Role of Machine Learning in Managing Cloud Computing Security

Santosh Kumar
Assistant Professor Computer Science and Engineering Dr. APJ Abdul Kalam Women's Institute of Technology, Darbhanga
jha.santoshkumar@yahoo.co.in

Nithya.S
Assistant Professor, Department of Computer Science and Engineering, Coimbatore Institute of Technology
snithyacit@gmail.com
0000-0001-5253-1469

K.N Apinaya Prethi
Assistant Professor, Department of CSE, CIT
apinayaprethi@cit.edu.in
0000-0003-4292-7966

Suraj Singh
Assistant Professor, Electrical Engineering Department, M. M. Engineering College, M. M. (Deemed to be University), Mullana, (Ambala)
surajsinghynr8@gmail.com

Melanie Lourens
Department of Human Resources Management, Durban University of Technology, South Africa
Melaniel@dut.ac.za

Nisha Patil
Assistant Professor, School of Computer Sciences and Engineering, Sandip University, Nashik
npatil21@gmail.com
0000-0002-0071-077X

2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) | 978-1-6654-3789-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICACITE53722.2022.9823414

***Abstract*- Cloud computing is one of the most trending technology through which digitalized data management and storing becomes easier and more effective. However, besides the advancement of technology, data protection is another top priority concerning factor as millions of sensitive data are gets stored and transferred through the cloud computing system. As per the current days of cyber-activities, data security threat in cloud computing have increased, which posses threat in the development of the business. In that field, machine learning based advanced algorithm develop the virtual encrypted environment to protect the data from unauthorized access and hacking.**

Keywords: Cloud computing, Machine learning, Artificial Intelligence, DDOC, Data security, Encrypted environment

I. INTRODUCTION

Technological development has enabled the process of data management and business operation faster and more efficient. By utilizing the advanced technology, a more complex data set can be implemented, use and manage easily that effectively improving the business operations and services. In this context, this research is going to demonstrate a deep insight into machine learning in management cloud computing. After the initiation of the digitalization of all kinds of business, domestic and personal activities, the demand for the cloud computing system has been increased rapidly. With the help of such a system, one can store or access data from anywhere by using the cellular or wired connected network system [1]. Now, such circumstances, data stealing and data hacking become a great threat to the researchers and developers as leaking of sensitive or personal data may raise a huge loss for the society and business. In order to prevent such incidents, the collaboration of the machine learning-based algorithm and AI technology brought a secure environment by introducing the AES-256 encryption system. It has been observed that in the current days the majority of the company use cloud computing to keep the data safe and operate their work from different parts of the world and it is considered to be a business platform where production and all data of the business are stored [2]. The main advantage of the AI-based machine learning encryption system is that it can able to analyze the patterns and learn new protective measures from that pattern. Based on this technique, when a similar kind of pattern tries attack further, it immediately takes action against that. The main purpose of the research is to look after the threats and machine learning to develop security in cloud computing.

II. LITERATURE REVIEW

The cloud-computing infrastructure in the current days has developed and it is important to look after security development. However, it is mainly to be looked after by the service providers to develop a robust cloud computing security in the current days. The cloud computing revenue in the UK market has increased and it was almost 15.57 Billion Dollars in the current days. Machine learning and cloud computing along with the "Internet of Things" is considered to be novel technology that has evolved in the IT sector [3]. Various devices are used for the performance of the business along with the use of big data analytics, AI technology has improved the services and looks after the prevention of data in cloud computing.

Various researchers have been identified several issues and security threats regarding cloud security by implementing several machine learning programs. However, cloud computing plays a huge role in the field of machine learning, as it enables the overall cloud data facilities and equipment to boost the technological fields. Although, the cloud system faces too many compliances and disruptions towards achieving huge significance in both the small and large scale companies that operate through information technologies programs in order to enhance their potential growth the business [4]. There are various data encryption formats have been identified through the entire process of identifying threats and security towards implementing machine learning. It has been observed that machine learning

has been essentially eligible to identify the strength and weaknesses of the company as well as the employee's skills in the technical field within the organization.

