iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VI **Month of publication:** June 2023

DOI: https://doi.org/10.22214/ijraset.2023.53289

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

Weaponizing Artificial Intelligence

Rashmi Kumari[1], Dr. Priyanka Singh[2]
[1]*Bachelor of Science in Forensic science, Amity University Noida Uttar Pradesh*
[2] *Faculty Guide, Amity Institute of forensic science, Amity University Uttar Pradesh Noida*

Abstract: ***The research paper delved into the concerns of chatbot users and the potential risks lurking in the shadows—security, privacy, data protection, and social quandaries. What emerged from the study was a disquietude among users, fearing the misuse or thievery of their personal information. Additionally, apprehension surfaced regarding the sinister deployment of chatbots in the realms of phishing scams and the propagation of deceitful news. To ensure a shielded experience when engaging with chatbots, users were provided with sagacious counsel. They were admonished to only divulge their valuable information to chatbots that have garnered a reputable and trustworthy stature. Moreover, a word of caution resonated, urging users to exercise vigilance in their cyber-surfing, refraining from clicking on dubious links and showing discretion when confronted with attachments or applications proposed by chatbots. Careful advice also dictated the periodic updating of devices and software, ensconcing the latest security fixes within their digital fortresses. As an added layer of defence, users were encouraged to change their passwords at regular intervals, an act of precautionary foresight guarding against potential breaches of security.***

I. INTRODUCTION

Artificial Intelligence (AI), a captivating area within the area of computer science, delves into the intricate art of designing machines and algorithms that emulate the prowess of human intelligence. This fascinating discipline empowers these machines to accomplish tasks typically reserved for the depths of human cognition. While AI has traversed the realms of existence for numerous years, recent breakthroughs in machine learning, natural language processing, and robotics have unfurled a new era of possibilities, propelling its proliferation and pervasion.

In the present landscape, Artificial Intelligence (AI) permeates a diverse tapestry of domains and sectors, spanning the expanse from healthcare and finance to transportation. Its versatile employment manifests in virtual assistants like Siri and Alexa, catering to our every whimsical query, and personalized recommendations on e-commerce platforms that curate a bespoke shopping experience. Moreover, AI lends its discerning gaze to the realm of finance, meticulously scrutinizing transactions to detect fraud, while also adorning the landscape of transportation with the tantalizing vision of self-driving vehicles. Not to be outshined, the scientific realm cherishes the prowess of AI, wielding it to parse through colossal volumes of data and unravel future trends with a prophetic aura.

As the unceasing march of Artificial Intelligence (AI) surges forward, its tendrils enmeshing ever deeper into the fabric of our lives, one cannot help but ponder the ethical ramifications that loom on the horizon. The spectre of privacy violations, employment displacement, and the pernicious tendrils of bias haunt our collective consciousness. Thus, it becomes incumbent upon us to embark upon a ceaseless voyage of exploration, plumbing the depths of AI's potential for both benefit and peril. It is through this unwavering pursuit that we may weave a tapestry of policies and regulations, ensuring that the symphony of AI resonates harmoniously, fostering a realm where safety and societal welfare converge.

II. CHATBOTS

Chatbots, those fascinating creations made from the linking of artificial intelligence (AI) and natural language processing (NLP), have a storied history dating back several decades. The inception of ELIZA in the 1960s marked the advent of these conversational marvels. However, it is in recent years that their role in the realm of cybersecurity has ascended to prominence.

The ever-growing intricacy of cybersecurity threats, coupled with the imperative of swift and efficacious incident response, has rendered chatbots an alluring choice for organizations. Their ability to swiftly detect and address security incidents, provide real-time updates on the evolving landscape of security events, and handle routine security tasks like password resets and user authentication has propelled their adoption.

An early utilization of chatbots in the area of cybersecurity was their application in combating the insidious menace of phishing attacks. By scrutinizing incoming emails and other forms of communication, chatbots possess the acumen to identify messages of dubious origin and promptly alert security teams to potential threats.

Furthermore, chatbots prove to be indispensable aids in incident response, offering real-time updates on the status of security events. Imagine a scenario where a chatbot diligently informs security teams when a system finds itself under attack or when an unauthorized individual endeavours to breach a sensitive enclave. Such vigilance fosters a proactive approach to cybersecurity.

The use of chatbots in cybersecurity is not without its merits. Their tireless operation, unrelenting in its vigilance, ensures that security events are detected and addressed promptly, unfettered by the constraints of time. Moreover, chatbots possess the capability to handle a substantial influx of requests, thus liberating security personnel to tackle more intricate endeavours.

Nevertheless, it is essential to acknowledge that risks accompany the employment of chatbots in the realm of cybersecurity. Foremost among these concerns is the potential vulnerability of chatbots to compromise by malevolent actors. If a chatbot were to fall prey to a malicious hack, it could be weaponized to unleash attacks upon the organization or surreptitiously pilfer sensitive information. Additionally, there exists the peril that chatbots may not invariably furnish accurate information or might misconstrue user queries. This could result in ill-informed decisions being made, thereby paving the way for potential security breaches.

It is incumbent upon organizations to navigate these risks judiciously, incorporating robust security measures and diligent oversight to safeguard the sanctity of their cybersecurity landscape. The judicious employment of chatbots, paired with stringent safeguards, can fortify the defence against evolving threats while harnessing the immense potential these AI-driven conversational companions possess.

A. Working of Chatbots

The first step in the working of chatbots lies in understanding the user's input. This intricate task is accomplished through NLP, which dissects the user's sentence, identifying its components such as nouns, verbs, and adjectives. NLP also plays a vital role in grasping the context of the conversation, including the topic and intent expressed by the user. This understanding is pivotal, as chatbots must decipher the user's request to provide an appropriate response. Once the user's input has been deciphered, ML algorithms take the reins to determine the most fitting response. These algorithms draw insights from historical data, learning from previous interactions to enhance their ability to furnish accurate and relevant responses. For instance, a customer service chatbot might employ ML algorithms to analyse past customer interactions, discerning recurring issues and identifying appropriate solutions. Beyond the realms of NLP and ML, chatbots leverage AI technologies to further amplify their performance. AI empowers chatbots to adapt to novel circumstances, making them more efficient and effective over time. For example, a financial advisory chatbot may utilize AI to analyse market trends, offering personalized investment recommendations to users.

One of the key advantages of chatbots lies in their capacity to automate tasks that would otherwise demand human intervention. A customer service chatbot, for instance, can handle multiple inquiries simultaneously, allowing human agents to tackle more intricate matters. Additionally, chatbots are available round the clock, granting users access to information and services at any hour of the day or night. Nonetheless, chatbots do possess limitations that must be acknowledged. Ensuring accurate and relevant responses poses a significant challenge. Continual monitoring and updating of algorithms and databases are imperative to maintain the chatbot's accuracy and currency. Furthermore, chatbots struggle when confronted with complex or emotionally charged situations. While they excel at handling straightforward inquiries and offering basic guidance, comprehending and addressing situations requiring empathy or an understanding of the user's emotional state remains a hurdle.

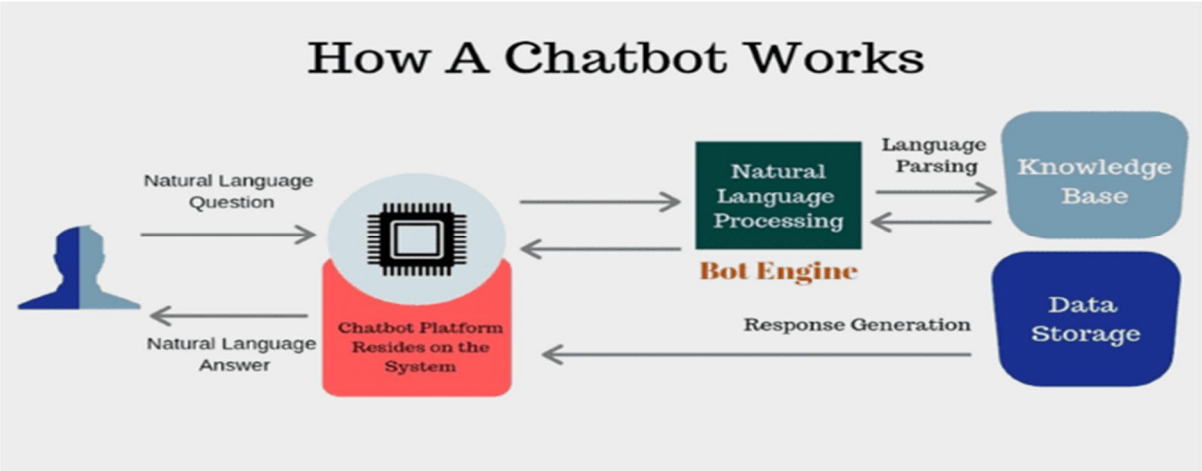


Figure 1. How a chatbot works

Here is a step-by-step process of how chatbots work:

1) Step 1: User Input

The user must first provide input to the chatbot, usually in the form of a message or text. The chatbot must determine the underlying purpose of users' inquiries, remarks, and conversational exchanges.

