IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834, p- ISSN: 2278-8735.Volume 19, Issue 6, Ser. 1 (Nov. – Dec. 2024), PP 33-40
www.iosrjournals.org

Design And Implementation Of A Decision System For Chatbot Applications

Olanrewaju, Babatunde Seyi, Pius, Chinedu Kevin; Okunade, Oluwasogo Adekunle, Osunade, Oluwaseyitanfunmi
Department Of Computer Science, Wellspring University, Benin City, Edo State, Nigeria.
Department Of Computer Science, Wellspring University, Benin City, Edo State,
Department Of Computer Science, Faculty Of Sciences, National Open University Of Nigeria, Abuja, Nigeria.
Department Of Computer Science University Of Ibadan, Ibadan, Nigeria.

Abstract
Information should be shared effectively and securely to protect users' personal identifiable information. Using a chatbot, or a computer application to share information presents a likelihood of identity theft if not properly secured. In communicating with chatbots, the user's information is held in the chatbot application database. The availability of user information on this application may give opportunity to attackers to hijack personal user information to perpetrate crime. Unfortunately, current chatbot applications do not have a mechanism to delete or remove personal identifiable information of users. Some chatbots accept users' personal identifiable information with no recourse to the user on what happens after the chat session. To prevent a third party from trading, selling, or hacking the data, this research designed a decision system to be added to the chatbot application that will enable the user to consciously decide on how their personal identifiable information should be treated or kept. The chatbot was implemented in Hypertext Markup Language (HTML), using PHP and MySQL for standard web development. Also, a PHP server was installed for the system to relate properly with the database server in fetching and storing the data. The system was tested using likelihoods that may lead to the success of the program. This was done repeatedly with different test data. The new system provides users consent on whether their personal information is left on the chatbot app or removed completely.

Keywords: *Personal Identifiable Information; chatbot; identity theft; decision system*

Date of Submission: 04-12-2024 Date of Acceptance: 14-12-2024

I. Introduction

Information sharing is an important aspect of human existence because it touches every critical sector of human lives which includes education, banking, agriculture, business and so on (Patchara, 2022). Therefore, sharing information effectively and securely is a process that has been involved for generations in the past. The evolution of computers from the first generation to the present era of Artificial Intelligence (AI) has brought the idea of having a computer application known as a chatbot to be able to share information with human beings (Dong-Min et al., 2022). The chatbot is a concept that began when interaction between human beings and computers was developed. The presence of Artificial Intelligence (AI)/Cognitive Computing contributed to the emergence of chatbots (Vajinepalli et al., 2022).

According to Team Capacity, (2021), the chatbot has been around for about 50 years now. It started with the work of Alan Turing's theory in the early 20th century that the brain is a computing machine that can learn over time to become a universal machine.

Currently, businesses, organizations, and institutions are now deploying chatbots as part of the organization's 'personnel'. It functions as a Customer Service personnel or an admissions assistant. However, Vadapalli, (2022), identified data privacy and security as a challenge affecting chatbots. Securing the Personal Identification Information (PII) of anyone sharing information with computers in this era of cybercrime is key in the operations of chatbots (Daga et al., 2021). The security of information and data integrity it offers makes the operations of chatbot to be widely accepted.

Today, because of the benefits it provides, the operations of chatbots in businesses is growing and its awareness is equally growing. This will grow more in the coming years, but the accompanying security of personal identifying information is lacking or not adequately implemented (Daga et al., 2021).

The interaction between chatbots and humans involves the processing of a huge amount of important personal information that needs to be protected. The security of personal data is crucial especially to avoid identity theft when dealing with personal data that could be used by any other person (Kaushal and Kaushal, 2011). In

communicating with chatbots, the users' information is held in the database of the chatbot application. The availability of user information on this application may give opportunity to attackers to hijack personal user information to perpetrate crime. According to David *et al.* (2018), it has been predicted that the datasphere will continue to grow and may get to about 175 trillion gigabytes by 2025. This growth is a risk to the security and privacy of personal data such as customer information or employee data because security becomes more difficult due to the widespread of personal data on various applications. It is therefore important to provide the best industrial practices to secure employees' PII.

