Chatbots in Cybersecurity: Enhancing Security Chatbot Efficacy through Iterative Feedback Loops and User-Centric Approaches

Thawbaan Adam, Song Shombot Emmanuel, Gilles Dusserre, Nasir-Baba Ahmed, Zahir Babatunde, Lawan Mohammed Isa, Danladi Ayuba Job

American Journal of Innovation in Science and Engineering (AJISE)

Volume 3 Issue 2, Year 2024
ISSN: 2158-7205 (Online)
DOI: https://doi.org/10.54536/ajise.v3i2.2919
https://journals.e-palli.com/home/index.php/ajise

Chatbots in Cybersecurity: Enhancing Security Chatbot Efficacy through Iterative Feedback Loops and User-Centric Approaches

Thawbaan Adam[1*], Song Emmanuel[1], Gilles Dusserre[1], Nasir Baba Ahmed[1], Zahir Babatunde[2], Lawan Mohammed Isa[1], Danladi Ayuba Job[1]

Article Information

Received: July 15, 2024
Accepted: August 18, 2024
Published: November 29, 2024

Keywords

AI Chatbot, Cybersecurity, Cyber Threat, Feedback, Security Assistant Bot

ABSTRACT

Chatbots are of continuous importance in our interactive lives. Although used in several domains, there are questions about its security assurance; therefore, there is a need to know its capabilities, limitations, and challenges in cybersecurity. The research explores the use of chatbots in enhancing cyber defences and their potentials. It examines chatbots' current applications in cybersecurity, including IT services, information protection, and user education. Furthermore, the research proposes implementing an Intelligent Chatbot Security Assistant (ICSA) model on WhatsApp to detect and respond to cyberattacks based on user conversations and identifies the challenges with this implementation. To address these challenges, it suggests incorporating enhanced privacy measures, real-time monitoring, rigorous evaluation and validation, and concludes with user-centric design principles using iterative feedback. This research provides valuable insights into the use of chatbots in cybersecurity, their current level of research and implementation as a cybersecurity tool, and directions for future research.

INTRODUCTION

In the digital transformation era, cybersecurity has become a crucial concern for individuals and organisations alike. As the threat landscape continues to evolve, so must our defences. Cybersecurity threats are increasingly sophisticated and prevalent, targeting individuals and organisations on a global scale. Traditional methods of detection and prevention are no longer sufficient (Shaqiri, 2021). In this context, AI chatbots show promise in enhancing cybersecurity (Gómez Mármol *et al.*, 2016). However, the extent and potential of their use in this domain remain to be thoroughly explored. This research aims to shed light on this underexplored area by conducting a comprehensive literature survey on the use of chatbots in cybersecurity and proposing improvements for an Intelligent Chatbot Security Assistant (ICSA) model. The primary objective of this research is (1). To explore the level at which chatbots are being used in cybersecurity and their potential. With a specific focus on chatbots used in cybersecurity and their role in detecting cyberattacks. (2). Investigate a specific work on the use of chatbots in real-time phishing attack detection in a social network service (SNS) chat room. (3). Propose the implementation of an identified model of a chatbot assistant bot on WhatsApp and highlight challenges faced by the model and (4). Propose improvements to address the highlighted challenges, including user privacy, false positives, and false negatives.

An overview of chatbots and their functionality in cybersecurity will be provided, along with the scope of cyber threats they may help defend against. This research will rely more on state-of-the-art analysis, which will explore the most up-to-date research knowledge of chatbots in cybersecurity. It will examine methods for using chatbots for cyberattack detection to improve cyber defence. Answering the questions: how are chatbots used for cybersecurity, and how effective are they in detecting cyberattacks?

The importance of this work is twofold. Firstly, it contributes to the existing body of knowledge by providing a much-needed review of the current state of the art regarding the use of chatbots for cybersecurity. Secondly, it offers concrete suggestions for improving an existing ICSA model, thereby providing a practical guide for researchers and practitioners interested in leveraging chatbots for cybersecurity.

Chatbots and Artificial Intelligence

Chatbots are AI-powered conversational agents designed to interact with users through natural language processing (NLP) and machine learning (ML) algorithms to understand user input and respond appropriately by drawing on a large dataset of possible responses (Alazzam *et al.*, 2023; Gómez Mármol *et al.*, 2016). They simulate human conversation through text or voice (Gómez Mármol *et al.*, 2016) and can also be integrated into various platforms, such as websites, messaging apps, and social media, to provide personalised customer service, support, and information (Følstad & Brandtzæg, 2017). Chatbots have been of rising use in various industries, including customer service, healthcare, and education, to provide personalised services, support, and information (Gómez Mármol *et al.*, 2016; Yoo & Cho, 2022).

Artificial intelligence (AI) has recently become prominent. Aiming to use search and pattern matching techniques to provide answers to questions. AI employs algorithms and

[1] IMT Mines Ales, France
[2] AirMatrix, Canada
* Corresponding author's e-mail: adasabaa1@gmail.com

advanced cognitive technologies. As an interdisciplinary field, AI is used for medical diagnosis, law enforcement, and creating artificial instructions. It has a wide scope of data related to developments in these fields, as it includes the ability to simulate human cognition while processing natural language (NL) to enable human-computer communication. AI focuses on using search and pattern recognition strategies to offer solutions to the demands for answers. It uses logical sequences called algorithms and sophisticated cognitive computing technologies. It has access to a wide range of data related to advancements in these areas since it includes the ability to reason while processing natural language to develop communication between humans and computers (McTear *et al.*, 2016).

Artificial Intelligence (AI) enables chatbots to understand and process natural language inputs and generate human-like responses by breaking down the user's input into individual words and phrases, then using Natural Language Processing (NLP) to analyse the meaning to determine the appropriate response. This process involves identifying keywords and patterns in the user's input and understanding the context and intent behind their message. It then generates a response using pre-written scripts or by generating new text based on its programming and training data (Dale, 2016).

AI use in chatbots differs from traditional IT innovations in their ability to learn, adapt, and connect to provide solutions (Huang & Rust 2021). For example, Amazon Alexa is an AI-powered service that self-learns through data and machine learning algorithms to adapt to changing customer needs (Kaplan & Haenlein, 2019). This self-learning is enabled by connectivity through the Internet of Things and data sharing (Hoffman & Novak, 2016).

