applied sciences

MDPI

Systematic Review

A Systematic Literature Review of Information Security in Chatbots

Jing Yang [1], Yen-Lin Chen [2,*], Lip Yee Por [1,*] and Chin Soon Ku [3,*]

[1] Department of Computer System and Technology, Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur 50603, Malaysia
[2] Department of Computer Science and Information Engineering, National Taipei University of Technology, Taipei 106344, Taiwan
[3] Department of Computer Science, Universiti Tunku Abdul Rahman, Kampar 31900, Malaysia
* Correspondence: ylchen@mail.ntut.edu.tw (Y.-L.C.); porlip@um.edu.my (L.Y.P.); kucs@utar.edu.my (C.S.K.)

Abstract: Chatbots have become increasingly popular in recent years, but they also present security risks and vulnerabilities that need to be addressed. This systematic literature review examines the existing research relating to information security in chatbots, identifying the potential threats, proposed solutions, and future directions for research. The review finds that chatbots face various security threats, including malicious input, user profiling, contextual attacks, and data breaches, and that solutions such as blockchain technology, end-to-end encryption, and organizational controls can be used to mitigate these concerns. The review also highlights the importance of maintaining user trust and addressing privacy concerns for the successful adoption and continued use of chatbots. A taxonomy developed in this review provides a useful framework for categorizing the articles and their findings. The review concludes by identifying future research directions that include developing more sophisticated authentication and authorization mechanisms, exploring the use of privacy-enhancing technologies, and improving the detection and prevention of security threats, among others. This review contributes to the growing body of literature on information security in chatbots and can guide future research and practice in this field.

Keywords: chatbot; information security; systematic literature review (SLR); ChatGPT; security

check for updates

Citation: Yang, J.; Chen, Y.-L.; Por, L.Y.; Ku, C.S. A Systematic Literature Review of Information Security in Chatbots. *Appl. Sci.* **2023**, *13*, 6355. https://doi.org/10.3390/app13116355

Academic Editor: Luis Javier García Villalba

Received: 6 March 2023
Revised: 17 April 2023
Accepted: 20 April 2023
Published: 23 May 2023

1. Introduction

Chatbots are also known as conversational agents [1]. They are computer programs designed to simulate human conversation through artificial intelligence, natural language processing, and machine learning technologies [2]. The rise of chatbots has brought new levels of convenience and efficiency to a wide range of industries and applications, from e-commerce and healthcare to finance and education. However, as these systems become more ubiquitous, they also become more vulnerable to a range of security threats and attacks, raising concerns about the safety and privacy of users' sensitive data [3].

Recently, information security has actually received increasing attention [4,5]. One of the major challenges of information security in chatbots is the protection of users' sensitive data [6–11]. As chatbots become more widely used across various industries and applications, the amount of personal information being shared through them is increasing, including financial data, health information, and personally identifiable information. This makes them an attractive target for cybercriminals, who may try to exploit vulnerabilities in chatbots to gain unauthorized access to user data.

For example, if a healthcare chatbot is compromised, an attacker may gain access to sensitive patient data such as medical histories, prescriptions, and other personal information. Similarly, if a finance chatbot is breached [12,13], an attacker may gain access to users' financial data, such as credit card numbers, bank account details, and transaction histories.Another important aspect of information security in chatbots is the need to maintain user trust and confidence in these systems [6–9,14–18]. Users must feel confident that their personal information is secure and protected when using chatbots. A security breach or data leak can erode user trust, which can have significant consequences for businesses and organizations that use chatbots to provide services and support.

For example, the companies set hidden rules in the website's terms and conditions and disclaimers to get user consent to use their data. In this case, the companies can store personal data legally. However, the user might not be aware that their data is disclosed to third parties [19,20].

In addition, an aspect to take into special consideration for user trust is that older adults seem to differ from younger adults when choosing a chatbot for customer service versus connecting to a live agent [21,22]. Older adults may still value the human touch more, which would mean that relying on chatbot communication solely or predominantly can alienate older consumers, whereas they constitute such a large share of the population [23].

In terms of research challenges, one of the major challenges is the evolving nature of security threats and vulnerabilities [6–10,16]. As chatbots become more intelligent and capable, new types of attacks may emerge that exploit previously unknown vulnerabilities. This requires ongoing research and development to identify and mitigate emerging threats. For example, GPT-4 (which surpasses ChatGPT) was trained on Microsoft Azure AI supercomputers. It uses a deep learning approach that leverages more data and more computation to create increasingly sophisticated and capable language models [24]. It needs to be trained on large datasets of respective domain information (such as patient information and user conversation information) to predict outcomes [25]. However, a chatbot cannot train on encrypted data. Therefore, there is a risk of the disclosure of data to third parties when decrypting data for training purposes.

Additionally, the development of secure chatbots requires a multidisciplinary approach that encompasses not only technical security measures but also user trust, privacy, and ethical considerations [6–9,14–17]. Developers must consider the potential impact of chatbots on society and ensure that chatbots are designed and deployed in an ethical and responsible manner [26]. This can be a challenging task that requires collaboration between security experts, developers, policymakers, and users.

Furthermore, the diversity of chatbot contexts and scenarios presents unique security challenges that require tailored solutions. For example, a chatbot used in healthcare may require different security measures than one used in finance or e-commerce [27–29]. This requires a nuanced approach to security that takes into account the specific needs and requirements of each use case.Overall, the importance of information security for chatbots cannot be overstated. The protection of user data and the maintenance of user trust are critical factors in the success and widespread adoption of chatbots. To address these challenges, we conducted a systematic literature review to identify and analyze studies focused on the security of chatbots. The goal of this review was to provide a comprehensive analysis of the major security threats and vulnerabilities faced by chatbots and to highlight the strategies and technologies that can be used to mitigate these risks.

2. Method

Figure 1 shows the literature review methodology used in this study. To ensure a comprehensive and transparent review of the literature, we followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidance in conducting this systematic literature review on chatbots and security.

The PRISMA methodology is a widely recognized and accepted approach for conducting systematic literature reviews (SLRs) [30]. It provides a transparent and reproducible framework for conducting literature searches, screening and selecting relevant articles, and synthesizing the findings.

In the context of a SLR focused on security threats and vulnerabilities in chatbots, the PRISMA methodology was considered an appropriate approach as it helps to ensure a comprehensive and systematic search of the literature and a rigorous process for screening and selecting relevant articles. Additionally, the PRISMA methodology includes a detailed reporting checklist, which can help ensure that the review is reported in a clear and transparent manner.

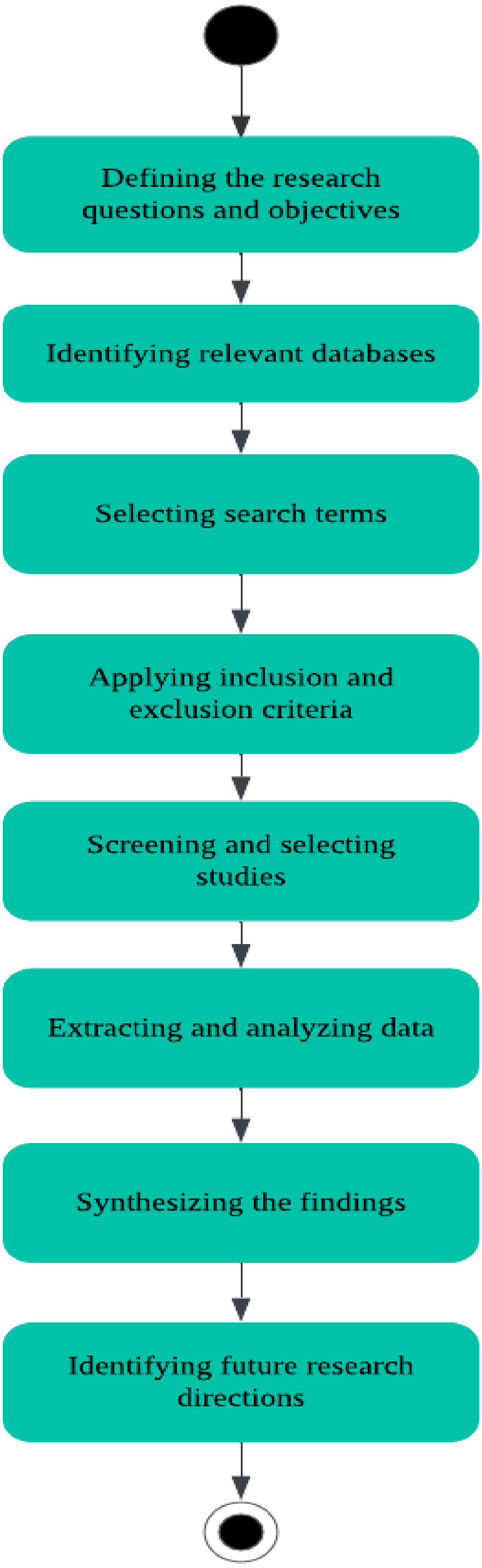
Defining the research questions and objectives
Identifying relevant databases
Selecting search terms
Applying inclusion and exclusion criteria
Screening and selecting studies
Extracting and analyzing data
Synthesizing the findings
Identifying future research directions