The new system will provide for users' consent on whether their personal information be left on the chatbot application or be removed completely. The removal or retaining of their personal identity is completely in their interest and consent.

This research aims to design and implement a chatbot application that enables users to consciously decide on how their personal identifiable information should be treated after a chat session is completed. The aim is achieved with the objectives to design and implement a decision system in a chatbot application to either keep or delete PII from the system.

The research used object-oriented Methodology (OOM) to achieve the stated aim and objectives. The following steps were taken to accomplish the research goals:

1) Development of a Use Case diagram for the chatbot application decision system
2) Design an algorithm for the chatbot application decision system.
3) Implement the algorithm using PHP and scripting languages such as HTML, JavaScript, and CSS
4) Test the system developed.

The work is to develop and implement how users' personal identifying information (PII) is protected in the chatbot application.

II. Literature Review

Chatbot is an Artificial intelligence application that communicates with humans via a command or voice. The application could be referred to as conversational AI, chat robot, or a bot. In Figure 1, Sukumar, (2020) provided a sample of a chatbot architecture that consists Natural Language Understanding (NLU) toolkit, a Dialog management system, a Frequently Asked Questions (FAQ) retrieval system, and a Document search module.

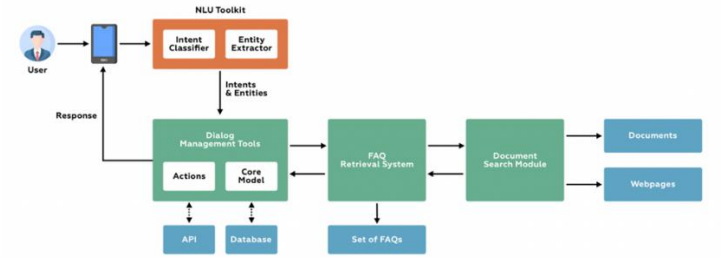

Figure 1: The Architecture of the chatbot. Source: (Sukumar, 2020)

In the architecture, the user sends a query either from a mobile phone or computer system into the NLU Toolkit where it is broken down into units that will enable an easy understanding of the system. The Dialog management system further breaks the query down or narrows it to a specific concern. The FAQ retrieval system, on the other hand, further breaks the query in case a suitable answer is not found in the above systems and so does the Document search module. This is a simple analogy of how it works.

Personal Identifiable Information (PII)

Some chatbots request users to supply some sensitive information like their Personal Identifiable Information (PII) which is a category of data that identifies a person or an individual. Examples of PII include but are not limited to Bank Verification Number (BVN), National Identity Number (NIN), bank account details, and personal data in medical records, educational records, license plate information, criminal records, and biometric data such as personal name, date of birth, race, gender, phone numbers, and age.

The PII is any specific data or information that is tied or linked to an individual that can personally track them in any way. This information is very sensitive and is high-risk data. Because of its sensitivity, securing the PII is important especially as chatbot acceptance is increasingly growing. PII can be sold. According to (Nelson, 2015), he pointed out that individuals can sell their PII to businesses and advertisers. Why? To grant free subscriptions to their websites.

According to Melindez and Pasternack (2019), it is well known that personal data could be bought and sold for financial purposes or any criminal activity. The PII makes a big market because of its sensitivity. Therefore, protecting and securing it is paramount.

When PII is bought or hacked, the theft company can organize the data and use it against unsuspecting individuals. Sometimes you receive unsolicited SMS, emails, and messages from advertising companies and people you have not exchanged a piece of information with. How did they locate you or get your number? Have you ever asked?

