhkova et al. 2020). Threats originating in cyberspace have the potential to bring down big company networks and get access to sensitive and confidential info that highly sophisticated protection systems and procedures would otherwise protect. Putting all your faith in cybersecurity professionals might not be the most surefire method to prevent catastrophic cyber attacks from cybercriminals (Perumal 2018). Because of the need for more effective security systems, financial institutions have made significant investments in artificial intelligence and its capabilities.

Conclusion

The banking industry in Qatar has placed a significant emphasis on cyber security, with Qatar National Bank (QNB) proposing a systematic plan and Doha Bank viewing cyber security management as not only a critical area to be focused on but also essential for the financially viable growth of the country. Advancing swiftly is the rate during which cybercriminals create new methods of breaching systems and obtaining access to important bank and consumer data. Perumal (2018) states that the financial services sector is perpetually operating at a disadvantage as it must compete to reduce potential dangers posed by an unending stream of newly discovered threats to online security. Controlling cyberspace should receive significant attention, as it is an important topic to concentrate on, and pragmatic governance of cyberspace is essential to Qatar's continued economic development.

According to Petit and Shladover (2014), several AI implementation difficulties were explored, and among those challenges, security was thought to be among the most difficult. Advanced AI systems are now more susceptible to a wide range of cyber-attacks (Cerrudo and Apa 2017), which aim to compromise the data or systems' privacy, authenticity, availability, and secrecy (Dash, Karimibiuki, and Pattabiraman 2021). The most significant security risks and flaws that robotic systems could exploit have been outlined in (Lacava et al. 2021). In addition, a collection of known AI cyber-attacks was published in (Chowdhury, Karmakar, and Kamruzzaman 2017), and several efforts were integrated to limit the susceptibility of the AI Operating System to a variety of security flaws. In addition, a collection of security measures that are low in energy consumption was discussed (Hellaoui, Koudil, and Bouabdallah 2017). Guiochet et al. looked into the safety of applications based on the interaction between humans and robots in the study of Guiochet, Machin, and Waeselynck (2017). Dieber et al. (2017) examined the security of AI by performing penetration tests and offering methods to strengthen its defenses in their paper further. Recent research (Rubio et al. 2019) summarized the most recent developments in cyber-defence for control systems. In addition, Guiochet, Machin, and Waeselynck (2017) reviewed the secure design of automated driving, including AI ones, and published their findings. Regrettably, the associated work does not have a worldwide grasp of the AI security challenges and the factors contributing to them. In addition, there has been no consultation regarding developing guidelines for constructing safe AI systems. Therefore, the study aims to explore the impact of AI on the cybersecurity system in Qatar banking industry. Particularly, the study finds out the risks and challenges in the proper implementation of AI system and cyber defense system for banking industry. A thematic analysis of interviews of 9 experts in the banking industry of Qatar was conducted. Four key themes emerged from the analysis: 1) AI is a major tool for enhancing cybersecurity of banks in Qatar; 2) banks face challenges in using AI for improving cybersecurity; 3) AI can be used destructively and thus poses a threat to cybersecurity in banks of Qatar; 4) employed AI-based tools have vulnerabilities that can be exploited.

Based on the results, it can be argued that AI plays an increasingly important role in cybersecurity in Qatar banks. AI helps address threats related to web-based and DDoS attacks, KYC checks, external and internal fraud, and phishing. Furthermore, AI-powered systems are more robust and flexible compared to rule-based tools and allow for deployment across multiple channels. However, there appear to be many challenges faced by banks in Qatar when implementing AI-based security systems. These challenges include a lack of skilled employees, infeasibility of in-house development of AI systems, compatibility issues with legacy systems, and regulatory compliance. AI-powered attacks pose a new challenge for Qatari banks, which is likely to become even more impactful as the availability of AI-based malware increases.

The present study is subject to certain limitations. The study relied on thematic analysis for making conclusions about the banking industry in Qatar. The validity of the results is dependent on the reliability of the responses provided by the experts. In particular, it is possible that experts conveyed their perceptions about the industry, which may be different from the actual use of AI in Qatari banks. Furthermore, only 9 experts were interviewed for the study. The sample size suggests that the obtained data may be insufficient to draw conclusions about the industry as a whole. Future research may expand on the present analysis to address these limitations. Notably, the challenges faced by banks in Qatar could be explored in greater detail. This may help inform the decisions of policymakers and enhance the stability of the financial system as a whole. Future studies could explicitly compare the practices of banks in Qatar to the practices adopted in major developed economies.