Figure 1. Literature review methodology.

Other approaches to conducting SLRs, such as the Cochrane methodology [31], may also be appropriate for certain research questions or topics. However, in the case of this specific SLR, we may have found that the PRISMA methodology was the most suitable based on its emphasis on transparency and reproducibility.

There are 8 sequential steps involved the literature review methodology, and they are as follows:

Step 1. Defining the research questions and objectives: The research questions and objectives were defined to guide the search and analysis of the literature. The research questions and objectives are as follows:

Research Questions:

1. What are the major security threats and vulnerabilities faced by chatbots?
2. What strategies and technologies can be used to mitigate these risks?

Objectives:

1. To provide a comprehensive analysis of the major security threats and vulnerabilities faced by chatbots.
2. To highlight the strategies and technologies that can be used to mitigate these risks.

We believe that the findings of this literature review can guide future research and practice in the field of information security in chatbots.

Step 2: Identifying relevant databases: Several databases, including the ACM Digital Library, IEEE Xplore, ScienceDirect, and Web of Science, were selected to ensure a comprehensive search of the literature.

Step 3. Selecting search terms: The search terms were selected based on the research questions and objectives. The chosen search terms were "chatbot" OR "ChatGPT" AND "security" OR "information security".

Step 4. Applying inclusion and exclusion criteria:

Inclusion Criteria:

We included peer-reviewed research articles that focused specifically on the security of chatbots and were published between 2016 and 2023. Additionally, we only considered studies that were available in full-text format and published in English.

Exclusion Criteria:

We excluded studies not relating to the security of chatbots, such as those that focused on the development, technology, and applications of chatbots, natural language processing, or user experience. Only peer-reviewed research articles were considered for inclusion in this review.

Step 5. Screening and selecting studies: The selected studies were screened based on their relevance to the research questions and objectives. Full-text articles were then reviewed, and studies that did not meet the inclusion criteria or were not relevant to the research questions were excluded.

Step 6. Extracting and analyzing data: Relevant data, such as the research methods used, the types of chatbots examined, and the specific security issues addressed, were extracted from the selected studies. The extracted data were then analyzed to identify common themes, patterns, and gaps in the literature.

Step 7. Synthesizing the findings: The synthesized findings were presented in a narrative format, with tables and figures used to provide visual representations of the data.

Step 8. Identifying future research directions: Based on the analysis of the literature, future research directions were identified and presented in the conclusion section of the paper.

3. Result

Figure 2 shows the PRISMA flow diagram [30] for a systematic review of the security aspects of chatbots. There are three phases involved (identification, screening, and eligibility phases). During the initial identification phase, we retrieved 1193 articles from the electronic database search. After removing duplicates, 179 articles remained. The screening phase involved reviewing the titles and abstracts of the articles, resulting in the exclusion of 62 articles. During the eligibility phase, full-text screening was conducted on the remaining 19 articles, and 10 articles were excluded for not meeting the inclusion criteria.

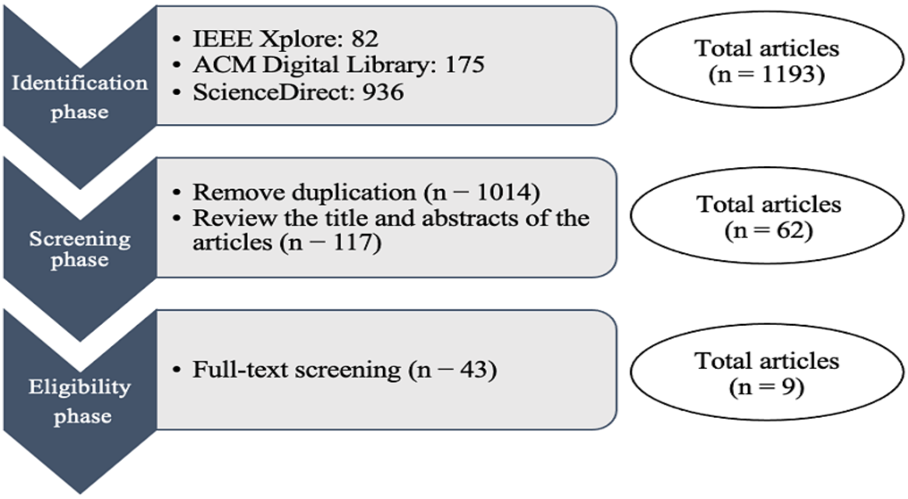
Identification phase
• IEEE Xplore: 82
• ACM Digital Library: 175
• ScienceDirect: 936
Total articles (n = 1193)
Screening phase
• Remove duplication (n – 1014)
• Review the title and abstracts of the articles (n – 117)
Total articles (n = 62)
Eligibility phase
• Full-text screening (n – 43)
Total articles (n = 9)

Figure 2. PRISMA flow diagram [30] for systematic review of security aspects of chatbots.

The nine articles that met the inclusion criteria were analyzed and synthesized to provide an overview of the major security threats and vulnerabilities associated with chatbots and the approaches that have been proposed to address them. The following presents the results of our systematic literature review.

Figure 3 shows the articles and their corresponding fields relating to information security. From the systematic literature review, we have identified several articles related to security threats and vulnerabilities in chatbots. Specifically, five articles [6–8,10,16] were found to be related to security threats and vulnerabilities in chatbots. These articles discussed potential attacks that could compromise the security of chatbots, such as malicious input, user profiling, contextual attacks, and data breaches. The articles emphasized the importance of developers being aware of these potential vulnerabilities and taking measures to secure their systems against attacks.

The review also identified seven articles [6–10,14,16] relating to approaches proposed to address chatbot security threats and vulnerabilities. These articles proposed various solutions to mitigate security concerns relating to chatbots, such as the use of blockchain technology, the implementation of end-to-end encryption, and the provision of organizational, managerial, and technical controls in the service level agreement.

The review identified one article [17] relating to determinants of continuance intention in the domain of AI assistants with a focus on information security. This article emphasized the importance of maintaining user trust and addressing privacy concerns in order to ensure the successful adoption and continued use of AI assistants.

Additionally, one article [14] discussed the importance of raising cyber threat awareness and improving the cyber security of companies. It proposed an AI-based conversational bot that acts as a personal assistant to enhance cyber threat awareness and deliver the latest information and training to the employees of a company.

Article [15] discussed security risks and ethical problems relating to information security in chatbot implementation. It emphasized that human behavior provides neural networks with examples of both appropriate and inappropriate behavior and proposed a mechanism for detecting socio-cultural and information security threats by monitoring the interests and motivations of users, specialists, and programmers.