Cybersecurity, Threats and Attacks

Cybersecurity refers to the practice of protecting computer systems, networks, and data from unauthorised access. This unauthorized access poses threats with potential dangers, they could be unintentional or intentional forms of attacks intents aimed at compromising the confidentiality, integrity, or availability of digital assets ('Computer and Information Security Handbook', 2017). Examples include data breaches, malware infections, and DDoS attacks. These threats can compromise computer systems, networks, and digital data and cause severe damages. They can originate from various sources, such as hackers, cybercriminals, nation-states, or even insiders within an organization (Pfleeger & Pfleeger, 2012). With the growing reliance on digital technologies, the importance of cybersecurity has never been more apparent.

The Evolution of AI Chatbots and Cybersecurity

AI chatbots have seen substantial evolution over the years in several sectors, including cybersecurity. Despite having been around since 1965, the renewed interest in chatbots was aroused in the spring of 2016, as a result of drastic advancements in artificial intelligence (Følstad & Brandtzæg, 2017).

The integration of chatbots with artificial intelligence (AI) has unleashed a vast potential in chatbots that is still evolving (Adamopoulou & Moussiades, 2020). Recent advancements in chatbot technologies, such as deep learning and transformer-based models, have led to significant improvements in NLP capabilities. These technologies paved the way for the creation of more sophisticated chatbots. Chatbots that could understand natural language, carry out contextual conversations, and provide more accurate responses are evidenced by the renowned AI chatbot model ChatGPT (Brown *et al.*, 2020), which is recognised as one of the most advanced chatbots available now with a wide range of services (Akter *et al.*, 2023). Although cybersecurity threats have evolved over time, from simple viruses and worms in the 1980s to advanced persistent threats (APTs) and ransomware attacks in recent years (Zimba *et al.*, 2020).

In cybersecurity, these models do better than understand context or generate human-like text in order to give a conversational response; they are very effective for complex tasks such as understanding intricate patterns of cyberattacks, predicting potential vulnerabilities, and generating detailed reports of security incidents.

Machine Learning in Chatbots

According to Lin *et al.* (2016), chatbots that employ machine learning approaches, as opposed to relying on pattern matching, extract the content from user input using natural language processing (NLP), allowing them to learn from conversations and consider the entire dialogue context. Unlike rule-based chatbots, they do not require a predefined response for every possible user input but instead rely on extensive training sets. However, finding appropriate datasets for training can be challenging, as the available datasets may be inadequate. For example, a movie script corpus may be too broad, or an IT helpline dataset may be too specific. Artificial Neural Networks (ANNs) are often used to implement these chatbots, with retrieval-based models using neural networks to score and select the most probable response from a set of predefined responses. In contrast, generative models use deep learning techniques to generate a response from scratch (Alazzam *et al.*, 2023).

Natural Language Processing (NLP) in Chatbots

Chowdhury (2003), define natural language processing (NLP) as a field of artificial intelligence that explores how computer systems can interpret and manipulate natural language in text or speech. The goal is to gather information on human language comprehension and usage to develop appropriate techniques for computer systems to handle natural language and perform various tasks (Jung, 2019). Machine learning is commonly used in most NLP techniques, including natural language understanding, which focuses on comprehending text, and natural language generation (Langner *et al.*, 2010; Perera & Nand, 2017), which involves generating text, often accomplished using artificial neural networks

(ANNs). NLP allows humans to learn and machines to reason. NLP, as described by Verspoor *et al.* (2012), involves using computational methods to analyse linguistic data, especially textual data like documents. The goal is to develop representations of text that integrate linguistic and structural information. NLP seems crucial for creating software that allows human-computer interaction by storing information, solving problems, and performing repetitive tasks requested by users.

Using NLP, questions on specific topics consisting of words, phrases, and sentences requested by users can be processed appropriately and answered by AI-enabled devices like chatbots, which are programmed within the scope of AI (Goksel Canbek & Mutlu, 2016).

Natural Language Understanding (NLU) in Chatbots

Chatbots use natural language understanding (NLU) to make sense of unstructured user input in human language and respond appropriately based on the user's intent (Jung, 2019; McShane, 2017). There are three main challenges in the NLU process: mechanisms of thought, interpretation, and knowledge of the user (Chowdhury, 2003). NLU supports intent classification and entity extraction, taking context into account. Entities can be system-defined or user-defined, and contexts store objects the user refers to (Ramesh *et al.*, 2017). The intent classification model can be a classifier like an SVM algorithm or a pretrained model created by manually classifying collected text messages into intents. Similarly, the entity extraction model can be pre-trained by manually annotating entities in user text messages. An annotated training corpus can be created by labelling each word block.

Once the models are trained, they can automatically classify new user text messages into intents and extract entities (Hien *et al.*, 2018).

The Convergence of Chatbots and Cybersecurity

The convergence of chatbots and cybersecurity offers an opportunity to leverage AI and machine learning techniques to enhance threat detection, prediction, and prevention (Dan *et al.*, 2019). As both fields continue to evolve, the potential applications and benefits of chatbots in cybersecurity will become increasingly apparent. The use of chatbots in cybersecurity has gained traction in recent years due to their potential to enhance threat detection and response capabilities like collecting and analysing data from various sources, such as network logs, social media, and other online platforms, to identify potential threats (Buczak & Guven, 2016). This integration of chatbots and AI technologies in cybersecurity has the potential to revolutionise the way organisations detect and respond to cyber threats.

State of the Art Analysis

It is undeniable that chatbots have gained fame in the last decade, and research has been conducted to explore their potential as a cybersecurity tool. Most of which have shown their potential and future direction.

This section reviews the existing literature on chatbots and cybersecurity, including key studies and findings. It discusses the current peak of research on detecting cyberattacks via chatbots (Barry *et al.*, 2022).