Acknowledgment

The authors wish to thank, Qatar University, College of Engineering for their Guidance in coming up with the research.

References

Abu-Taieh, E., A. Alfaries, S. Al-Otaibi, and G. Aldehim. 2018. Cyber security crime and punishment: Comparative study of the laws of Jordan, Kuwait, Qatar, Oman, and Saudi Arabia. *International Journal of Cyber Warfare and Terrorism* 8 (3):46–59. doi:10.4018/IJCWT.2018070104.

Akinbowale, O. E., H. E. Klingelhöfer, and M. F. Zerihun. 2020. Analysis of cyber-crime effects on the banking sector using the balanced score card: A survey of literature. *Journal of Financial Crime* 27 (3):945–58. doi:10.1108/JFC-03-2020-0037.

Alghazo, J. M., Z. Kazmi, and G. Latif. 2017. Cyber security analysis of internet banking in emerging countries: User and bank perspectives. In 2017 4th IEEE international conference on engineering technologies and applied sciences (ICETAS) (1–6). IEEE. doi:10.1109/ICETAS.2017.8277910.

Al-Hamar, Y., H. Kolivand, and A. Al-Hamar. 2019. Phishing attacks in Qatar: A literature review of the problems and solutions. In 2019 12th International Conference on Developments in eSystems Engineering (DeSE) (pp. 837–842). IEEE. doi:10.1109/DeSE.2019.00155.

Al-Mhiqani, M. N., R. Ahmad, Z. Z. Abidin, W. M. Yassin, A. Hassan, A. N. Mohammad, and N. L. Clarke. 2018. A new taxonomy of insider threats: An initial step in understanding authorised attack. *International Journal of Information Systems and Management* 1 (4):343–59. doi:10.1504/IJISAM.2018.094777.

Almutairi, M, and H. Nobanee. 2020. Artificial intelligence in financial industry. Available at *SSRN 3578238*

Braun, V, and V. Clarke. 2013. *Successful qualitative research: A practical guide for beginners*. London: Sage.

Caldwell, M., J. T. A. Andrews, T. Tanay, and L. D. Griffin. 2020. AI-enabled future crime. *Crime Science* 9 (1):1–13. doi:10.1186/s40163-020-00123-8.

Cerrudo, C, and L. Apa. 2017. Hacking robots before skynet. *IOActive Website* 1–17.

Chowdhury, A., G. Karmakar, and J. Kamruzzaman. 2017. Survey of recent cyber security attacks on robotic systems and their mitigation approaches. In *Detecting and Mitigating Robotic Cyber Security Risks*, 284–99. IGI global.

Chui, M., J. Manyika, and M. Miremadi. 2016. Where machines could replace humans-and where they can't (yet).

Dash, P., M. Karimibiuki, and K. Pattabiraman. 2021. Stealthy attacks against robotic vehicles protected by control-based intrusion detection techniques. *Digital Threats: Research and Practice* 2 (1):1–25. doi:10.1145/3419474.

Deep, V, and P. Sharma. 2018. Analysis and Impact of Cyber Security Threats in India using Mazarbot Case Study. In *2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS)* (499–503), IEEE, December.

Dieber, B., B. Breiling, S. Taurer, S. Kacianka, S. Rass, and P. Schartner. 2017. Security for the robot operating system. *Robotics and Autonomous Systems* 98:192–203. doi:10.1016/j.robot.2017.09.017.

Dilek, S., H. Çakır, and M. Aydın. 2015. Applications of artificial intelligence techniques to combating cyber-crimes: A review. *arXiv Preprint arXiv:1502.03552*

Dworkin, S. L. 2012. Sample size policy for qualitative studies using in-depth interviews. *Archives of Sexual Behavior* 41 (6):1319–20.

EBF. 2019. "AI in the banking industry." European Banking Federation position paper, https://www.ebf.eu/cybersecurity-innovation/ai-in-the-banking-industry-ebf-position-paper/.

Elzamly, A., B. Hussin, S. S. Abu-Naser, T. Shibutani, and M. Doheir. 2017. Predicting critical cloud computing security issues using Artificial Neural Network (ANNs) algorithms in banking organizations.