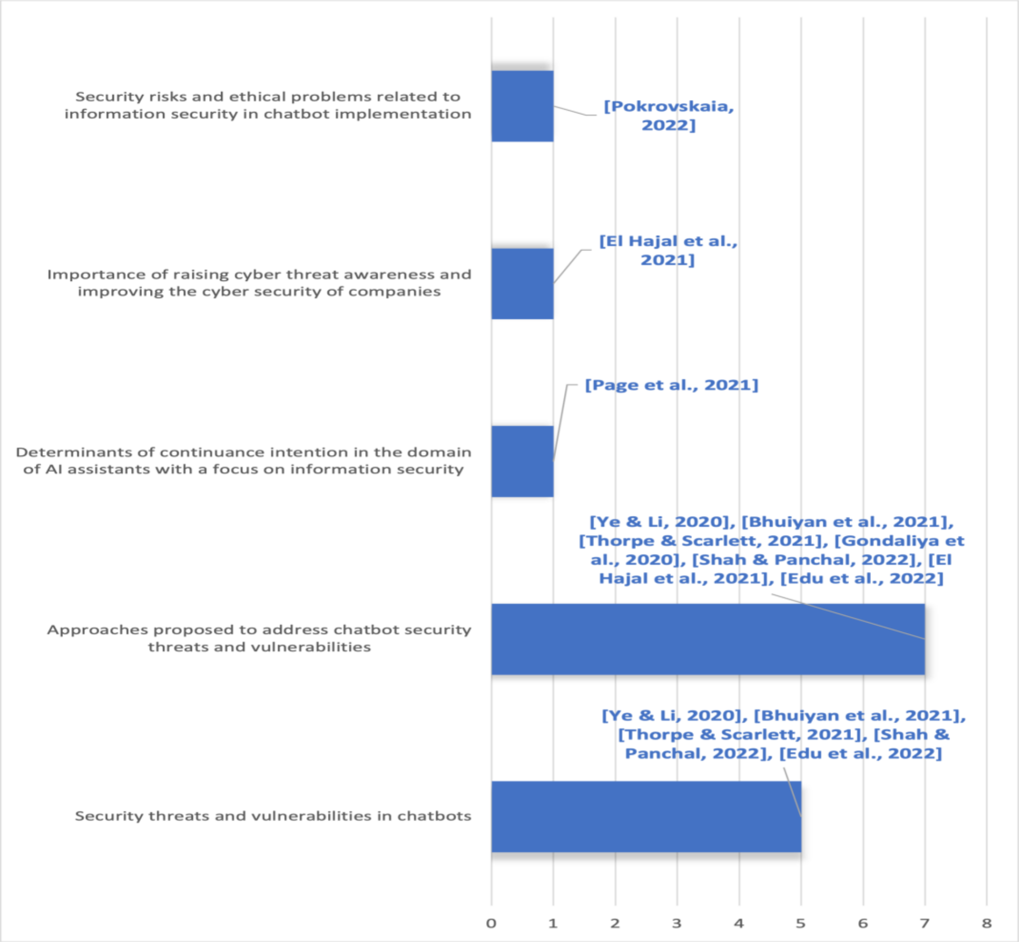

Figure 3. Articles and their corresponding fields relating to information security [6–10,14–16,30].

Table 1 shows the finding and their related articles. Article [6] focuses on the security and privacy vulnerabilities in the chatbot. The article highlights the potential vulnerabilities that could compromise the security of the system and the privacy of the user. These include malicious input, user profiling, contextual attacks, and data breaches. Attackers could insert malicious input into the chatbot, such as SQL injection or cross-site scripting, to exploit vulnerabilities in the system. Chatbots could collect sensitive information about the user, such as personal data or behavioral patterns, which could be exploited by attackers for identity theft or targeted attacks. Attackers could exploit the context of the conversation to manipulate the user or the chatbot, for example, by impersonating the chatbot or deceiving the user into revealing sensitive information. Chatbots could be vulnerable to data breaches, where the user data or chatbot data are exposed to unauthorized parties. The article suggests that developers should be aware of these potential vulnerabilities and take measures to secure their systems against attacks. Despite the great potential of chatbots for many applications, it is important to address these vulnerabilities to ensure the security and privacy of users.

Article [7] discusses some of the vulnerabilities identified in chatbots, which include insecure authentication, data integrity issues, system availability, transparency, and privacy concerns. These vulnerabilities can potentially be exploited by attackers to compromise the security of a chatbot, gain unauthorized access to sensitive information, or disrupt the chatbot's operations. The paper proposes the use of blockchain technology to mitigate some of these security concerns in financial chatbots. However, chatbot vulnerabilities may vary depending on the specific implementation and context, and other studies may identify additional or different types of vulnerabilities.

Table 1. Finding and their related articles.

Findings	Related Articles
Chatbot vulnerabilities exist in various modules	[6,7]
Chatbots can collect sensitive information	[6]
Attackers can exploit the context of the conversation	[6]
Chatbots could be vulnerable to data breaches	[6]
The use of end-to-end encryption in chatbots enhances security	[10]
Trust and concerns about the surroundings are major determinants of continuance intention in using AI assistants	[17]
A comprehensive security analysis of chatbots is important	[6–9,16]
Raising cyber threat awareness among employees is important	[14]
Machine learning procedures can ensure etiquette and data protection	[15]
Static and dynamic analysis can assess security and privacy issues in messaging platform chatbots	[16]

The vulnerabilities in chatbots are not explicitly discussed in article [8]. The paper proposes a design and framework for a cyber-aware chatbot service that detects and helps prevent malware behavior from spreading on the user's machine. The malicious behavior modeled in the paper is based on the vulnerabilities observed within the Open Web Application Security Project (OWASP) top ten, which outlines the security vulnerabilities of the Web. However, the paper does not discuss vulnerabilities specific to chatbots.

Article [9] highlights the potential risks associated with chatbots, including risks relating to the confidentiality and integrity of user data, the reliability of chatbot responses, and risks relating to the service level agreement (SLA) provided by chatbot providers. The proposed checklist provides security managers with a tool to assess these risks prior to chatbot implementation. The paper also proposes a set of controls that can be provisioned in the SLA to manage these risks, such as organizational, managerial, and technical controls, and provides examples of how these controls can address specific risk factors, such as DDoS attacks on third-party infrastructure. The proposed analysis allows customers to be informed about the risks associated with the service before signing an SLA with a chatbot provider.

Article [10] highlights the security issues in chatbots, which could provide opportunities for information flowing through the chatbot interface to be accessed by cybercriminals or hackers. As a result, the authors propose a solution to make chatbots secure by utilizing authentication (session) timeouts in combination with encryption mechanisms, such as the Double Ratchet algorithm modified with Paillier Cryptosystems. The use of end-to-end encryption in the proposed chatbot ensures that only the intended recipients can decrypt messages, thus protecting an organization's valuable data. The primary goal of a secure educational chatbot is to protect students' data from cyber-criminals, hackers, or attackers, so the conversation is entirely secure using end-to-end encryption (E2EE), thus maintaining data privacy, confidentiality, integrity, and authentication.

Article [14] discusses the importance of raising cyber threat awareness and improving the cyber security of companies by focusing on the weakest link—the human factor layer. The paper proposes an AI-based conversational bot that acts as a personal assistant to enhance cyber threat awareness and deliver the latest information and training to the employees of a company. The bot is designed to communicate with the user through WhatsApp and is capable of maintaining records of each employee, evaluating their progress, and proposing training to reduce weaknesses. The implementation of this bot has shown great impact on the employees, and the bot is able to update its database of any security breach and suggest ways to behave in case of an attack. However, the paper also highlights that cyber security is a constantly evolving field, and there is a need to add new features to the bot to keep up with the latest threats. The paper suggests adding a feature to verify the application of procedures and to inform the IT team immediately in case of a fatal attack. The addition of a voice generation alternative is also proposed to keep the employee focused, and the linkage of the bot to the most up-to-date security webpage and databases is suggested to inform employees and the IT department about new threats.

Article [15] discusses the security risks and ethical problems relating to information security in chatbot implementation. It emphasizes that human behavior provides neural networks with examples of both appropriate and inappropriate behavior, and it proposes a mechanism for detecting socio-cultural and information security threats by monitoring interests and motivations of users, specialists, and programmers. The article identifies key approaches to ensuring etiquette and data protection and proposes procedures for machine learning in relation to chatbots in corporate ecosystems. The article suggests that the society members should conceive a system of cultural transmission, transfer of knowledge, and civic education to foster the clear identity of a national society, and a regional or professional community.