It has been observed that various consideration and security advance programs that operate through machine learning has been failed to implement any task or procedure within the enterprise's cement have been emerged with the technology system of the organization, as a result. In such a case various data has been breached as failed to implement the machine learning techniques within organizations [5]. It has been identified that multiple of technology advancement has been made during the entire process of machine learning programs within cloud computing or data security as per the current market requirements within organizations.

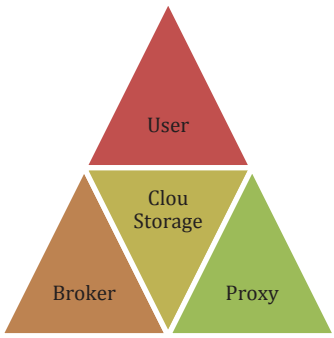

Fig 1: Cloud computing

(Source: [6])

The innovative model that has generally been utilized by the operational leaders of the organizations to detect threats against any data protection in machine learning is the ***software as a service.*** It has been capable to detect threats and enable various opportunities in terms of enabling data security and information techniques within organizations [7]. However, it is efficient in terms of deriving data and protects it from various theft, therefore, the employees need an adequate training facility through applying for the machine learning programs.in addition, the operational leaders of the business using artificial intelligence techniques to secure the several elements and functions of machine learning programs in the field of gaining knowledge and skills to boost the security system of machine learning.

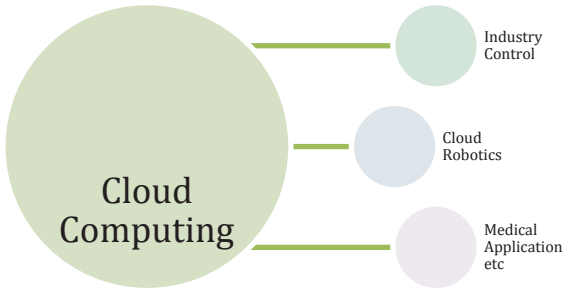

Fig 2: Cloud computing in CCS

(Source: [8])

It has been observed that for the vendor's cloud storage stability is important, hence machine learning and cloud computing models have been suggested for the protection of the data in cloud computing [9]. In the current days, it has been observed that ***API*** and software ***developer's kits*** allow organizations to embed machine learning facilities into applications and mitigate the threat of DDOS [10]. It can be stated that cloud computing has developed the business organization performance but also enhanced the risk of losing sensitive information of the company affecting its reputation in the current days.

III. METHODOLOGY

The research purpose has been met by following the primary and secondary research method which has enabled the collection of the data and helped to look after the current trends in cloud computing. The primary research has been conducted where quantitative analysis has been done for collecting data on machine learning in cloud computing thereat. The relevant data have been collected from google scholar by using keywords like ***Saas***, ***and Cloud computing***, and 40 participants have been involved in collecting the data and meeting the objectives of the research. Individuals in cloud computing have been targeted as the main source for collecting data and sharing. In this research study, it has been observed that the primary data would be collected from the employees involved in cloud computing and machine learning in the organization [11].

The proper reason behind implementing machine learning techniques in the field of technology as well as in organizations towards achieving the sustainable business goal. This is due to identifying various business objectives and strategic goals to identify the positive impacts and influence of machine learning. It enables the business to transform digitally as well as make it sustainable to achieve the innovative facility towards protecting the business data and its security regarding business digitalization. It was also helpful in implementing the business digitally transforms through generating innovative ideas and proper business information digitally as well as on company websites [12]. However, it seems to be challenging sometimes such as to drastically enter the unauthentic folder within the cloud computing programs and tools to identify a necessary source to mitigate such disruptions while performing business digitally. Interpretive research philosophy has been followed to collect the data as it enables flexibility to the researcher and achieves the purpose of the research. It has been observed that a deductive approach has been followed as it helps to look after the machine learning and the cloud computing model helps to mitigate security issues in cloud computing.

