Title: Privacy and security challenges in artificial intelligent agents.

BSc(Honors)

Student Name

Student No.

Supervisor

Date of submission

**Introduction.**

Artificial intelligence has become one of the marvels in which modern technology has been anchored10. It has made many of the institutions a very significant component in modern days as it has been used by different sectors of the economy in order to enhance their profit and improve their productivity. Ideally, it is worthwhile to note that the deployment of artificial intelligence has attracted more good and bad in different dimensions and perspectives depending on who has performed all the contexts in enhancing the business in place.

In a more classical sense, the security and privacy of data exhibited by the artificial intelligent agent have a greater milestone in ensuring and enhancing the security of data in the artificial intelligence sector as more captivating. Therefore the security of the artificial intelligent component should be very important.

The already articulated business sector in ensuring and enhancing the activities of tourism and travel business is worthwhile to understand the field of artificial intelligence has become one of the important business environments which needs to be articulated in order to improve profit realized9. This is one of the motives for venturing into this kind of business. This field remains unutilized, but few companies have managed to deploy artificial intelligence such as robots in serving tourists and managed to acquire significant profits.

**Problem statement.**

The evolution of technology has led to the utilization of technology in different fields. In fact, this has enhanced and enabled the mechanism in which the security of artificial intelligence can be secured. Normally statements can be identified that systems which are in place are prone to attacks, and this can become detrimental to many companies trying to find the best mechanism for enhancing this area. Ideally, there could be mechanism which could inhabit a mechanism of enhancing the security of the data without compromising productivity. It has been identified most of the systems available were prone and susceptible to attacks.

The refuge was found to be adopting artificial intelligence in improving productivity, helps in making better insight through prediction algorithms, hence better decision making. But the classical sense is that productivity should be increased while maintaining the security of the data. Therefore this led to the deployment of artificial intelligence in order to enhance the productivity of different sectors. Therefore due to continuous internet supply to the data, it was imminent to understand that the internet is one of the critical components which was required by different organizations in order to operationalize various activities. Therefore artificial intelligence had to have connections in order to work effectively. Therefore these agents being more exposed to the network were more susceptible to attack by the digital assailants.

**Proposed solutions.**

Security and privacy of data are important not only for the artificial intelligent agent. Therefore, to ensure that there is security for the AI agent, ensure that the system will have a singular effect and aspect of ensuring that their component is secure8. Most AI agents have their data stored in their knowledge base to ensure that there are matched goals that enhance the process by which a decision was made as per the required algorithm.

The antiquity in the manner in which data was made actually ensured they are not subject to attacks as all the data transmitted or used to control specific agents must be located in a specific place. Therefore, the security and privacy of this data can be enhanced. By any chance that the data which controls the robots has been manipulated, it will become very dangerous for robots to perform their task objective while following all optimistic goals and functions present in the research.

All data communicated to an artificial intelligence agent needs to be encrypted such that the digital assailant cannot have the mechanism to access your data. It should be noted that the security of data is very important. The sectors, though have marked a large milestone in ensuring that the sectors have been revolutionized so that they cannot be phased; technology such as artificial intelligence has brought a number of impacts into the sector. However, some of the challenges experienced in these sectors are the inability to predict exactly what particular number of months we can have a steady flow of business4. But this can be achieved or enhanced by the decision tree simply because individuals need to undertake a robust process in ensuring what mechanism needs to be put in place to have accurate statistics of such kind of client.

Covid-19 has led to less profit margin realization due to restrictions in movement. Therefore robotics can be deployed to assist in all this. The figure below represents the acquisition of robots in the tourism and travel industries.

**Supervisor Meeting Discussion.**

In the development of this project, there were a number of meetings carried out throughout the research to establish thorough criticism and provide me with critical areas of improvement. Without the criticism from the supervisor, such kind of work could not be thorough as it should be.