Thousands of personal data are being hacked or purchased by political consultants and parties who want to influence votes. If PII is not important, no one will trade it; often, one tends to easily give out information on the web while filling out one form or the other (Radha, 2015)

Numerous cases of PII fraud have been established. US Attorney (2018) reported that two people who were caught in PII fraud between March 2014 and March 2016 were charged for purchasing PII to file false tax returns in a deal of about $12 million. In another scenario, very recently according to the reports from the US Attorney (2023), "a former Orange County social worker was sentenced to 57 months in federal prison for stealing PII Social Security numbers specifically from clients then using the stolen information to fraudulently obtain tax refunds, welfare benefits, and credit cards."

An immeasurable harm can be done to a company or an individual when their PIIs are compromised.

Securing Personal Identifiable Information (PII)

To secure PIIs, several works have been done. Nate (2018) stated that for a company that handles PII to secure personal data, there is a need to identify the types and know the storage areas of PII. Nate (2018) also advised that there is a need to classify sensitive PII, delete old ones, and encrypt the current ones.

However, Meyer, (2021) came up with things to do on the browser or while you are on the web to avoid exposing your PII. They are:

- Change your passwords regularly.
- Check through your social media account settings.
- Use public Wi-Fi with caution.
- Make your security questions tricky.
- Use a random password generator.
- Use private browsing.
- Hide your IP address.
- Choose your device carefully.
- Think twice before giving out your NI (National Insurance) number.
- Make your browser always use HTTPS.
- Sign out!
- Beware of phishing scams
- Read the fine print.
- Use antivirus tools.
- Use a VPN

In securing PII, relevant government agencies should provide regulations on how such information should be handled. In Nigeria, the framework is contained in the Nigeria Data Protection Regulation, (NITDA, 2019). This framework is to protect users' data and programmers and software developers are to comply with the framework.

Unfortunately, no chatbot has a deletion or the removal of PII included as part of the module. Some chatbots accept users' PII with no recourse to the user what happens after the chat session. To avoid third-party trading, selling, or hacking the data, this research proposed a module to be added to the chatbot application that will enable the user to consciously decide on how their PII should be treated or kept and this was accomplished.

Related Work

Kelley, (2019) proposed the use of placeholders instead of identifiable data. This way, the customer's identity will not be revealed but the conversation will still be understood. This appears intelligent and good but the masked (placeholder) customer PII could be decrypted or gleaned by an attacker or even company staff since the data still resides in the company's database.

In another work, Thorbecke, (2023) shared how Italy has banned ChatGPT temporarily in the country and JPMorgan queried staff using ChatGPT because of privacy concerns. In a further review, Doherty and Braithwaite (2023), revealed a CNN report that "Regulators in Italy issued a temporary ban on ChatGPT Friday, effective immediately, due to privacy concerns and said they had opened an investigation into how OpenAI, the US company behind the popular chatbot, uses data". The disclosure of users' sensitive personal identifying information is a big challenge faced as chatbot usage is increasing.

Furthermore, Doherty and Braithwaite (2023) pointed out that OpenAI, the company that developed ChatGPT was collecting the personal information of its users for analysis and to improve the application. They also indicated that such personal information will be provided to third-party companies without recourse to the users except where there is a law restriction.

Yang, *et al*. (2023), in their work, say that the major challenge is the evolving nature of security threats and vulnerabilities". Since chatbots are also continuously evolving, new kinds of attacks also evolve that mitigate already known security measures. They also identify that chatbots may be a risk of disclosing data to third parties due to the inability to understand how to handle some data for training purposes. They also identified that "the development of secure chatbots requires a multidisciplinary approach that encompasses not only technical security measures but also user trust, privacy, and ethical considerations". Based on this, a healthcare chatbot will require a measure of security that is different from the transportation, finance or even ordering of food. The needs and purposes that the chatbots are going to serve will determine the approach and measure of the security. Although, their work reviewed some security and vulnerability but did not provide outright removal or how the user may be able to get rid of their personal information at the end of the chat session.

