IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AN ELABORATE REVIEW ANALYSIS ON THE EFFECTIVENESS OF AI BASED CHATGPT IN THE CONTEXT OF UNIVERSITY EDUCATION ON COMPUTER SECURITY ORIENTED SPECIALIZATION

[1]G. Dhanabalan, [2]L. Saravanan

[1]Associate Professor, [2]II[nd] Year Student M.Sc in Data Analytics

[1]Department of Computer Science and Engineering

[1]Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India

Abstract: OpenAI has released a new version of ChatGPT, a sophisticated natural language processing system which is able to hold natural conversations by preserving and responding to the context of the discussion. However, ChatGPT has also been utilized in negative aspects despite its usage in different fields of applications. Data has been gathered regarding the effectiveness and usability of this tool for completing examinations, programming assignments, and term papers. This work has analyzed the impact of ChatGPT system in the field of education especially in the field of computer science higher education and also evaluated how it is misused in different levels of applications, ranging from utilizing it as a consultant to simply copying its outputs. The analysis indicates that ChatGPT is able to cope up with "Programs" and performs better. It is not able to compete effectively in other fields like examinations / term papers.

Index Terms **– Artifical Intelligence, ChatGPT, education, Virtual Assistant, Computer Security.**

I. INTRODUCTION

Researchers investigate the use of artificial intelligence in the field of education ever since these techniques reached sufficient maturity. It primarily focuses on improving the learning process by helping the students and simplifying some repeated processes for teachers. A comprehensive survey of the current state of the art in natural language generation – Core tasks, applications and evaluation has been discussed in [1].

The launch of a new version of the ChatGPT, kind of chat pot system, attracted the attention of large audience. One can summarize the reactions as shocked, to say the least. Although AI's capabilities were certainly not as shocking to the community dealing with this technology for a longer time, the availability to broader audience caused a strong reaction. Although it is not the first publicly available AI (e.g., DALLE for image generation, FaceApp for face alterations, or Copilot for code completion), it has certainly seen the biggest response as it gained over 1M users in a week. The tool is able to produce high quality texts of various focuses even with the ability to respond in various languages (internally, they are machine translated into English similar to DeepL or Google Translate). An elaborate literature review on the use of artificial intelligence in education including the impact of models such as ChatGPT on various educational fields like language learning, mathematics, and science has been discussed in [2]. Strength of ChatGPT is its contextual querying, where ChatGPT and creates new results based on an earlier conversation by recalling previous queries [3]. This has started to end of the classically written essays teaching in selected disciplines of education. While this technology might be misused for cheating [4], there are also implications for technical fields, especially computer science, as it can simplify create activities such as

programming. The student's ability to adopt this technology in subverting the text produced by ChapGPT has been proved to be very good and fast. Dutch students have already admitted this technology to write homework and as confirmed cases of cheating began to emergevery quickly, the reaction in education system was similarly swift [5]. On the contrary, establishment of developing a tool to detect ChatGPT generated texts has been started. It is also becoming a nightmare in the field of computer security and IT security in general. Many researchers have already experimented for solving their course examinations or assignments. However, it has been identified that there is no in depth testing of ChatGPT capabilities. It was witnessed that students utilize AI tools to solve assignments. Researchers also examine the use of Natural Language Processing (NLP) in education, including the impact of models such as ChatGPT on various educational fields [6]. Recent studies indicate that there are many potential benefits and also challenges while using NLP in education.

II. EXISTING SYSTEM

OpenAI has developed a large scale artificial neural network language model based on the GPT (Generative Pre trained Transformer) architecture [7**,** 8]. ChatGPT has been pre trained on massive amount of text data and can be fine tuned for various natural language processing tasks, such as language translation, summarization, and question answering [9]. Current version of ChatGPT is GPT-3 which contains 175 billion parameters and has demonstrated remarkable performance on a wide range of natural language processing tasks, including answering questions, generating coherent text, and completing sentences. ChatGPT is designed to mimic human like language processing, using a transformer based architecture that allows for efficient training and inference. The model uses self attention mechanisms to identify and prioritize the most relevant information in a given context, enabling it to generate fluent and coherent responses to user input.