Therefore it should be noted that a clear and appropriate meeting with the supervisor greatly impacts what kind of work you are likely to produce, starting from the literature review and research gap up to future enhancement of the research. In its entirety, the process through which this work is enhanced should be fully articulated and enhanced through proper documentation on each and every work to tell the supervisor what you have achieved since the last assessment.

Once the professor has routinely anchored the assessment, then it becomes easier for someone to articulate exactly what has been taught and required by the professor. To underpin and enhance the success of the project, the student must demonstrate progress with the milestone provided in the Gantt chart just to show how the project will be articulated.

Therefore, criticism is very important as it enhances your understanding and all other salient aspects which were required in the project.

1. **Preparatory Work**

The tool to be used for the implementation will require an appropriate detection system which will enhance the security of the system7. This will include and is not limited to the following: appropriate system security implementation through the use of firewall configuration, intrusion detection system, and intrusion prevention system.

Python and C programming languages will be the ones that will be used to articulate all the works of creating a security system and enhancing the security of our data. Naturally, the security of the data is very important. Python has been very supportive in implementing the security aspects simply because they all available libraries to support that work2.

Software and hardware requirements

Python frameworks such as pycharm will be used to articulate the project in place. This will ensure and provide the platform which is required for implementation purposes and approaches.

Microcontroller, which is required for the process of implementation. This will ensure that the data which will be in the knowledgebase must be stored here.

Database server: this is where all data will be installed in controlling all the artificially intelligent.

1. **Stakeholders**

Chief security information officer: This role has a supervisory role with gallant security in enhancing the security of the data. This mechanism will enhance the security of the AI agent through the junior ICT officers.

ICT Security Officer: These individuals need and must be involved in ensuring agents are the surrounding networks of an artificially intelligent agent is secure by ensuring appropriate protocols and system security have been effectively configured3.

Risk analyst: The analysis of most risks pertaining to the budget will be involved, especially during the implementation, i.e., during the artifact development stage. They ensure proper budget planning normally takes place.

Maintenance engineers: These are support staff who normally deal with and help in maintaining the day-to-day operations of the artificial intelligence agents. They undertake all the business activity effectively through them.

1. Risk – during project implementation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk type | Stakeholder | Likelihood | Consequences | Mitigation |
| DDoS | Chief security information officer | High | * This will breach all data stored in the knowledge, interfering with the normal functioning of the artificial intelligence agent. * This also has an impact on reduced productivity during the period of attacks. | * There should be   Regular audit of  the system dealing  With this kind of  attack.   * Ensure that the   The system is well  Configured such that  There is no vulnerability  Required. |
| Malware | ICT Security Officer. | Low | * Their impact not only has impacts on software but also impairs the hardware. * They cannot affect the entire system. | * Install intrusion system * Install prevention system * Configure firewall,   Well. |
| Residual risk. | Maintenance engineer. | Medium | * They can impair the operation of the business. | Ensure all the common  Risk which appears  They are bound to  Happen. |
| Budget Overestimated | Risk analyst | High | * The entire project may not become   Successful   * Audit the system continuously and effectively. | * Perform business   Analysis. |

1. **Statement of Success**

The success of this project will be of great consequence and cannot be neglected without the appropriate mechanism for ensuring and enhancing knowledge acquisition, especially in the field of artificial intelligence. Having undertaken various artifacts which are required and need to be articulated fully. The purpose and the sole aspect of undertaking the activities in enhancing this project will be undertaken and enshrined through understanding are key concepts that make most artificial intelligent agent becomes very vulnerable to attacks. Ideally, when all the relevant ideas pertaining to the causes of attacks have been documented effectively, it will be worthwhile to identify what needs to be undertaken in order to ensure that the issue at hand has been articulated and mitigated effectively.

The automated success will be anchored on the basis of the best mechanism and methodology, which proposes the best mechanism for enhancing the security of the data at all artificial intelligence agents and the privacy of the data.