Article [16] discusses the security and privacy issues that arise from the use of chatbots in messaging platforms. It highlights the potential risk that chatbots pose to users, as they could steal information from channels without the victim's awareness. The paper proposes a methodology that incorporates static and dynamic analysis for automatically assessing security and privacy issues in messaging platform chatbots. The research focused on the popular Discord platform and found that 55% of chatbots from a leading Discord repository request the "administrator" permission, which could be a security risk. Additionally, only 4.35% of chatbots with permissions actually provide a privacy policy. These findings suggest that there are significant security and privacy concerns associated with the use of chatbots in messaging platforms that need to be addressed to protect users.

Article [17] investigated the determinants of continuance intention in the domain of AI assistants, with a focus on information security. The results revealed that trust and privacy concerns regarding the surroundings are major antecedents of continuance intention. This suggests that users consider the security of their personal information when using AI assistants and that maintaining trust and privacy are essential factors for the successful adoption and continued use of these technologies.

As a summary, the articles reviewed address various types of chatbots and security threats, including malicious chatbots, unsecured communication channels, authentication and authorization, data privacy, and social engineering. The studies also proposed various approaches to address these threats, such as utilizing end-to-end encryption, incorporating static and dynamic analysis, and implementing organizational, managerial, and technical controls. The determinants of continuance intention in the domain of AI assistants were also explored, with a focus on information security.

Table 2 summarizes the research methods used, types of chatbots examined, specific security issues addressed, and related articles for nine studies relating to chatbot security. The studies employed various research methods, including case studies, surveys, and experimental studies, and examined different types of chatbots, such as financial chatbots, educational chatbots, and messaging platform chatbots. The specific security issues addressed in the studies include malicious chatbots, unsecured communication channels, authentication and authorization, data privacy, social engineering, and user trust and privacy concerns. The related articles provide further insights into the importance of maintaining user trust, addressing privacy concerns, and improving cyber threat awareness and security. Overall, the table provides a comprehensive overview of the major security threats and vulnerabilities associated with chatbots and the approaches proposed to address them.

Table 2. Overview of research methods, chatbot types, and security issues addressed in the chatbot security literature review.

Study	Research Methods	Chatbot Types	Specific Security Issues Addressed
[6]	Comprehensive analysis	N/A	Malicious input, user profiling, contextual attacks, and data breaches
[7]	Analysis and proposal	Financial chatbots	Insecure authentication, data integrity, system availability, transparency, and privacy concerns
[8]	Proposal and modeling	Malware-detecting chatbots	Open Web Application Security Project (OWASP) top ten vulnerabilities
[9]	Proposal and case studies	N/A	Confidentiality and integrity of user data, reliability of chatbot responses, and risks relating to SLA
[10]	Proposal and testing	Educational chatbots	Information exposure, data privacy, confidentiality, integrity, and authentication
[14]	Proposal and implementation	Conversational bot	Cyber threat awareness, employee training, and security breach verification
[15]	Proposal and case studies	Corporate chatbots	Socio-cultural and information security threats, and machine learning procedures
[16]	Proposal and testing	Messaging platform chatbots	User information theft, administrator permission requests, and privacy policy provision
[17]	Survey and analysis	AI assistants	Trust and privacy concerns

Note: N/A means the study did not focus on a specific type of chatbot.

4. Taxonomy

Table 3 summarizes the common themes and patterns identified across the literature on chatbot security. The literature highlights the importance of identifying security threats and vulnerabilities in chatbots and implementing approaches to address them. There is also an emphasis on the importance of maintaining user trust and addressing privacy concerns, as well as the need for improved user education and awareness. The role of AI and machine learning in chatbot security is also highlighted, along with the importance of secure communication channels and encryption. Standardized security measures and regulations are seen as necessary, but there are challenges in evaluating and testing chatbot security. The literature also points to the lack of focus on insider threats and social engineering attacks.

Table 3. Common themes and patterns of the literature.

Common Themes and Patterns	Related Articles
Identification of security threats and vulnerabilities	[6–8,10,16]
Approaches proposed to address chatbot security threats and vulnerabilities	[6–10,14,16]
Importance of maintaining user trust and addressing privacy concerns	[14,15,17]
Need for improved user education and awareness	[7,8,10,14,16]
Role of AI and machine learning in chatbot security	[7,9,15]
Importance of secure communication channels and encryption	[6,8,10,15]
Need for standardized security measures and regulations	[7–9,15]
Challenges in evaluating and testing chatbot security	[8,10,16]
Lack of focus on insider threats and social engineering attacks	[8,16]

Figure 4 depicts the taxonomy of information security in chatbots that we developed based on the information in Table 3. The taxonomy is used to provide a framework for understanding the different aspects of information security in chatbots and to help identify gaps and areas for further research. In general, the common themes and patterns identified across the literature on chatbot security can be classified into four themes: Themes 1: Security threats and vulnerabilities; 2: Solutions to mitigate security concerns; 3: User trust and privacy concerns; and 4: Ethical and socio-cultural issues. Theme 1 covers four aspects, and they are malicious input, user profiling, contextual attacks, and data breaches. Theme 2 covers three aspects: the use of blockchain technology, the implementation of end-to-end encryption, and the provision of organizational, managerial, and technical controls. Theme 3 covers two aspects: maintaining user trust and addressing privacy concerns. Theme 4 also covers two aspects: the impact of human behavior on neural networks and the need for a system of cultural transmission and civic education.

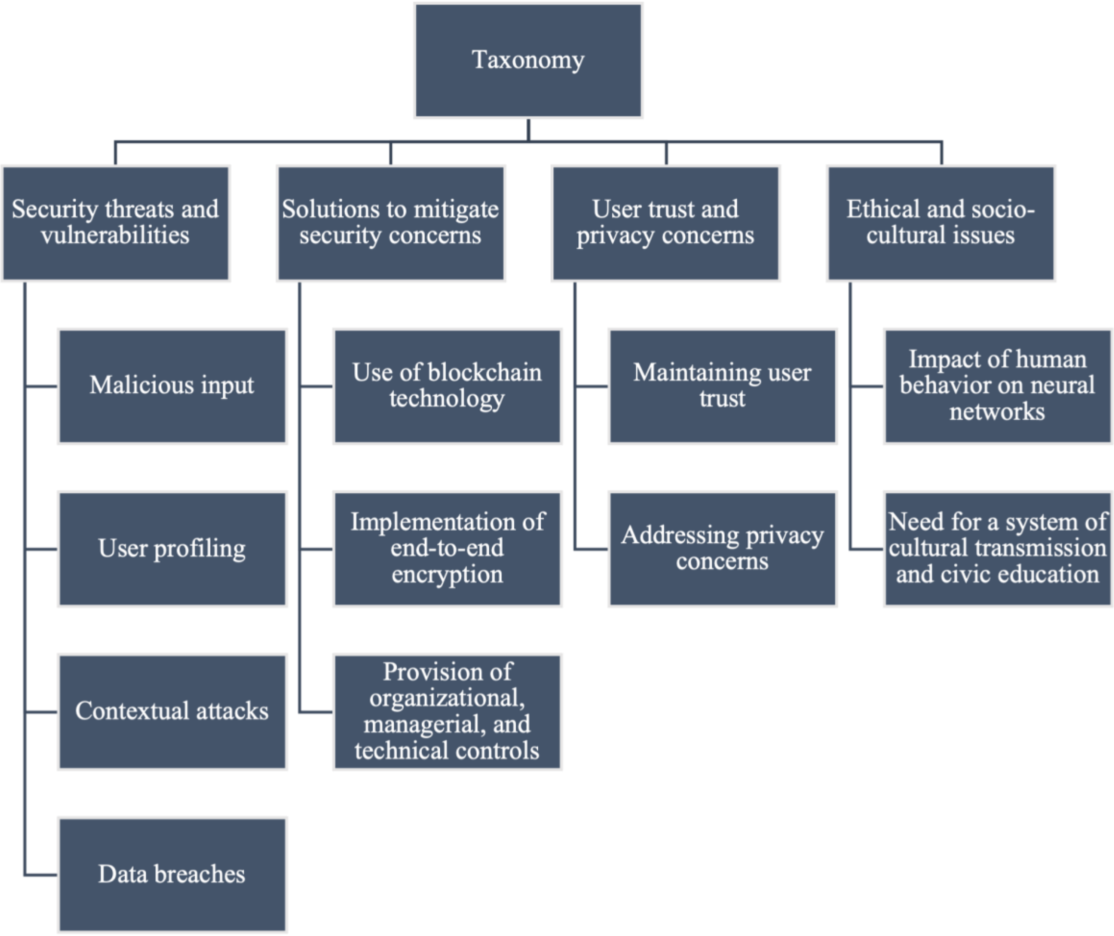
Taxonomy
Security threats and vulnerabilities
Solutions to mitigate security concerns
User trust and privacy concerns
Ethical and socio-cultural issues
Malicious input
User profiling
Contextual attacks
Data breaches
Use of blockchain technology
Implementation of end-to-end encryption
Provision of organizational, managerial, and technical controls
Maintaining user trust
Addressing privacy concerns
Impact of human behavior on neural networks
Need for a system of cultural transmission and civic education

