Enhancing Data Privacy and Security of Artificial Intelligence in Combating World Hunger

Surrya Raj A/L Ramanathan
School of Computing
Asia Pacific University of Technology and innovation (APU)
Kuala Lumpur, Malaysia
TP061539@mail.apu.edu.my

Dr. Intan Farahana Binti Kamsin
School of Computing
Asia Pacific University of Technology and innovation (APU)
Kuala Lumpur, Malaysia
intan.farahana@staffemail.apu.edu.my

***Abstract*- This paper focuses on improving data privacy and security for an AI based machine to combat world hunger. World leaders saw reducing hunger and malnutrition (SDG 2) as a key step to a more safe, fair, and sustainable communities in 2014. Ironically, hunger has not abated ever since. According to the most recent figures, the number of people who are severely underweight has increased for the second season in a row. To overcome this issue, machine learning has been implemented to flexibly learn and come up with solutions quicker than humans based on data collected throughout the world. There is however one problem with this, and it is of course, the security that is used to protect these data. Many different data security software has been released to overcome this particular issue, but they were all separated into different platforms such as Data Loss Prevention Software (DLP), Data Centric Software (DCS) and Database Security Software (DSS). Hence, this research is carried out to figure out a more efficient way to protect these valuable data stored by the Artificial Intelligence.**

***Keywords*—Artificial Intelligence, Data Privacy, Security, Combating World Hunger, Data Loss**

I. INTRODUCTION

Artificial Intelligence (AI) methods have been adopted in a variety of applications as a result of recent technological advancements and increased processing capacity. Machine learning models, for example, are often used to encourage growth in the fields of health care, gaming, and finance, while deep learning models are being utilised by autonomous car manufacturers to construct pipelines for self-driving automobiles (OSENI, MOUSTAFA and JANICKE, 2022). Machine learning (ML) frameworks and, more importantly, deep learning (DL) algorithms, which are now used in various AI systems, allow for the automation of jobs and processes, resulting in new capabilities and functions that were previously unavailable.

In the video game StarCraft II, for example, DeepMind's AlphaStar, an AI machine built on deep reinforced learning, achieved Grandmaster status by defeating many high-level human players in 2019.The use of AI techniques in a variety of applications gives a once-in-a-lifetime opportunity to address a variety of socioeconomic and environmental issues. However, without dedicated study on safeguarding these technologies, this will not be possible. Adversarial machine learning has lately attracted a lot of research attention, and a continued focus on this topic will surely secure the widespread adoption of transformative AI technology (OSENI, MOUSTAFA and JANICKE, 2022). Robust algorithms are critical to the advancement of a secured and safe inventive future as AI becomes growingly incorporated into all aspects of human operations and lifestyles.

II. LITERATURE REVIEW

A. DATA PRIVACY AND SECURITY

Data privacy, also known as information privacy, is a subset of data protection that deals with the proper confidentiality of sensitive data, most notably personal data, as well as other sensitive information, such as certain financial documents and intellectual asset data, in order to comply with regulatory requirements while maintaining the data's confidentiality and immutability. As indicated in the diagram below, data protection is divided into three categories: conventional data security (such as backup and restoration copies), data protection, and data privacy. Protecting the security of sensitive and personal data is a result of excellent data protection and security practises, with the overarching purpose of ensuring the continuous accessibility and immutability of vital business data. Data security is the procedure of preventing unwanted access to sensitive information. It encompasses all of the many cybersecurity techniques you employ to protect your privacy from misuse, such as encryption, physical and digital access limitations, and more. Data protection has always been a priority (Poza, 2022). However, as a result of the present health crisis, more individuals are working remotely (and cloud usage has surged to match), there are many more potential for unwanted access to your information than ever before. And it's being exploited by hackers. Since the epidemic began, both Interpol and the US Chamber of Commerce have reported a dramatic rise in the number of cyberattacks (Poza, 2022). So, regardless of what your company does, if it handles personally identifiable information (PII), increasing data security is an essential in 2021. The first thing that springs to mind when people think of data security issues is a hacker sneaking into your servers. However, the fact is that the most serious dangers to data protection are frequently internal and stem from your workers' risky behaviour. For example, IBM and The Ponemon Institute investigated the fundamental causes of data breaches in 2020 and discovered that stolen credentials (typically due to weak passwords) and cloud misconfigurations were the top two reasons (leaving sensitive data accessible to the public) (Poza, 2022). One of the other leading causes of data theft (phishing scams) is something that may be avoided with proper employee training. Based on the research, it can be said that data privacy and security is not something that can be