Current Applications of Chatbots in Cybersecurity

Chatbot technology can be used in the IT service area, particularly in the cybersecurity field, to counter cyberattacks (Gómez Mármol *et al.*, 2016). Educational chatbots are being developed to enhance security awareness and incident responses among end-users and cyber analysts. For instance, Sabbagh *et al.* (2012) introduced the HI2P TOOL that promotes information security culture among users by incorporating various learning methods and topics including incident response and security policies. Similarly, Kowalski *et al.* (2013) presented Chatbot Sally, which can interact with employees in a company who have different levels of education or experience in security. Another area of development is the creation of chatbots for information protection. Buczak and Guven (2016) developed an AI chatbot-based advanced digital locker that provides a user-friendly environment for protecting crucial information. This digital locker allows users to select an appropriate encryption method to safeguard their critical information. Additionally, Trivino *et al.* (2019) proposed C3-Sex, a chatbot that is suggested for detecting online sex offenders. The chatbot is based on an Artificial Conversational Entity (ACE) that connects to various online chat services to initiate a conversation. The ACE was developed using generative and rule-based models of machine learning, which are responsible for generating posts and replies from the chatbot and use knowledge-based systems to interact with suspects about child pornography and prevent cybercrime. After the conversation, some ML algorithms were utilised to analyse the chat logs, generate the suspect's profile, and classify them into one of three categories (Indifferent, Interested, and Pervert). Additionally, the proposed solution includes a module to analyse the conversations conducted by the chatbot and calculate 25 features that describe the suspect's behaviour. Another chatbot is BotHook, developed by Zambrano *et al.* (2017), this a chatbot designed to identify cyber paedophiles and catch cybercriminals. The researchers created a module to attract paedophile interests and characterise them. Another study of AÇAR (2017) examines the effectiveness of current methods for detecting cyber perverts and proposes futuristic approaches such as analysing metadata and content data of VoIP communications, as well as using fully automated chatbots for undercover operations. Similarly, a system designed to detect online child grooming is proposed in the work of (Anderson *et al.*, 2019). This system uses Bag of Words (BoW) to select words related to grooming and Fuzzy-Rough Feature Selection (FRFS) to identify the most significant features. Finally, a fuzzy twin Support Vector Machine was employed for text classification using two training datasets: one from

Perverted Justice and another from PAN13. Hamad and Yeferny (2020) proposed a chatbot that serves as an advisor in information security by using a knowledge base with a JSON file. This chatbot offers accurate advice based on different opinions from information security experts, raising awareness in the field of information security for many users on different platforms. Currently, the main aims of the current applications of chatbots in cybersecurity has been to contributing to strengthening cybersecurity posture, enhancing incident response capabilities, promoting user education and awareness, and improving overall operational efficiency in cybersecurity operations.

Using Chatbots for Cyber Attack Detection

Detecting cyberattacks is a complex task that requires the analysis of large volumes of data from various sources (Zikopoulos, 2012). Machine learning techniques, such as supervised and unsupervised learning, have been employed to develop predictive models for cyberattack detection (Buczak & Guven, 2016).

There is limited research focused specifically on the use of chatbots to detect cyberattacks, and the existing studies also acknowledge that more research is needed to fully explore the potential of chatbots in cyberattack detection. Among these studies, Lee *et al.* (2020) suggested the Integrated Messenger Antivirus System (IMAS), which uses a chatbot service to identify malware attacks that target messengers. The IMAS combines various messenger chatbots into a single adapter, enabling it to support any messaging platform. It also includes multiple anti-virus scanners for detecting malware, allowing users to check detection outcomes. The researchers implemented a real-world environment based on the proposed design of the IMAS and demonstrated the detection of suspected malware using various Messenger chatbots. The paper proposes the IMAS, which includes a chatbot webhook adapter that manages the webhook APIs of the chatbot service offered by a messenger, a multi-antivirus scanner that recognises malicious files, and a broker server that acts as a mediator for message delivery. In the design, if a user suspects a URL or file is malicious and sends it to the messenger's chatbot, the messenger server will redirect the message to the IMAS's chatbot handler callback URL, which is registered in the webhook. The chatbot handler will then receive the message, parse it to extract the URL or file, and save it in storage if it is found to have been dropped from the URL or uploaded by the user. The chatbot handler will then send an analysis request message to the message queue broker server via the producer client. The message will be sent to the multi-antivirus scanner's consumer client for inspection, and the scanner will save the result in the database. The multi-antivirus scanner will then send the analysis result via its producer client to the chatbot handler that sent the request. Finally, the chatbot handler will send a response message to the user via the chatbot.

Another source of research is the work of (Yoo & Cho, 2022). The study defined and formalised Social Network Service (SNS) phishing attack phases based on the existing social engineering attack cycle into 4 different phases to design an Intelligent Chatbot Security Assistant (ICSA) that can detect the phase of SNS phishing attacks in a social media chat room. It defends against the attacks by using text-based CNN-based attack phase classifiers and AI chatbot technology. The ICSA counters the attack and provides victims with appropriate defence suggestions in the form of alerts, information, and defence actions, depending on the detected attack phase. It does this based on defence procedures predefined by security experts. This ICSA was implemented on a Telegram messenger (as a Telegram chatbot) by using Google Dialogflow and an AWS (Amazon Web Services) server. The researchers validated that their Telegram chatbot functions properly in real-time against SNS phishing attacks by conducting extensive experiments. Additionally, they compared two ML models (Text-CNN and LSTM) in terms of training and made a test of accuracy to explain why they chose Text-CNN to generate attack phase classifiers.

The simplified working steps of ICSA (Assistant Bot) against SNS phishing attacks are:

Step 1: Conversation Collection

ICSA (Assistant Bot) collects every conversation (chat sentence) between the attacker and the victim. This data serves as the input for subsequent analysis and detection.

Step 2: Attack Phase Detection

Using SNS Phishing Attack Phase Classifiers (SPAPC), which are generated using a text-CNN machine learning model, ICSA analyses each chat sentence to determine the current attack phase (Phase 1–Phase 3). These phases represent different stages of the phishing attack.

Step 3: Victim Alert and Assistance

Based on the detected attack phase, ICSA initiates a private chatroom with the victim. This chatroom serves as a secure and confidential space for communication between ICSA and the victim. Within the private chatroom, ICSA provides appropriate alerts and suggests defence actions to the victim.

These suggestions are tailored to the specific attack phase detected and aim to help the victim mitigate the impact of the phishing attack.

By following these steps, ICSA aims to effectively detect SNS phishing attacks in real-time through actively monitoring conversations, classify the attack phase, and provide personalised alerts and defence recommendations to the victim in a secure and private environment. ICSA (Assistant Bot) classifies the attack phase and intervenes to support the victim in mitigating the phishing attack.