ChatGPT is widely used in spectrum of applications like virtual assistants, chatbots and language translation services. It has also been integrated into a range of products and services, such as Microsoft Office and Google Translate. It shall be fine tuned for various natural language processing tasks, such as language translation, summarization, and question-answering, making it a versatile tool for a range of applications [10]. Apart from the features of ChatGPT, it has its own demerits as listed below:

- Like other language models, it can reflect and even amplify biases present in the training data. This could lead to problematic and biased language generation that may be harmful or discriminatory.
- It lacks a deep understanding of common sense knowledge and the world beyond the text in which it has been trained on. This can lead to errors or misunderstandings when generating language in response to complex or nuanced queries.
- The effectiveness of ChatGPT heavily depends on the quality and size of the training data. Without access to large and diverse data sets, the accuracy and reliability of the model may be compromised.
- ChatGPT is a resource-intensive model that requires significant computational power and storage space. This can limit its accessibility for some users or applications.
- ChatGPT's transformer based architecture can be difficult to interpret, making it challenging to understand how the model is making decisions or toidentify and rectify the errors.

An in-depth evaluation of ChatGPT's abilities to solve assignments of various levels in computer security specialization has been performed especially in IT oriented university. It discusses this technology's possible positive and negative impacts on university education by taking into account of the capabilities of AI, how the educational process (adaptation, detection, and prevention) should be revised to benefit both students and educators [11]. It evaluated four courses related to computer security. The courses consist of different combinations of examination methods and their weights for final assessment. It used a minimum of 50 assignment types for each category of examination method (except essays, where there were created twenty different essays). The assignments were solved by AI and compared with the results of students solving examinations from the same question pool [12]. In the scope of programming assignments, a different number of tasks were used depending on difficulty, i.e., small project, term project, and code completion.

III. PROPOSED SYSTEM

3.1 Methodology I

3.1.1. Categories of examination methods

This work has included examination methods from four courses focused on the security of information systems, cryptography,secure coding, and secure hardware for the purpose of experimentation. Three basic methods have been defined which are written examinations, term essays, and programming assignments.

Written examinations

Written examinations are used to test student's knowledge and his/her ability to apply it. All examinations combine general knowledge and practical questions (e.g., knowledge and understanding of key terms, encryption using transposition cipher, calculating the output of several runs of a specific LFSR generator, explanation of the principle of the selected attack, knowledge of the responsibilities of the information security administrator role, designing security measures for a given scenario, etc.). Used questions cannot be published due to yearly reuse. Two different types of written exams have been formulated as listed in the Table 3.1.

Table 3.1 : Examination categories matrix, AI usage modes

Content	Text	Full text	Essay	Programming
Copy and paste	Partially Used	Used	Partially Used	Partially Used
Interpretation	Partially Used	Not used	Partially Used	Partially Used
Assistant	Not used	Not used	Used	Partially Used

Full text examination

Full text examination expects the students to answer a question using their own words or demonstrate a solution to a problem.

Text

Students choose from a predefined set of responses in which one or more is correct. The points for a question are assigned based on the number of correct responses that have been selected. Selection of an incorrect response will lead the deduction of a point meant for the whole question.

Term essays

Students are involved to study security related topics and write a short research paper based on the knowledge they acquired as the Term essays is concerned [13]. It is possible to write a tutorial paper, perform a security analysis of a certain product or execute a new exploit and document it.

Programming assignments

Select three types of programming assignments prescribed by the faculty.

3.1.2. Completing predefined code

In an individual project, students will be provided with a predefined structure in the form of methods, variables, or usage definition. Students are typically assigned to implement selected methods. This work has chosen a machine learning class homework, where students implement formulae for simple distributions and classifiers in Python. This type of assignment allowed for testing both Copy and Paste and interpreted variants. An individual project typically consists of less than 1,000 lines of code. RSA implementation in C++ has been selected in this case. The requirements are to generate the keys, encrypt, decrypt, and break messages with small key lengths. Additionally, it is not allowed to use special libraries for the generation of prime numbers.