In another work by Hasal, *et al*. (2021), they listed some security, privacy, and data protection measures. Some of the security issues identified are "STRIDE model as Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privileges". They proposed that it should be mitigated by implementing the following: "Authenticity, Integrity, Non-repudiation, Confidentiality, Availability, Authorization". In the areas of vulnerability, they said that weak coding, lack of current drivers on the hardware side, and a lack of a weak firewall, largely lead to a system vulnerability.

Their work on security measures such as authentication methods where a user is prompted to verify their login by providing the account login details (username), phone number password, and any other personal data, are rarely used with chatbots. This then leaves or creates a security issue for the user.

III. Methodology

Analysis of the Existing System

The general chatbots, especially the ones available in Nigeria do not possess the ability to remove Personal Identification Information. As such, users do not have any idea what happens to their data and hence, may be vulnerable. The concern for a compromised vulnerability may rise when a breach or damage occurs. Most of the chatbots do not provide or share information on how the user information is being treated. It keeps them from knowing what their data is. For instance, the Uber bot keeps the user data, share it with third parties, and may even sell them. This illegal and fraudulent way of handling user information is what is predominant in the existing system.

Analysis of the Developed System

This paper developed a chatbot application that will include the aspect of PII deletion after the conversation session ends. This will restore confidence to anyone doing a transaction that involves their finances and other transactions that require the release of personal information. The system was designed to provide users' information integrity and security by providing a dialogue box that gives the users the privilege to confirm that their PIIs should be removed/deleted.

The use case diagram of the system is shown in Figure 2. The figure shows two users: the admin and a client using the Chatbot application. The admin has the role of starting and ending a chat while the client can add, view, update, and delete any information. The client also has the privilege of ending the chat.

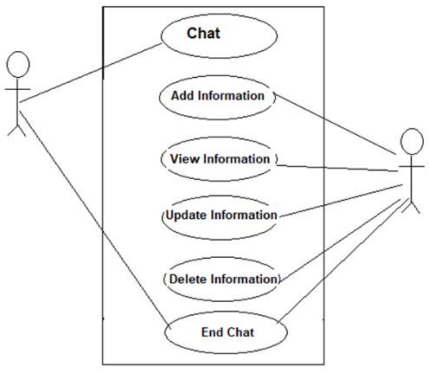

Figure 2: Use Case diagram of user and admin role

The activity diagram as shown in Figure 3 starts by launching the Chatbot application on a browser. This marks the first phase of the Activity diagram. In the second phase, the URL of the Chatbot (http://localhost/chatbotapp) is entered on the Address bar of the browser. The enter key is pressed to accept and process the action. In phase three, the login page is displayed. The phase helps to authenticate and establish a user signage. Phase four provides for the entering of the admin information. Once it is authenticated the User Dashboard is displayed. Users are created at this point.

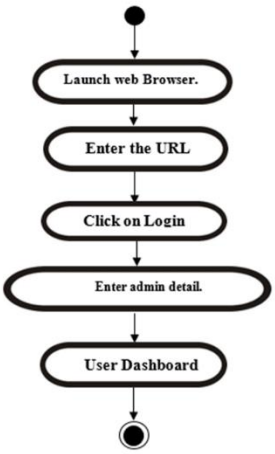

Figure 3: Activity Diagram to Log in to the system.

The flow of the program sequence of the Chatbot Decision System is shown in Figure 4. It begins with the START diagram. The arrow shows the path of the flow. Once the Chatbot conversation begins, it continues as long as long as the customer queries are open. The customer initiates a termination of the conversation when he is ready. The system then prompts if the customer wants his PII to be killed. If he accepts No to the system prompts the conversation ends and the app closes, but if the user selects 'Yes', the PII is automatically removed from the system and the database of the bot. Shown below is the flowchart.