For the Telegram chatbot to comprehend and identify a current attack stage, it requires an SNS phishing attack phase classifier (SPAPC). To achieve this, they begin by creating the SPAC using the Text-CNN machine learning model and then proceed to build the TC using

the Finite State Machine model and integrate it with the SPAC. Initially, a dataset was created for the purpose of training and testing the Text-CNN machine learning model. However, since no existing dataset was available for SNS phishing attacks, the authors gathered attack sentences from various articles on the internet and classified them into three attack phase datasets. This resulted in the creation of 100 attack sentences and 150 non-attack sentences for each attack phase, with the non-attack sentences being generated from SNS conversations between the authors and their acquaintances. To create the attack phase classifiers, the authors trained the Text-CNN model using the pre-processed collected sentences, which were processed using the Tokenizer, Text_to_sequence, and Pad_sequence functions of Tensorflow. The Text-CNN model structure was designed using Python 3.8.5, Tensorflow 2.4.0, Pandas 1.1.3, and Numpy 1.19.2, and the CNN model used for learning was based on Word2Vec. The Text-CNN structure consisted of one convolution layer, one max-pooling layer to prevent overfitting, and one fully connected layer, with normalisation being performed by applying dropout to prevent co-adaptation, as proposed in the study by (Kim, 2014).

Limitations and Challenges of Chatbots in Cybersecurity

Despite the advancements in chatbot technologies, there are still limitations and challenges, such as ensuring data privacy and addressing potential biases in AI models (Chowdhury, 2003; Gebru *et al.*, 2018). It is also logical to hypothesise that because chatbot relies heavily on AI tools for its use in cybersecurity, the current limitations and challenges of these AI tools will also apply to chatbot. Addressing these limitations will require further research and development, as well as collaboration between researchers, developers, and policymakers, to ensure that chatbots are designed and deployed responsibly. Some are:

Language Understanding

A primary limitation of chatbots is their imperfect understanding of natural human language. While NLP techniques have significantly improved over the years, chatbots still struggle with understanding context, sarcasm, and idiomatic expressions (Caldarini *et al.*, 2022). Ambiguity in language also poses challenges, as chatbots might interpret user queries differently from their intended meaning (Bender *et al.*, 2021). Furthermore, chatbots may generate responses that are lexically and syntactically correct but lack coherence or relevance to the user's query (Radziwill & Benton, 2017).

Domain Specificity

Chatbots are typically designed to be either domain-specific or domain-general. Domain-specific chatbots excel in a particular subject area but may struggle outside of their expertise, while domain-general chatbots are designed to handle a broader range of topics but may not be as proficient in any one area (Yang *et al.*, 2020). Striking the right balance between these two approaches is a challenge, as creating a chatbot that can handle a wide range of topics with high proficiency remains a difficult task (Gao *et al.*, 2019).

Ethical Considerations

As chatbots become more prevalent, ethical concerns have been raised about their use and potential impact on society. Issues such as privacy, data security, and accountability are of increasing importance (Cath *et al.*, 2017). Ensuring that chatbots are designed and deployed ethically is crucial to mitigating these potential risks (Floridi & Cowls, 2021).

Limited Understanding of Context

According to a study by Deterding *et al.* (2011), chatbots often struggle to understand the context of a conversation, which can lead to misunderstandings and errors. The authors note that chatbots may need to be trained on a specific domain or topic to improve their understanding of context.

Limited Emotional Intelligence

According to a study by Adam *et al.* (2021), chatbots lack the emotional intelligence of humans. This limited ability to recognise and respond to human emotions can make them less effective in certain situations, like when responding to a victim of a cyberattack. Users often expect chatbots to understand and react to their emotions, which can influence their overall satisfaction. However, current chatbot technologies struggle to accurately detect emotions from text-based inputs, and even when they do, generating appropriate responses remains a challenge (Cambria *et al.*, 2020). Chatbots may need to be programmed with empathy and emotional support capabilities to improve their effectiveness. Another limitation of chatbots is that they are limited.

METHODOLOGY

The research method for this study systematically and structurally examines the role and potential of chatbots in cybersecurity. The research was divided into distinct stages, each focusing on a different aspect of the study.

Stage I: Literature Review

The research began with a comprehensive literature review, scouring various academic sources, research papers, and databases to find relevant works on chatbots in cybersecurity. With the knowledge gathered from relevant works that have explored the use of chatbots in cybersecurity and their role in detecting cyberattacks, information on the benefits, limitations, and potential applications of chatbots in the cybersecurity domain was obtained. The aim was to identify the current understanding of chatbot technology in the cybersecurity domain. We focused on works that investigated the use of chatbots in this context. This stage was crucial in

setting the foundation for the study and understanding the existing body of knowledge.

Stage II: Focused Research

After the preliminary literature review, the research was narrowed down to the works that directly answered the research questions: how are chatbots used for cybersecurity, and how effective are they in detecting cyberattacks? The research at this stage involved an in-depth review of these works, with an understanding of the methodologies used, the results obtained, and the conclusions drawn.

Stage III: Case Study Analysis

A specific study on the use of chatbots in real-time phishing attack detection in a social network service (SNS) chat room was selected for a detailed analysis. This work was thoroughly studied to understand its methodology, findings, and implications. The purpose of this stage was to gain a detailed understanding of the practical application of chatbots in cybersecurity and a deep comprehension of chatbots' potential in addressing specific cybersecurity challenges.

Stage IV: Use Case Development

Building on the case study analysis, a use case was proposed for the implementation of the studied chatbot model on WhatsApp. The challenges of implementing this model, such as user privacy issues and dealing with false positives and negatives, were highlighted. Furthermore, improvements were proposed for the model to tackle these challenges. This stage aimed to provide practical insights into the application of chatbots in real-world cybersecurity scenarios.

Stage V: Conclusion

The research was concluded by summarising the findings and insights gained through the literature review, focused research, case study analysis, and use case development. The conclusion aimed to answer the research questions and provide a comprehensive understanding of the role and potential of chatbots in cybersecurity.

Use Case

Chatbot for Real-Time Phishing Attack Detection on WhatsApp

Based on the design of the Intelligent Chatbot Security Assistance (ICSA) which was originally implemented on Telegram for real-time phishing defence and is briefly explained in the state-of-the-art.

In this use case, we will be choosing WhatsApp because it is the most used instant messaging app in the world right now, with over 2 billion active users around the globe (Huang & Ling, 2023).