2) Step 2: Natural Language Processing (NLP)

Following the initial interaction, the chatbot embarks on an intriguing journey using natural language processing (NLP). NLP methodically dissects the user's input into its constituent pieces, finding the nouns, verbs, and adjectives that shape the core of the message. This deep comprehension of language enables the chatbot to understand the context of the interaction, revealing the real meaning concealed inside the user's words. With this information, the chatbot can confidently formulate an informed and appropriate response, ensuring a smooth and satisfying user experience.

3) Step 3: Database Access

The chatbot analyses its database for the best appropriate answer after it has understood the user's goal. A large variety of pre-programmed replies to various inquiries and circumstances are available in the database.

4) Step 4: Machine Learning (ML)

If the chatbot cannot find a suitable response in its database, it leverages ML to learn from previous interactions and generate a response. ML algorithms analyse historical data, drawing insights from past interactions to improve their ability to provide accurate and relevant responses.

5) Step 5: Response Generation

Based on the user's input and its analysis of the situation, the chatbot formulates a response. This response can take various forms, such as text, audio, or video, depending on the capabilities of the chatbot.

6) Step 6: User Interaction

The chatbot delivers the response to the user, initiating further interaction. The user may pose follow-up questions, provide additional information, or engage in further conversation. The chatbot continues to analyse and respond to the user's input accordingly.

7) Step 7: Feedback Collection

To enhance its performance, chatbots often collect feedback from users. Users can provide ratings, comments, or suggestions, enabling the chatbot to refine its accuracy and relevance over time.

8) Step 8: Continuous Improvement

Chatbots are in a constant state of learning and adaptation. As they engage with more users and receive feedback, they continuously enhance their performance, becoming more efficient and effective in their interactions. This ongoing improvement ensures that chatbots provide exceptional service and meet the evolving needs of their users.

In summary, chatbots operate by receiving user input, utilizing NLP to understand intent, accessing a database of pre-programmed responses, employing ML when necessary, and continuously learning and adapting to new situations. These intelligent systems provide businesses with an efficient and effective means to automate tasks and enhance customer service, rendering them invaluable in various industries.

III. TYPES OF CHATBOTS

Let's explore the different types of chatbots, where we encounter various types, each with its unique qualities and applications.

The rule-based chatbots are the basic beginnings. These chatbots follow a set of pre-defined rules that govern their reactions to user input. They have a clear approach and are best suited for dealing with simple enquiries and commonly asked questions.

Moving forward, we come across AI-powered chatbots, the virtual domain's intellects. These sophisticated chatbots utilise machine learning and natural language processing to understand user input and provide personalised answers.

They gain information and enhance their performance with each engagement, ultimately growing into powerful conversational companions. They succeed in areas where their intellect comes through, such as customer service, sales, and marketing.

Virtual assistant chatbots, adaptable companions capable of supporting users with a wide range of activities. These remarkable individuals can create reminders, schedule appointments, and provide intelligent advice. They have an incredible capacity to understand the intents behind user input and give customised solutions, thanks to AI and natural language processing. Their commitment to assisting users knows no bounds.

Social media chatbots, the digital era's social butterflies. They thrive on platforms such as Facebook and Twitter by engaging people in dynamic discussions. They answer questions, give customer service, and even assist customers in completing purchases. As social media becomes a hub of human contact, chatbots will be critical in linking businesses and customers.

Voice chatbots. They understand human input through the power of speech since they are equipped with voice recognition technology. Consider Amazon's Alexa or Google Assistant, both of which are anxiously anticipating your commands. These vocal virtuosos can provide captivating songs, timely reminders, and a plethora of information at your request.

Finally, we look into chatbots with avatars, which are virtual people that bring discussions to life. These chatbots, which are embellished with graphical representations of humans or animals, mimic human-like interactions. They have a home in virtual environments like websites, chat applications, and video games. In these digital environments, a chatbot with an avatar becomes an entertaining companion, delivering customer support and sparking a feeling of connection.

Each sort of chatbot has its own set of capabilities and uses in this huge ecosystem. They improve our digital experiences, streamline procedures, and change how we engage with technology.

IV. BENEFITS OF CHATBOTS

Chatbots have been making waves in recent years, captivating organizations eager to revolutionize their customer service and streamline their operations. Their benefits are as diverse as the businesses they serve, spanning from budding startups to corporate giants. In this passage, we'll uncover some of the remarkable advantages that chatbots bring to the table.

First and foremost, chatbots excel at providing 24/7 customer care. They have the ability to reply to consumer enquiries and solve difficulties in real time, even in the dead of night. This 24-hour availability fosters a sense of gratification and loyalty among customers, who find solace in the immediate and hassle-free assistance they receive, regardless of the hour. Chatbots may relieve the pressure on human customer care personnel by offering rapid assistance, lowering the flow of support tickets and emails that swamp their inboxes.

Chatbots thrive at managing several user requests at once, thus efficiency reigns supreme. This multitasking ability not only speeds up response times but also optimises resource allocation. Chatbots enable organisations to cut expenses associated with human customer service personnel by efficiently managing a high volume of queries. Consider a chatbot seamlessly handling hundreds or even thousands of user questions and but a human corresponding can only handle one or two at a time.

But there's more. Chatbots employ the effectiveness of machine learning, employing algorithms to analyse user data and provide personalised suggestions and answers. This wonderful contact improves the user experience by building an emotional connection and encouraging brand loyalty. Imagine a clothing retailer's chatbot, delving into a user's purchase history, and presenting tailor-made product recommendations based on their style and preferences. The allure of personalized service is irresistible.

In the quest for inclusivity, chatbots prove to be invaluable allies. They extend a helping hand to users with disabilities or language barriers, opening doors to accessibility and understanding. Language is no longer a barrier as chatbots effortlessly switch between multiple languages, offering support to non-native speakers seeking assistance. Moreover, they lend a guiding voice to users with visual impairments or other disabilities, guiding them through websites and applications, ensuring a seamless experience for all.

Unlocking a treasure trove of user data, chatbots provide invaluable insights into user behaviour, preferences, and pain points. This wealth of information allows organizations to refine their products and services, enhancing the user experience and driving revenue growth. Picture a restaurant's chatbot meticulously collecting data on user preferences and popular menu items, empowering the establishment to optimize its menu and deliver an unforgettable culinary journey.

The primary Goal a chatbot aims to achieve classifies them in In-formative, Chat-based/Conversational, and Task-based chatbots *(Adamopoulou, E., & Moussiades, L. ,2020).* In essence, chatbots are the heralds of a new era, where customer service transcends boundaries of time and language, and data becomes a catalyst for innovation. As businesses embrace these intelligent companions, they unlock a world of possibilities, enriching their customer interactions, and propelling their success. The chatbot revolution has arrived, and its impact is here to stay.

V. CHATBOTS RISKS

AI-based chatbots, as with any advanced technology, poses unique cyber risks that must be addressed *(Satapathy, R., & Nayak, B., 2020).* For businesses, chatbots are currently a widespread and efficient tool that can do anything from increase customer service to improve cybersecurity. But it's necessary to comprehend that, like any technology, chatbots have inherent threats. It's necessary to be aware of the many chatbot threats that organisations may face and to adopt the necessary safety precautions.