Financial Stability Board. 2017. Artificial intelligence and machine learning in financial services: Market developments and financial stability implications. Financial Stability Board Research Paper, https://www.fsb.org/2017/11/artificial-intelligence-and-machine-learning-in-financial-service/.

Galvin, R. 2015. How many interviews are enough? Do qualitative interviews in building energy consumption research produce reliable knowledge? *Journal of Building Engineering* 1:2–12. doi:10.1016/j.jobe.2014.12.001.

Geluvaraj, B., P. M. Satwik, and T. A. Ashok Kumar. 2019. The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. In *International Conference on Computer Networks and Communication Technologies* (739–47). Springer, Singapore.

Goosen, R., A. Rontojannis, S. Deutscher, J. Rogg, W. Bohmayr, and D. Mkrtchian. 2018. Artificial intelligence is a threat to cybersecurity. It's also a solution. *Boston Consulting Group (BCG), Tech. Rep.*

Guerrero-Higueras, Á. M., N. DeCastro-García, and V. Matellán. 2018. Detection of cyber-attacks to indoor real time localization systems for autonomous robots. *Robotics and Autonomous Systems* 99:75–83. doi:10.1016/j.robot.2017.10.006.

Guiochet, J., M. Machin, and H. Waeselynck. 2017. Safety-critical advanced robots: A survey. *Robotics and Autonomous Systems* 94:43–52. doi:10.1016/j.robot.2017.04.004.

Hellaoui, H., M. Koudil, and A. Bouabdallah. 2017. Energy-efficient mechanisms in security of the internet of things: A survey. *Computer Networks* 127:173–89. doi:10.1016/j.comnet.2017.08.006.

Kaloudi, N, and J. Li. 2020. The AI-based cyber threat landscape: A survey. *ACM Computing Surveys* 53 (1):1–34. doi:10.1145/3372823.

Kirschgens, L. A., I. Z. Ugarte, E. G. Uriarte, A. M. Rosas, and V. M. Vilches. 2018. Robot hazards: From safety to security. *arXiv Preprint arXiv:1806.06681*

Kochhar, K., H. Purohit, and R. Chutani. 2019. The rise of artificial intelligence in banking sector. In *The 5th International Conference on Educational Research and Practice (ICERP) 2019*(127).

Lacava, G., A. Marotta, F. Martinelli, A. Saracino, A. La Marra, E. Gil-Uriarte, and V. M. Vilches. 2021. Cybsersecurity issues in robotics. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 12 (3):1–28.

Lai, S. T., F. Y. Leu, and J. W. Lin. 2018. A banking chatbot security control procedure for protecting user data security and privacy. In *International conference on broadband and wireless computing, communication and applications* (561–71). Springer, Cham, October

Ling, L., Z. Gao, M. A. Silas, I. Lee, and E. A. Le Doeuff. 2019. An AI-based, multi-stage detection system of banking botnets. *arXiv Preprint arXiv:1907.08276*

Lukonga, M. I. 2018. Fintech, inclusive growth and cyber risks: Focus on the MENAP and CCA regions. IMF Working Papers 2018/201.

McNiff, K. 2016. "What is qualitative research?" The NVivo Blog QSR International.

Mosteanu, N. R. 2020. Artificial intelligence and cyber security–face to face with cyber-attack–A maltese case of risk management approach. *Ecoforum Journal* 9 (2):12–25.

Ortiz, J., A. Marin, and O. Gualdron. 2016. Implementation of a banking system security in embedded systems using artificial intelligence. *Advances in Natural and Applied Sciences* 10 (17):95–101.

Perumal, S. V. 2018. Cyber security vital for Qatar's sustainable growth, say banks.

Perumal, S. V. 2018. Cyber security vital for Qatar's sustainable growth, say banks. Gulf Times, http://desktop.gulf-times.com/story/613378. 2018.

Petit, J, and S. E. Shladover. 2014. Potential cyberattacks on automated vehicles. *IEEE Transactions on Intelligent Transportation Systems* 16 (2):546–56.

Qatar Banking Perspectives. 2021. Technology, innovation and sustainability, https://assets.kpmg/content/dam/kpmg/qa/pdf/2021/09/qatar-banking-perspective-2021-v2.pdf

Radanliev, P, and D. De Roure. 2021. Review of algorithms for artificial intelligence on low memory devices. *IEEE Access*. 9:109986–93. doi:10.1109/ACCESS.2021.3101579.