The students here must undertake thorough research in order to ensure that, once developing a sensor that requires some data in order to acquire some functionality needs salient security features. Artificial intelligence agents have suffered distributed denial of service attacks which made the agent ineffective in providing useful services to the body6.

Therefore the success of the implementation of up to project will depend on the knowledge acquisition available from the research and the outcome which has been proposed in the problem statement domains.

Some of the pertinent questions need to be implemented and analyzed in order to get the causes of attacks and what can be done in order to alleviate some of the challenges which are brought by the inappropriate configuration in our artificial intelligence agent. Something worthwhile to note is that system development needs to be articulated fully in order to enhance security through the use of technological advancement tools that enable the enhancement of the security of AI agents. This will ensure the success and knowledge acquisition of the projects.

1. **Project Plan**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Timelines | | 1 week | 1-week | 2-weeks | 3-weeks | 4 weeks | 5-weeks | 6-weeks |
| Activities |  |  |  |  |  |  |  |  |
| Literature review |  |  |  |  |  |  |  |  |
| Feasibility study |  |  |  |  |  |  |  |  |
| Proposed methodology |  |  |  |  |  |  |  |  |
| Experimental design |  |  |  |  |  |  |  |  |
| Conclusion and discussion |  |  |  |  |  |  |  |  |
| Future work and discussion |  |  |  |  |  |  |  |  |

1. **Ethics**

The research ethics included in this proposal will be articulated such that it demonstrates there is no conflict of interest in the research. This simply means that the research is the original authors’ work. Therefore there will be a disclosure of conflict of interest in the research.

No plagiarized work in the research all the works which has been used is original and otherwise, they have been referenced or acknowledged. The proposed information is important simply because it will enhance the work of the research effectively. The study has not acquired any material support such as research funds. This could have helped in furthering the unarticulated part of the research.

References

1. Chi OH, Denton G, Gursoy D. Artificially intelligent device use in service delivery: a systematic review, synthesis, and research agenda. Journal of Hospitality Marketing & Management. 2020 Oct 2;29(7):757-86.
2. Lukanova G, Ilieva G. Robots, artificial intelligence, and service automation in hotels. InRobots, artificial intelligence, and service automation in travel, tourism and hospitality 2019 Oct 14. Emerald Publishing Limited.
3. Lukanova G, Ilieva G. Robots, artificial intelligence, and service automation in hotels. InRobots, artificial intelligence, and service automation in travel, tourism and hospitality 2019 Oct 14. Emerald Publishing Limited.
4. Solakis K, Katsoni V, Mahmoud AB, Grigoriou N. Factors affecting value co-creation through artificial intelligence in tourism: a general literature review. Journal of Tourism Futures. 2022 May 5(ahead-of-print).
5. Ananeva, D., 2019. Artificial Intelligence as Disruptive Innovation in the Hotel Industry: Finnish Boutique and Lifestyle Hotels Perspective.
6. Nam, I.H., 2020. *A Study on Chatbots and Computer Vision Applications using Social Media Mining* (Doctoral dissertation, University of Macau).
7. McCartney, G. and McCartney, A., 2020. Rise of the machines: towards a conceptual service-robot research framework for the hospitality and tourism industry. *International Journal of Contemporary Hospitality Management*.
8. Milman, A., Tasci, A. and Zhang, T.C., 2020. Perceived robotic server qualities and functions explaining customer loyalty in the theme park context. *International journal of contemporary hospitality management*.
9. Choi S, Mattila AS, Bolton LE. To err is human (-oid): how do consumers react to robot service failure and recovery?. Journal of Service Research. 2021 Aug;24(3):354-71.
10. Zhang D, Wang L, Zhang L, Dai BT, Shen HT. The gap of semantic parsing: A survey on automatic math word problem solvers. IEEE transactions on pattern analysis and machine intelligence. 2019 Apr 30;42(9):2287-305.