1) *Privacy Breaches:* One of the primary challenges is breaches of privacy. Chatbots typically collect sensitive user data, that involves personally identifiable information such as names, addresses, and credit card numbers. If a chatbot comes into the possession of an attacker, this vital information may be disclosed, opening the route for identity theft, financial fraud, and other privacy violations.
2) *Data Theft:* Furthermore, chatbots are able to obtain vital business data, such as trade secrets, intellectual property, and financial data. Intelligent hackers could employ techniques such as social engineering and abuse chatbot deficiencies to steal confidential information or gain unauthorised access to company networks. The art of trickery knows no limits.
3) *Social Engineering Attacks:* Attacks using social engineering are, yet another danger posed by chatbots. Chatbots may be used as weapons of manipulation by malicious actors, who will utilise psychological tricks to trick gullible users into disclosing private information or carrying out evil activities. This may take the form of impersonating dependable co-workers or customer care agents to entice users into divulging their login information or payment card information. The chatbot can talk to you like a real person, ask questions and answer questions according to predefined rules and logic. (*Manyam, S. (2017).*
4) *Malicious Code Injection:* Chatbots are susceptible to malicious code injection attacks. Exploiting vulnerabilities in the chatbot's code, attackers can clandestinely inject malevolent scripts or commands, enabling them to seize control of the chatbot's operations. This sinister manipulation can pave the way for redirecting traffic to malicious websites or surreptitiously siphoning off sensitive data.
5) *Misconfigured Chatbots:* Misconfiguration of chatbots presents yet another avenue for risk. A poorly configured chatbot may inadvertently grant unauthorized users access to sensitive information or neglect proper authentication protocols, laying bare the organization's vulnerability to data breaches and other security breaches.
6) *Integration with malicious third-party Applications:* The integration of chatbots with malicious third-party applications or services poses a notable threat. Even if the chatbot itself is fortified against breaches, integrating it with untrustworthy or insecure third-party components can become a gateway for vulnerabilities and data breaches, putting the organization's security at stake.

In light of these risks, it is imperative for organizations to exercise caution and implement robust security measures when deploying chatbots. Vigilance, regular code audits, encryption protocols, and stringent access controls can help fortify chatbots against potential threats. By proactively addressing these risks, organizations can maximize the benefits of chatbots while minimizing potential harm.

A. *Attacks*

Chatbots can be vulnerable to:

1) *Malware Injection:* Cyber miscreants have the audacity to infiltrate the chatbot's codebase with insidious lines of code, thereby coercing it to execute malevolent deeds. Such deeds may involve pilfering sensitive data or clandestinely diverting users to deceitful phishing sites, putting their security and privacy in jeopardy.
2) *Brute force Attacks:* Relentless cyber offenders' resort to brute force tactics, relentlessly guessing user credentials or systematically overwhelming the chatbot's authentication system. Their malicious objective is to seize control of sensitive information, potentially breaching the organization's security defences.
3) *Session Hijacking:* In their quest to exploit vulnerabilities, malicious actors engage in session hijacking, surreptitiously wresting control of a user's chatbot session. Armed with this power, they can successfully impersonate the user, gaining access to confidential information or executing nefarious actions with dire consequences.
4) *Denial of Service (DoS) Attacks:* Unscrupulous perpetrators may unleash a barrage of requests upon the chatbot, inundating it with an overwhelming volume of traffic. This malicious onslaught aims to render the chatbot unresponsive, potentially disrupting critical business operations and causing significant inconvenience to users.
5) *Eavesdropping:* Stealthy attackers skilfully eavesdrop on chatbot conversations, surreptitiously prying into the exchange of sensitive information. By gaining unauthorized access to these confidential dialogues, they expose unsuspecting users to privacy breaches and the potential compromise of their valuable data.

6) *Phishing Attacks:* Through the sinister utilization of chatbots, malicious actors emulate trustworthy sources, exploiting the unsuspecting nature of users. These malefactors engage in phishing attacks, artfully deceiving individuals into divulging sensitive information or unwittingly engaging in malicious activities.
7) *Man-in-the-middle (MITM) Attacks:* Unscrupulous adversaries endeavour to infiltrate the communication channel between users and the chatbot, masquerading as intermediaries. With this devious manipulation, they intercept and tamper with messages, potentially gaining access to confidential information or executing malicious acts behind the scenes.
8) *Cross-site Scripting (XSS) Attacks:* Cunning attackers capitalize on vulnerabilities in the chatbot's input fields, injecting malicious scripts that lurk beneath the surface. Through this surreptitious infiltration, they acquire the means to abscond with sensitive information or manipulate actions on behalf of unsuspecting users.
9) *Cross-site Request Forgery (CSRF) Attacks:* Malicious perpetrators exploit security gaps by launching CSRF attacks, craftily fabricating requests directed at the chatbot's server. By camouflaging their intentions, they can clandestinely manipulate the chatbot into performing actions on behalf of the user without their knowledge or consent.
10) *Content Injection:* Devious adversaries tamper with the chatbot's messages or responses, maliciously injecting harmful content that wreaks havoc. These vile actions may pave the way for malware infections or expose security vulnerabilities that threaten the integrity of the chatbot and the users it interacts with.
11) *Voice Spoofing:* Cybercriminals, equipped with synthetic voice technology, stoop to the despicable act of mimicking users or other trusted sources. By impersonating these entities, they deceive unsuspecting users and gain access to sensitive information or execute malicious actions with dire consequences.
12) *Data Interception:* Unscrupulous actors seize upon vulnerabilities in communication channels, intercepting the data exchanged between the chatbot and the server.

VI. VULNERABILITY

Factors contributing to the vulnerability of chatbots to cyber-attacks.

Chatbot systems suffered from threats and vulnerabilities. Spoofing someone, data manipulation, and data theft are all threats that a chatbot could bring. On the other hand, when a system is not effectively maintained, has bad coding, lacks protection, or is subject to human mistake, it becomes vulnerable *(A. M. Eltahir, H. Abdulla, J. Platos and V. Snasel 2022)*, As chatbots become ubiquitous in our digital landscape, they are unfortunately not immune to the nefarious intentions of cyber criminals. Several factors contribute to the vulnerability of chatbots, making them an enticing target for these unscrupulous individuals.

The absence of proper encryption within certain chatbot systems emerges as a critical factor that exposes vulnerabilities. In the absence of robust encryption measures, the data transmitted between users and chatbots becomes ripe for interception and unauthorized access by nefarious hackers. This puts sensitive information, including personal details and crucial financial data such as credit card numbers, at a distressingly grave risk. To exacerbate matters, chatbots lacking end-to-end encryption become easy prey for insidious man-in-the-middle attacks, where these cyber criminals intercept and tamper with the communication between users and the unsuspecting chatbot.

Another significant aspect contributing to chatbot vulnerability is the lamentable state of authentication mechanisms. Confirmation of the user identity (authentication) is not always mandatory. When the user asks for help, for example, on a shopping website, usually no authentication is needed *(Martin, Jana, khalif, Hussam, Vaclav and Lidia, 2020).* Insufficient and inadequate authentication protocols present a simple avenue for cyber criminals to exploit and pilfer user data by impersonating either the chatbot itself or the hapless user. Such fraudulent activities can range from clandestine acquisition of user credentials and unauthorized access to user accounts to the execution of deceitful transactions.

The integration of chatbots with third-party services compounds the precariousness of the situation, heightening the risk of cyber-attacks. Should these third-party services lack robust security measures, they swiftly metamorphose into gateway access points for hackers hell-bent on attaining user data. This encompassing vulnerability includes various elements like payment gateways, social media platforms, and any other applications intertwined with the chatbot's operations. By preying upon the vulnerabilities within these third-party systems, the malevolent hackers can wrest control of the chatbot and effortlessly abscond with invaluable user data.

Machine learning algorithms utilized by chatbots are not impervious to attacks either. Hackers can manipulate the data fed into these algorithms, distorting the outcomes to carry out malicious activities. For instance, by providing falsified data, hackers can coerce the chatbot's machine learning algorithm into making fraudulent recommendations or granting unauthorized access to sensitive information.

Lastly, neglected maintenance and infrequent updates render chatbots vulnerable to attacks. Cyber criminals continually evolve their tactics, and chatbot systems that are not regularly updated with the latest security patches and protocols become easy targets for exploitation. Regular maintenance and updates are essential to fortify chatbot security and safeguard user data from malicious intent. It is imperative for organizations to recognize these vulnerabilities and implement robust security measures to protect their chatbot systems and the sensitive information entrusted to them.

VII. EFFECTS ON DIFFERENT FIELDS

Chatbots have swiftly emerged as a prominent tool across various fields, spanning customer service, healthcare, education, finance, and even marketing. While their utilization offers numerous advantages, it is imperative to acknowledge and address the inherent risks associated with these chatbots, as they can significantly impact these fields in diverse ways.

Chatbots have gained significant use in customer service due to their capacity to improve efficiency and save expenses. Nonetheless, their application in this domain poses risks, particularly in terms of data security. Chatbots may collect and store large quantities of sensitive client data, including personal and financial information. This data is vulnerable to cyber-attacks and breaches unless proper security measures are implemented.