Radanliev, P., D. De Roure, P. Burnap, and O. Santos. 2021. Epistemological equation for analysing uncontrollable states in complex systems: Quantifying cyber risks from the internet of things. *The Review of Socionetwork Strategies* 15 (2):381–411.

Ranjan, S., D. R. Gupta, and D. A. Gupta. 2020. Artificial intelligence in financial acumen: Challenges and opportunities. *Cosmos Journal of Engineering & Technology* 10 (1):1–5.

Richards, T. 2002. An intellectual history of NUD* IST and NVivo. *International Journal of Social Research Methodology* 5 (3):199–214. doi:10.1080/13645570210146267.

Rubio, J. E., C. Alcaraz, R. Roman, and J. Lopez. 2019. Current cyber-defense trends in industrial control systems. *Computers & Security* 87:101561. doi:10.1016/j.cose.2019.06.015.

Ryzhkova, M., E. Soboleva, A. Sazonova, and M. Chikov. 2020. Consumers' perception of artificial intelligence in banking sector. In *SHS Web of Conferences* 80:1019. EDP Sciences. doi:10.1051/shsconf/20208001019.

Shmuratko, Y. A, and S. A. Sheludko. 2019. Financial technologies'impact on the development of banking. *Financial and Credit Activity: Problems of Theory and Practice* 4 (31): 61–9.

Soni, V. D. 2019. Role of artificial intelligence in combating cyber threats in banking. *International Engineering Journal for Research & Development* 4 (1):7–

Tao, Q., M. Jiang, X. Wang, and B. Deng. 2018. A cloud-based experimental platform for networked industrial control systems. *International Journal of Modeling, Simulation, and Scientific Computing* 09 (04):1850024. doi:10.1142/S1793962318500241.

Terry, G., N. Hayfield, V. Clarke, and V. Braun. 2017. Thematic analysis. *The SAGE Handbook of Qualitative Research in Psychology* 2:17–37.

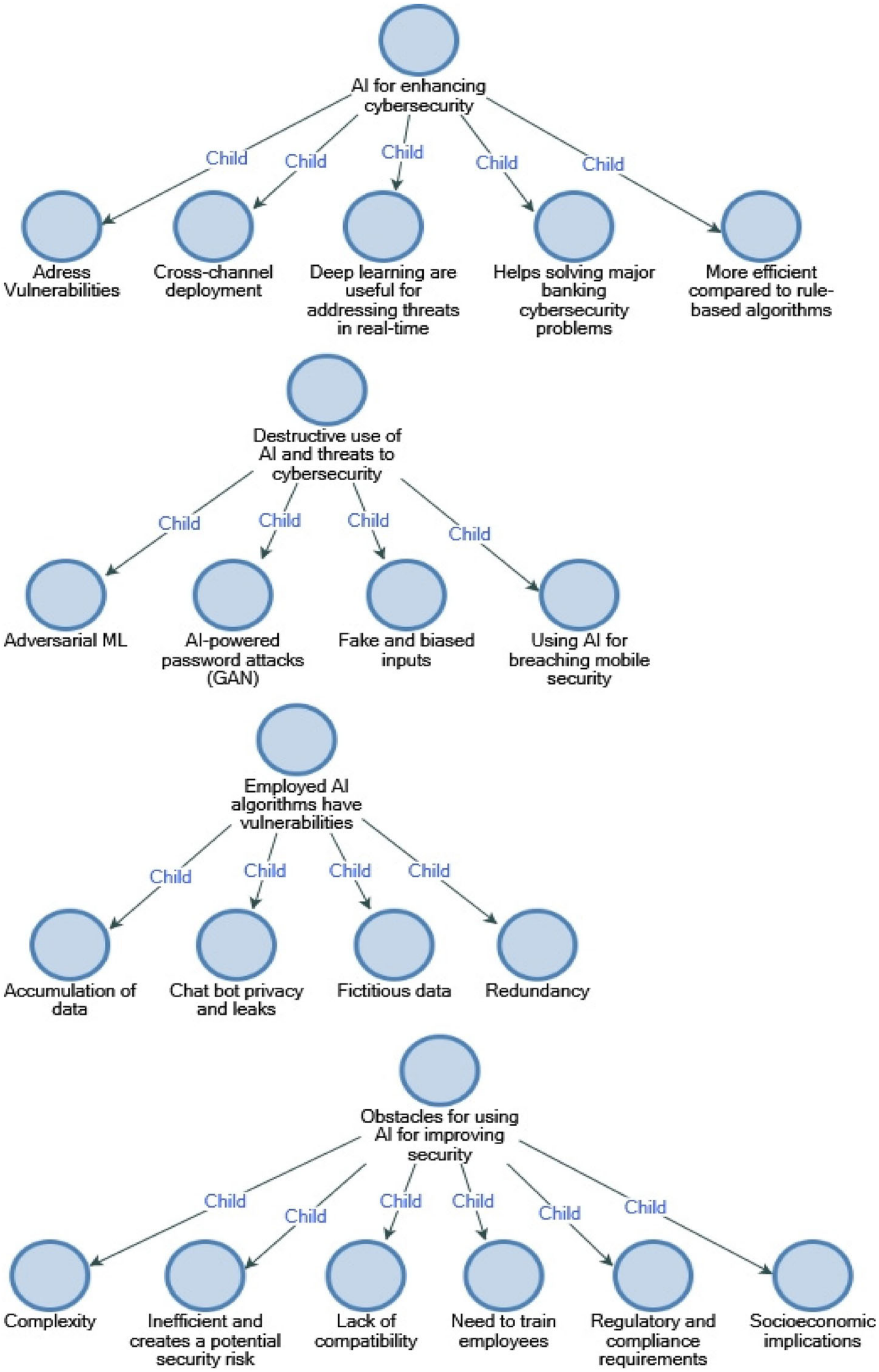
Thowfeek, M. H., S. N. Samsudeen, and M. B. F. Sanjeetha. 2020. Drivers of artificial intelligence in banking service sectors. *Solid State Technology* 63 (5):6400–11.