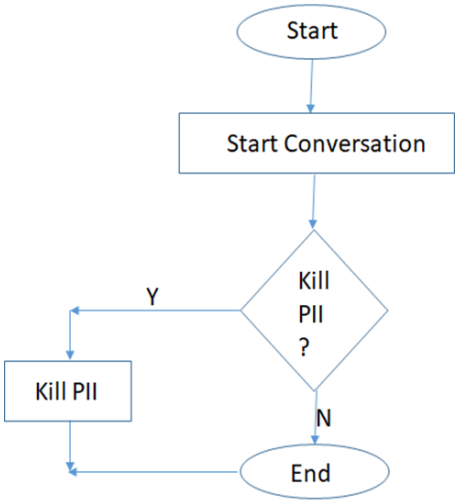

Figure 4 – Chatbot Decision System

System Implementation

The chatbot was implemented in Hypertext Markup Language (HTML), using PHP and MySQL for standard web development. Also, a PHP server (either online or offline) must be installed for the system to work on any system and to relate properly with the database server in fetching and storing the data. The system was tested using likelihoods that may lead to the success of the program. This was done repeatedly with different test data.

IV. Discussion Of Results

This section discusses the various user interfaces in the developed chatbot application system.

Launch Screen Page

The moment the page is launched from the browser, the screen page shown in Figure 5 opens. This page shows the Chatbot launch page. The Launch page is the first page that displays the Chatbot app. It bears the Chatbot app and the owner's name along with their trademark symbol.

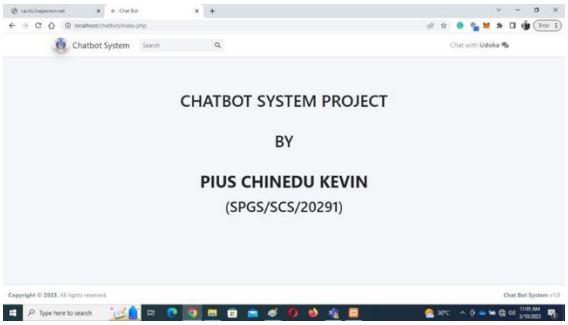

Figure 5: Launch Screen page

Login Page

This page shown in Figure 6 allows users to log in to the system. This page grants permission to users to access the app once they key in their login credentials. The app authenticates the user details and opens the app for online correspondence or inquiry.

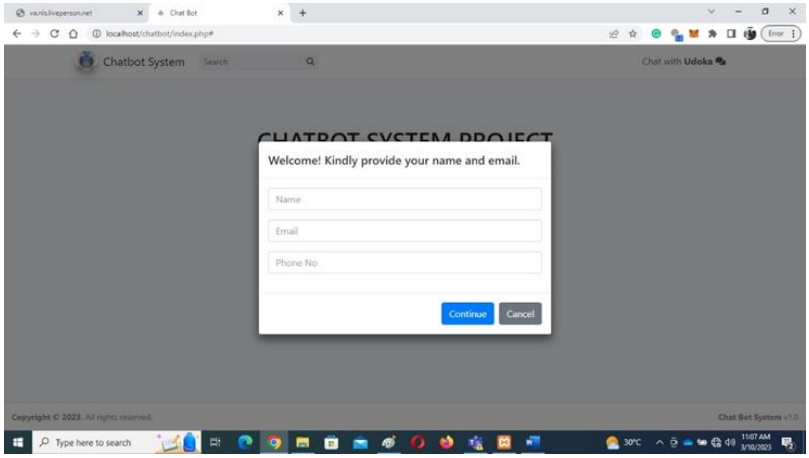

Figure 6: Login page

Chat Page

This page shown in Figure 7 allows users to engage in conversation. The user engages in live chat with the system. Interaction is ongoing as the bot has already collected the user's PII and other relevant information.