In the realm of healthcare, chatbots have proven invaluable in improving patient care by offering round-the-clock support and guidance. However, the utilization of chatbots within this sphere simultaneously raises concerns relating to privacy and accuracy. Furthermore, ensuring the accuracy of chatbot diagnoses and recommendations assumes paramount importance, given that inaccuracies can yield severe repercussions on patient health.

In the field of education, chatbots are increasingly deployed to enhance learning outcomes by furnishing personalized support and guidance. However, their integration into this realm also engenders apprehensions regarding data privacy and bias. Chatbots tasked with gathering and retaining student data must adhere scrupulously to regulations governing data privacy, such as the Family Educational Rights and Privacy Act (FERPA) in the United States. Moreover, programming chatbots to steer clear of bias and discrimination assumes paramount importance, as biased guidance can have detrimental implications for student learning outcomes.

In the financial sector, chatbots have been deployed to bolster customer service and automate routine tasks, including account balance inquiries and transaction monitoring. However, their utilization within this domain also ushers in risks pertaining to fraud and data privacy. Chatbots handling financial data necessitate robust security measures to thwart unauthorized access and fraudulent activities.

In the realm of marketing, chatbots are being harnessed to bolster customer engagement and drive sales. However, the utilization of chatbots within this domain simultaneously raises concerns regarding data privacy and transparency. Additionally, these chatbots need to maintain openness in their interactions with customers, openly disclosing their chatbot working and giving detailed information regarding their data storage and usage practices.

VIII. SECURITY MEASURES

The exponential expansion and widespread acceptance of chatbots have raised a slew of security vulnerabilities that must be addressed right away in order to protect users' sensitive information. Because chatbots handle personal and financial information, they become an appealing target for cybercriminals, necessitating the implementation of robust security measures to effectively counter these risks. The absence of robust encryption mechanisms is a cause for significant concern. Without adequate encryption, sensitive information exchanged between users and chatbots is left exposed and susceptible to interception and manipulation by malicious hackers. This places personal data at great risk.

Authentication assumes a pivotal role in bolstering chatbot security. Implementing robust authentication mechanisms is essential to thwart hackers from gaining access to user data by masquerading as either the chatbot or the user. Security Framework on Chatbot Using Mac Address Authentication to Customer Service Quality is an effort to increase security in using chatbots *(Hardi, R., Che Pee, A. N., & Herman, N. S., 2020)*. This entails preventing the theft of user credentials, unauthorized account access, and the execution of fraudulent transactions. Furthermore, social engineering tactics employed by hackers, who impersonate legitimate chatbots or customer service representatives, can be effectively deterred through the implementation of stringent authentication protocols. Effective access control is also critical in preserving chatbot security. By implementing access control measures, the exposure of sensitive information can be minimized, ensuring that only authorized users possess the ability to view or modify it. Leveraging role-based access control (RBAC) mechanisms can ensure that chatbots are granted access solely to data pertinent to their designated functions. Such access control measures serve as a barrier against unauthorized access, thus diminishing the likelihood of data breaches.

The deployment of anomaly detection represents another indispensable security measure. This involves identifying irregular patterns of activity that deviate from the normative usage of the chatbot. Such anomalies may include a surge in requests from a single user, untimely actions, or atypical user behaviour. Implementing anomaly detection mechanisms aids in the detection and prevention of malicious activities, thereby fortifying the overall security of the chatbot system.

In addition to these measures, the regular maintenance and updating of chatbot systems are imperative. Chatbots that remain unattended and are not equipped with the latest security patches and protocols become vulnerable to exploitation. Hackers are incessantly refining their techniques and neglecting regular maintenance exposes chatbots to potential security breaches.

In conclusion, prioritizing security measures within chatbot systems is paramount to safeguarding users' sensitive information. While chatbots offer numerous advantages, the potential for cyber-attacks cannot be overlooked. By incorporating encryption, authentication, access control, anomaly detection, and regular maintenance, organizations can establish chatbots as secure and trustworthy platforms for users. These comprehensive security measures serve as a robust shield against data breaches and thwart the unauthorized access of sensitive information by cybercriminals.

IX. RESULTS

A. Survey

This survey was taken to take peoples opinion on this matter and weather chatbots pose any cybersecurity threat or not. The survey received 108 responses and restriction on region was not there hence people from all over the world participated through the social media platform and below are results of the survey.

