IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

THE IMPORTANCE OF MACHINE LEARNING ALGORITHMS IN SECURING CLOUD APPS

[1]VijayRaj, [2]Manasa

[1]Asst.Prof, [2]Decsion Scientist

[1]Department of Computer Applications,

[1]V.V.N. Degree College, Bangalore, India

[2] Mu-Sigma Business Solutions Pvt. Ltd, BANGALORE, India

Abstract: As cloud services become more commonplace, it is very much required to secure those services from malicious attacks. There are many tools available to help secure cloud applications, one of the most promising is artificial intelligence (AI). Artificial Intelligence is being used in cloud computing in a variety of ways. One of the main areas where artificial intelligence is being applied to secure cloud-based application from threats. Machine learning is a technology that has proved to produce better results in securing the cloud applications in the recent times. Machine learning algorithms are trained on the various authentic datasets to build models that can automate the process of detecting the attacks on cloud apps with higher accuracy in comparison with any other technology. This research paper reviews the role of machine learning algorithms in securing cloud apps

Index Terms **– Cloud Computing, Artificial Intelligence, Machine Learning, Cloud Apps, Threats**

I. INTRODUCTION

Artificial intelligence and cloud computing are two of the most important technological advances of this era. Artificial intelligence (AI) refers to the ability of machines to simulate human intelligence and perform tasks that normally require human intelligence. Artificial intelligence can be used to automate complex tasks, analyze large amounts of data and make predictions. Cloud service refers to the delivery of computing services, including servers, storage, databases and software, over the Internet. Cloud computing allows organizations to use computing resources as needed and pay only for what they use, instead of investing in and maintaining their own IT infrastructure. The integration of artificial intelligence in cloud computing has improved accuracy, speed and efficiency. Artificial intelligence can automate complex tasks in cloud services, optimize system performance, personalize services, improve security and user experience. ML algorithms are used to solve data security problems and manage data more efficiently. ML is the use of human-made consciousness to allow frameworks to be adopted normally and truly evolve without explicitly adapting them. ML focuses on developing computer programs that find the appropriate pace to be used for independent learning. Learning begins with observations or information such as models, immediate understanding or rubrics to channel knowledge structures and then make better decisions about the subject based on the models provided.

II. RELATED WORK

In this section, we study related papers that considered the issue of cloud security using ML algorithms. Then, we discuss the comparison of the related papers with our paper.

in order to enhance the healthcare services on the cloud computing environment, Abdelaziz et al. [1] designed a machine learning model. The results show that the proposed model is 50% more efficient than the current state of the art models in terms of total execution time. Furthermore, the system efficiency in terms of real-time data extraction improves by 5.2% and the hybrid intelligent model predicts CKD with 97.8% accuracy.

Masetic et al[2] looked at three criteria types: Types of classification: Type of learning algorithm Input features Cloud computing level Masetic et al Proposed the Cloud Computing Threat Classification Model Fully Feasible Machine Learning Algorithms to Detect Threats SIGMM Spam Detection Scheme SIGMM is a Spam Identification scheme that uses machine learning to identify Spam on industrial mobile networks SIGMM provides intelligent Spam Identification without Flexible and Reliable Relationships

Kumar et al., [4] recommend an intrusion detection methodology using deep learning technique, which is based on fuzzy min max neural network-based intrusion detection system, FMMNN-IDS. Nguyen et al., [5] discuss a preventive approach to identify and isolate cyberattacks before they can have a significant impact on mobile cloud computing system, and proposes a novel framework that uses a deep learning approach in mobile cloud environment to detect cyberattacks. Using experimental results, Nguyen et al., [6] demonstrate that their proposed framework not only detects diverse types of cyberattacks, but achieves a high accuracy of up to 97.11% in detecting the attacks.

Chkirbene et.al [6] propose another firewall conspire named Upgraded Interruption Identification and Order (EIDC) framework for secure distributed computing climate. Aljamal et.al [7] propose an organization-based peculiarity recognition framework at the Cloud Hypervisor level that uses a crossover calculation: a mix of K-implies bunching calculation and SVM characterization calculation, to work on the precision of the oddity location framework.

Singh, A., & Chatterjee, K.[7]. describes several key topics related to the cloud, namely cloud architecture framework, service and deployment model, cloud technologies, cloud security concepts, threats, and attacks.
Y. Xin *et al* [8],describes key literature surveys on machine learning (ML) and deep learning (DL) methods for network analysis of intrusion detection and provides a brief tutorial description of each ML/DL method.