taken lightly. A simple data breach or data loss that occurs can ruin years' worth of work in an instant. Hence why, implementing a more secure software to protect these data is significant.

B. Artificial Intelligence

Artificial intelligence (AI) is the capacity of a computer or a computer-controlled robot to accomplish activities that would normally be performed by intelligent individuals. The phrase is widely used to refer to a project aimed at creating systems with human-like cognitive abilities, such as the capacity to reason, discern meaning, generalise, and learn from prior experiences. Since the invention of the digitized computer in the late 1930s, it has been proved that machines can be programmed to perform extremely complicated jobs with ease, such as finding proofs for logical theorems or playing chess ("artificial intelligence summary", 2022). Despite ongoing increases in computer processing power and memory capacity, no programmes have yet to equal human flexibility across broader areas or in activities requiring a great deal of common knowledge("artificial intelligence summary", 2022). However, certain programmes have surpassed the performance levels of human specialists and professionals in completing specific tasks, and artificial intelligence in this restricted sense may be found in software as varied as clinical diagnosis, computer online databases, and voice or handwriting detection. Artificial intelligence is capable of solving issues and completing a variety of tasks: Making it practical for an AI software or "robot" to perform several tasks has been one of the most challenging challenges to overcome. It is fairly simple to programme a machine to perform a specific task. It can, for example, transport an object from location A to location B. Artificial Intelligence is also claimed to be preparing for a big data boom: big data is indeed the large-scale, and often even random, collecting of data on people's lives, habits, conversations, and other activities. AI will be able to do far more with this data analysis than humans ever could, resulting in a boom in datadriven research, advertising, and content. To summarise, Machine Learning and Ai have benefited from both theory and fiction. The idea that computers could understand and perform tasks in the similar method that people do has been around for thousands of years. Machine learning and artificial tools have uncovered cognitive realities that are not new. These technologies could be thought of as the engineering implementation of robust and well perceptual properties. Accept the fact that we have a proclivity to consider all noteworthy breakthroughs as a Rorschach test over which we project our worries and dreams about just what create an effective or happy world. The beneficial potential of AI and machines cognition, on the other hand, does not exist solely or even mostly in the underlying technology.

C. World Hunger

According to an FAO research published in 2016, global food production is sufficient to feed the world's 7.3 billion inhabitants. The math does not add up with 821 million people struggling from hunger throughout the planet and kids still dying of malnutrition. Food supply in the world significantly outnumbers consumption, but most of it is wasted. According to the FAO, approximately 1.3 billion tonnes of food are not consumed each year, accounting for one-third of all food produced. Only 25% of what is thrown out would be enough to feed the whole starving world. Instead of increasing output and providing temporary assistance, a territorial strategy is increasingly emerging as a means of valorising and potentializing local production. In this regard, artificial intelligence has the potential to integrate new technology into structural, particular, and local policies to minimise economic disparity and ensure that people have enough to eat. AI can deliver a variety of scenarios and solutions, each tailored to a certain area and population. In truth, this is the purpose of FAM, a collaboration between digital giants Microsoft, Amazon, and Google, as well as international agencies like the United Nations Bank. According to the World Food Program, the number of hungry children would rise by 24 million by 2050, or roughly one-fifth greater than it would be if climate change did not exist. These professional insights constitute a forceful call to action, but they are far from a proclamation that famine and starvation are unavoidable. Instead, we might choose to see climate change as an opportunity to effect constructive change. We have lots of opportunity to expand food available before we reach Earth's true limits since the world food system is so ineffective and unequal. Fortunately, the food and agricultural solutions to best tackle climate change also benefit the world's starving mouths, the environment, and everyone's health (Lappé & Collins, 2022). Our food system, if reformed, has the potential to assist rebalance the climate system by reducing emissions and increasing carbon storage in the soil. Low-cost climate-friendly farming approaches assist small-scale farmers and farm laborers, who account for the bulk of hungry people. While climate change is unavoidable, vulnerability may be managed to a significant extent. We can assure that no one starves while we tackle the climate crisis if we address the grave disparities and inefficiency in our food system. Based on this research, the international community possesses all of the necessary resources to prevent and combat hunger and poverty. Even if there is ample food, people go hungry as it is not distributed evenly and because of political upheaval. Providing food assistance to the destitute is not a long-term solution to poverty and hunger. To end hunger and poverty, we must find a long-term solution. We must address issues like bad farming techniques, deforestation, overcropping, and overgrazing, which deplete land fertility and lead to hunger. Battles are another underlying problem that needs to be addressed when it comes to poverty and hunger, as millions of people are uprooted from their homes every year, resulting in hunger and poverty. We ought to find better strategies to combat poverty and starvation by addressing the problem early on.