The ICSA's concept, while applicable, necessitates key modifications to cater to the distinct APIs and protocols of Telegram and WhatsApp. For instance, WhatsApp's end-to-end encryption might pose challenges for real-time monitoring, unlike Telegram's more open API. Hence, the direct integration is admittedly infeasible without appropriate modifications by re-augmenting the existing one by building separate integrations for each platform. This means that there would be a need to develop a specific integration for Telegram and a separate integration for WhatsApp by using platforms and tools available that can help in building chatbots that can work across multiple messaging platforms. For example, using a chatbot development framework like Botpress, Dialogflow (the authors of ICSA used this), or IBM Watson Assistant to build a chatbot that can be deployed on both Telegram and WhatsApp.

Another option is to use a third-party service that provides cross-platform chatbot integration by following these steps:

i. A WhatsApp API client would be selected. Initially, a WhatsApp API client has to be chosen to integrate the chatbot, as previously highlighted. Popular options include the WhatsApp Business API and the Twilio API for WhatsApp. Each API client has its own requirements and documentation that must be familiarised with.

ii. WhatsApp chatbot creation: There would be a need for the chatbot's code to be modified to make it compatible with the selected WhatsApp API client. This could involve rewriting or restructuring certain sections of the code to meet the API's requirements.

iii. Webhooks set up: Webhooks are necessary for receiving and processing incoming messages from WhatsApp. A webhook endpoint must be created on the server that listens for incoming messages, processes them, and sends the appropriate responses using the WhatsApp API client.

iv. Testing stage: Once the chatbot is ready, it will be thoroughly tested to ensure that it performs as expected on WhatsApp. To ensure it will effectively handle user messages, provide accurate responses, and comply with WhatsApp's rules and regulations.

V. The chatbot would then be deployed and monitored. Finally, the chatbot can be deployed, and its performance can be monitored while any necessary adjustments are made. Any issues that arise, such as scaling, security, and compliance with WhatsApp's policies, should be addressed.

Model Challenges

This concept is not perfect because chatbot itself, when used as a cybersecurity tool, presents challenges and has limitations, but specifically for this use case, it is observed that the following challenges would need to be investigated and will require more improvements and research:

False Positives and False Negatives

This could pose a huge challenge for the use of this chatbot as it works by identifying sentences, especially if

an attacker is well aware of its integration. They may use more intent camouflage to deceive the chatbot or even train themselves with multiple accounts to figure out how it works and its sensitive entities in order to manipulate it with mastery.

New Attack Vectors and Complex Attacks
This is also a challenge, as cyber threats don't sleep or rest but evolve constantly.

Integration Challenge
As we briefly saw in the case of trying to implement WhatsApp from Telegram, more challenges will exist in the further integration of various social network services.

User Privacy and Data Security
This can pose a problem for users as this chatbot is designed to work by monitoring all the conversations of users to be able to detect phishing attempts.

Maintenance and Training
There will be a need for constant maintenance of the chatbot to keep it up-to-date with current attack trends.

Proposed Improvement
Continually striving for improvement is a necessity for all models. With improvements, the ICSA model can provide users with a more reliable, accurate, and valuable cybersecurity assistant on the WhatsApp platform. These improvements will ensure that the model remains relevant, effective, and capable of addressing the evolving cybersecurity challenges faced by users. These additions would enhance the security, usability, and efficacy of chatbots as cybersecurity tools, paving the way for more reliable and user-centric solutions in the fight against cyberattacks and threats. For this purpose, we propose some useful improvements that can be adopted in the ICSA design to tackle some of its challenges for better performance.

Enhanced Privacy Measures
It is essential to ensure that chatbots are used in a way that is both effective and safe for users. This enhanced privacy can be built upon two layers of the ICSA structure.

User Experience Focus
To focus on the user experience, one way to address user privacy concerns would be to give users the option to opt out of having their conversations monitored by the chatbot. This would allow users to use the chatbot for cybersecurity purposes without having to worry about their privacy being compromised.

Model Design Focus
The ICSA model can be incorporated with robust privacy protection techniques like end-to-end encryption, data anonymization techniques.
Another ethical measure would be transparent privacy policies that can win user trust and confidence in the chatbot system. Including communication regarding data handling practices to users.

Real-Time Monitoring and Response
Implementing real-time monitoring capabilities in the ICSA model to continuously analyse user conversations and detect potential cyber-attacks as they occur can be valuable. This can involve integrating the chatbot with threat intelligence feeds, security analytics platforms, and automated response systems. This integration can enable ICSA to provide timely and accurate alerts to users, enhance their awareness, and help the chatbot stay up-to-date with the latest threat trends, new attack techniques, and vulnerabilities. Hence, be more capable of immediate action against detected attacks, resulting in better enhancement of the chatbot's proactive defence capabilities against emerging threats.

Evaluation and Validation
Rigorous evaluation and validation of the ICSA model's performance using real-world datasets and scenarios can help the ICSA evolve over time for better productivity. This can be achieved by comparing its accuracy, efficiency, and effectiveness against existing approaches and benchmarks. This evaluation process can help identify areas for further improvement and validate the practicality and reliability of the proposed model.

User-Centric Design and Usability
Enhancing the chatbot's effectiveness and user satisfaction is crucial for the life span of the ICSA. As a translation of its long-term maintenance, focus on user-centric design principles to ensure the ICSA model is intuitive, easy to use, and provides a seamless user experience is a key factor. This can be achieved by conducting user studies and feedback sessions to gather insights on how to improve the chatbot's interface, interaction flow, and overall usability. An implementation, such as the ICSA which relies on users to measure its long-term efficiency, will also require constant feedback to monitor user experience and adapt to evolving threats. Thus, incorporating user feedback into iterative design cycles to continually enhance the model's effectiveness and user satisfaction can greatly improve its efficacy. This can be in form of feedback loop as further explained below.

Iterative Feedback Design for a Security Chatbot
Incorporating an iterative feedback loop mechanism not only refines the chatbot's responses over time but also ensures that the ICSA remains adaptive to evolving user needs and cybersecurity threats. ICSA more advantages.