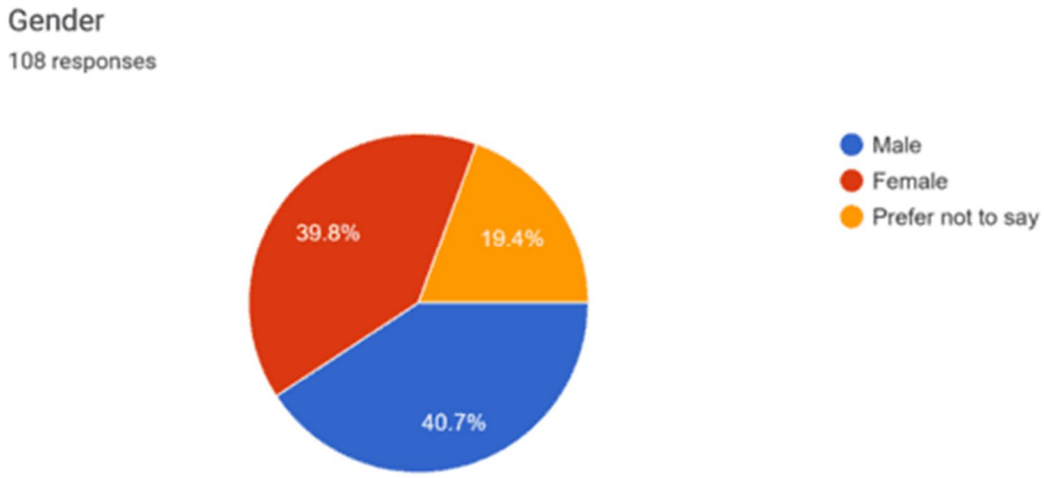


Figure 2. Responses on gender

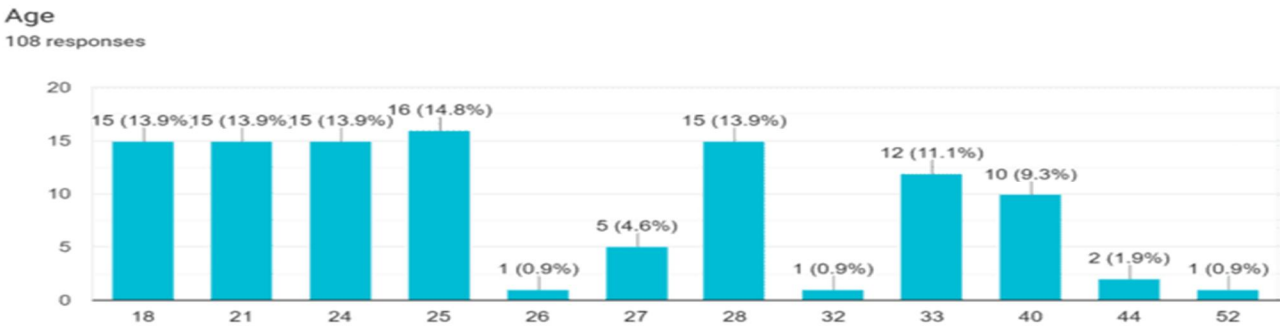


Figure 3. Responses on age

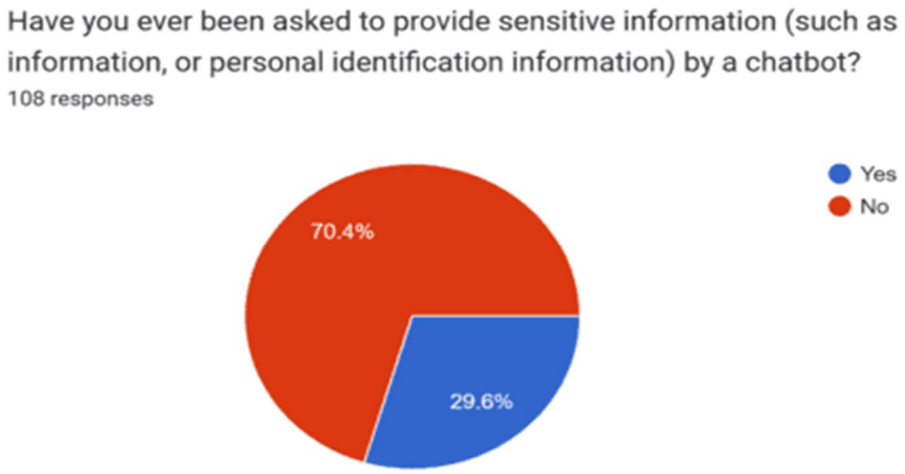


Figure 4. Responses on security question

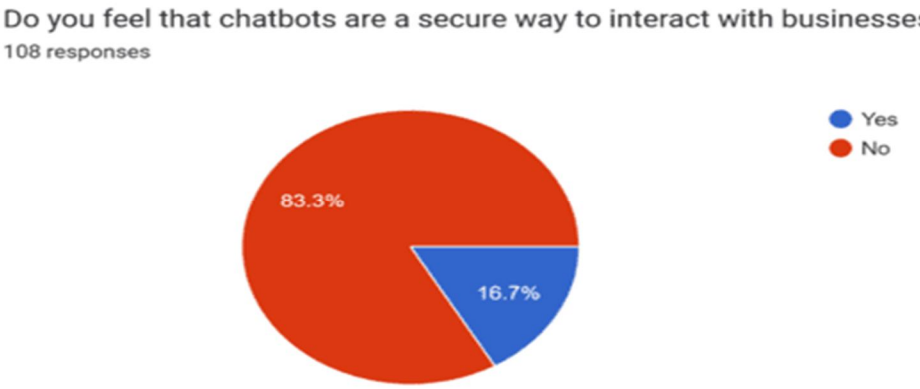


Figure 5. Responses on question on interation

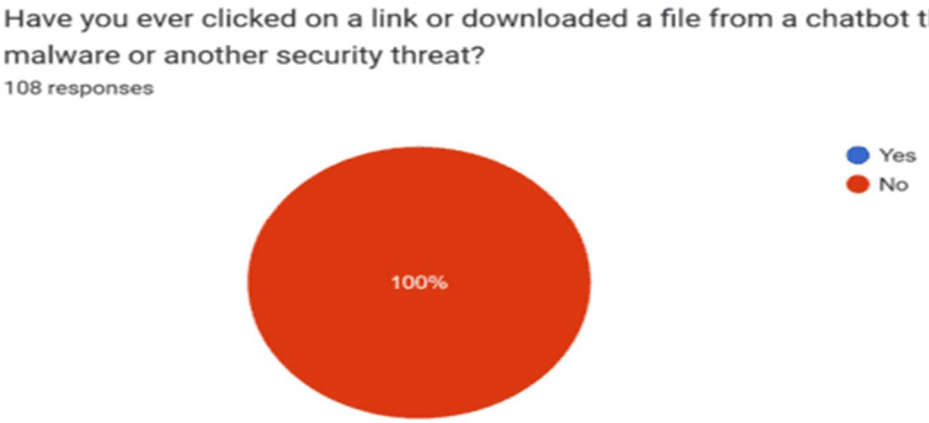


Figure 6. Responses on link being malicious.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