III. SIMILAR SYSTEM

A. Oracle Data Safe

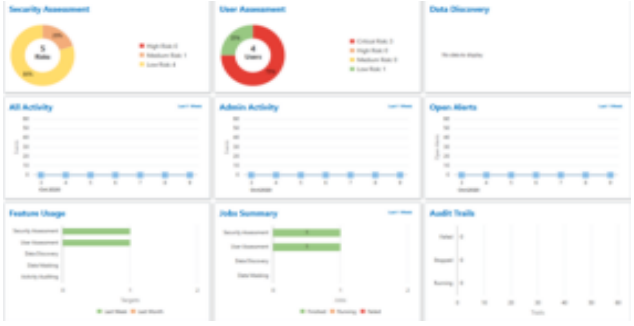

Fig. 1 Oracle data safe menu

Oracle Data Safe is a centralized control centre for Oracle databases that lets you analyse data sensitivity, evaluate data risks, mask sensitive data, create and monitor security measures, assess user safeguards, monitor user activities, and manage data security compliance needs. A range of Oracle Cloud Services, especially Oracle Data Safe, come with a free tenancy as well as a 30-day complimentary trial ("Using Oracle Data Safe", 2022). You may create an Oracle cloud account for free and then use Oracle Data Safe alongside your Oracle cloud or on databases. You must first create an Oracle Data Safe ecosystem before you can utilise Oracle Data Safe capabilities with your databases. Oracle Data Safe must be enabled in a province of your tenancy, and target databases must be registered ("Using Oracle Data Safe", 2022). The Home tab appears when you first log into the Oracle Data Safe. The Home page is a dashboard with many charts that you may use to keep track of your activity.