Table 1: ICSA iterative feedback design

Proposed Feedback	Impact on ICSA	Effect
Immediate User Feedback	After the chatbot makes a decision (e.g., flagging a message as a phishing attempt), an immediate user feedback can prompt the user to confirm or refute its decision. For instance, if a message is flagged as suspicious, the chatbot could ask, "Did I correctly identify this as a phishing attempt? Yes/No/Not sure."	False positive/ negative, user satisfaction
Feedback Collection	Implement a simple interface within the chat platform that allows users to provide feedback easily. This could be as simple as clickable buttons or as complex as a short survey. Save collected response for further use.	Maintenance, model training
Feedback Analysis	Collect and analyze the feedback data to determine common areas where the chatbot might be making incorrect decisions. Use metrics to determine the accuracy, false positive rate, and false negative rate based on user feedback.	Model training, new & complex attacks identification
Feedback data use	Use the feedback data as additional training data for the chatbot's machine learning model. For instance, if a message was incorrectly flagged as phishing, and the user provided feedback indicating the error, this data point can be used to retrain the model to reduce such errors in the future.	Model training, maintenance
Feedback iterative collection	Continuously collect feedback, analyze it, and retrain the model. This iterative process ensures that the chatbot improves over time and adapts to new phishing tactics or user behaviors.	Model training, new attacks
Feedback Incentivization	Encourage users to provide feedback by offering incentives. This could be in the form of recognition, badges, or even tangible rewards. The more feedback the system receives, the better it can become.	User satisfaction
Feedback Transparency	Share with users how their feedback is being used to improve the system. This can build trust and encourage more users to participate in the feedback process.	Privacy concerns, user satisfaction
Handling Conflicting Feedback	There might be instances where feedback from different users' conflicts. Implement mechanisms to handle such scenarios, such as weighing feedback based on user expertise or seeking additional input.	Maintenance, model training
Feedback Storage and Privacy	Ensure that feedback data, especially if linked with user identities, is stored securely. Address any privacy concerns users might have about providing feedback.	Privacy concerns, user satisfaction
Continuous Monitoring	Even after implementing a feedback loop, continuously monitor the system's performance to ensure that it's improving and not introducing new errors.	Model training, maintenance

By collecting feedback from users regarding the chatbot's performance, accuracy, and usability, the system can continuously learn and adapt to user needs and preferences. The feedback loop can be implemented by providing users with an option to rate the chatbot's responses, suggest improvements, or report false positives/false negatives. This feedback in return, can then be used to refine the chatbot's algorithms, enhance its detection capabilities, and address any shortcomings. Regularly analysing and incorporating user feedback will ensure that the chatbot evolves and improves over time, leading to a more reliable and effective cybersecurity tool. The proposed feedback loop is shown in the table above, along with the impact it will have on the ICSA assistant bot as a function and the effect it can have on tackling some of the previously highlighted challenges.

CONCLUSION

This research embarked on an in-depth exploration of the use of AI chatbots in the realm of cybersecurity, providing a comprehensive literature survey and a detailed examination of a specific case study. The study has illuminated the considerable potential that chatbots hold for enhancing cybersecurity measures by leveraging AI and machine learning tools, along with the challenges that must be addressed for their effective implementation. Through the literature review, it was found that AI chatbots are being increasingly used in various aspects of cybersecurity, including their use in IT services, information protection, incident response, and user education and awareness. Thus, making chatbots a tool capable of cyber threat mitigation. The detailed study of a specific model used for real-time phishing attack

detection in a Social Network Service (SNS) chatroom further reinforced this finding, demonstrating the practical efficacy of chatbots in real-world cybersecurity scenarios. However, the research also highlighted some challenges to the implementation of chatbots for cybersecurity, including issues related to user privacy and the potential for false positives and negatives. The case study analysis underscored these challenges, particularly in the context of implementing the studied model on a platform like WhatsApp.

To overcome these challenges, this research proposes some improvements to the ICSA model, like introducing user authorization options and implementing feedback loops. The user authorization option would allow users to control the chatbot's access level to their data, addressing privacy concerns. The feedback loop, on the other hand, would enable continuous model improvement by incorporating user inputs into the model's learning process, enhancing its accuracy, and reducing false positives and negatives.

In light of these findings and proposed improvements, further research is encouraged to refine the ICSA model and other similar chatbot models. Future research could focus on developing more sophisticated mechanisms that can further enhance user privacy. In addition, research could explore how to effectively solve the integration challenges of the ICSA model in other social network services for greater use as well as better ways to incorporate user feedback into the chatbot learning process without compromising user privacy or the model's speed and performance.

This research posits that, with appropriate improvements, AI chatbots could serve as powerful tools for enhancing cybersecurity resilience. The proposed improvements to the Intelligent Chatbot Security Assistant (ICSA) model aim to address the identified challenges and offer a path forward for the development of more effective and reliable chatbot-based cybersecurity systems.

In conclusion, this research delves into the burgeoning field of AI chatbots in cybersecurity. While their potential is evident, challenges like user privacy and false positives necessitate continuous refinement. The proposed feedback loop and enhanced privacy measures aim to address these challenges, paving the way for chatbots to be formidable tools in cybersecurity.

Given the findings and potential improvements identified in this research, the following are some key proposals for future research in the context of chatbots in cybersecurity:

Testing Proposed Improvements

Future studies could empirically test the proposed improvements to the Intelligent Chatbot Security Assistant (ICSA) model. Future research could validate these suggestions through implementation and user testing to validate their effectiveness.

Ethical Research

Considering AI's potential implications in cybersecurity and its sensitive nature, studies could explore the ethical aspects of using chatbots in this field.

User Acceptance and Trust

Research could be conducted to understand user acceptance and trust in chatbots for cybersecurity. This could involve conducting surveys or interviews to gather users' perspectives.

Scalability of Model

Research could explore how the ICSA bot assistant model can be scaled effectively for extensive use in larger networks or platforms.

Multi-Modal Capabilities

Having extended capabilities beyond text-based analysis to include image and voice recognition opens up new avenues for threat detection. Research can investigate techniques to analyse and interpret images or audio content shared by users to identify potential security risks. This can involve leveraging computer vision and audio processing algorithms, integrating with existing image or audio recognition APIs, or developing novel deep learning architectures tailored for cybersecurity applications.

Longitudinal Studies

A longitudinal study could be undertaken to assess the effectiveness of chatbots in real-world cybersecurity applications over an extended period of time.