3.1.3. Term project

A large programming project was assigned to a team of two to three students. This work has selected a term project from the Information Systems course as the security related courses do not have this type of project. The assignment is to implement a simple information system as a web application in PHP. Name of the assignment is "Smart City". This system should allow the citizens of a city to report issues and the city manager is expected to manage the issues.

3.1.4. Interactive project

An individual interactive project requires the student to get familiar with an unknown environment (system) and complete tasks. One of the courses involve the Capture The Flag (CTF) task. Students will be given cyber security related challenges, such as encryption cracking, reverse engineering, web exploitation, etc., Users must solve these challenges to retrieve hidden messages in the system. The assignment consists of six secrets within a virtual network environment of four servers. Tasks are designed for all the students whose talent level is from beginners to intermediate.

3.2 Methodology II

Experiment scope

This work ultimately evaluates four courses related to computer security. These courses consist of different combinations of examination methods and their weightage for final assessment. Minimum of 50 assignment types for each category of examination method (except essays in which twenty different essays were created) are used. These assignments are solved by AI and compared with the results of students solving examinations from the same question pool. For CTF, the approach was selected in such a way that there is only one AI-based relevant solution exists. In the scope of programming assignments, different number of tasks was used depending on difficulty, i.e., small project, term project, and code completion.

IV. RESULTS AND DISCUSSIONS

Methodologies discussed in Section III were exposed to both the students and the AI based ChatGPT system and its impact is discussed in this section. Figure 4.1 displays the performance of scores by both AI based ChatGPT system and genuine students [14].

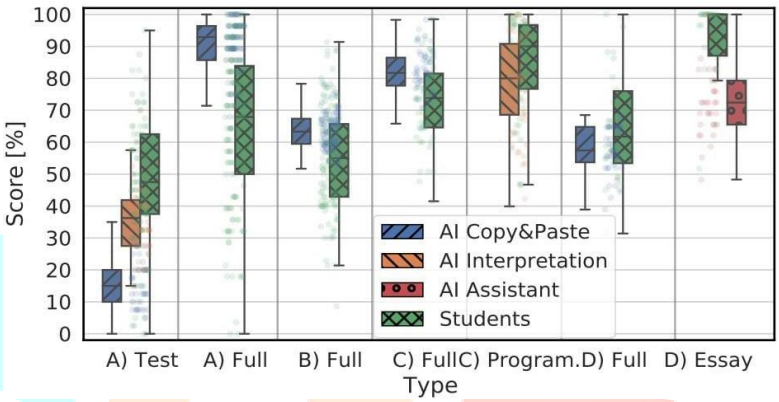

Figure 4.1 AI based ChatGPT & students scores

Full text exam

Figure 4.1 [A) Full, B) Full, D) Full] compares AI to students based on the scores received from full text examination questions. It is evident that ChatGPT is able to produce correct answers wherein the answers are broader and less specific. Problems can arise when answering those questions which demands knowledge in terms of application. Employing Bell-Lapadua model for document access is one such an example. In this situation, ChatGPT has no sense of context. It shall be noted that answers derived by ChartGPT is similar to ordinary students. Figure 4.1 [A) Test] demonstrates that the selected solutions are not always correct in the Copy Paste mode. This is deteriorated by the fact that this specific test has harsh scoring, with an incorrect answer resulting in negative score for the given question. On the other hand, Interpretation mode has considerably improved response quality.

Term essays

Section D) in the Figure 4.1 indicates the score owned by AI and the students in the category "Term essays". It shall be noted that AI has dominated in the categories of A, B, C and the students dominate in Essay. Essay category indicates that approximately four page Copy Pasted essay has been completed in less than an hour. It consumed longer time with an assistance as fact-checking was required. However, the generation of threat modeling instrument descriptions has saved time.

Completing Predefined Code

ChatGPT helps the users to perform their homework even without referring the necessary formulas or algorithm steps (e.g., Mathematical expressions for Gaussian Mixture Model). ChatGPT allows copying the predefined structure to easy code generation with necessary properties for the template. Even a native implementation (copy paste) received at least 30 percent of points in less than 10 minutes of time.