Figure 4. Taxonomy of information security in chatbot.

Theme 1: Security threats and vulnerabilities.

One of the major challenges in addressing security threats and vulnerabilities in chatbots is the constantly evolving nature of cyber threats. New attack vectors and vulnerabilities are being discovered all the time, and developers need to stay up to date with the latest security measures to ensure ongoing protection of their chatbots. For example, the recent rise in phishing attacks using chatbots highlights the importance of implementing measures to prevent malicious input and contextual attacks.

Another challenge is the need to balance security with usability. Chatbots need to provide a user-friendly experience while also ensuring the confidentiality, integrity, and availability of user data. Developers must carefully consider the trade-offs between security measures and user experience and find a balance that meets both requirements. For instance, chatbots in the healthcare industry must comply with strict regulations regarding data privacy and security while also providing timely and accurate medical advice.

Theme 2: Solutions to mitigate security concerns

The lack of standardized security measures for chatbots poses a significant challenge in addressing security concerns. Developers need to determine which security measures to implement, how to implement them, and how to ensure their effectiveness. For example, while end-to-end encryption is a promising solution to protect user data, its implementation may be difficult for small- or medium-sized chatbot providers due to cost constraints.

Another challenge is the need for effective organizational, managerial, and technical controls. Chatbots are often developed and deployed by teams with varying levels of expertise and experience in information security. Developers must ensure that all team members are properly trained in information security and follow best practices to prevent security breaches. Additionally, developers must ensure that their chatbots have appropriate technical controls, such as access control mechanisms and monitoring tools, to detect and respond to security threats in a timely manner.

Theme 3: User trust and privacy concerns

One of the challenges in addressing user trust and privacy concerns is the lack of transparency in chatbot operations. Users may be uncomfortable sharing sensitive information with chatbots if they do not know how their data are being used or who has access to it. Developers must ensure that their chatbots are transparent about how user data are collected, stored, and used. For example, chatbots that collect user data for personalized marketing must provide clear and concise information about how the data are used and allow users to opt out if they choose.

Another challenge is the need to address cultural and regional differences in privacy expectations. Different cultures and regions may have different expectations and norms around data privacy and security. Developers must take these differences into account when designing and implementing chatbots to ensure that they are culturally appropriate and respectful of user privacy.

Theme 4: Ethical and socio-cultural issues

One challenge in addressing ethical and socio-cultural issues in chatbots is the potential for unintended consequences. Chatbots are designed to interact with humans and learn from those interactions, but their ability to do so can also lead to unintended biases and discrimination. For example, chatbots that are trained on biased datasets may unintentionally perpetuate stereotypes or discriminate against certain groups of users.

Another challenge is the need for effective cultural transmission and civic education. Chatbots may interact with users from a variety of cultural and linguistic backgrounds, and developers must ensure that their chatbots are sensitive to these differences. This may involve incorporating cultural sensitivity training into the development process or partnering with local organizations to better understand cultural norms and expectations.

The following are some potential solutions to achieve the security goals outlined in each of the themes:

Security threats and vulnerabilities: To address the potential security threats and vulnerabilities in chatbots, developers can conduct regular security audits and vulnerability assessments, implement appropriate security measures to address any weaknesses, and stay up to date with the latest security threats and vulnerabilities by attending security conferences and training sessions, participating in online forums, and following industry experts on social media.

Regular security audits and vulnerability assessments entail reviewing the chatbot system's security controls and identifying any weaknesses or vulnerabilities that attackers could exploit. To identify and address potential security issues, developers can use a variety of tools and techniques, such as penetration testing and vulnerability scanning. Once vulnerabilities have been identified, proper security measures can be put in place to address them. This could include updating software and firmware to address known security flaws, implementing access controls to limit who has access to sensitive data, and encrypting data in transit and at rest.

Staying up to date with the latest security threats and vulnerabilities is also crucial. Developers can attend security conferences and training sessions to learn about emerging threats and best practices for addressing them. They can also participate in online forums and follow industry experts on social media to stay informed about the latest developments in chatbot security.

Solutions to mitigate security concerns: To mitigate security concerns in chatbots, developers can implement end-to-end encryption to protect user data from unauthorized access, use blockchain technology to enhance data security, and provide organizational, managerial, and technical controls to ensure the confidentiality, integrity, and availability of user data.

End-to-end encryption is an essential security measure that can be implemented in chatbots to protect user data. This encryption method ensures that the data transmitted between the chatbot and the user is secure and cannot be intercepted or accessed by unauthorized third parties. End-to-end encryption provides users with privacy and security, and it can also help to build trust in the chatbot system.

For example, a chatbot used by a financial institution may use end-to-end encryption to protect users' financial information, such as bank account details and transaction history. With end-to-end encryption, the data transmitted between the user and the chatbot is encrypted and can only be decrypted by the user or the chatbot, ensuring that it remains confidential and secure.

Another security measure that can be implemented is the use of blockchain technology. Blockchain is a distributed ledger that can be used to store and share data securely. By leveraging blockchain technology, chatbots can store sensitive data in a decentralized and tamper-proof way, ensuring that it remains secure and cannot be tampered with or altered by unauthorized parties.

For example, a healthcare chatbot may use blockchain to store and share sensitive patient data, such as medical histories and prescriptions, securely. By using blockchain technology, the data can be stored in a decentralized manner, making it more resistant to cyberattacks and ensuring that patient data remain secure and private.

In addition to these technical solutions, developers can also implement organizational, managerial, and technical controls to ensure the confidentiality, integrity, and availability of user data. This includes implementing access controls, conducting regular security assessments, and providing security awareness training for employees and users.

For example, a chatbot used by a government agency may implement access controls to ensure that only authorized personnel can access sensitive data. Regular security assessments can also be conducted to identify vulnerabilities and ensure that the chatbot system remains secure. Finally, security awareness training can be provided to users to help them understand the importance of data security and how to protect their personal information.

User trust and privacy concerns: To address user trust and privacy concerns, developers can maintain transparency and open communication with users regarding the data that are collected and how they are used, obtain explicit consent from users before collecting or processing their data, and implement appropriate security measures to protect user data from unauthorized access or disclosure.

Maintaining user trust and addressing privacy concerns are critical for the successful adoption of chatbots. To achieve this, developers can implement a number of strategies. Firstly, they can ensure that users are fully informed about the data that are collected and how they are used. This can be performed by providing clear and concise privacy policies and terms of service that are easily accessible to users. These policies should explain what data are collected, how they are used, and with whom they are shared.