Truby, J., R. Brown, and A. Dahdal. 2020. Banking on AI: Mandating a proactive approach to AI regulation in the financial sector. *Law and Financial Markets Review* 14 (2): 110–20. doi:10.1080/17521440.2020.1760454.

Zamawe, F. C. 2015. The implication of using NVivo software in qualitative data analysis: Evidence-based reflections. *Malawi Medical Journal: The Journal of Medical Association of Malawi* 27 (1):13–5. doi:10.4314/mmj.v27i1.4.

Appendices

Appendix 1. Project map

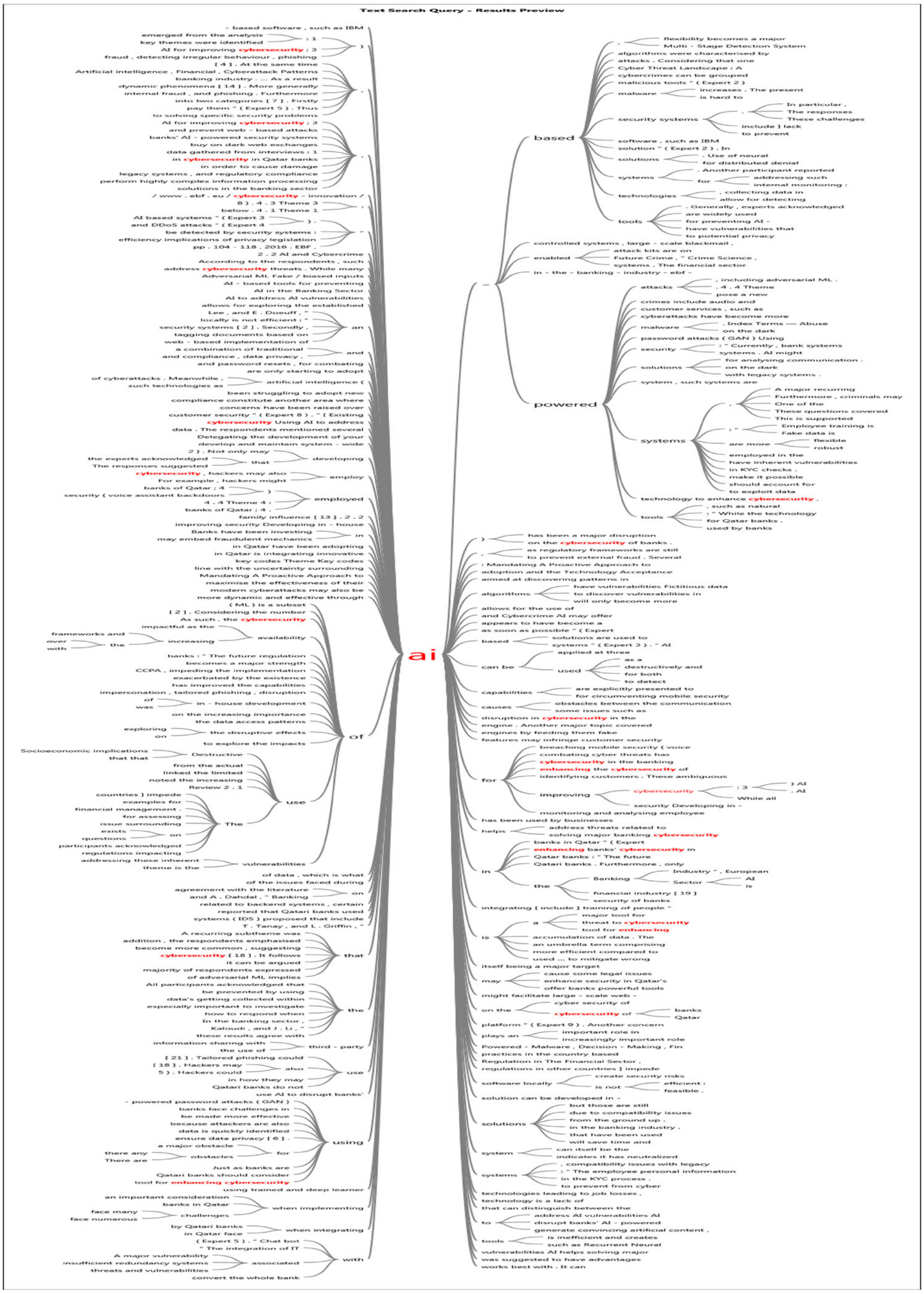

AI for enhancing cybersecurity
Child
Child
Child
Child
Child
Adress Vulnerabilities
Cross-channel deployment
Deep learning are useful for addressing threats in real-time
Helps solving major banking cybersecurity problems
More efficient compared to rule-based algorithms
Destructive use of AI and threats to cybersecurity
Child
Child
Child
Child
Adversarial ML
AI-powered password attacks (GAN)
Fake and biased inputs
Using AI for breaching mobile security
Employed AI algorithms have vulnerabilities
Child
Child
Child
Child
Accumulation of data
Chat bot privacy and leaks
Fictitious data
Redundancy
Obstacles for using AI for improving security
Child
Child
Child
Child
Child
Child
Complexity
Inefficient and creates a potential security risk
Lack of compatibility
Need to train employees
Regulatory and compliance requirements
Socioeconomic implications

Appendix 2. Themes and key codes

Theme	Key codes