Small Projects

ChatGPT is smart enough to implement algorithms such as Miller-Rabin, Solovay-Strassen, and Pollard-Rho easily. Copying the output from ChatGPT significantly reduced the time and effort required. However, this has reduced the educational effect of the assignment as no study of the algorithms was needed.

Term Projects

ChatGPT generated database schema in the form of executable SQL script based on the assignment it is given. The proposed folder structure represented the MVC architecture, while most students neglected this. ChatGPT easily generated code for database models, sample data, or views for login or registration pages. Interactive querying allows modifying the generated code to include styles or refactoring code. Moreover, the generated code was tailored to fit the context of the initial database design (i.e., registration form fields).

Interactive Projects

Caesar's cipher encrypted a secret message, which appears as the MOTD (Message Of The Day). A simple request for AI to solve it failed; However, ChatGPT suggested frequency analysis and attempted to perform it, resulting in a bad outcome. It eventually found that the substitution cipher had been utilized. AI attempts at decoding produced only incorrect results, similar to what was observed with examinations. On the contrary, ChatGPT has successfully completed the easy task of finding a secret in a hidden file using Linux commands. It also successfully solved a more advanced task of obtaining a password from an obfuscated Javascript and reverting the SHA-1 hash. ChatGPT identified the hash type and provided advice for revealing the password but was not allowed to help crack the hash (due to ethical constraints of the AI system). Instead, it successfully directed towards online tools for revealing the original message. ChatGPT cannot solve such an assignment independently. It can only navigate students through the problem or demonstrate novel approaches or technologies. In summary, ChatGPT is able to support the knowledge needed to complete this assignment. However, most of the work remains to be done by students.

Final Assessment

Figure 4.2 portrays the final assessment results based on scored points for three courses [14]. A student is declared "pass" by earning at least 50% of the total points available throughout the semester via various tasks, tests, and exams. The evaluations for each course is different. Subject A had a test worth 60% and a full text exam worth 40% total points, Subject C had a programming assignment (30%) and a full text exam (70%), and Subject D had an essay (35%) and a full text exam (65%). The key takeaway is that the ChatGPT did well overall and can pass all courses, except for a minor loss in Subject A when the AI was used in Copy Paste mode during the test examination technique.