These proposals could help to advance our understanding of the use of chatbots in cybersecurity and contribute to their effective development and implementation for enhanced cyber defence. By delving deeper into these research areas, we can make chatbots in cybersecurity more intelligent, transparent, and privacy-respecting. These advancements will contribute to the development of trustworthy and effective chatbot systems that have a positive impact on cyber resilience strategies.

REFERENCES

AÇAR, K. V. (2017). *Webcam Child Prostitution: An Exploration Of Current And Futuristic Methods Of Detection.* https://doi.org/10.5281/ZENODO.495775

Adam, M., Wessel, M., & Benlian, A. (2021). AI-based chatbots in customer service and their effects on user compliance. *Electronic Markets, 31*(2), 427–445. https://doi.org/10.1007/s12525-020-00414-7

Adamopoulou, E., & Moussiades, L. (2020). An Overview of Chatbot Technology. In I. Maglogiannis, L. Iliadis, & E. Pimenidis (Eds.), *Artificial Intelligence Applications and Innovations* (Vol. 584, pp. 373–383). Springer International Publishing. https://doi.org/10.1007/978-3-030-49186-4_31

Akter, S., Hossain, M. A., Sajib, S., Sultana, S., Rahman, M., Vrontis, D., & McCarthy, G. (2023). A framework for AI-powered service innovation capability: Review and agenda for future research. *Technovation, 125,* 102768. https://doi.org/10.1016/j.technovation.2023.102768

Alazzam, B. A., Alkhatib, M., & Shaalan, K. (2023). Artificial Intelligence Chatbots: A Survey of Classical versus Deep Machine Learning Techniques. *Information Sciences Letters, 12*(4), 1217–1233. https://doi.org/10.18576/isl/120437

Anderson, P., Zuo, Z., Yang, L., & Qu, Y. (2019). An intelligent online grooming detection system using AI technologies. In *Proceedings of the 2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)* (pp. 1–6). IEEE. https://doi.org/10.1109/FUZZ-IEEE.2019.8858973

Barry, E. S., Merkebu, J., & Varpio, L. (2022). State-of-the-art literature review methodology: A six-step approach for knowledge synthesis. *Perspectives on Medical Education, 11*(5), 1–8. https://doi.org/10.1007/S40037-022-00725-9

Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the dangers of stochastic parrots: Can language models be too big? In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (pp. 610–623). ACM. https://doi.org/10.1145/3442188.3445922

Brandtzaeg, P. B., & Følstad, A. (2018). Chatbots: Changing user needs and motivations. *Interactions, 25*(5), 38–43. https://doi.org/10.1145/3236669

Brown, T. B., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., Neelakantan, A., Shyam, P., Sastry, G., Askell, A., Agarwal, S., Herbert-Voss, A., Krueger, G., Henighan, T., Child, R., Ramesh, A., Ziegler, D. M., Wu, J., Winter, C., … Amodei, D. (2020). *Language models are few-shot learners* (arXiv:2005.14165). arXiv. http://arxiv.org/abs/2005.14165

Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

Caldarini, G., Jaf, S., & McGarry, K. (2022). A Literature Survey of Recent Advances in Chatbots. *Information, 13*(1), 41. https://doi.org/10.3390/info13010041

Cambria, E., Li, Y., Xing, F. Z., Poria, S., & Kwok, K. (2020). SenticNet 6: Ensemble application of symbolic and subsymbolic AI for sentiment analysis. In *Proceedings of the 29th ACM International Conference on Information & Knowledge Management* (pp. 105–114). ACM. https://doi.org/10.1145/3340531.3412003

Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2017). Artificial intelligence and the 'good society': The US, EU, and UK approach. *Science and Engineering Ethics*. https://doi.org/10.1007/s11948-017-9901-7

Chowdhury, G. G. (2003). Natural language processing. *Annual Review of Information Science and Technology, 37*(1), 51–89. https://doi.org/10.1002/aris.1440370103

Computer and Information Security Handbook. (2017). *Network Security, 2017*(11), 4. https://doi.org/10.1016/S1353-4858(17)30090-9

Dale, R. (2016). The return of the chatbots. *Natural Language Engineering, 22*(5), 811–817. https://doi.org/10.1017/S1351324916000243

Dan, A., Gupta, S., Rakshit, S., & Banerjee, S. (2019). Toward an AI Chatbot-Driven Advanced Digital Locker. In M. Chakraborty, S. Chakrabarti, V. E. Balas, & J. K. Mandal (Eds.), *Proceedings of International Ethical Hacking Conference 2018* (Vol. 811, pp. 37–46). Springer Singapore. https://doi.org/10.1007/978-981-13-1544-2_4

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: Defining 'gamification'. In *Proceedings of the 15th International Academic MindTrek Conference: Envisioning future media environments* (pp. 9–15). ACM. https://doi.org/10.1145/2181037.2181040

Floridi, L., & Cowls, J. (2021). A unified framework of five principles for AI in society. In L. Floridi (Ed.), *Ethics, governance, and policies in artificial intelligence* (Vol. 144, pp. 5–17). Springer International Publishing. https://doi.org/10.1007/978-3-030-81907-1_2

Følstad, A., & Brandtzæg, P. B. (2017). Chatbots and the new world of HCI. *Interactions, 24*(4), 38–42. https://doi.org/10.1145/3085558

Gao, J., Galley, M., & Li, L. (2019). Neural Approaches to Conversational AI. *Foundations and Trends® in Information Retrieval, 13*(2–3), 127–298. https://doi.org/10.1561/1500000074

Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Wallach, H., Daumé, H., & Crawford, K. (2018). *Datasheets for datasets* (arXiv:1803.09010). arXiv. https://doi.org/10.48550/arXiv.1803.09010

Goksel Canbek, N., & Mutlu, M. E. (2016). On the track of Artificial Intelligence: Learning with Intelligent Personal Assistants. *International Journal of Human Sciences, 13*(1), 592. https://doi.org/10.14687/ijhs.v13i1.3549

Gómez Mármol, F., Gil Pérez, M., & Martínez Pérez, G. (2016). I don't trust ICT: Research challenges in cyber security. In S. M. Habib, J. Vassileva, S. Mauw, & M. Mühlhäuser (Eds.), *Trust management X* (Vol. 473, pp. 129–136). Springer International Publishing. https://doi.org/10.1007/978-3-319-41354-9_9

Hamad, S., & Yeferny, T. (2020). *A chatbot for information security* (arXiv:2012.00826). arXiv. http://arxiv.org/abs/2012.00826