B. Zscaler Internet Access

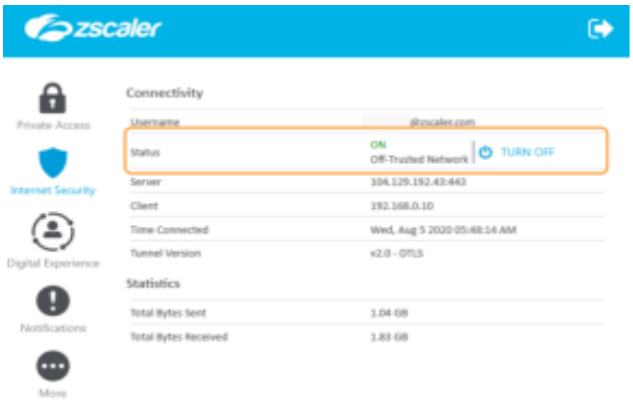

Fig. 2 Zscaler internet access

Zscaler Internet Access is a protected internet and web gateway supplied as a services from the cloud. Consider it a secured network onramp—all you have to do is establish Zscaler your future internet connection. Set up a router tunnel (GRE or IPsec) to a nearest Zscaler data centre for offices. You may redirect traffic to mobile employees using our lightweight Zscaler Client Connector (previously Zscaler App/Z App) or PAC file ("Zscaler Internet Access", 2022). Users are protected the same regardless of where they connect-a coffee cafe in Milan, a resort in China, or the office. Zscaler Internet Access stands between your consumers and the internet, checking every byte of data in real time using a variety of security mechanisms, including SSL ("Zscaler Internet Access", 2022). You receive comprehensive protection from online and internet hazards. You can start with the services you need today and add additional as your needs develop with a cloud structure that enables Cloud Firewall, Cloud IPS, Cloud Sandbox, Cloud DLP, CASB, and Cloud Browser Isolation. Since 2011, the Zscaler Cloud Security System has been a leader for both Gartner Magic Quadrant for Secure Web Gateways and the Forrester Wave. Without the expense and complexity of hardware, Zscaler Internet Access allows businesses to improve their security. Zscaler secures all clients with policy-based accessibility and inline protection against malware and other threats by transferring the secure stacks to the cloud. It also allows businesses to accept local breakouts and streamline Office 365 installations, allowing them to reap the benefits of the cloud and mobility ("Zscaler Internet Access", 2022). To summarize, both these software/cloud services has shown its advantages in preventing data loss or data breach and as such through 'SecureServ', it encapsulates not just these two discussed software but also many more such as Endpoint Protector, Egnyte, Cisco ACI, Immuta and etc. This software will be almost impossible to hack into or even cause any data loss as it is technically a system that is integrated by many different software to function as one.

IV. Problem Statement, Aims and Objectives

Only back in 2014, world leaders saw eradicating hunger and all kinds of malnourishment (SDG 2) as a critical step toward a more secure, fair, and peaceful world. Hunger, ironically, has not abated since then. The number of individuals who are undernourished has risen for the third year in a row, as per the latest statistics. In 2017, 821 million individuals (11 percentage of the global population, or one in every nine people) were hungry. Family farmers from Sub-Saharan Southern and Eastern Africa make up the majority of the data's face. Hunger and malnutrition continue to be major roadblocks to long-term growth. (medium.com) It sets up a trap that leads to lower production, sickness, and poverty perpetuation. Other types of malnutrition, on the other hand, are on the rise. While over 800 million people live in severe poverty and are chronically malnourished, approximately 1.9 billion are overweight, with 600 millions of them being obese. (medium.com) Obesity is rampant all across the world, and it's just getting worse. Hunger, on the other hand, is confined to select regions, particularly those ravaged by violence, drought, and extreme poverty. (medium.com) As an important component in a front-line strategy to solve world hunger, attain food and nutrition security, enhance nutrition, and promote sustainable agriculture, artificial intelligence (AI) could become particularly useful in anticipating food shortages. It is critical to build political will among decisionmakers to deploy early warning systems in order to avoid a food catastrophe. (medium.com) When it concerns to the way of life of agricultural workers, timely information delivered in the appropriate manner and through the proper channels helps to create resilience and accelerate growth. The ability of data would be used more effectively to assess scenarios, foresee risk solutions, and act before hunger becomes a humanitarian disaster when AI technology is produced under decentralised governance and governed in a transparent, participative, and caring manner. (medium.com) The data availability and materials to train intense machine learning frameworks is the most important element to consider. Yes, we possess data, but because it is created by millions of people throughout the world, there is a risk that it may be misused (Vadapalli, 2022). Let's say a healthcare service provider serves 1 million people in an area, and due to a computer hackers, all of the one million consumers' personal information ends up in the arms of everyone else on the dark web (Vadapalli, 2022). This information contains information about illnesses, health issues, medical history, and more. To make the matter worse, we're now dealing with information about the size of planets. With so much data coming in from all sides, there would almost certainly be some data leakage. Some businesses have already begun to develop inventive solutions to overcome these obstacles. It uses smart devices to train the data, so it isn't transported back to the servers; just the training set is returned to the company (Vadapalli, 2022).