Secondly, developers can obtain explicit consent from users before collecting or processing their data. This can be achieved through a variety of methods, such as pop-up consent forms, checkboxes, or other interactive mechanisms that clearly explain what data are being collected and why. It is also important for developers to ensure that users have the option to opt out of data collection or processing if they do not wish to share their information.

Thirdly, developers can implement appropriate security measures to protect user data from unauthorized access or disclosure. This can include implementing encryption, access controls, and other technical safeguards to prevent data breaches or leaks. Additionally, developers can ensure that their chatbots comply with relevant data protection laws and regulations, such as the General Data Protection Regulation or the Health Insurance Portability and Accountability Act, and obtain appropriate certifications or third-party audits to demonstrate compliance.

Ethical and socio-cultural issues: To address ethical and socio-cultural issues in chatbots, developers can consider the potential impact of chatbots on society and ensure that chatbots are designed and deployed in an ethical and responsible manner. This could involve developing a system of cultural transmission and civic education to ensure that users understand the potential risks and benefits of chatbots and implementing appropriate safeguards to prevent the use of chatbots for malicious or unethical purposes.

For instance, chatbots may perpetuate biases or stereotypes if they are not programmed to be inclusive and respectful of diversity. Developers need to ensure that chatbots are designed and trained to be culturally sensitive, taking into account the diversity of the users they will interact with. Moreover, chatbots may impact the social dynamics of communication, especially in sensitive areas such as mental health, where chatbots are increasingly being used to provide support and guidance to users. In such cases, developers need to ensure that the chatbots are not replacing human interaction but rather supplementing it, and users are given the option to seek human help if needed.

Developers also need to consider the potential for malicious use of chatbots, such as the spread of disinformation or the manipulation of public opinion. In such cases, appropriate safeguards need to be implemented, such as robust authentication mechanisms and controls to prevent unauthorized access to chatbots.

Overall, it is important for developers to take a holistic approach to chatbot security, considering not only technical security measures but also user trust, privacy, and ethical considerations. By following best practices and staying up to date with the latest security threats and vulnerabilities, developers can ensure that their chatbots provide a secure and user-friendly experience.

5. Discussion

Although the reviewed literature provides a comprehensive overview of the security threats and vulnerabilities associated with chatbots and the approaches proposed to address them, there are still areas where additional research is needed to address specific security issues.

One such area is the need for more research on authentication and authorization mechanisms for chatbots. Article [7] highlights the vulnerability of chatbots to insecure authentication and data integrity issues, which can be exploited by attackers to gain unauthorized access to sensitive information. While some studies, such as article [10], propose solutions for secure authentication and encryption mechanisms, more research is needed to identify effective and scalable solutions that can be implemented in different chatbot contexts and scenarios.

Another area where additional research is needed is the detection and prevention of malicious chatbots. Article [3] discusses the potential of malicious chatbots to harm users and highlights the need for more research on identifying and detecting malicious chatbots. Additionally, more research is needed to develop effective and efficient methods for monitoring chatbots and detecting suspicious behavior, such as that described in article [8], which proposes a design and framework for a cyber-aware chatbot service that detects and helps prevent malware behavior from spreading on the user's machine.

Furthermore, more research is needed on the security risks and ethical issues relating to information security in chatbot implementation, as highlighted in article [15]. Specifically, more research is needed to develop frameworks and guidelines for ensuring the confidentiality, integrity, and availability of user data, as well as address ethical concerns relating to user privacy and data ownership.

Lastly, there is a need for more research on the impact of chatbots on social engineering attacks. Article [2] suggests that chatbots could be exploited by attackers to conduct social engineering attacks, but more research is needed to understand the extent to which chatbots are vulnerable to these types of attacks and to identify effective countermeasures.

Besides additional research, we might also consider some best practices for developing secure chatbots. The following are some best practices for developing secure chatbots:

Conduct comprehensive security assessments: One of the best practices for developing secure chatbots is to conduct comprehensive security assessments throughout the entire chatbot development process. Developers should conduct security testing at different stages of development to identify and mitigate vulnerabilities before the chatbot is deployed. These assessments should cover all modules in the chatbot architecture, including the client module, communication module, response generation module, and database module. For example, a developer could use tools such as static analysis to identify code-level vulnerabilities such as buffer overflows or SQL injections and dynamic analysis tools to test for vulnerabilities during runtime.

Implement user authentication and authorization: Another best practice for developing secure chatbots is to implement user authentication and authorization. Developers should ensure that the chatbot requires users to authenticate themselves before accessing sensitive data or services. Authentication could involve traditional username and password combinations, two-factor authentication, biometric authentication, or autonomous inquiry-based authentication [32]. Additionally, authorization should be implemented to ensure that users only have access to data or services that they are authorized to access. For example, a chatbot used for banking should only allow users access to their own accounts.

Use encryption for data protection: To protect sensitive data in chatbots, developers should implement encryption. Encryption can protect data from being intercepted and viewed by unauthorized parties during transmission. Developers can use techniques such as end-to-end encryption or transport layer security to secure data in transit using authenticated key agreement schemes [33–35] in different environments and symmetric or asymmetric encryption to protect data stored on the chatbot's database.

Regularly update and patch chatbots: Chatbots should be regularly updated and patched to fix vulnerabilities and improve security [36]. Developers should monitor for security alerts and advisories and ensure that their chatbots are up to date with the latest security patches. Additionally, chatbots should be monitored for unusual activity, and logs should be analyzed regularly to detect potential security breaches.

Educate users on security best practices: Developers should educate users on security best practices to ensure that they are aware of the risks associated with chatbots and how to protect themselves [37]. For example, developers can provide guidance on creating strong passwords, avoiding clicking on suspicious links, and reporting suspicious activity. Additionally, chatbots should provide clear privacy policies and obtain user consent before collecting any personal data.

Based on the information presented above, the future directions for information security in chatbots indicate several areas that will necessitate ongoing research and development. These include concerns about privacy and security, regulations and ethics, and security threats and countermeasures.

5.1. Privacy and Security

In terms of privacy and security, chatbots present a unique set of challenges that require ongoing research and development to address. One potential area of future research is the development of more sophisticated authentication and authorization mechanisms to protect against unauthorized access to chatbot data. For instance, multi-factor authentication methods, which use blockchain, image recognition, a secure one-time PIN, and biometric authentication [38–40], may be used to improve the security of chatbots. Additionally, secure encryption [41] and end-to-end encryption can be used to ensure that messages and data are protected from interception or tampering [42]. Another area of research may focus on developing more comprehensive and user-friendly security and privacy policies for chatbots to ensure that users understand how their data is collected, used, and protected. Furthermore, chatbots may be vulnerable to data breaches where user data or chatbot data is exposed to unauthorized parties. As such, research in this area may focus on developing advanced threat detection systems that use artificial intelligence and machine learning algorithms to improve the detection and prevention of security threats. Overall, research and development in this area will be important for maintaining user trust and making sure that chatbot systems are safe and private.

5.2. Regulation and Ethical Concerns

In terms of regulation and ethical concerns, there is a growing need to ensure that chatbots are developed and deployed in a responsible and ethical manner, in accordance with relevant regulations and industry best practices [43,44]. Future research in this area may focus on developing more comprehensive frameworks for chatbot development and deployment that incorporate ethical considerations such as transparency, accountability, and non-discrimination. Additionally, research may explore the use of privacy-enhancing technologies, such as differential privacy or homomorphic encryption, to ensure that chatbots can process sensitive data while preserving user privacy. Another area of research may focus on developing more comprehensive and user-friendly privacy policies for chatbots to ensure that users understand how their data are collected, used, and protected. Moreover, regulatory bodies may need to monitor the development and use of chatbots to ensure that they comply with relevant laws and regulations and to hold developers and operators accountable for any violations. As chatbots become more prevalent in various industries, it will be increasingly important to ensure that they are used in a responsible and ethical manner and to maintain user trust and confidence in these systems. Overall, it will be important to keep researching and developing in this area to make sure that chatbots are made and used in a way that respects user privacy, rights, and freedoms and follows laws and ethical guidelines.