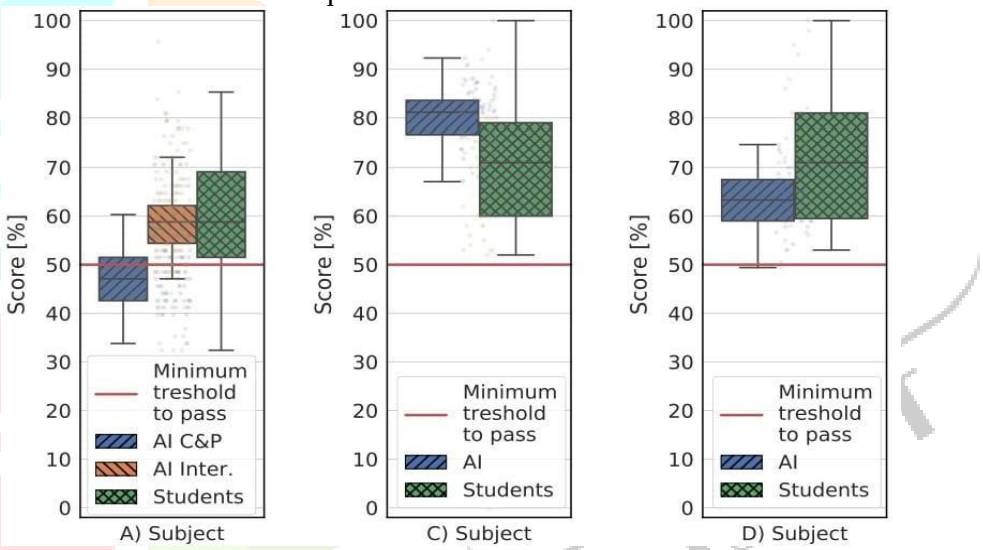

Figure 4.2: Assessment of overall scores for various subjects

Figure 4.2 shows that the impact of ChatGPT usage by students which is enormous. During the experiments with ChatGPT, it was observed that there is a great variability in the correctness of the ChatGPT answers. Several examinations included an almost identical question on deciphering a message using Vigenère cipher. The answers were diametrally different for each query. ChatGPT solved this task in some cases and has generated wrong results for the remaining tasks. It tends to make up events, links, and references. It has also generated a link to a non-existing image, GitHub repository or name of a publication was returned in the answer. If the author does not pay enough attention or does not understand the topic, such mistakes might be observed in the submitted text. This might serve as a good starting point for detecting AI-written papers.

REFERENCES

[1] Abid Haleem, Mohd Javaid, Ravi Pratap Singh, 2022. An era of ChatGPT as a significant futuristic support tool: A study on features, abilities, and challenges, BenchCouncil Transactions on Benchmarks, Standards and Evaluations, 2(4): 1 – 4.

[2] Sukhpal Singh Gill, Rupinder Kaur, 2023. ChatGPT: Vision and challenges, Internet of Things and Cyber-Physical Systems, 3: 262-271.

[3] Augustin Lecler, Loïc Duron, Philippe Soyer, 2023. Revolutionizing radiology with GPT-based models: Current applications, future possibilities and limitations of ChatGPT, Diagnostic and Interventional Imaging, 104(6): 269-274.

[4] G. Hurlburt, 2023. What If Ethics Got in the Way of Generative AI?, IT Professional, 25(2): 4-6.

[5] H. Ibrahim, R. Asim, F. Zaffar, T. Rahwan and Y. Zaki, 2023. Rethinking Homework in the Age of Artificial Intelligence, IEEE Intelligent Systems, 38(2): 24-27.

[6] Chan, 2023. A. GPT-3 and InstructGPT: technological dystopianism, utopianism, and "Contextual" perspectives in AI ethics and industry. AI Ethics 3: 53–64.

[7] Silvia Badini a, Stefano Regondi a, Emanuele Frontoni a b, Raffaele Pugliese a, 2023. Assessing the capabilities of ChatGPT to improve additive manufacturing troubleshooting, Advanced Industrial and Engineering Polymer Research, 6(3): 278-287.

[8] Nassim Dehouche. 2021. Plagiarism in the age of massive Generative Pre trained Transformers (GPT-3). Ethics in Science and Environmental Politics 21 (Jan. 2021), 17–23.

[9] X. Xue, X. Yu and F. Y. Wang, 2023. ChatGPT Chats on Computational Experiments: From Interactive Intelligence to Imaginative Intelligence for Design of Artificial Societies and Optimization of Foundational Models, IEEE/CAA Journal of Automatica Sinica, 10(6): 1357-1360.

[10] Patrick Mikalef, Manjul Gupta, 2021. Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance, Information & Management, 58(3): 103434.

[11] Margaret C. Keiper, Gil Fried, Joshua Lupinek, Heidi Nordstrom, 2023. Artificial intelligence in sport management education: Playing the AI game with ChatGPT, Journal of Hospitality, Leisure, Sport & Tourism Education, 33.

[12] Steven Moore, Huy A. Nguyen, Norman Bier, Tanvi Domadia, John Stamper. 2022. Assessing the Quality of Student Generated Short Answer Questions Using GPT-3. In Educating for a New Future: Making Sense of Technology-Enhanced Learning Adoption. Springer International Publishing, Cham, 243–257.

[13] Chin C, Brown DE, 201. Student-generated questions: a meaningful aspect of learning in science, International Journal of Science and Education, 24(5):521 – 549.

[14] Kamil Malinka, Martin Peresini, Anton Firc, Ondrej Hujnak, Filip Janus, 2023. On the Educational Impact of ChatGPT: Is Artificial Intelligence Ready to Obtain a University Degree?, International Conference on Innovation and Technology in Computer Science Education ITICSE. Pages 47-53.