The main purpose of this research is to create an integrated system that enhances the data privacy and security measures that is already implemented in Artificial Intelligence in

combating world hunger. While the objective of the research is:

- To integrate both Database Security Software(DSS) and Data Loss Prevention (DLP) Software into one system.
- To develop a software that captures all the pros of the different types of security software that is already in market.
- To reduce the number of times data leak or data breach occurs on a daily basis.

This research is primarily conducted to amplify the data security and privacy that is already in place for Artificial Intelligence in combating world hunger. The existing software in the market and the ones that are being used for Artificial Intelligence have one thing in common; they both have separate functionalities based on their specific roles. As an example, Oracle Data Safe mainly functions as a Database Security Software(DSS) while Cisco ACI and Incydr are Data Center Security Software(DCS) and Data Loss Prevention Software (DLP) respectively. Through 'SecureServ', the software that we are developing to prevent and thus stop data breaches and data loss/leak from happening will now increase the efficiency of Artificial Intelligence in combating world hunger. Data or information of people will now be 100% secured and safe from hackers or cybercriminals as the software now possess all the security features of available software in market. SecureServ is based on the three classic goals of data security software also known as CIA triad; Confidentiality, Integrity and Availability. By using this software, users such as the company head of security for the IT department will have access to configure the security options or features provided for the AI to do its dedicated job. This way, if there are any cases of data breach or data leak, only the person who has access to these features will be held accountable. It can also be said in a metaphorical way that only 1 person knows the nuclear codes; works for both security and responsibility wise.

V. METHODOLOGY

This study employs a quantitative method to investigate the requirements for implementing an enhanced data privacy and security for Artificial Intelligence. Quantitative research is the act of gathering and analysing numerical data in order to uncover trends, make predictions, and extrapolate findings to larger populations (Bhandari, 2020). Respondents are asked ten critical questions in a 5-point Likert Scale manner in order to better grasp their perspective on the scenario. To restrict the research, questions on efficiency and security are focused in the survey. The surveys are dispersed throughout the country, concentrating both on IT and non-IT areas, to get a big sample of people's opinions on the importance of privacy and data security. As a result, to increase response rates, the survey is given online using Google Forms. Aside from that, this survey is also done in person for 50 persons mainly focused on large IT company employees. Stratified sampling, a probability sampling strategy, is used to obtain more exact findings by guaranteeing that every subgroup in the sample is represented. Outliers are treated and missing data is handled before the data is analysed. The missing data will be imputed using mode imputation, which assigns the most common value to the incomplete data.

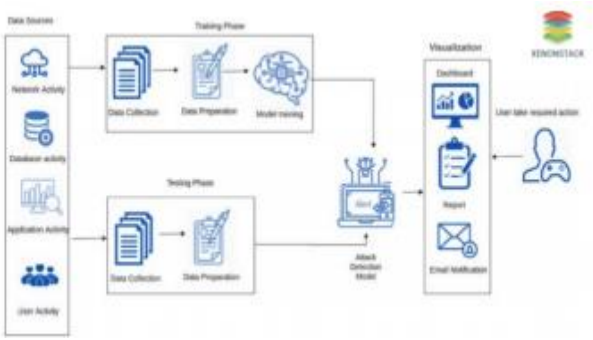

Fig. 3 Sample prototype, SecureServ

For this research, the training phase and the testing phase is the most critical part in providing a better result so that AI could function more efficiently to combat world hunger. As discussed above, the data that has been collected consists of hundreds of fields of information on each individual such as their location, background history, daily lifestyle and etc. These data's value is too high and can be risky to the company if there happens to be a data breach/loss as this would mean that they are in breach of the T&C of privacy and security of an individual. By implementing a stronger data security and privacy tool/software, this would reduce the risk of data loss and thus enhance the results of AI as the data are now 100% accurate. SecureServ is an integrated system software that helps protect data from being stolen or damaged, for an example, due to a 'virus' outbreak. The software is simple and basic which creates opportunity for bigger and better improvements to be made in the near future. As it focuses on simplicity, the software's main target is to protect the database of AI.