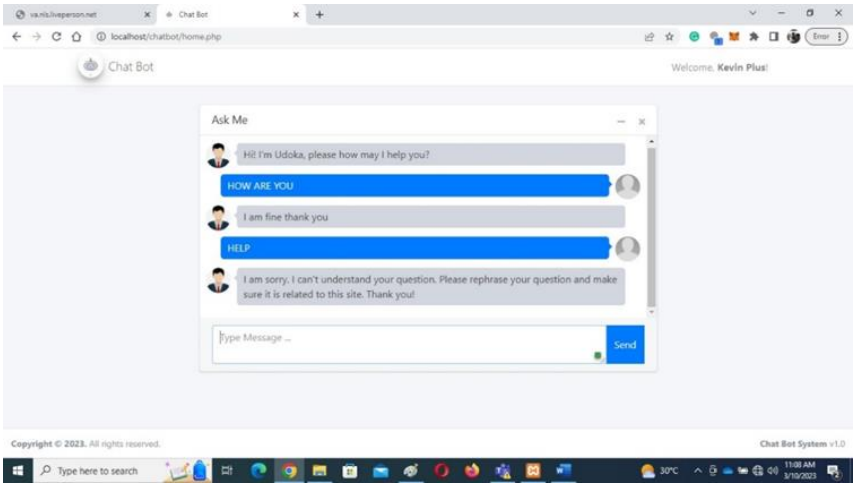

Figure 7: Chat page

Exit Page

This page shown in Figure 8 allows the exit of the conversation. Once the live chat is completed, a formal close or exit of the app is initiated by the user by clicking the close button, or the end button depending on the app structure.

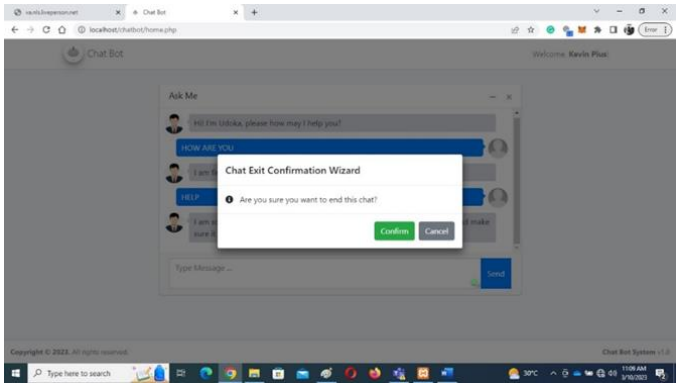

Figure 8: Exit page.

PII Deletion Confirmation Page

This page shown in Figure 9 allows users to confirm the removal of their PIIs. In this case, neither the users nor the admin terminates the process, but the decision system calls or prompts the attention of the user to confirm their willingness to remove the personal identifying information from the database.

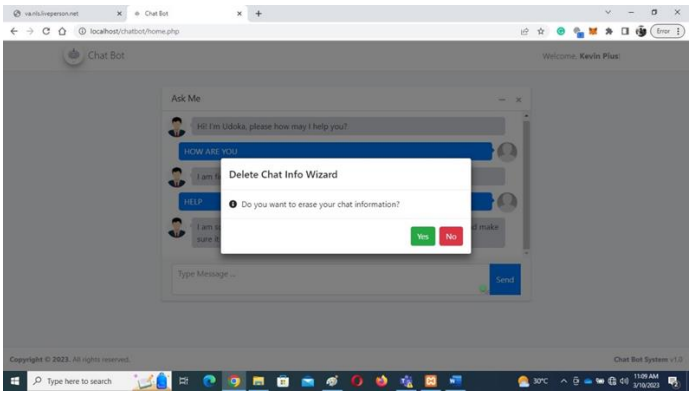

Figure 9: First Confirmation Page

System Confirms PII Removal Page

Figure 10 shown below is the most important task of the system. The system confirms to the user that their PII has been removed. This guarantees trust, void of breach of any kind. This page confirms that the user's PII has been removed. If the user responds 'Yes' to the confirmation prompt, their PIIs are completely removed. It provides the user confirmation that their information has been deleted from the system. The database clears every identifying information the user may have entered at the start of the authentication. They will no longer be able to fear the risk of their PII being compromised or shared with third parties without their permission or consent.