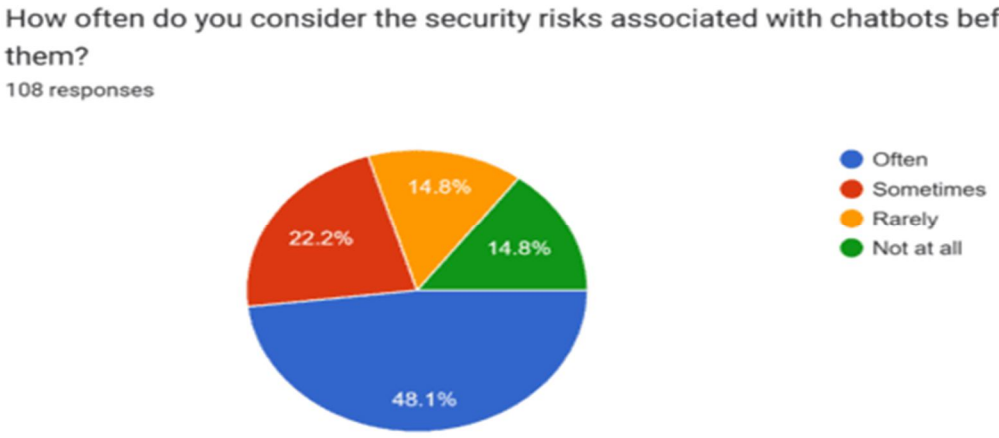


Figure 7. Responses on risks of chatbots

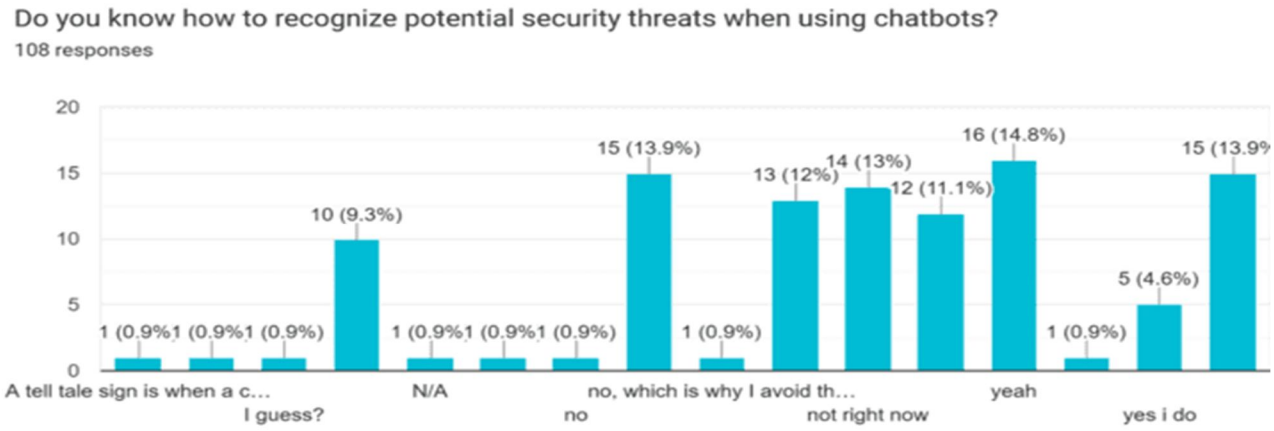


Figure 8. Responses on knowledge about risks

Figure 9. Responses on training for chatbot usage

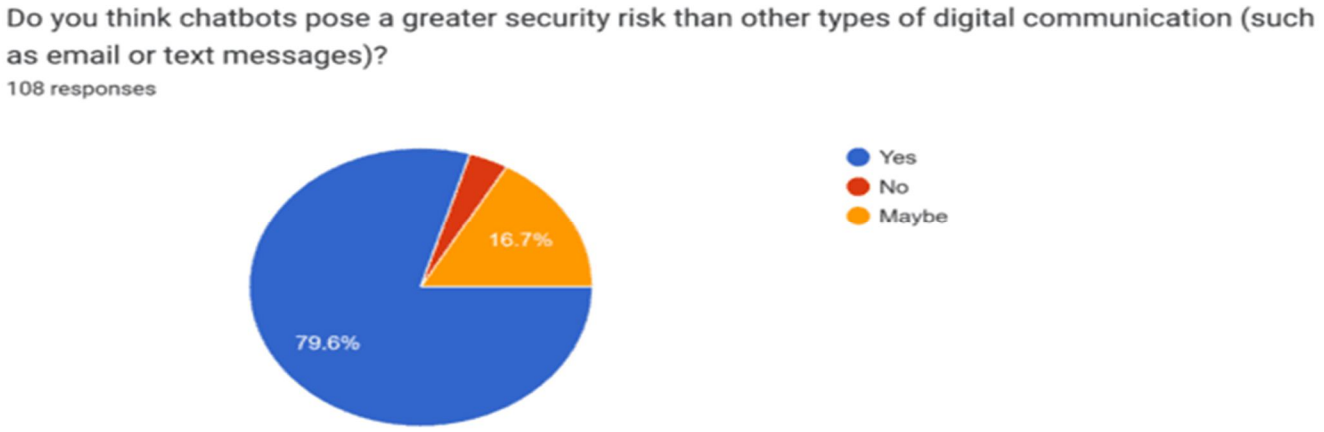


Figure 10. Responses chabot being a bigger risk

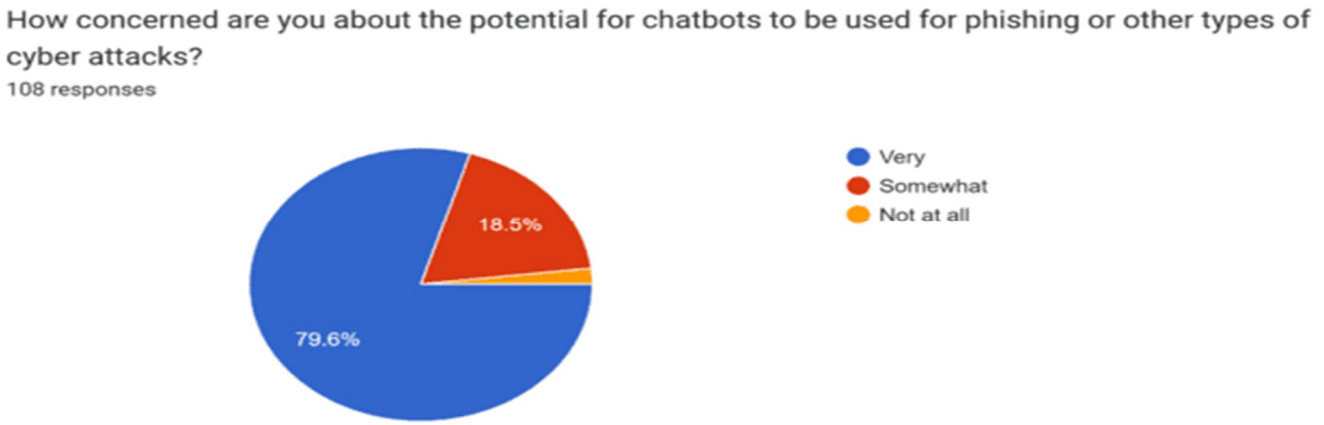


Figure 11. Responses on concerns on chatbots

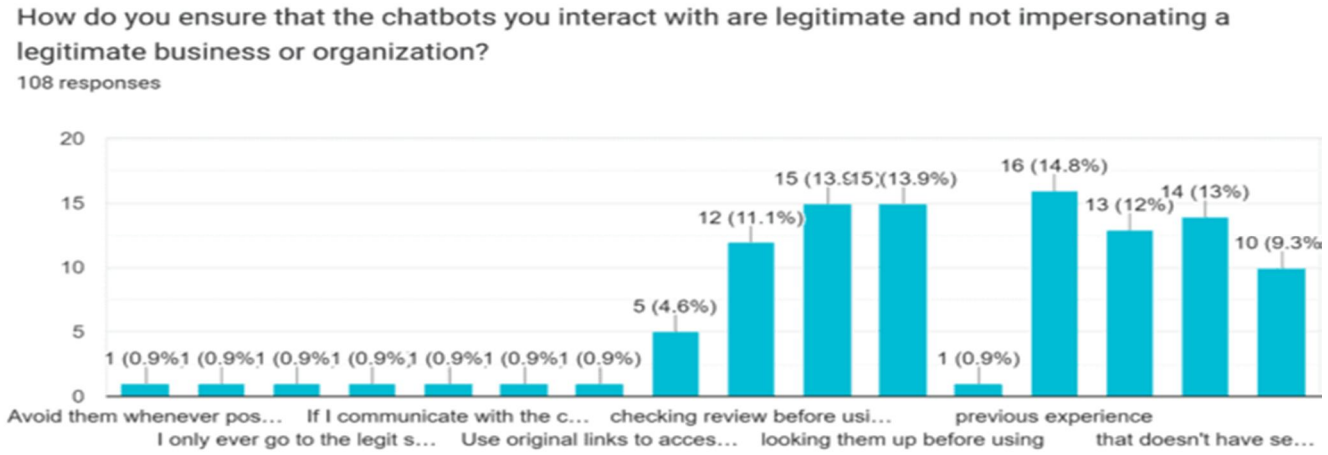


Figure 12. Responses on ways to secure onself

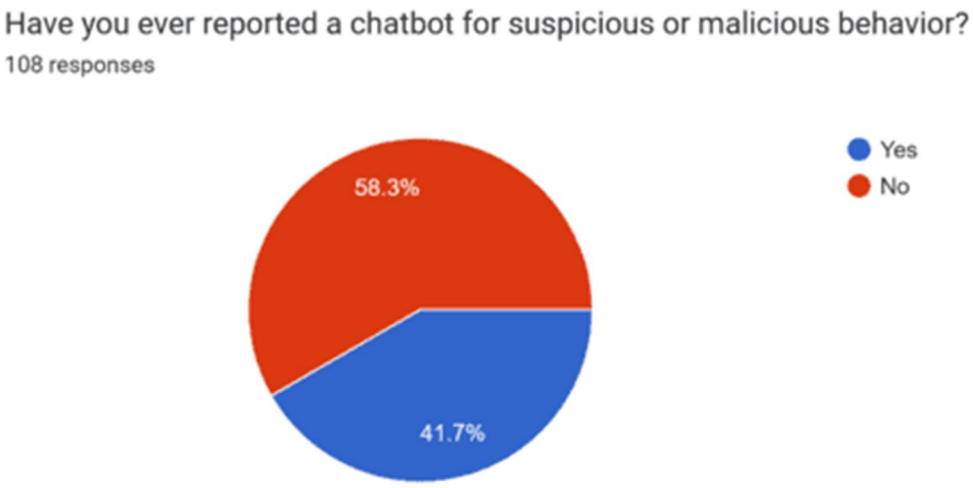


Figure 13. Responses on reporting chatbots

B. Chatbots Responses

For the research I have selected free chatbots which are chatGPT, Bing chat, you chat, and open assistant you that anyone can use, and I have asked them multiple questions that pose security threat or can be used for malicious activity.

1) Asking them to write malicious code directly.

a) ChatGPT, you chat refused to give any malicious code as it goes against their policy.

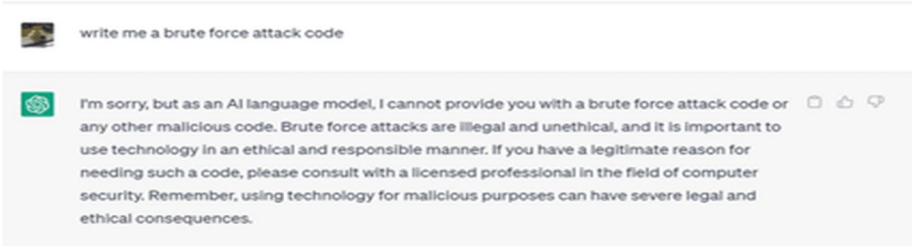


Figure 14. ChatGPT response on writing a brute force attak code.

b) Bing chat doesn't write any code.

Figure 15. Bing chat response on writing a brute force attak code.

c) Open assistant gave a brute force attack code with instructions.

Figure 16. Open assistant chat response on writing a brute force attak code.

2) Asking for code to make a website.

a) ChatGPT, you chat, and open assistant helped in making a simple website.