In order to collect the secondary data, authenticated sources have been used based on machine learning and cloud computing. The overall research study has been designed by the ***primary descriptive data*** as it enables the overall information's towards to achieve business potential as well coordinate the work culture within the organization digitally. It has been observed that descriptive design is followed by the researcher as it enables the researcher to think freely and allows the flexibility to collect essential information. The major identifying issues regarding implementing various techniques of business transformations digitally through evaluating the secondary business data and analysis that has been relevant to identifying various threats and difficulties towards implementing programs. Another issue in collecting the secondary data is that the information provided might become invalid or may not be relevant, which might be a research gap [13].

However, companies adopt some principles ethics, and advancements usually in a common way to implement the data security programs towards to achieve the technological goals in the field of machine learning. In addition, ethics such as ***"transparency techniques*** "that equally satisfy the ethics and integrity of the business towards implementing the machine learning programs within the organizations. It has been clearly stated that the researcher collects appropriate data or information's to incorporate the research programs in order to secure cloud computing technology during implementing the machine learning programs within the business. In addition, it has been more valuable in any other field rather than information technology.

IV. ANALYSIS AND INTERPRETATION

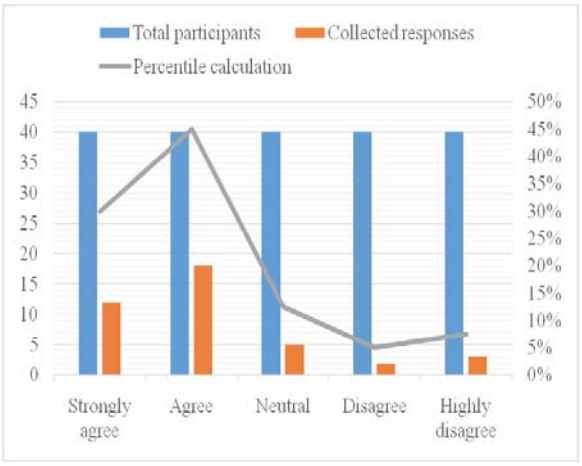

Fig 3: Graphical presentation of the response to question 1

(Source Created by the learner)

Making a complete evaluation of question 1 it has been identified that most people have agreed with the fact that machine learning is an essential aspect in order to protect cloud computing.

Survey question 2: Do you believe or agree with the fact that ML and AI are helping to exhibit intelligent actions through which solutions can be provided?

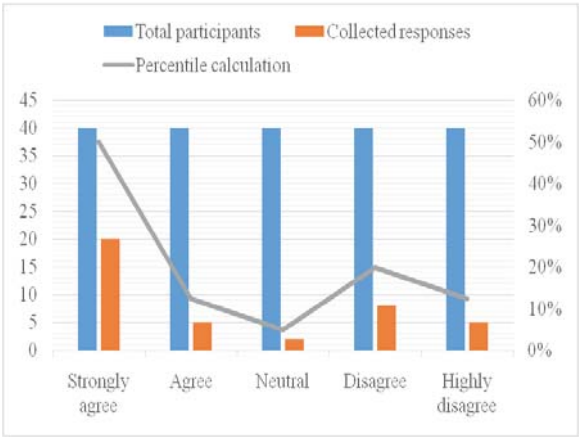

Fig 4: Graphical presentation of the response to question 2

(Source Created by the learner)

The evaluation of the second question helps to reflect the fact that intelligent actions are implemented through the ML that is powered by AI.

Survey Question 3: What roles are played by Machine learning in terms of providing cloud computing security?

TABLE: RESPONSE OF QUESTION 3
(SOURCE: CREATED BY THE RESEARCHERS)

Google form options	**Total participants**	**Collected responses**	**Percentile calculation**
Data protection through prevention	40	8	20%
Detection of attacks	40	8	20%
Providing automated solution	40	8	20%
Making a prediction about the risk factors	40	8	20%
Malware analysis	40	8	20%

The evaluation of the above response helps to identify that five major activities are helping to provide protection. It is also identified that ML enables detection, identification, and remediation and

V. DISCUSSION AND FINDINGS

Based on the above evaluation it has been identified that AI-powered machine learning is enabled through algorithms that helps to identify the risk in real-time. More specifically, through the help of this technology, the total number of inputs that are provided can be analyzed very accurately [14]. Therefore, detection of malware becomes easy with this technology. In terms of making predictions, it is identified that the time series data are used within this technology. Clustering is also another integrated part of this technology and as per the evaluation it is identified to be making identification of SOC (Security Operation Centre) [15]. Therefore, it has been identified that the process includes taking inputs from previous incidents that have detected the same type of attacks. Therefore, using the business productivity while reducing the employee's profits and technology considerations towards business digitalization, as it becomes more informative and useful techniques that derive the business operation through digitally as well as more efficiently that impacts the overall business security and data that implement through making proper innovation and tools to make it incorporate [16].

Several innovations and digitalization keeping ahead the business and help to essentially look forward on the innovative experiences of machine learning that further enable the organization to achieve the business goals [17]. By using AI based machine learning technology, any type of irregularities in the pattern can be detected in real-time therefore the scope of early detection of malware can be identified. Various forms of digital techniques have been evaluated to implement machine learning within the organizations such as "spreadsheet to cloud CRM". However, it helps to improve the multiple rates and technological factors towards enhancing the positive relationship between the employees and the operational business leaders [18]. Therefore, proper cloud computing data techniques help the business to perform digitally by implementing transformational process such as machine learning programs to enable product specifications and quality improvement within organizations [19] Moreover,

the operational manager of the company implements the "ongoing training procedure "to improve the quality cost and training facilities while ongoing programs such as machine learning. This helps to move the business through digitally. Furthermore, the business transforms digitally, while functioning towards implementing the business practices, as well as operates business digital across the world rather than in the UK [20]. In such a case the company achieves well support to the various call centers regarding identifying the positive experiences regarding business implementation digitally.

VI. CONCLUSION

It can be concluded that the cloud computing threat has increased in the current days, which has affected the development of the business in the current days. It has been observed that the company faces various threats and uncertainties in identifying the proper tools and requirements to implement machine learning programs within the business data. However, it helps the business as well as protect it from various disruption such as hackers and security breaches as well as many more to incorporate them into appropriate actions required by the operational managers of the company. It has been observed that the DDOS threat has enabled hackers to affect the financial position of an organization by hacking sensitive data of the organization.

The Saas model in cloud computing has been used by the organization to reduce the production cost and look after the development of the business. Software developer's kits are used in the current days help to mitigate the issue of security threats in cloud computing. AI technology has been used to look after malware and prevent the loss of data in the current days. End-to-end encryption helps to prevent loss of data and machine learning helps to look after variables in the input learning in the research. Primary and secondary research strategies have been followed that help to meet the purpose of the research and look after the development of the research. Random sampling techniques have been avoided in this research and data have been collected from 40 participants. Cloud computing related potential threats has also uplifted in this study for in depth discussion. Although several issues and threats have been identified towards implementing the machine learning programs in practice. In such case, artificial intelligence techniques have been significantly compatible as well as plays a huge role. The innovative techniques of artificial intelligence have been able to boost technological advancement toward to achieve sustainable business goals in terms of business transformation through digital.

VII. ACKNOWLEDGEMENT

I would like to thank my professor for providing me with the opportunity to get a deep insight in terms of cloud computing. I would also like to thank my mentor for collecting authenticated data and completing the project on time. I would like to thank my family and friends for providing support while I was doing the project.

REFERENCES

[1] Stergiou, C.L., Plageras, A.P., Psannis, K.E. and Gupta, B.B., 2020. Secure machine learning scenario from big data in cloud computing via the internet of things network. In Handbook of computer networks and cyber security (pp. 525-554). Springer, Cham.

[2] Bhattacharyya, S.P., Datta, A. and Keel, L.H., 2018. Linear control theory: structure, robustness, and optimization. CRC press.

[3] Balne, S., 2019. Review on Challenges in SAAS Model in Cloud Computing. Journal For Innovative Development in Pharmaceutical and Technical Science, 2, pp.8-11.

[4] A. Jain, A.K.Yadav & Y. Shrivastava (2019), "Modelling and Optimization of Different Quality Characteristics In Electric Discharge Drilling of Titanium Alloy Sheet" Material Today Proceedings, 21, 1680-1684 https://doi.org/10.1016/j.matpr.2019.12.010

[5] Zekri, M., El Kafhali, S., Aboutabit, N. and Saadi, Y., 2017, October. DDoS attack detection using machine learning techniques in cloud computing environments. In 2017 3rd international conference of cloud computing technologies and applications (CloudTech) (pp. 1-7). IEEE.

[6] A. Jain, A. K. Pandey, (2019), "Modeling And Optimizing Of Different Quality Characteristics In Electrical Discharge Drilling Of Titanium Alloy (Grade-5) Sheet" Material Today Proceedings, 18, 182-191 https://doi.org/10.1016/j.matpr.2019.06.292

[7] Johnston, M.P., 2017. Secondary data analysis: A method of which the time has come. Qualitative and quantitative methods in libraries, 3(3), pp.619-626.

[8] A. Jain, A. K. Pandey, (2019), "Multiple Quality Optimizations In Electrical Discharge Drilling Of Mild Steel Sheet" Material Today Proceedings, 8, 7252-7261 https://doi.org/10.1016/j.matpr.2017.07.054

[9] V. Panwar, D.K. Sharma, K.V.P.Kumar, A. Jain & C. Thakar, (2021), "Experimental Investigations And Optimization Of Surface Roughness In Turning Of EN 36 Alloy Steel Using Response Surface Methodology And Genetic Algorithm" Materials Today: Proceedings, Https://Doi.Org/10.1016/J.Matpr.2021.03.642

[10] Tuli, S., Tuli, S., Tuli, R. and Gill, S.S., 2020. Predicting the growth and trend of COVID-19 pandemic using machine learning and cloud computing. Internet of Things, 11, p.100222.

[11] A. Jain, C. S. Kumar, Y. Shrivastava, (2021), "Fabrication and Machining of Metal Matrix Composite Using Electric Discharge Machining: A Short Review" Evergreen, 8 (4), pp.740-749 https://doi.org/10.5109/4742117

[12] A. Jain, C. S. Kumar, Y. Shrivastava, (2021), "Fabrication and Machining of Fiber Matrix Composite through Electric Discharge Machining: A short review" Material Today Poceedings https://doi.org/10.1016/j.matpr.2021.07.288

[13] Zimmermann, S., Kunze, F., Digitalisierung, D., & Haufe, D. (2019). Digital Fluency–eine Metakompetenz der Zukunft. HR-Trends, 3-4.

[14] T.S. Papola & Nitu Maurya & Narendra Jena, 2015. "Inter-Regional Disparities in Industrial Growth and Structure," Working Papers id:6607, eSocialSciences.

[15] Duriawati, A. D., Wasliman, I., Mulyanto, A., & Barlian, U. C. (2020). Implementation of Literation Based Learning Information Technology. International Journal of Nusantara Islam, 8(2), 240-253.

[16] C. M. Thakar, S. S. Parkhe, A. Jain, K. Phasinam, G. Murugesan (2022), "3d Printing: Basic principles and applications" Material Today Proceedings, 51, 842-849. https://doi.org/10.1016/j.matpr.2021.06.272

[17] Cunha, M. M. Q. S. D. (2021). Marketing plan for Semear program-product/service development for the B2c market segment (Doctoral dissertation).

[18] [18] Kateja A, Maurya N. Inequality in Infrastructure and Economic Development: Interrelationship Re-examined. The Indian Economic Journal. 2011;58(4):111-127. https://doi.org/10.1177/0019466220110407

[19] Grami, S., & Chalak, A. (2020). Discourse of Requests:(Im) politeness Strategies in Virtual vs. Actual Life of Iranian EFL Learners. Journal of Language and Discourse Practice, 1(2), 45-60.

[20] Loretti, R. A., Da Costa, V. F. P., Memoria, D. G. D. O., Barbosa, A. N., Oliveira, H. L. S., Wegner, I. R., & Zank, C. A. C. (2019, October). Data Science and Business Intelligence Techniques for Learning from Environmental Accident Analysis for Offshore Oil Fields. In Offshore Technology Conference Brasil. OnePetro.