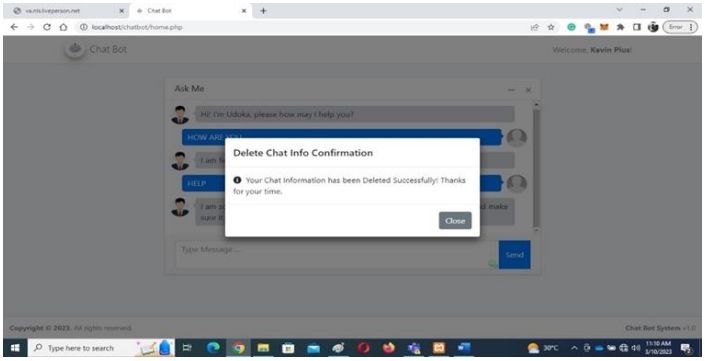

Figure 10: System Confirmation page

The new system has the ability (feature) to kill (delete/remove) the user's PII at the log-out point of the conversation. This will increase users' trust and confidence that their information will not be breached or used for a fraudulent act after they have gone.

V. Conclusions

The mining of an authorized user data from chatbots and the increasingly sales and purchase of users Personal Identifying Information from third party companies and the consequent harm done to unsuspecting user who is vulnerable, protecting and guaranteeing their date safety is vary important.

This research summarizes how the PII could be removed by user willingly once the chat session. The research has reviewed literature showing cases of fraudulent activities and theft committed with users PIIs that have been hacked.

The research also provided national and international framework that have been setup to guard the user safely in all their data usage. These regulations are referred to as GDPR and NDPR. They outlined the way data should be handled. Since it is difficult to confirm if data are removed via the GDPT and NPDR framework, adding the REMOVE module to chatbot application will be a great advantage if use data protection. Personal Identifying Information (PII) security in chatbot is a basic concern. Huge data is being generated which can be traded. Webpages cookies houses chat details, and other platforms on which chatbots are built are being mined by third parties. Hence, the need for a strict way to completely remove this data or keep them safe.

References

[1] Daga, S. S., Ahmed, U. And Kumawat, R. K. (2021). Forensic Tools And Techniques Of Absolute Human Identification: Physical And Molecular Approach. Journal Of Forensic Sciences And Criminal Investigation, Volume 15, Issue 3. Doi: 10.19080/Jfsci.2021.15.555913

[2] David, R., John G., John R., (2018). The Digitization Of The World From Edge To Core. Https://Www.Seagate.Com/Files/Www-Content/Our-Story/Trends/Files/Idc-Seagate-Dataage-Whitepaper.Pdf

[3] Doherty, L. And Braithwaite, S. (2023). Italy Blocks Chatgpt Over Privacy Concerns. Https://Edition.Cnn.Com/2023/03/31/Tech/Chatgpt-Blocked-Italy/Index.Html

[4] Dong-Min P., Seong-Soo J., And Yeong-Seok S. (2022). Systematic Review On Chatbot Techniques And Applications. Journal Of Information Processing Systems, Vol.18, No.1, Pp.26~47, February 2022 Issn 1976-913x (Print) Https://Doi.Org/10.3745/Jips.04.0232

[5] Hasal, M. Et Al. (2021). Chatbots: Security, Privacy, Data Protection, And Social Aspects. Https://Onlinelibrary.Wiley.Com/Doi/10.1002/Cpe.6426

[6] Kausal, N. And Kausal, P. (2011). Human Identification And Fingerprints: A Review. Journal Of Biometrics And Biostatistics. Doi: 10.4172/2155-6180.1000123

[7] Kelley, K. (2019). Address Anonymity And Data Privacy In Chatbot Security. Https://Www.Techtarget.Com/Searchenterpriseai/Feature/Address-Anonymity-And-Data-Privacy-In-Chatbot-Security#:~:Text=It's%20imperative%20that%20systems%20are,Not%20know%20the%20customer%20identity