Hien, H. T., Cuong, P.-N., Nam, L. N. H., Nhung, H. L. T. K., & Thang, L. D. (2018). Intelligent assistants in higher-education environments: The FIT-EBot, a chatbot for administrative and learning support. In *Proceedings of the Ninth International Symposium on Information and Communication Technology - SoICT 2018* (pp. 69–76). ACM. https://doi.org/10.1145/3287921.3287937

Hoffman, D. L., & Novak, T. P. (2016). *Consumer and Object Experience in the Internet of Things: An Assemblage Theory Approach. SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2840975

Jung, S. (2019). Semantic vector learning for natural

language understanding. *Computer Speech & Language, 56,* 130–145. https://doi.org/10.1016/j.csl.2018.12.008

Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons, 62*(1), 15–25. https://doi.org/10.1016/j.bushor.2018.08.004

Khurana, D., Koli, A., Khatter, K., & Singh, S. (2023). Natural language processing: State of the art, current trends and challenges. *Multimedia Tools and Applications, 82*(3), 3713–3744. https://doi.org/10.1007/s11042-022-13428-4

Kim, Y. (2014). Convolutional neural networks for sentence classification. In *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP)* (pp. 1746–1751). Association for Computational Linguistics. https://doi.org/10.3115/v1/D14-1181

Kowalski, S., Pavlovska, K., & Goldstein, M. (2013). Two Case Studies in Using Chatbots for Security Training. In R. C. Dodge & L. Futcher (Eds.), *Information Assurance and Security Education and Training* (Vol. 406, pp. 265–272). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-39377-8_31

Langner, B., Vogel, S., & Black, A. W. (2010). Evaluating a dialog language generation system: Comparing the Mountain system to other NLG approaches. In *Proceedings of Interspeech 2010* (pp. 1109–1112). International Speech Communication Association. https://doi.org/10.21437/Interspeech.2010-353

Lee, S., Lee, J., Lee, W., Lee, S., Kim, S., & Kim, E. T. (2020). Design of integrated messenger anti-virus system using chatbot service. In *Proceedings of the 2020 International Conference on Information and Communication Technology Convergence (ICTC)* (pp. 1613–1615). IEEE. https://doi.org/10.1109/ICTC49870.2020.9289514

Lin, L., D'Haro, L. F., & Banchs, R. (2016). A web-based platform for collection of human-chatbot interactions. In *Proceedings of the Fourth International Conference on Human-Agent Interaction* (pp. 363–366). ACM. https://doi.org/10.1145/2974804.2980500

McShane, M. (2017). Natural Language Understanding (NLU, not NLP) in Cognitive Systems. *AI Magazine, 38*(4), 43–56. https://doi.org/10.1609/aimag.v38i4.2745

McTear, M., Callejas, Z., & Griol, D. (2016). *The conversational interface.* Springer International Publishing. https://doi.org/10.1007/978-3-319-32967-3

Perera, R., & Nand, P. (2017). Recent Advances in Natural Language Generation: A Survey and Classification of the Empirical Literature. *Computing and Informatics, 36*(1), 1–32. https://doi.org/10.4149/cai_2017_1_1

Pfleeger, C. P., & Pfleeger, S. L. (2012). *Analyzing computer security: A threat* (2nd ed., intern. ed). Pearson Education International.

Radziwill, N. M., & Benton, M. C. (2017). *Evaluating quality of chatbots and intelligent conversational agents* (arXiv:1704.04579). arXiv. http://arxiv.org/abs/1704.04579

Ramesh, K., Ravishankaran, S., Joshi, A., & Chandrasekaran, K. (2017). A survey of design techniques for conversational agents. In S. Kaushik, D. Gupta, L. Kharb, & D. Chahal (Eds.), *Information, communication and computing technology* (Vol. 750, pp. 336–350). Springer Singapore. https://doi.org/10.1007/978-981-10-6544-6_31

Sabbagh, B. A., Ameen, M., Watterstam, T., & Kowalski, S. (2012). A prototype for HI2Ping information security culture and awareness training. In *Proceedings of the 2012 International Conference on E-Learning and E-Technologies in Education (ICEEE)* (pp. 32–36). IEEE. https://doi.org/10.1109/ICeLeTE.2012.6333397

Verspoor, K., Cohen, K. B., Lanfranchi, A., Warner, C., Johnson, H. L., Roeder, C., Choi, J. D., Funk, C., Malenkiy, Y., Eckert, M., Xue, N., Baumgartner, W. A., Bada, M., Palmer, M., & Hunter, L. E. (2012). A corpus of full-text journal articles is a robust evaluation tool for revealing differences in performance of biomedical natural language processing tools. *BMC Bioinformatics, 13*(1), 207. https://doi.org/10.1186/1471-2105-13-207

Yang, Z., Dai, Z., Yang, Y., Carbonell, J., Salakhutdinov, R., & Le, Q. V. (2020). *XLNet: Generalized autoregressive pretraining for language understanding* (arXiv:1906.08237). arXiv. http://arxiv.org/abs/1906.08237

Yoo, J., & Cho, Y. (2022). ICSA: Intelligent chatbot security assistant using Text-CNN and multi-phase real-time defense against SNS phishing attacks. *Expert Systems with Applications, 207,* 117893. https://doi.org/10.1016/j.eswa.2022.117893

Zambrano, P., Sanchez, M., Torres, J., & Fuertes, W. (2017). BotHook: An option against cyberpedophilia. In *Proceedings of the 2017 1st Cyber Security in Networking Conference (CSNet)* (pp. 1–3). IEEE. https://doi.org/10.1109/CSNET.2017.8241994

Zikopoulos, P. (Ed.). (2012). *Understanding big data: Analytics for enterprise class Hadoop and streaming data; Learn how IBM hardens Hadoop for enterprise-class scalability and reliability, gain insight into IBM's unique in-motion and at-rest Big Data analytics platform, learn tips and tricks for Big Data use cases and solutions, get a quick Hadoop primer.* McGraw-Hill.

Zimba, A., Chen, H., Wang, Z., & Chishimba, M. (2020). Modeling and detection of the multi-stages of Advanced Persistent Threats attacks based on semi-supervised learning and complex networks characteristics. *Future Generation Computer Systems, 106,* 501–517. https://doi.org/10.1016/j.future.2020.01.032