5.3. Security Threats and Countermeasures

In terms of security threats and countermeasures, chatbots face a range of potential vulnerabilities and attacks that can compromise the security and privacy of users [37,45]. Future research in this area may focus on developing more comprehensive threat models for chatbot systems that take into account the various types of attacks that may be used against them, such as social engineering attacks, phishing attacks, and malware attacks. For example, as chatbots become more intelligent and capable of carrying out more complex tasks, they may also become more vulnerable to social engineering attacks. Social engineering is a type of attack where an attacker uses psychological manipulation to trick a user into revealing sensitive information or taking an action that may compromise the security of a system [46]. Future research in this area may focus on developing algorithms and techniques for detecting and preventing social engineering attacks on chatbots. This could include the use of natural language processing and machine learning to identify patterns of suspicious behavior and language that may indicate a social engineering attack. Additionally, research may explore the use of user education and training to improve awareness of social engineering tactics and help users avoid falling victim to such attacks. Overall, continued research and development in this area will be important to make sure that chatbot systems are safe and that people keep trusting and using them.

These are some of the future directions for chatbot research in information security. Addressing these areas will be important for the continued growth and success of the technology in the information security research and beyond.

6. Conclusions

It is important to provide context on how chatbot security differs from security in other areas. While security threats and vulnerabilities exist across various technologies and systems, the unique nature of chatbots and their use of natural language processing present specific security challenges. For example, chatbots rely heavily on user input, which can be manipulated or altered by malicious actors to exploit vulnerabilities. Additionally, chatbots may inadvertently reveal sensitive information based on the context of a conversation, which requires careful attention paid to privacy and confidentiality.

Furthermore, the use of chatbots for customer service and support presents additional security considerations, such as the authentication and authorization of users, protection of personal information, and maintaining the integrity of the chatbot's responses.

By understanding the specific security concerns and challenges relating to chatbots, researchers and practitioners can develop targeted solutions and best practices to mitigate these risks and ensure the secure use of chatbots.

This systematic literature review (SLR) provides a comprehensive summary of the research relating to information security in chatbots. This SLR highlights the significant security threats and vulnerabilities that chatbots face. The review reveals that malicious input, user profiling, contextual attacks, and data breaches are among the most common security concerns for chatbots. The findings also demonstrate that there is a need for effective and scalable solutions for chatbot security that can be implemented in different contexts and scenarios.

To address these challenges, the studies reviewed suggest various solutions, such as the use of blockchain technology, end-to-end encryption, and organizational, managerial, and technical controls. Furthermore, the review emphasizes that maintaining user trust and addressing privacy concerns are critical factors for the successful adoption and continued use of chatbots and AI assistants.

The taxonomy developed in this review provides a useful framework for categorizing the articles and their findings, which could inform future research and practice in this field. Based on the review, it is clear that there is still much research to be conducted in the field of chatbot security. Future research should focus on developing more sophisticated authentication and authorization mechanisms, comprehensive and user-friendly security and privacy policies, advanced threat detection systems, and frameworks for chatbot development and deployment that incorporate ethical considerations.

Overall, the findings of this review suggest that information security is a critical factor that must be addressed for the successful adoption and continued use of chatbots and AI assistants. The failure to address these security concerns could undermine user trust and lead to negative consequences for organizations and individuals alike. The insights provided in this review can serve as a roadmap for researchers and practitioners to develop and implement effective security solutions for chatbots and AI assistants.

7. Limitations

Several limitations should be considered when interpreting the results of this review. First, this review only includes articles published up to 31 December 2022, which means that more recent research may not be included. Additionally, the review focuses solely on information security relating to chatbots and does not cover other potential issues, such as usability concerns. Furthermore, the studies included in this review used different methods and approaches to assess chatbot security, which could limit the comparability of findings across studies. Finally, the review is limited by the quality and scope of the articles included, as some articles may be more comprehensive or relevant than others. Despite these limitations, this review provides a valuable overview of the current state of research in this area, and it highlights areas for future research to address the limitations identified.

Author Contributions: Conceptualization, J.Y. and L.Y.P.; methodology, J.Y.; validation, L.Y.P., Y.-L.C. and C.S.K.; formal analysis, J.Y.; investigation, J.Y.; resources, J.Y.; data curation, L.Y.P.; writing—original draft preparation, L.Y.P.; writing—review and editing, L.Y.P., Y.-L.C. and C.S.K.; visualization, J.Y.; supervision, L.Y.P.; project administration, L.Y.P.; funding acquisition, Y.-L.C. and C.S.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Science and Technology Council in Taiwan, grant number NSTC-109-2628-E-027-004–MY3, NSTC-111-2218-E-027-003, and NSTC-111-2622-8-027-009 and the Ministry of Education of Taiwan, official document number 1112303249.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Dhinagaran, D.A.; Martinengo, L.; Ho, M.-H.R.; Joty, S.; Kowatsch, T.; Atun, R.; Car, L.T. Designing, Developing, Evaluating, and Implementing a Smartphone-Delivered, Rule-Based Conversational Agent (DISCOVER): Development of a Conceptual Framework. *JMIR Mhealth Uhealth* **2022**, *10*, e38740. [CrossRef] [PubMed]
2. Adamopoulou, E.; Moussiades, L. An Overview of Chatbot Technology. In Proceedings of the Artificial Intelligence Applications and Innovations 2020, Neos Marmaras, Greece, 5–7 June 2020.
3. Adamopoulou, E.; Moussiades, L. Chatbots: History, technology, and applications. *Mach. Learn. Appl.* **2020**, *2*, 100006. [CrossRef]
4. Chen, C.-M.; Liu, S.; Li, X.; Islam, S.H.; Das, A.K. A provably-secure authenticated key agreement protocol for remote patient monitoring IoMT. *J. Syst. Arch.* **2023**, *136*, 102831. [CrossRef]
5. Chen, C.-M.; Li, Z.; Kumari, S.; Srivastava, G.; Lakshmanna, K.; Gadekallu, T.R. A provably secure key transfer protocol for the fog-enabled Social Internet of Vehicles based on a confidential computing environment. *Veh. Commun.* **2023**, *39*, 100567. [CrossRef]
6. Ye, W.; Li, Q. Chatbot Security and Privacy in the Age of Personal Assistants. In Proceedings of the 2020 IEEE/ACM Symposium on Edge Computing, San Jose, CA, USA, 12–14 November 2020.
7. Bhuiyan, M.S.I.; Razzak, A.; Ferdous, M.S.; Chowdhury, M.J.M.; Hoque, M.A.; Tarkoma, S. BONIK: A Blockchain Empowered Chatbot for Financial Transactions. In Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, Guangzhou, China, 29 December 2020–1 January 2021.
8. Thorpe, S.; Scarlett, H. Towards a Cyber Aware Chatbot Service. In Proceedings of the 2021 IEEE International Conference on Big Data, Orlando, FL, USA, 15–18 December 2021.
9. Gondaliya, K.; Butakov, S.; Zavarsky, P. SLA as a mechanism to manage risks related to chatbot services. In Proceedings of the 2020 IEEE 6th Intl Conference on Big Data Security on Cloud, IEEE Intl Conference on High Performance and Smart Computing, and IEEE Intl Conference on Intelligent Data and Security, Baltimore, MD, USA, 25–27 May 2020.
10. Shah, M.; Panchal, M. Privacy Protected Modified Double Ratchet Algorithm for Secure Chatbot Application. In Proceedings of the 2022 3rd International Conference on Smart Electronics and Communication, Trichy, India, 20–22 October 2022.
11. Belen-Saglam, R.; Nurse, J.R.C.; Hodges, D. An Investigation Into the Sensitivity of Personal Information and Implications for Disclosure: A UK Perspective. *Front. Comput. Sci.* **2022**, *4*, 1–22. [CrossRef]
12. Patil, K.; Kulkarni, M.S. Artificial intelligence in financial services: Customer chatbot advisor adoption. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *9*, 4296–4303. [CrossRef]
13. Ali, H.; Aysan, A.F. What will ChatGPT Revolutionize in Financial Industry? *Soc. Sci. Res. Netw.* **2023**, 4403372. [CrossRef]
14. El Hajal, G.; Daou, R.A.Z.; Ducq, Y. Human Firewall: Cyber Awareness using WhatApp AI Chatbot. In Proceedings of the 2021 IEEE 3rd International Multidisciplinary Conference on Engineering Technology, Beirut, Lebanon, 8–10 December 2021.
15. Pokrovskaia, N.N. Sociocultural and Information Security Issues in the Implementation of Neural Network Technologies in Chat-bots Design. In Proceedings of the 2022 XXV International Conference on Soft Computing and Measurements, Saint Petersburg, Russia, 25–27 May 2022.
16. Edu, J.; Mulligan, C.; Pierazzi, F.; Polakis, J.; Suarez-Tangil, G.; Such, J. Exploring the security and privacy risks of chatbots in messaging services. In Proceedings of the 22nd ACM Internet Measurement Conference, Nice, France, 25–27 October 2022.
17. Jo, H. Impact of Information Security on Continuance Intention of Artificial Intelligence Assistant. *Procedia Comput. Sci.* **2022**, *204*, 768–774. [CrossRef]
18. Nadarzynski, T.; Miles, O.; Cowie, A.; Ridge, D. Acceptability of artificial intelligence (AI)-led chatbot services in healthcare: A mixed-methods study. *Digit. Health* **2019**, *5*, 1–12. [CrossRef]
19. Waheed, N.; Ikram, M.; Hashmi, S.S.; He, X.; Nanda, P. An Empirical Assessment of Security and Privacy Risks of Web-Based Chatbots. In Proceedings of the International Conference on Web Information Systems Engineering, Biarritz, France, 1–3 November 2022.
20. Hasal, M.; Nowaková, J.; Saghair, K.A.; Abdulla, H.; Snášel, V.; Ogiela, L. Chatbots: Security, privacy, data protection, and social aspects. *Concurr. Comput. Pract. Exp.* **2021**, *33*, 1–13. [CrossRef]
21. Følstad, A.; Nordheim, C.B.; Bjørkli, C.A. What makes users trust a chatbot for customer service? An exploratory interview study. In Proceedings of the International Conference on Internet Science, St. Petersburg, Russia, 24–26 October 2018.
22. van der Goot, M.J.; Pilgrim, T. Exploring Age Differences in Motivations for and Acceptance of Chatbot Communication in a Customer Service Context. In Proceedings of the International Workshop on Chatbot Research and Design, Amsterdam, The Netherlands, 19–20 November 2019.
23. United Nations, Department of Economic and Social Affairs, Population Division. Available online: http://esa.un.org/wpp/ (accessed on 12 May 2023).
24. GPT-4 Is OpenAI's Most Advanced System, Producing Safer and More Useful Responses. Available online: https://openai.com/product/gpt-4 (accessed on 12 May 2023).

