IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Role of Neural Networks and Cookies using AI in Data Privacy policies

Janak Limbachia
Dept of Artificial Intelligence & Data Science
KJSIEIT, Sion
Mumbai, India

Heet Kalaria
Dept of Artificial Intelligence & Data Science
KJSIEIT, Sion
Mumbai, India

Dr. Vaishali Wadhe
Dept of Artificial Intelligence & Data Science
KJSIEIT, Sion
Mumbai, India

Bhavik Sachani
Dept of Artificial Intelligence & Data Science
KJSIEIT, Sion
Mumbai, India

***Abstract*—This research paper is all about the manipulation of privacy policies performed by the leading tech companies and the technology used in it viz. cookies and neural networks using AI.**

Keywords—manipulation, privacy, cookies, neural networks, AI.

I. INTRODUCTION TO COOKIES

An http cookie[4] is a component of a data transaction that occurs between a server and a user's web browser. The user's browser receives it from the server, and after the necessary request has been satisfied, the browser sends it back to the server with any additional information. The internet era's essential component, http cookies, makes user privacy vulnerable. HTTP cookies permits browser to access your most recent login information, your shopping cart, your most recent searches, and more are all remembered by online browsers and websites.

The following are the cookies' three primary uses:[8]

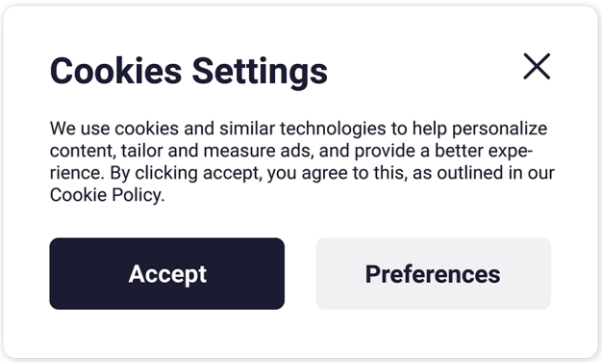
1) Session Management: The ultimate responsibility is whenever a user is exploring or reviewing specific online shops, the purpose of the cookies is to record the user's.
2) Customization: Using CSS, JavaScript, React, and NodeJS, a user can now modify a webpage or in accordance with his or her preferences of theme selection and specification, the cookies store user interest data that is individually tailored.
3) Tracking: Currently, random internet browsing is not completely random because we utilise the internet merely for browsing purposes, but also to quell our curiosity about specific issues. In these circumstances, cookies track the online activities of the user and monitor the consumer identity.

Initially, cookies were only used for user-side (client-side) storage, but recently, they began taking up an increasing amount of data on the user's device, particularly on mobile devices, as (*localstorage*), and (*sessionstorage*)

II. WHAT ARE COOKIES?

Cookies are merely tiny text files which include bits of information like usernames, passwords, and other credentials for logging in that are used to find your IP address or the location of your computer network.

The information kept in the cookie file is made specifically for your computer by the server that is now in use. This unique user ID is then added to the created data.[9]



III. DISTINCT COOKIE TYPES:

1) Magic cookies
2) HTTP Cookies

A. Magic Cookies

A magic cookie[5], or simply cookie, is a token or brief data packet transmitted between interacting programmes in computing. The cookie is frequently used as "handle, transaction ID, or other sign of agreement between cooperating programmes" or to identify a specific event. The phrase is derived from the fortune cookie, a type of cookie that contains a hidden message..

B. HTTPCookies

- HTTP cookies are short data packets created by a web server while a user is accessing a website and stored on the user's computer or other device by the user's web browser. HTTP cookies are also known as web cookies, Internet cookies, browser cookies, or just cookies. A website may store many cookies on a user's device throughout a session. Cookies are stored on the device being used to view the website.