AI is a tool for enhancing cybersecurity	• Using AI to address AI vulnerabilities • AI helps solving major banking cybersecurity problems (web-based attacks, DDoS, KYC, fraud, detecting irregular behavior, phishing) • AI is more efficient compared to rule-based algorithms • Deep learning and reinforced learning are useful for addressing threats in real-time • Cross-channel deployment
There are obstacles for using AI for improving security	• Developing in-house AI tools is inefficient and creates a potential security risk • Lack of compatibility between locally developed systems and third-party software • Complexity • Need to train employees • Regulatory and compliance requirements (transparency, privacy) • Socioeconomic implications
Destructive use of AI is a threat to cybersecurity of banks in Qatar	• Adversarial ML • Fake/biased inputs • AI-powered password attacks (GAN) • Using AI for breaching mobile security (voice assistant backdoors)
Employed AI algorithms have vulnerabilities	• Fictitious data • Chat bot privacy/leaks • Accumulation of data • Redundancy

The themes are analyzed in greater detail below.

Appendix 3. Word tree of AI


Text Search Query - Results Preview
ai
based
powered
systems
security systems
solutions
technologies
tools
attacks
malware
security
enabled
of
use
The
that
the
using
with
an
and
employ
employed
in
for
is
may
can be
used
helps
algorithms
capabilities
causes
improving
solution
system
cybersecurity
enhancing