25. Corsello, A.; Santangelo, A. May Artificial Intelligence Influence Future Pediatric Research?—The Case of ChatGPT. *Children* **2023**, *10*, 757. [CrossRef] [PubMed]
26. Kooli, C. Chatbots in education and research: A critical examination of ethical implications and solutions. *Sustainability* **2023**, *15*, 5614. [CrossRef]
27. Giansanti, D. The Chatbots Are Invading Us: A Map Point on the Evolution, Applications, Opportunities, and Emerging Problems in the Health Domain. *Life* **2023**, *13*, 1130. [CrossRef]
28. Aggarwal, A.; Tam, C.C.; Wu, D.; Li, X.; Qiao, S. Artificial Intelligence–Based Chatbots for Promoting Health Behavioral Changes: Systematic Review. *J. Med. Internet Res.* **2023**, *25*, e40789. [CrossRef]
29. Sallam, M. ChatGPT utility in healthcare education, research, and practice: Systematic review on the promising perspectives and valid concerns. *Healthcare* **2023**, *11*, 887. [CrossRef]
30. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Syst. Rev.* **2021**, *10*, 89. [CrossRef]
31. Tarsilla, M. Cochrane Handbook for Systematic Reviews of Interventions. *J. Multidiscip. Eval.* **2010**, *6*, 143–148. [CrossRef]
32. Voege, P.; Abu Sulayman, I.I.M.; Ouda, A. Smart Chatbot for User Authentication. *Electronics* **2022**, *11*, 4016. [CrossRef]
33. Wu, T.-Y.; Meng, Q.; Chen, Y.-C.; Kumari, S.; Chen, C.-M. Toward a secure smart-home IoT access control scheme based on home registration approach. *Mathematics* **2023**, *119*, 2123. [CrossRef]
34. Wu, T.-Y.; Kong, F.; Meng, Q.; Kumari, S.; Chen, C.-M. Rotating Behind Security: An enhanced authentication protocol for IoT-enabled devices in distributed cloud computing architecture. *EURASIP J. Wirel. Commun. Netw.* **2023**, *2023*, 36. [CrossRef]
35. Wu, T.-Y.; Meng, Q.; Yang, L.; Kumari, S.; Pirouz, M. Amassing the Security: An Enhanced Authentication and Key Agreement Protocol for Remote Surgery in Healthcare Environment. *Comput. Model. Eng. Sci.* **2023**, *134*, 317–341. [CrossRef]
36. Chow, J.C.; Sanders, L.; Li, K. Design of an educational chatbot using artificial intelligence in radiotherapy. *AI* **2023**, *4*, 319–332. [CrossRef]
37. Addington, S. ChatGPT: Cyber Security Threats and Countermeasures. *Soc. Sci. Res. Netw.* **2023**, 4425678. [CrossRef]
38. Carrillo-Torres, D.; Pérez-Díaz, J.A.; Cantoral-Ceballos, J.A.; Vargas-Rosales, C. A Novel Multi-Factor Authentication Algorithm Based on Image Recognition and User Established Relations. *Appl. Sci.* **2023**, *13*, 1374. [CrossRef]
39. Ahmad, M.O.; Tripathi, G.; Siddiqui, F.; Alam, M.A.; Ahad, M.A.; Akhtar, M.M.; Casalino, G. BAuth-ZKP—A Blockchain-Based Multi-Factor Authentication Mechanism for Securing Smart Cities. *Sensors* **2023**, *23*, 2757. [CrossRef] [PubMed]
40. Binbeshr, F.; Por, L.Y.; Kiah, M.M.; Zaidan, A.A.; Imam, M. Secure PIN-Entry Method Using One-Time PIN (OTP). *IEEE Access* **2023**, *11*, 18121–18133. [CrossRef]
41. Alexan, W.; Chen, Y.L.; Por, L.Y.; Gabr, M. Hyperchaotic Maps and the Single Neuron Model: A Novel Framework for Chaos-Based Image Encryption. *Symmetry* **2023**, *15*, 1081. [CrossRef]
42. Bartusek, J.; Garg, S.; Jain, A.; Policharla, G.V. End-to-end secure messaging with traceability only for illegal content. In Proceedings of the Advances in Cryptology–EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, 23–27 April 2023; pp. 35–66.
43. Rivas, P.; Zhao, L. Marketing with ChatGPT: Navigating the Ethical Terrain of GPT-Based Chatbot Tech-nology. *AI* **2023**, *4*, 375–384. [CrossRef]
44. Torres-Castaño, A.; Abt-Sacks, A.; Toledo-Chávarri, A.; Suarez-Herrera, J.C.; Delgado-Rodríguez, J.; León-Salas, B.; Serrano-Aguilar, P. Ethical, Legal, Organisational and Social Issues of Teleneurology: A Scoping Re-view. *Int. J. Environ. Res. Public Health* **2023**, *20*, 3694. [CrossRef]
45. Uma, S. Conversational AI Chatbots in Digital Engagement: Privacy and Security Concerns. In *Trends, Ap-plications, and Challenges of Chatbot Technolog*; IGI Global: Hershey, PA, USA, 2023; pp. 274–317.
46. Salahdine, F.; Kaabouch, N. Social Engineering Attacks: A Survey. *Future Internet* **2019**, *11*, 89. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.