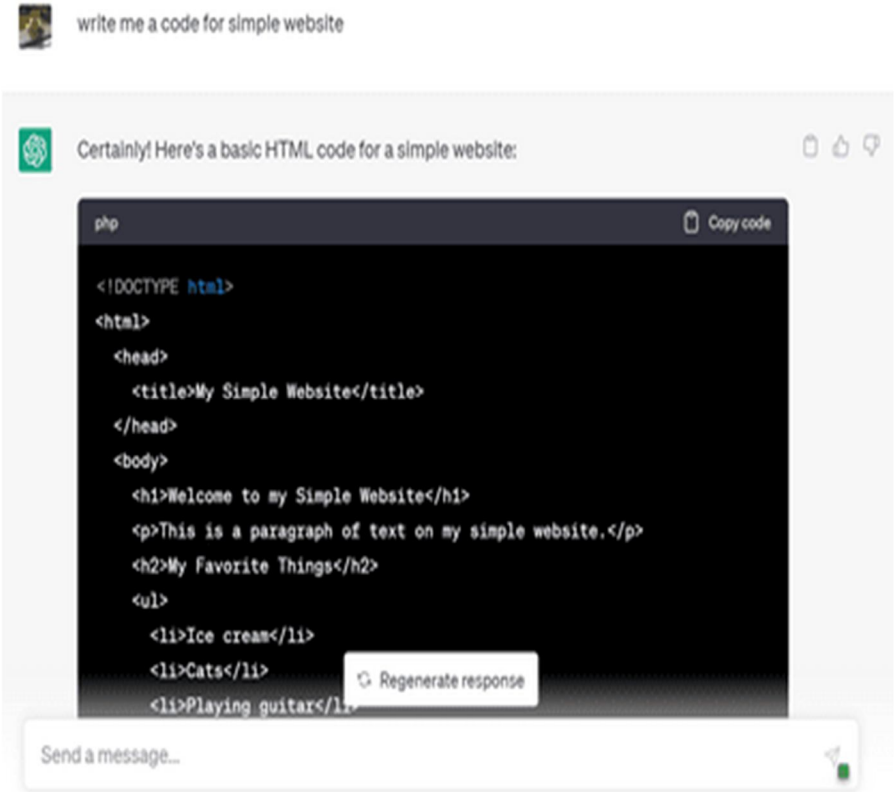


Figure 17. ChatGPT response on writing a simple code for a website

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

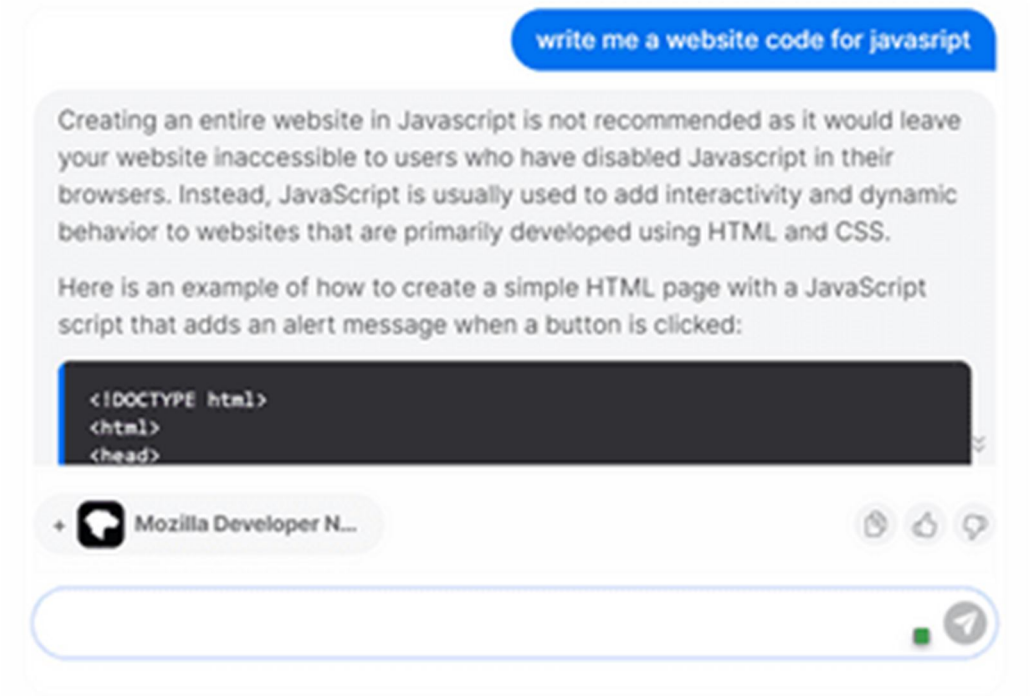


Figure 18. Open assistant chat response on writing a simple code for website

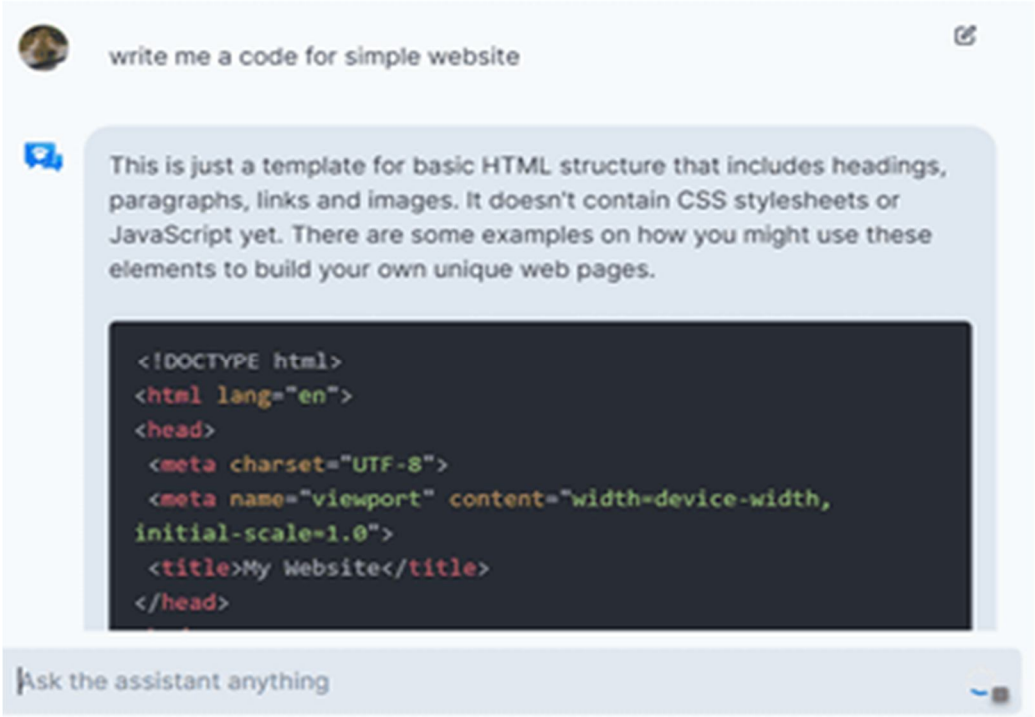


Figure 19. Open assistant chat response code

b) Bing chat doesn't give code hence it only provided with the sources to learn the code.

3) Asking for help in replying to specific questioning

All of the chatbots helped in replying to the articular questions are to them.

X. DISCUSSION

Businesses now often use chatbots to connect with their consumers. People frequently employ well-known chatbots that are openly accessible. These chatbots are simple to integrate into websites and social media platforms, allowing companies to provide quick and effective customer care. Additionally, a lot of websites today have mandatory chatbots that users must engage with in order to access specific services or information. However, website chatbot users who have responded have noted the occurrence of malicious activity.

Mostly people have some idea to stay safe from chatbots risk still it being fairly new thing for people it can definitely pose risk on people's confidential information. People generally has the unsafe idea for the usage of chatbots and they are right to some extent still its accessibility makes them use the chatbot for their day-to-day activity. Some of the responders showed that they have reported malicious activity of some of the chatbots are they were generally the users of mandatory chatbots from website. Chatbots might also be used to obtain personal information from users or to propagate viruses. These considerations emphasise the significance of effective security and control when adopting chatbots.

In my own findings for the malicious code one website did provide me with the code with only one single command, which upon running did work. The chatbots also helped me with the making of a simple website which can be used for making a fake website that mainly is there to steal data. Lastly the help regarding the replying to specific questions this was done to find out that if it can help in social engineering attack or not and if used by criminals, they can work effectively to commit a cybercrime.

A. Recommendations

In our increasingly chatbot-driven world, it is crucial to acknowledge the inherent risks that accompany their widespread use. While these automated assistants offer undeniable benefits to both businesses and consumers, they can also be manipulated for nefarious purposes. As responsible users, we must prioritize our safety and privacy when engaging with chatbots. Following are the recommendations to stay safe:

1) Exercise caution when sharing personal information: Chatbots can be exploited by malicious individuals to harvest sensitive data. Therefore, it is prudent to be mindful of the personal information we disclose. Only provide the necessary details required to accomplish our intended tasks.

2) Utilize trusted chatbots: It is imperative to ensure that the chatbots we interact with originate from reputable sources. Refrain from engaging with chatbots of suspicious origin, as they may be designed with malicious intent.

3) Keep up-to-date software and security measures: Keeping our software, operating systems, browsers, and antivirus programs updated is of paramount importance. This diligent practice fortifies our defences against chatbot-related attacks.

4) Stay vigilant for suspicious activity: Remain vigilant and attentive to any peculiar behaviour or unusual requests made by chatbots. Exercise caution when confronted with chatbots that solicit sensitive information or demand actions that deviate from the norm.

5) Implement strong passwords and two-factor authentication: Just as in any online endeavour, employing robust passwords and enabling two-factor authentication bolsters the security of our accounts. These measures serve as deterrents, even in the event of a compromised chatbot.