- On the internet, cookies perform useful and occasionally necessary tasks. They allow web servers to track a user's browsing activity (such as clicking specific buttons, checking in, or noting which pages were visited in the user's browser history) or save stateful information (such as products added to the shopping cart in an online store) on the user's device.

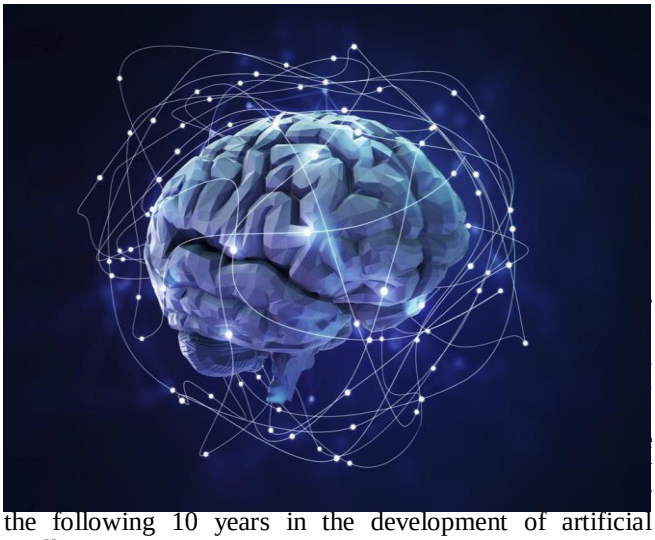
- Additionally, they can be used to store data that users previously provided into form fields, such as names, addresses, passwords, and credit card numbers, for later use.

IV. NEURAL NETWORK

Neural networks,[6] which are a subset of machine learning and are at the core of deep learning algorithms, are also known as artificial neural networks (ANNs) or simulated neural networks (SNNs). Their structure and nomenclature are modelled after the human brain, mimicking the communication between organic neurons.

A node layer of an artificial neural network (ANN) consists of an input layer, one or more hidden layers, and an output layer. Each node, or artificial neuron, is connected to others and has a weight and threshold that go along with it. Any node whose output exceeds the defined threshold value is activated and begins providing data to the network's uppermost layer. If not, no information is transferred to the next tier of the network.

Training data is essential for neural networks to develop and enhance their accuracy over time. However, these learning algorithms become effective tools in computer science and artificial intelligence once they are adjusted for accuracy, enabling us to quickly classify and cluster data. When compared to manual identification by human experts, tasks in speech recognition or picture recognition can be completed in minutes as opposed to hours. Google's search algorithm uses a neural network, one of the most well-known ones.



the following 10 years in the development of artificial intelligence.

The 1980s saw a resurrection in AI thanks to increased funding and the growth of the algorithmic toolbox. Deep learning techniques, developed by John Hopefield and David Rumelhart, let computers gain knowledge via practise. "Expert systems," which resembled human decision-making, were first proposed by Edward Feigenbaum. Despite a lack of government support and media hoopla, AI flourished and several significant objectives were accomplished during the following two decades. Grandmaster and current chess World Champion Gary Kasparov lost to IBM's Deep Blue, a chess-playing computer programme, in 1997. The same year, Windows users could use voice recognition software created by Dragon Systems. In addition, Kismet, a robot that could recognise and express emotions, was created by Cynthia Breazeal. A poker-playing supercomputer named Libratus defeated the top human players in 2017 and Google's AlphaGo software defeated Go master Lee Se-dol in 2016.

This were just the starting phase of instances where AI began to dominate humans. The training set of data that humans contributed to different systems served as the beginning of cases when AI started to outpace humans. These same systems also received the small text data saved in the form of cookies, which are utilized to breach users' privacy walls.

VI. REVIEW ON COMPUTING MACHINERY AND INTELLIGENCE

BY *A. M. TURING*

Alan M. Turing, a computer scientist and philosopher, asks the question "Can machines think?" in Computing Machinery and Intelligence. He contends that there is no compelling evidence to support the claim that machines cannot think intelligently like humans and that various approaches can be used to advance machine intelligence.[10]

The "Imitation Game" (p. 1), in which an interrogator tries to tell a machine from a person in order to infer a difference in thinking capacity, can be used to ask the question "Can machines think?" "Digital computers" (p. 3) are machines that play the game and follow fixed instructions without error. Several presumptions concerning digital computers are true: Digital computers are universal machines that can duplicate any machine with discrete, non-continuous states and have an infinite amount of storage. These presumptions are important conceptually because they suggest that just one digital computer has to be designed for each situation.

According to Turing, who takes into account opposing views, human interrogators will not be able to distinguish between computers and humans in the Imitation Game with a probability greater than 70% in 50 years. The claim that

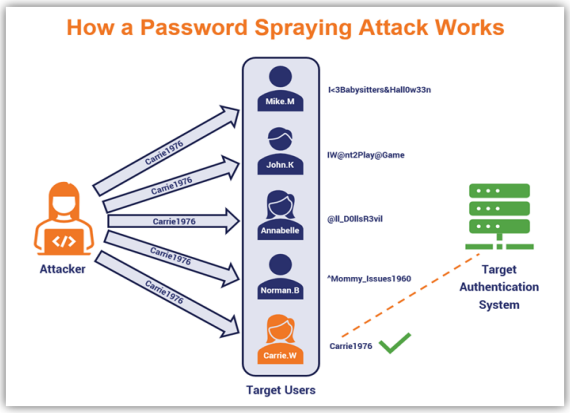
machines cannot think because God has not endowed them with souls is unfounded since an almighty God would have no trouble endowing a soul on a machine. The absence of evidence that humans are not constrained by the same restrictions can be used to refute a mathematical argument that discrete state machines are limited in their ability to provide answers.

The capacity of machines to think may be interpreted as the ability of machines to learn given the evident potential that robots might "learn" (p. 14) based on a "conditioned reflex" (p. By programming a child's brain, which has comparatively few functions, and then influencing it with "education and other experiences," it is possible to recreate the human mind (p.19). Through the use of intelligent teaching techniques, the learning process for improving a machine may be accelerated beyond the rate of evolution. You may use a carrot-and-stick strategy to influence the machine to improve.

Because the laws of a traditional machine don't change, a computer that learns may appear illogical. In the course of learning, rules do alter over time, but these changes are only transitory. The inclination to respond favourably toward predetermined goals is part of the learning process. In the future, it is hoped that machines will be able to compete with humans across all intellectual disciplines, but for the time being, there is still considerable room for investigation and research.

VII. METHODOLOGY

1. With their user ID and password, the user starts a session (usage of online services). These details are kept on the remote server in the form of cookies, which are just little text files. Some firms and tech giants save these text files (cookies) just briefly until the user's session ends; once the session ends, these cookies are removed; nevertheless, some organizations retain some of these text files permanently with the user's location and I. P. address.
2. In addition to the user's sensitive information, the user's session-related actions are also in some way recorded in the form of cookies with the user's preferences. The data kept in such cookies reflects the preferences the user expressed throughout the session.
3. These text files or cookies that certain tech companies keep permanently have now been evolved into training data sets. In order to train their algorithms in line with user preferences and sensitive personal information, neural networks utilize this data collection which are then employed to generate suggestions based on our prior choices.
4. These trained neural networks are a component of well-integrated artificial intelligence systems that use a variety of networks and algorithms. To keep these systems fully stacked with all the information, they all use the same data sets. Now that there are so many algorithms, AI systems employ one in particular called the Brute Force algorithm.[1]
5. **WHAT IS BRUTE FORCE ALGORITHM**?
   Brute Force is an intuitive, direct, and uncomplicated method of problem-solving in which all potential paths or solutions to a particular issue are listed.[2]
   The brute force approach is used to solve many issues in daily life, such as finding the quickest route to a local market by examining all possible routes, arranging the books in a rack to make the most use of the available space, etc.
   Even if optimum algorithms are also conceivable, daily tasks often employ a brute force approach.



6. A brute force assault attempts guesses at encryption keys, login credentials, and hidden web pages through trial and error. Hackers try every combination in the hopes of making an accurate approximation. These assaults are carried out using "brute force," or extreme force, in an effort to "force" their way into your private account (s).
   Although it's an old attack strategy, hackers still choose it because it works. Because it can take anything from a few seconds to several years to crack a password, depending on its length and complexity.[3]
7. The user-id and passwords of the user can be obtained by these hackers if they manage to gain access to the cloud where user preferences and part of their personal information are kept. They can then use these credentials to access private and sensitive data. But what if the organizations themselves access, store and utilize this information under the pretext of privacy policy?

VIII. CONCLUSION

After conducting extensive study on data privacy policies, the usage of cookies, neural networks, and AI, it is clear that in order to combat such scenarios, we must never consent to any cookies or privacy policies without first reading them. If we do so for certain websites that contain sensitive data or involve online transactions, we may then use a VPN to prevent the information of data like user-id, password, and IP address.

IX. ACKNOWLEDGEMNETS

This informational cluster describes how cookies, neural networks, and AI may be used to manipulate data privacy laws. The authors Harsh Mange, Vraj Parekh, Heet Kalaria, Sameera Jathar, Mansi Gohil, Siddharth Tanna, Bhavik Sachani and Janak Limbachia would like to thank our guide **Dr. Vaishali Wadhe** who is Artificial Intelligence professor *at K. J. Somaiya Institute of Engineering & Information Technology, Sion* who was there at every instance to guide us throughout the research.

X. REFERENCES

[1] *Artificial intelligence just made guessing your password a whole lot easier*. (2017, September 15). Science. Retrieved August 8, 2022, from https://www.science.org/content/article/artificial-intelligence-just-made-guessing-your-password-whole-lot-easier

[2] *Brute Force Approach and its pros and cons*. (2021, May 4). GeeksforGeeks. Retrieved August 8, 2022, from https://www.geeksforgeeks.org/brute-force-approach-and-its-pros-and-cons/

[3] *Brute Force Attack: Definition and Examples*. (n.d.). Kaspersky. Retrieved August 8, 2022, from https://www.kaspersky.com/resource-center/definitions/brute-force-attack

[4] *HTTP Cookie*. (2022, July 31). Wikipedia. Retrieved August 5, 2022, from https://en.wikipedia.org/wiki/HTTP_cookie

[5] *Magic Cookie*. (2022, February 18). Wikipedia. Retrieved August 5, 2022, from https://en.wikipedia.org/wiki/Magic_cookie#:~:text=In%20computing%2C%20a%20magic%20cookie,data%20passed%20between%20communicating%20programs.

[6] *Neural Networks*. (2020, August 17). IBM. Retrieved August 6, 2022, from https://ibm.com/cloud/learn/neural-networks#:~:text=Neural%20networks%2C%20also%20known%20as,neurons%20signal%20to%20one%20another.

[7] Turing, A. M. (1950). A. M. Turing (1950) Computing Machinery and Intelligence. Mind 49: 433–460. COMPUTING MACHINERY AND INTELLIGENCE, 1–10. https://www.csee.umbc.edu/courses/471/papers/turing.pdf

[8] *Using HTTP Cookies*. (2022, April 27). MDN Web Docs. Retrieved August 5, 2020, from https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

[9] *What are Cookies?* (n.d.). Kaspersky. Retrieved August 8, 2022, from https://www.kaspersky.com/resource-center/definitions/cookies

[10] A Summary of Alan Turing's Computing Machinery and Intelligence. (2020, August 12). Medium.Com. Retrieved August 8, 2022, from https://medium.com/@jetnew/a-summary-of-alan-m-turings-computing-machinery-and-intelligence-fd714d187c0b