[8] Melendez, S. And Pasternack, A. (2019). Here Are The Data Brokers Quietly Buying And Selling Your Personal Information. Https://Www.Fastcompany.Com/90310803/Here-Are-The-Data-Brokers-Quietly-Buying-And-Selling-Your-Personal-Information

[9] Meyer, B. (2021). 15 Tips To Protect Your Pii. Https://Cybernews.Com/Privacy/15-Tips-To-Protect-Your-Pii/

[10] Nate, S. (2018). How To Secure Personally Identifiable Information Against Loss Or Compromise. Https://Www.Digitalguardian.Com/Blog/How-Secure-Personally-Identifiable-Information-Against-Loss-Or-Compromise

[11] National Information Technology Development Agency (Nitda) (2019). Nigeria Data Protection Regulation 2019: Implementation Framework. File:///C:/Users/Maranatha/Downloads/Ndpr-Implementation-Framework.Pdf

[12] Nelson, P. (2015). 3 Ways You Can Sell Your Own Personal Data.

[13] Https://Www.Networkworld.Com/Article/2999878/3-Ways-You-Can-Sell-Your-Own-Personal-Data.Html

[14] Patchara, V. (2022). Impact Of Chatbots On Student Learning And Satisfaction In The Entrepreneurship Education Programme In Higher Education Context. International Education Studies; Vol. 15, No. 6; 2022. Issn 1913-9020 E-Issn 1913-9039. Published By Canadian Center Of Science And Education. Available On: Https://Files.Eric.Ed.Gov/Fulltext/Ej1373320.Pdf

[15] Radha A. D. (2015). Need For Newer Techniques For Personal Identification. Journal Of Forensic Research. Deshmukh, J Forensic Res 2015, 6:3. Doi: 10.4172/2157-7145.1000284

[16] Sukumar, A. (2020). Conversational Ai Chatbot: Architecture Overview.

[17] Https://Blog.Qburst.Com/2020/09/Conversational-Ai-Chatbot-Architecture-Overview/

[18] Team Capacity. (2021). The Evolution Of Chatbots. Https://Capacity.Com/Chatbots/Evolution-Of-Chatbots/

[19] Terrance, L. (2022). The Benefits And Drawbacks Of Implementing Chatbots In Higher Education: A Case Study For International Students. Master Thesis At Jönköping University. Https://Www.Diva-Portal.Org/Smash/Get/Diva2:1673913/Fulltext01.Pdf

[20] Thorbecke, C. (2023). Don't Tell Anything To A Chatbot You Want To Keep Private. Https://Edition.Cnn.Com/2023/04/06/Tech/Chatgpt-Ai-Privacy-Concerns/Index.Html

[21] United States Attorney's Office (2023). Former Social Worker Sentenced To Nearly 5 Years In Federal Prison For Masterminding Multiple Frauds By Using Clients' Stolen Identities. Https://Www.Justice.Gov/Usao-Cdca/Pr/Former-Social-Worker-Sentenced-Nearly-5-Years-Federal-Prison-Masterminding-Multiple

[22] United States Attorney's Office (2018). Nigerian Leader Of Nationwide Identity Theft And Irs Tax Fraud Scheme Sentenced To Federal Prison. Https://Www.Justice.Gov/Usao-Or/Pr/Nigerian-Leader-Nationwide-Identity-Theft-And-Irs-Tax-Fraud-Scheme-Sentenced-Federal

[23] Vadapalli, P., (2022), Top 7 Challenges In Artificial Intelligence In 2022, Https://Www.Upgrad.Com/Blog/Top-Challenges-In-Artificial-Intelligence/

[24] Vajinepalli, S. H. V., Parsi, A., And Richa, S. (2022). Research Paper On Rule Based Chatbot. International Research Journal Of Modernization In Engineering Technology And Science. Volume:04/Issue:05/May-2022