III. ABOUT CLOUD COMPUTING:

A. Cloud Computing:

The term "cloud" in distributed computing is utilized synomously with "server farm". Today the figuring field can imagine changing into the distributed computing time due to the amazing advances in processing and data advances during the beyond thirty years. The advances incorporate the development of the Web spine, the far and wide reception of broadband admittance to the Web, the strong organization of servers and capacity in server farms, the advances in elite execution and versatile programming framework for the server farms and the Internet, and so on.

Cloud computing alludes to both the applications conveyed as administrations over the Web and the equipment and frameworks programming in the server farms that offer those types of assistance. The actual administrations have for quite some time been alluded to as Programming as a Help (SaaS).a A few sellers use terms like IaaS (Foundation as an Assistance) and PaaS (Stage as an Assistance) to depict their items, however we shun these on the grounds that acknowledged definitions for them actually change broadly. The line between "low-level" framework and a more elevated level "stage" isn't fresh. We accept the two are more similar than various, and we consider them together. Essentially, the connected term "framework registering," from the elite exhibition figuring local area, recommends conventions to offer shared calculation and capacity over significant distances, yet those conventions didn't prompt a product climate that developed past its local area.

The server farm equipment and programming is what we will call a cloud. At the point when a cloud is made free in a pay-more only as costs arise way to the overall population, we call it a public cloud; the help being sold is utility figuring. We utilize the term private cloud to allude to inward server farms of a business or other association, not made accessible to the overall population, when they are sufficiently huge to profit from the upsides of distributed computing that we examine here. Accordingly, distributed computing is the amount of SaaS and utility processing, however does exclude little or medium-sized server farms, regardless of whether these depend on virtualization for the board. Individuals can be clients or suppliers of SaaS, or clients or suppliers of utility registering. We center around SaaS suppliers (cloud clients) and cloud suppliers, which stand out than SaaS client

B. Cloud Service Models:

There are the following three types of cloud service models –

- **Infrastructure as a Help (IaaS):** IaaS is otherwise called Equipment as a Help (HaaS). It is a registering foundation overseen over the web. The fundamental benefit of utilizing IaaS is that it assists clients with keeping away from the expense and intricacy of buying.
- **Platform as a Services (PaaS):** PaaS is a cloud administration model that gives a prepared to-utilize improvement climate where engineers can have practical experience recorded as a hard copy and executing excellent code to make redid applications. It assists with making an application rapidly without dealing with the hidden framework. For instance, while conveying a web application utilizing PaaS, you don't need to introduce a working framework, web server, or even framework refreshes. Nonetheless, you can scale and add new elements to your administrations.
- **Software as a Service (SaaS):** Cloud customers discharge their applications on a facilitating climate, which can be gotten to through networks from different clients (for example internet browser, PDA, and so on.) by application clients. Cloud purchasers don't have command over the Cloud foundation that frequently utilizes a multi-occupancy framework engineering, specifically, unique cloud buyers' applications are coordinated in a solitary coherent climate on.

C. Characteristics of Cloud Computing:

- In Cloud computing, clients access the information, applications or some other administrations with the assistance of a program no matter what the gadget utilized and the client's area. The framework which is by and large given by an outsider is gotten to with the assistance of web. Cost is diminished to a huge level as the framework is given by an outsider and need not be procured for periodic concentrated figuring errands.
- Reliable Service can be acquired by the utilization of various destinations which is appropriate for business congruity [4] and debacle recuperation [4]. Be that as it may, some of the time many distributed computing administrations have endured blackouts and in such occasions its clients can barely do anything [5].
- Sharing of Resources and expenses among a huge assortment of clients permits effective use of the framework.
- Upkeep is more straightforward if there should be an occurrence of distributed computing applications as they need not be introduced on every client's PC

D. Cloud Computing Architecture:

Cloud computing framework can be isolated into two areas: the front end and the back end. The two of them are associated with one another through an organization, generally the web. Front end is what the client (client) sees while the back end is the haze of the framework. Front end has the client's PC and the application expected to get to the cloud and the back has the distributed computing administrations like different PCs, servers and information stockpiling

The below diagram shows the different layers of cloud computing architecture.

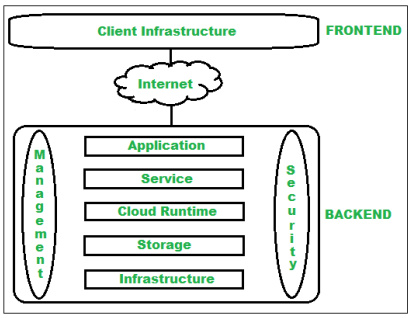

Figure 1: Cloud Computing Architecture

Frontend: Frontend of the cloud design alludes to the client side of distributed computing framework. Implies it contains all the UIs and applications which are utilized by the client to get to the distributed computing administrations/assets. For instance, utilization of an internet browser to get to the cloud stage

- **Client Infrastructure –** Client Framework is a piece of the frontend part. It contains the applications and UIs which are expected to get to the cloud stage. As such, it gives a GUI (Graphical UI) to cooperate with the cloud.

Backend: Backend alludes to the actual cloud which is utilized by the specialist co-op. It contains the assets along with deals with the assets and gives security systems. Alongside this, it incorporates colossal capacity, virtual applications, virtual machines, traffic light instruments, sending models

- **Application:** Application in backend alludes to a product or stage to which client gets to. Implies it offers the support in backend according to the client necessity.
- **Service:** Organization in backend implies the huge three sorts of cloud-based organizations like SaaS, PaaS and IaaS. Moreover, regulates which sort of organization the client gets to.
- **Runtime Cloud:** Runtime cloud in backend gives the execution and Runtime stage/climate to the Virtual machine.
- **Storage:** Capacity in backend gives adaptable and versatile capacity administration and the board of put away information.
- **Infrastructure:** Cloud Foundation in backend alludes to the equipment and programming parts of cloud like it incorporates servers, capacity, network gadgets, virtualization programming and so forth.
- **Management:** Management in backend refers to management of backend components like application, service, runtime cloud, storage, infrastructure, and other security mechanisms etc.
- **Security:** Security in backend alludes to execution of various security components in the backend for secure cloud assets, frameworks, documents, and foundation to end-clients.
- **Internet:** Web association goes about as the medium or a scaffold among frontend and backend and lays out the cooperation and correspondence among frontend and backend.
- **Database**: Data set in backend alludes to give data set to putting away organized information, like SQL and NOSQL data sets. Illustration of Information bases administrations incorporate Amazon RDS, Microsoft Purplish blue SQL data set and Google Cloud SQL.
- **Networking**: Organizing in backend administrations that give organizing foundation to application in the cloud, for example, load adjusting, DNS and virtual confidential organizations.
- **Analytics**: Examination in backend administration that gives examination abilities to information in the cloud, for example, warehousing, business knowledge and AI.

E. Benefits of Cloud Computing:

- Cloud computing frameworks can permit ventures to accomplish more productive utilization of their IT equipment and programming speculations. They do this by stalling the actual boundaries innate in segregated frameworks, and computerizing the administration of the gathering of frameworks as a solitary substance.
- Cloud computing is an illustration of an at last virtualized framework, and a characteristic development for server farms that utilize robotized frameworks the board, responsibility adjusting, and virtualization innovations.
- A cloud framework can be an expense proficient model for conveying data administrations, diminishing IT the board intricacy, advancing development, and expanding responsiveness through continuous responsibility adjusting.
- A lot of PC asset, as Xen virtual machines, can be provisioned and made accessible for new applications inside the space of minutes rather than days or weeks. Engineers can get to these assets through an entryway and put them to quickly utilize.

F. Threats to the cloud Apps:

Cloud Computing has a huge potential to develop and is turning out to be broadly well known. Notwithstanding, even with its exceptional attributes, it has different security dangers and insurance challenges.

Cloud Security Threats:

The Major security threats in cloud are confidentiality, Integrity and Availability

- **Confidentiality:** Comparable to security maintains a strategic distance from unapproved access of data. It includes guaranteeing the information is available by the people who are permitted to utilize it and obstructing admittance to other people.
- **Integrity:** This rule guarantees that the information is real, precise, and shielded from unapproved adjustment by danger entertainers or incidental client alteration.
- **Availability:** This guideline makes the data to be accessible and valuable for its approved individuals generally. It guarantees that these gets to are not frustrated by framework breakdown or digital assault.

Types of Attacks on the cloud apps:

- **Network based attacks:** Network-based assaults are assaults intended to think twice about security by either snooping on or catching and controlling organization traffic. These might be dynamic assaults, wherein the programmer controls network action progressively; or on the other hand inactive assaults, wherein the assailant sees network movement yet doesn't endeavour to change it.
- **Storage-based attacks**: Capacity security is the gathering of boundaries and settings that make capacity assets accessible to approved clients and confided in networks - - and inaccessible to different elements. Capacity security can envelop equipment the executives, application improvement, network security controls, correspondences conventions, hierarchical strategy, actual security and client conduct. Capacity security likewise incorporates a scope of issues, including network security and cyberthreats. Insurance should be given against online dangers, for example, infections, worms, Trojans and other noxious code.
- **Application-based attacks:** Web application assaults are malevolent exercises that target web applications by taking advantage of weaknesses in their plan or execution. These assaults can bring about unapproved access, information burglary, or other hurtful outcomes. Normal kinds of web application assaults incorporate SQL infusion, cross-webpage prearranging (XSS), cross-webpage demand imitation (CSRF), and record consideration assaults. Assailants might utilize robotized devices or physically create their assaults to sidestep safety efforts and get close enough to delicate data or frameworks.

Security Issues in Cloud Services:

A detail discussion on different security issues and challenges of cloud computing are presented in . The summary of each security issue is discussed as follows.

- **Authentication**: It is the process of verifying the credentials of the users requesting access to cloud applications and data.
- **Authorization**: It is the system through which the privileges are granted to the users to access the cloud resources.
- **Key Management**: It refers to the management of cryptographic keys such as key creation, key storage, key backup, key rotation, key expiration, key archival and key destruction activities etc.
- **Data Confidentiality**: It allows sensitive or confidential data should be accessible only to authorized users.
- **Data Security** at Rest: It refers to when the data is stored on permanent storage devices like hard disk or tapes, such data must be prevented from unauthorized access.
- **Data Security in Transit**: It refers to protecting the sensitive data while the data is moving from one, location to another such as across the Internet.

IV. IMPORTANCE OF MACHINE LEARNING ALGORITHMS TO SECURE CLOUD APPS FROM THREATS:

Because they provide scalable and effective ways to handle and store data, cloud services are a crucial component of contemporary enterprises. But as organizations rely more and more on cloud services, making sure they are safe has become a top concern. With the threat landscape always changing, using artificial intelligence (AI) and machine learning (ML) has become a useful way to make the cloud more secure

Importance of using Machine Learning in Cloud Security:

- **Improving Threat Detection and Prevention**

  Because they are able to identify and stop potential threats in real time, AI and ML are particularly helpful for cloud security. By analyzing vast volumes of data and searching for trends, AI and ML systems may swiftly identify issues and potential security breaches. By enabling early detection and prompt response, this technique aids enterprises in staying ahead of cyber threats. AI-powered systems can recognize a sudden increase in data requests from a particular IP address as possibly suspicious and send out a warning for further investigation, assisting in the prevention of a distributed denial-of-service (DDoS) assault.

- **Intelligent Authentication and Access Control:**

  Cloud Computing must employ reliable techniques for access control and authentication if you want cloud-managed services to remain secure. By monitoring user behavior, recognizing suspicious activity, and making sure that multi-factor login is implemented, AI and ML technologies can be very helpful in this area. By continuously learning from user behavior, AI-driven systems can alter and enhance access control mechanisms to lower the risks associated with unlawful access.

  For instance, an AI-driven system can prompt additional authentication measures, such as requiring multi-factor authentication or even temporarily blocking access until the user's identity can be verified, if a user suddenly displays unusual browsing patterns, such as accessing a large number of sensitive files they don't typically interact with.

- **Advanced Threat Intelligence and Response**

  When it comes to gathering and analyzing threat intelligence data, AI and ML are invaluable resources. In order to discover fresh threats and vulnerabilities, these systems can acquire data from a variety of sources, including incident reports, security blogs, and threat feeds. Organizations

can use this information to create security plans that are proactive and quick to respond to any threats. As a result, their cloud infrastructures sustain less damage from security events. For instance, AI-powered systems may quickly learn the characteristics of a new form of malware or phishing campaign and proactively update security procedures across cloud managed services to stop possible infections and data breaches.

- **Automating Security Operations**

Manual security operations can be difficult to perform in cloud settings due to their size and complexity. AI and ML can automate many security functions, such as analyzing logs, finding vulnerabilities, and responding to security breaches. While most security teams see response tools as AI/ML engines that help turn false positives into "low levels," human analysts are still critical in making the final incident response decisions. Thus, AI/ML is seen as a powerful tool for detection and response teams.

Organizations can effectively manage information security risks in their cloud services, reducing human error and speeding up response time. For example, if a data security incident triggers an outage in cloud management, AI-based systems can automatically analyze logs associated with the incident, compare them to known threat indicators and initiate incident response actions, such as isolating affected resources. and notify the security team without manual intervention. A good example is AI/ML-based security, instrumentation, automation and response (SOAR) engines that can automatically respond to certain types of threats, reducing the overall burden on security teams.z

- **Predictive Security Analytics**

AI and ML enable predictive security analytics. This allows companies to anticipate potential security risks and address them before they occur. By looking at past data, these technologies can identify trends, identify gaps and predict potential future threats. This proactive approach allows organizations to take steps to prevent problems and improve cloud security.

V. CONCLUSION:

Cloud-based client data is extremely important, and its security cannot be jeopardized in any way. The researchers apply a number of innovative technologies that employ different security methods to improve the security of the cloud environment. There is a lot of room for machine learning to improve accuracy and automate security against known and undiscovered cloud assaults. The primary goal of this survey article is to provide readers with an up-to-date overview of the state of machine learning research in the subject of cloud security.

REFERENCES

[1] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). A survey on machine learning techniques for cyber security in the last decade. *IEEE access*, *8*, 222310-222354.

[2] Yavanoglu, O., & Aydos, M. (2017, December). A review on cyber security datasets for machine learning algorithms. In *2017 IEEE international conference on big data (big data)* (pp. 2186-2193). IEEE.

[3] Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018, May). On the effectiveness of machine and deep learning for cyber security. In *2018 10th international conference on cyber Conflict (CyCon)* (pp. 371-390). IEEE.

[4] Prasad, R., Rohokale, V., Prasad, R., & Rohokale, V. (2020). Artificial intelligence and machine learning in cyber security. *Cyber Security: The Lifeline of Information and Communication Technology*, 231-247.

[5] Handa, A., Sharma, A., & Shukla, S. K. (2019). Machine learning in cybersecurity: A review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *9*(4), e1306.

[6] Geetha, R., & Thilagam, T. (2021). A review on the effectiveness of machine learning and deep learning algorithms for cyber security. *Archives of Computational Methods in Engineering*, *28*, 2861-2879.

[7] A. Singh and K. Chatterjee, "Cloud security issues and challenges:A survey," J. Netw. Comput. Appl., vol. 79, pp. 88–115, 2017

[8] Xin, Yang, Lingshuang Kong, Zhi Liu, Yuling Chen, Yanmiao Li, Hongliang Zhu, Mingcheng Gao, Haixia Hou, and Chunhua Wang. "Machine learning and deep learning methods for cybersecurity." *Ieee access* 6 (2018): 35365-35381.

[9] M. D. H. Parekh, "An Analysis of Security Challenges in CloudComputing," IJACSA) Int. J. Adv. Comput. Sci. Appl., vol. 4, no. 1,pp. 38–46, 2013.

[10] Fraley, J. B., & Cannady, J. (2017, March). The promise of machine learning in cybersecurity. In *SoutheastCon 2017* (pp. 1-6). IEEE.

[11] Martínez Torres, J., Iglesias Comesaña, C., & García-Nieto, P. J. (2019). Machine learning techniques applied to cybersecurity. *International Journal of Machine Learning and Cybernetics*, *10*, 2823-2836.

[12] Vinayakumar, R., Soman, K. P., Poornachandran, P., & Menon, V. K. (2019). A deep-dive on machine learning for cyber security use cases. In *Machine Learning for Computer and Cyber Security* (pp. 122-158). CRC Press.

[13] Rekha, G., Malik, S., Tyagi, A. K., & Nair, M. M. (2020). Intrusion detection in cyber security: role of machine learning and data mining in cyber security. *Advances in Science, Technology and Engineering Systems Journal*, *5*(3), 72-81.

[14] Alghamdi, M. I. (2020). Survey on Applications of Deep Learning and Machine Learning Techniques for Cyber Security. *International Journal of Interactive Mobile Technologies*, *14*(16).

[15] Makawana, P. R., & Jhaveri, R. H. (2018). A bibliometric analysis of recent research on machine learning for cyber security. *Intelligent Communication and Computational Technologies: Proceedings of Internet of Things for Technological Development, IoT4TD 2017*, 213-226.

[16] Virmani, C., Choudhary, T., Pillai, A., & Rani, M. (2020). Applications of machine learning in cyber security. In *Handbook of research on machine and deep learning applications for cyber security* (pp. 83-103). IGI Global.

[17] De Lucia, M. J., & Cotton, C. (2019). Adversarial machine learning for cyber security. *Journal of Information Systems Applied Research*, *12*(1), 26.

[18] Soni, S., & Bhushan, B. (2019, July). Use of Machine Learning algorithms for designing efficient cyber security solutions. In *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)* (Vol. 1, pp. 1496-1501). IEEE.

[19] Ali, R., Ali, A., Iqbal, F., Khattak, A. M., & Aleem, S. (2020). A systematic review of artificial intelligence and machine learning techniques for cyber security. In *Big Data and Security: First International Conference, ICBDS 2019, Nanjing, China, December 20–22, 2019, Revised Selected Papers 1* (pp. 584-593). Springer Singapore.

[20] Gupta, A., Gupta, R., & Kukreja, G. (2021). Cyber security using machine learning: techniques and business applications. *Applications of Artificial Intelligence in Business, Education and Healthcare*, 385-406.

[21] Proko, E., Hyso, A., & Gjylapi, D. (2018). Machine Learning Algorithms in Cyber Security. In *RTA-CSIT* (pp. 203-207).

[22] Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, *19*(12), 1462-1474.

[23] Rege, M., & Mbah, R. B. K. (2018). Machine learning for cyber defense and attack. *Data Analytics*, *2018*, 83.

[24] Choraś, M., & Kozik, R. (2015). Machine learning techniques applied to detect cyber attacks on web applications. *Logic Journal of IGPL*, *23*(1), 45-56.

[25] Dushyant, K., Muskan, G., Annu, Gupta, A., & Pramanik, S. (2022). Utilizing Machine Learning and Deep Learning in Cybesecurity: An Innovative Approach. *Cyber Security and Digital Forensics*, 271-293.

[26] Thanuja, N., & Deepak, N. R. (2021, April). A convenient machine learning model for cyber security. In *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 284-290). IEEE.

[27] Hasan, Z., & Jishkariani, M. (2022). Machine Learning and Data Mining Methods for Cyber Security: A Survey. *Mesopotamian journal of cybersecurity*, *2022*, 47-56.

[28] Taleqani, A. R., Nygard, K. E., Bridgelall, R., & Hough, J. (2018, May). Machine learning approach to cyber security in aviation. In *2018 IEEE international conference on electro/information technology (EIT)* (pp. 0147-0152). IEEE.

[29] Goni, I., Gumpy, J. M., Maigari, T. U., Muhammad, M., & Saidu, A. (2020). Cybersecurity and cyber forensics: Machine learning approach. *Machine Learning Research*, *5*(4), 46-50.

[30] Vinayakumar, R., Soman, K. P., Poornachandran, P., & Akarsh, S. (2019). Application of deep learning architectures for cyber security. *Cybersecurity and Secure Information Systems: Challenges and Solutions in Smart Environments*, 125-160.

[31] M. D. H. Parekh, “An Analysis of Security Challenges in Cloud Computing,” IJACSA) Int. J. Adv. Comput. Sci. Appl., vol. 4, no. 1,pp. 38–46, 2013.

[32] Y. Z. An, Z. F. Zaaba, and N. F. Samsudin, “Reviews on Security Issues and Challenges in Cloud Computing,” IOP Conf. Ser. Mater. Sci. Eng., vol. 160, no. 1, 2016

[33] A. Verma and S. Kaushal, “Advances in Computing and Communications,” vol. 193, no. May 2014, 2011.

[34] T. Radwan, M. A. Azer, and N. Abdelbaki, “Cloud computing security: challenges and future trends,” Int. J. Comput. Appl.
Technol., vol. 55, no. 2, p. 158, 2017.

[35] Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, “Data Security and Privacy in Cloud Computing,” Int. J. Distrib. Sens. Networks, vol. 2014,2014.

[36] K. Hashizume, D. Rosado, E. Fernández-Medina, and E. Fernandez, "An analysis of security issues for cloud computing," J. Internet Serv. Appl., vol. 4, no. 5, pp. 1–13, 2013.

[37] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Futur. Gener. Comput. Syst., vol. 28, no. 3, pp. 583–592,2012.

[38] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," Inf. Sci. (Ny)., vol. 305, no. January, pp. 357–383, 2015.

[39] D. Puthal, B. P. S. Sahoo, S. Mishra, and S. Swain, "Cloud computing features, issues, and challenges: A big picture," Proc. -1st Int. Conf. Comput. Intell. Networks, CINE 2015, pp. 116–123, 2015.

[34] S. Singh, Y. S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," J. Netw. Comput. Appl., vol. 75, no. September 2016, pp. 200–222, 2016.