VI. CONCLUSION

We began this project with an assessment of recent survey papers concentrating on AI security and privacy challenges. We discovered that many of the prior surveys did not include attacks and countermeasures throughout all machine learning task groups, with the majority focused solely on deep neural networks in computer sight, natural language processing, and cybersecurity (OSENI, MOUSTAFA and JANICKE, 2022). We begin by presenting a theoretical backdrop of machine learning task types and making a clear difference between shallow learning techniques and the more current deep learning methods as a foundation for explaining adversarial assaults on machine learning models. Then, by first specifying an adversary's goals, knowledge, and capabilities, we propose a novel framework for a holistic evaluation of adversarial assaults on AI systems, followed by a detailed assessment of attacks and response mechanisms covering numerous machine learning models (OSENI, MOUSTAFA and JANICKE, 2022).

REFERENCES

Artificial Intelligence and Global Challenges—A plan for progress. Medium. (2022). Retrieved 10 February 2022, from https://medium.com/daia/artificial-intelligenceand-global-challenges-a-plan-for-progress603efece1905.

Artificial intelligence summary. Encyclopedia Britannica. (2022). Retrieved 10 February 2022, from https://www.britannica.com/summary/artificial-intelligence.

Best Data Security Software. (2022). Retrieved 10 February 2022, from https://www.g2.com/categories/data-security.

Brooks, R. (2022). Must-Have Data Protection Controls. Blog.netwrix.com. Retrieved 10 February 2022, from

https://blog.netwrix.com/2020/02/06/musthave-data-security-controls/.

Brownlee, J. (2022). Data Leakage in Machine Learning. Machine Learning Mastery. Retrieved 10 February 2022, from https://machinelearningmastery.com/dataleakage-machine-learning/.

Bhandari, P. (2022). An introduction to quantitative research. Scribbr. Retrieved 10 February 2022, from https://www.scribbr.com/methodology/quantitative-research/.

Data Breach 101: Top 5 Reasons it Happens WHOA.com. WHOA.com. (2022). Retrieved 10 February 2022, from https://www.whoa.com/data-breach-101-top-5- reasons-it-happens/.

How To Prevent Data Breaches In 2021: 12 Best Practices. Paysimple. (2022). Retrieved 10 February 2022, from https://paysimple.com/blog/how-to-preventdata-breach/.

Vadapalli, P. (2022). Top 7 Challenges in Artificial Intelligence in 2022 | upGrad blog. upGrad blog. Retrieved 10 February 2022, from https://www.upgrad.com/blog/top-challengesin-artificial-intelligence/.

8 Most Common Causes of Data Breach. Sutcliffe Insurance. (2022). Retrieved 10 February 2022, from https://www.sutcliffeinsurance.co.uk/news/8- most-common-causes-of-data-breach/.

Oracle Data Safe. Oracle.com. (2022). Retrieved 10 February 2022, from https://www.oracle.com/a/tech/docs/dbsec/data-safe/faq-security-data-safe.pdf.

Using Oracle Data Safe. Oracle Help Center. (2022). Retrieved 10 February 2022, from https://docs.oracle.com/en/cloud/paas/datasafe/udscs/get-started-oracle-data-safe.html.

Poza, D. (2022). What is Data Security? Learn Data Security Best Practices. Auth0 - Blog. Retrieved 10 February 2022, from https://auth0.com/blog/what-is-data-security/.

Lappé, F., & Collins, J. (2022). Foodfirst.org. Retrieved 11 February 2022, from https://foodfirst.org/wpcontent/uploads/2015/08/Summer-2015-Backgrounder-10-Myths.pdf

The 16 Best Data Protection Software Companies for 2022. Best Backup and Disaster Recovery Tools, Software, Solutions & Vendors. Retrieved 10 February 2022, from https://solutionsreview.com/backup-disasterrecovery/the-best-data-protection-softwareofferings/.

Using Oracle Data Safe. (2022). Retrieved 10 February 2022, from https://docs.oracle.com/en/cloud/paas/datasafe/udscs/get-started-oracle-data-safe.html