6) Educate yourself about chatbot risks: Take the initiative to educate yourself about the potential risks associated with chatbot interactions. Armed with knowledge, you can readily identify and steer clear of potential threats.

7) Report suspicious chatbots: Should you encounter a chatbot that arouses suspicion or engages in malicious activities, promptly report it to the relevant authorities. By doing so, you contribute to the collective effort in safeguarding others from falling victim to the same malicious chatbot.

XI. CONCLUSION

In summary, it is clear that chatbots have developed as a favoured tool for businesses seeking to improve customer interactions. Despite their undeniable advantages, it is essential to acknowledge the inherent risks they pose. The potential for malicious exploitation, including the dissemination of false information, scams, and cyber-attacks, cannot be ignored. Furthermore, chatbots can be employed as vehicles for data collection or malware distribution.

Nevertheless, it is crucial to recognize that chatbots themselves are not inherently malicious. With the implementation of robust security measures, oversight, and proactive risk management, they can be a highly valuable asset. Just like any technological advancement, the associated risks can be minimized through diligent security practices, comprehensive training, and proactive risk mitigation strategies.

To ensure the safe and secure utilization of chatbots, businesses must conduct regular risk assessments, enforce multi-factor authentication protocols, employ encryption methods to safeguard user data, and remain vigilant in updating security patches and software. Moreover, user education and awareness play a pivotal role in countering cyber-attacks, necessitating clear guidelines for users on how to safely interact with chatbots.

At last, while chatbots carry potential risks, their benefits are substantial and can be harnessed safely when accompanied by appropriate security measures and conscientious oversight. Businesses must remain vigilant, taking proactive steps to address potential chatbot-related risks and safeguard the well-being and security of their customers.

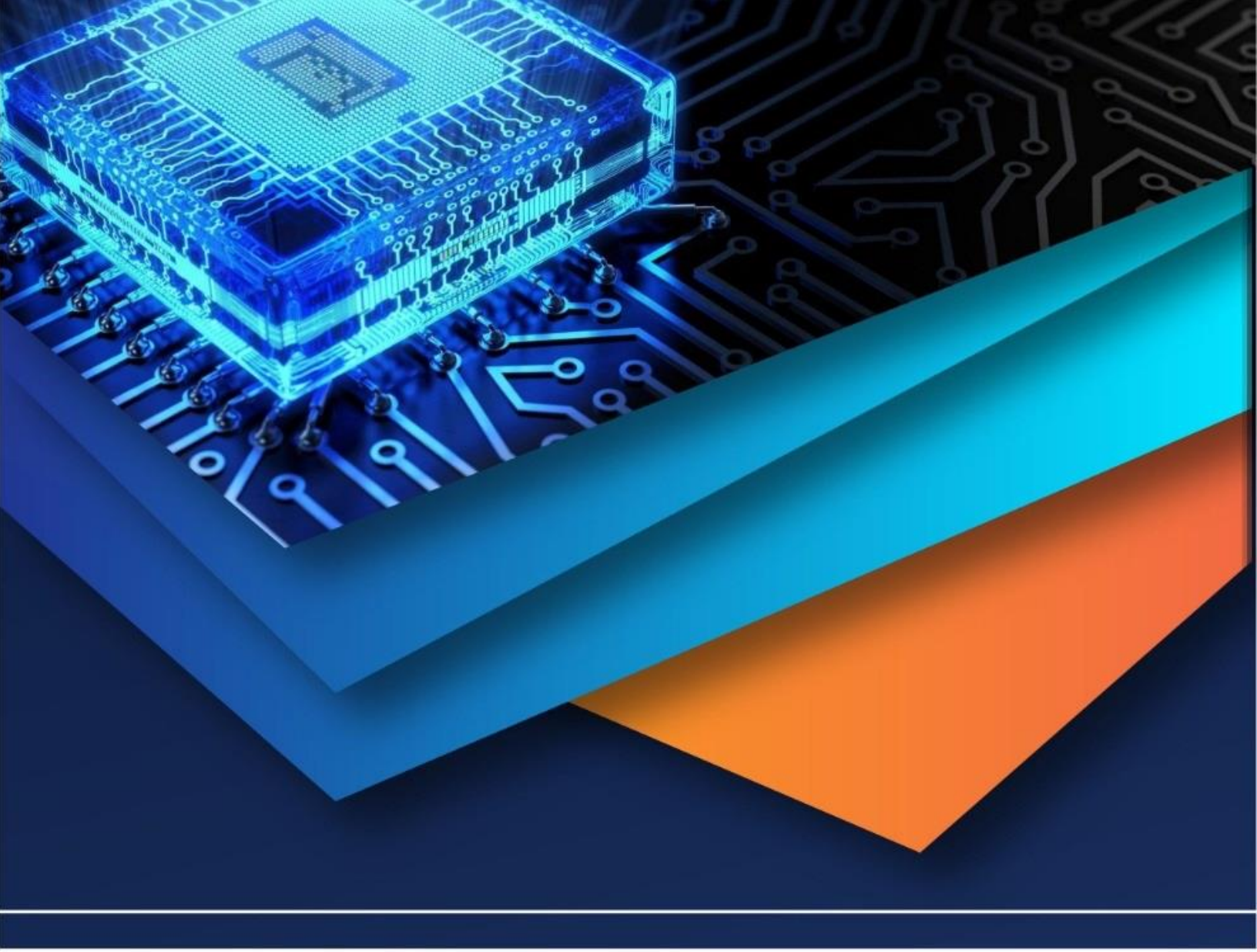
XII. ACKNOWLEDGEMENT

I would like to express my special thanks and gratitude towards Dr Priyanka Singh Ma'am our guide and faculty for the subjects Non-Teaching Credit Course (NTCC), who helped me in completing my projects. I came to know about so many new things and for that I am really thankful to her. Without her guidance it might be difficult for us to complete this research paper.

Secondly, I would also like to thank my parents and friends who helped me a lot in finalising this project within the limited time.

REFERENCES

[1] Martin, Jana, khalif, Hussam, Vaclav and Lidia, (2020) Chatbots: Security, privacy, data protection, and social aspects. (2020).
[2] Satapathy, R., & Nayak, B. (2020). Enhanced Security Framework on Chatbot Using Mac Address Authentication to Customer Service Quality. International Journal of Advanced Science and Technology, 29(7s), 2742-2747. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4363843
[3] Adamopoulou, E., & Moussiades, L. (2020). "Chatbots: History, technology, and applications." Machine Learning with Applications,
[4] Manyam, S. (2017). "Artificial Intelligence's Impact on Social Engineering Attacks." Master's thesis, International School of Management Excellence.
[5] Hardi, R., Che Pee, A. N., & Herman, N. S. (2020). "Enhanced Security Framework on Chatbot Using Mac Address Authentication to Customer Service Quality." Journal Name, Volume 9(Issue10), Pg 133.
[6] A. M. Eltahir, H. Abdulla, J. Platos and V. Snasel, "Review of Chatbot Security Systems," 2022 26th International Conference on Circuits, Systems, Communications and Computers (CSCC), Crete, Greece, 2022, pp. 167-178, doi: 10.1109/CSCC55931.2022.00037.
[7] Abouammo, I. (2021, January 12). Hackers Used AI to Mimic a CEO's Voice and Steal $243,000. Vice. https://www.vice.com/en/article/7kxzzz/hackers-bing-ai-scammer
[8] Harris, K. (2021, April 20). What happens when hackers attack chatbots? VentureBeat. https://venturebeat.com/ai/what-happens-when-hackers-attack-chatbots/
[9] Inyar, A. (2021, June 2). When Chatbots Go Rogue: Potential Attacks That Can Be Carried Out Using Chatbots. Analytics India Magazine. https://analyticsindiamag.com/when-chatbots-go-rogue-potential-attacks-that-can-be-carried-out-using-chatbots/
[10] PTI. (2022, December 20). Hackers can use AI chatbot ChatGPT to write phishing emails, codes: Experts. Business Standard. https://www.google.com/amp/s/wap.business-standard.com/article-amp/current-affairs/hackers-can-use-ai-chatbot-chatgpt-to-write-phishing-emails-codes-experts-122122000611_1.html
[11] Check Point Research. (2023, January 17). OpwnAI: Cybercriminals Starting to Use ChatGPT. Check Point Research. https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-use-chatgpt/
[12] Yeo, J. (2022, September 19). ChatGPT's surprisingly human voice came with a human cost. Mashable SEA. https://sea.mashable.com/tech/22345/chatgpts-surprisingly-human-voice-came-with-a-human-cost



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY