Artificial Intelligence Based Architecture to Enhance Cloud Computing Security

Noman Mazher[1], Zartashya Asharaf[1], and Mr Avinash Ganne[1]

[1]Univresity of Gujrat

January 23, 2023

Artificial Intelligence Based Architecture to Enhance Cloud Computing Security

Zartashya Asharaf[1], Mr. Avinash Ganne[2],Noman Mazher[3]

Univresity of Gujrat,Pakistan[1,2]

Sr. SAP Basis Cloud Architect, Raley's, Sacramento, California, USA[3].

ABSTRACT

Cloud computing (CC) provides users with online access to network services, including enhanced, transparent user management and the capacity to gather and process data. A shared Internet gateway is offered by CC, which is evolving into a private and public data center set. The integration of AI technologies into a substantial amount of computer resources, especially integrated systems, presents a number of resource problems that require careful adjustment. The IoT paradigm recently evolved in an application for smart environments. Security and privacy are seen as being of the utmost importance in any smart IoT environment in the real world. Digital environments face security threats as a result of security flaws in IoT-based networks. Because AI has excellent learning capabilities, it is more dependable and effective at spotting harmful threats. The current architecture presented in this article will support several applications of AI in digital homes detailed study of security concerns and issues.

I. INTRODUCTION

Since the first invention of the client-server paradigm in 1958, cloud computing has been driven by creative communications and distributed architecture. Rapid growth in cloud infrastructure has made it a necessary tool for many parts of society, including academic institutions, governmental organizations, and commercial enterprises. Furthermore, contemporary incarnations of technology, such as serverless computing, enable the autonomous deployment of innovative energy-use patterns. The customizable virtual machine based on containers will boost cloud use and offer low latency for the database environment. Deep learning techniques based

on Artificial Intelligence (AI) are projected to be used in cloud computing to predict regional resource demand as well as new equipment architecture and planning guidelines[1, 2]. The goal of AI as technology is to create tools that need information, whether that knowledge comes from human understanding or knowledge gleaned from encounters and forecasts in the past[3]. Additionally, it is anticipated that AI-based safety tactics would be more effective at responding to new dangers than traditional safety measures[4]. Deep learning, classification algorithms, and other AI-based techniques have lately been suggested as effective ways to address security concerns[5]. AI-based solutions have become more prevalent in business and other applications as processing power and data availability increase[6-8]. A wealth of information is accessible to prevent risks by analyzing and identifying trends of susceptibility utilizing AI approaches. In order to assess, detect, and mitigate security issues, each IoT device should consider having IoT-based data capabilities. It is now considerably more reliable to identify potential malware assaults from a large volume of data. AI is also well adapted for identifying and countering emerging and ongoing dangers, such as those that may go unnoticed for an extended period of time. It is crucial to develop IoT regulations and choose various factors due to the expanding IoT and such clever assaults for potential interaction in various and complex networks in the security protocols.[9]

II. Cloud computing

Cloud computing is the use of the Internet to access various services. In addition to data storage, this includes hardware and systems for servers, databases, networking, and applications[10-13]. Files may now be stored in a central archive rather than on a personal hard drive or storage device, thanks to cloud computing [10]. Any time a digital user gets access to the Internet, they may access apps and information. People and businesses alike embrace cloud storage because it offers financial savings, increased productivity, speed, dependability, and customizability.[14]

Cloud Security Threat

CC is a phrase that will see significant and wide development. There are several threats to difficulties with protection and security. The CIA feature and cloud risks are the basis for the analysis. Confidentiality, integrity, authenticity, and availability

have been identified by CC as the main weaknesses. Below, we briefly discuss these issues.

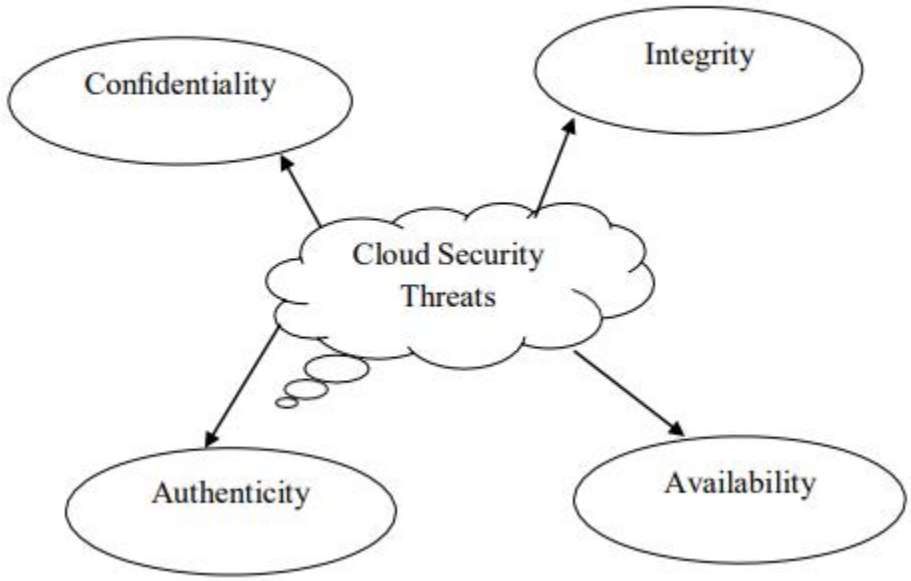

Figure.1 Security threats in Cloud computing

Threats to confidentiality include issues with the software, risk from external dangers, and threats to client information from inside. An important security risk to client data is the illegal or unauthorized use of personal information by an intruder of a cloud service provider. Second, the likelihood of outside assaults is quite high for cloud systems in exposed places. This approach incorporates centralized hardware or software for online and cloud services. Third, data loss is a vulnerability that cannot be avoided when negotiating cloud-related terms. It is caused by human error, a lack of tools, and, whenever feasible, access failures.

Threats to integrity include those related to record division, lax client access controls, and data level vulnerability. First, there is a chance that customers' off-base virtual servers and poorly educated VM design will result in exclusion from facts that are vaguely related to protection requirements[15, 16]. Customer connections are provided by this sophisticated cloud challenge; asset adjustments might affect the data's dependability. The second issue is bad client access management, which has a

variety of issues and dangers and enables attackers to harm data assets owing to improper influence and personality sharing.[17]

The equipment and its associated components are original and reliable thanks to the authentication process. For instance, different treatment facilities within the medical and health system receive patient criteria. The patient's therapy will be difficult if someone else handles and obtains this information.[18]

Risks to transparency, panel expansion's effects, organizational inaccessibility, external equipment disruption, and insufficient recovery methods are some of the threats to availability. First, attention has been drawn to the board, which also includes the results of basic adjustments and the implications of different consumers' entrance into test customers. Infrastructure, as well as cloud condition impacts, have a negative impact on how usable cloud companies are. The second issue is the inability to access systems, which includes DNS applications, properties, and device data transmission. a threat from outside that is present in all cloud iterations. Thirdly, there is a physical disruption to an institution that specializes in big networks (WAN), cloud users, and providers of IT services. Fourth, inadequate recovery mechanisms, such as ineffective failure recovery, impact retrieval time and effectiveness if a stage occurs.[19]

Criteria for IoT applications' security

The development of several technologies, including those used in hospitals, smart grid applications, smart cities, smart homes, etc., is made possible by the Internet of Things. The emergence of limited IoT and IoT systems causes new security and confidentiality issues in these crucial applications. In this section, we discuss a few pertinent IoT implementations and illustrate the safety issues and specifications of each application.

Smart Grids

A key contributor to economic growth and a commodity with ever-increasing commercial importance is electricity. Modern IT techniques are being used to maximize electricity production while taking customer demand along the power distribution line into account. The smart grid is the main emphasis of this transmission line. It consists of a linked network connecting power-producing

facilities and end users, commonly known as the smart metering system (AMI), whose primary purpose is to coordinate energy generation with end-user demand. [20]

Several studies emphasized the necessity for intelligent grids to satisfy safety requirements. The most important security and protection criteria are highlighted by users. For requests for automation and control orders, network infrastructure, smart meters, and control centers should always be available. Additionally, authorized users are not rejected by unauthorized users when processing inquiries. Smart meters and control systems exchange sensitive information and requests, which cannot be disclosed to uninvited parties. They are highly useful for making choices about the information communicated by the intelligent system in terms of maximizing energy transfer. It is crucial for making sensible judgments that this data be reliable. [21]

Healthcare

In order to sense and record actions, sensors and actuators have been incorporated into patient bodies for use in healthcare applications. In order to monitor patient health, IoT is employed in healthcare. The sensors that are already within the device will effectively collect data from the patient's body and send it to the doctor. While maintaining continual touch with the clinician, this technology has the power to remove the patient from the main hospital network[22].

We provide the following summary of the healthcare safety standards based on conceptual studies:

By using PHRs (Personal Health Records), which can only be viewed by medical professionals, each particular patient may be protected from prying eyes. Safe communication between patients and hospitals must be used to ensure the confidentiality and integrity of the exchanged data.

Smart cities

Smart cities are one of the most important IoT applications. Although the phrase "smart city" is not technically defined, it is a relatively recent idea that aims to encourage the use of public resources and raise the level of service provided to inhabitants. In this sense, sensors are employed on all roads, structures, and

intelligent cars to manage traffic, react to the environment, track sunlight-directed illumination, prevent home accidents with alerts, etc. Data confidentiality and sensitive data authentication are essential components of the security that smart cities require. Authentication of users and the sources of information. Data privacy is equally important since this data bundle responds, aids in decision-making, and improves people's everyday lives in intelligent cities.

Setting Security Features

A new IoT device needs this procedure before it can connect to the intelligent home system. The IoT platform provides a number of cryptographic algorithms that are adapted to the applications and systems that make use of the device's confidentiality, integrity, and encryption requirements. The reliability of their potential customers is essential to the effectiveness and widespread acceptance of reliable IoT infrastructures and the numerous applications they support. Such assurance is essential due to the harm that stolen or misused private information may do to people's social, financial, and physical life. To handle potential safety hazards, it is crucial to make sure that proper security is implemented. This action is crucial in defending the smart home against numerous security threats. Forged or tainted A data-damaging incident will prevent the surveillance system from operating as intended since judgments made using false information won't achieve the system's intended goals, such as lowering energy consumption. The fundamental reasons for this assault are as follows:

The intentional, suspicious setting of an IoT system produces inaccurate data. For instance, the overall amount of power used is rising. IoT computers that process data in-depth and fraudulently. Including electricity use as a likelihood variable, for instance. Multi-Hop Interaction with Data Change via a Hacked IoT Gateway. IP spoofing and identity espionage: IoT devices that connect to the same network without encrypting the source of the data via a complex protocol, like IP sec, will be effectively threatened by identity espionage and IP spoofing assaults.

Insights of Data on the Cloud

The cloud typically stores, processes, and analyses the data collected and transmitted by IoT gateways. The collected data will first be archived due to the planned use to make sure that it does not contain information on the impacted

people's attribute disclosure. There won't be any encryption of the data. Google employs a range of data security techniques for this goal, including Data Generalization and Differential Privacy.[23] The key problem in developing solutions for data generalization is figuring out how to anonymize the data while limiting identity losses arising from changes in the initial data at the same time. In order to establish a realistic understanding of the controlled environment, important information from examined and assessed data is then extracted and provided to the AI-based data analytics tool, often using a machine-learning algorithm. This information will motivate many optimal behaviors or actuator system changes. After that, the investigated data would be preserved, and historical data would be used to improve the development and testing of machine-learning models, modernizing the data analytics platform to increase precision.[24]

III. CONCLUSION

Companies are producing a wide range of resources by utilizing IoT data and computational software. These tools offer information mining solutions through the application of statistical modeling, prediction, and classification technologies. IoT changes how politicians make decisions. With the development of IoT and related technologies like cloud computing, data sources may be removed from a variety of areas. Current systems would benefit from the emergence of the IoT and AI. Combining computerization and comprehensive analysis, development's benefits are harvested while producing enormous economic gain. The potential to use IoT and artificial intelligence now seem to be greater. The most difficult issues in CC are examined in this study as security vulnerabilities.

References:

[1] T. H. Aldhyani and H. Alkahtani, "Artificial Intelligence Algorithm-Based Economic Denial of Sustainability Attack Detection Systems: Cloud Computing Environments," *Sensors,* vol. 22, no. 13, p. 4685, 2022.

[2] J. P. Wahle, T. Ruas, N. Meuschke, and B. Gipp, "Are neural language models good plagiarists? A benchmark for neural paraphrase detection," in *2021 ACM/IEEE Joint Conference on Digital Libraries (JCDL)*, 2021: IEEE, pp. 226-229.

[3] J. P. Wahle, T. Ruas, N. Meuschke, and B. Gipp, "Incorporating Word Sense Disambiguation in Neural Language Models," *arXiv preprint arXiv:2106.07967,* 2021.

[4] X. Fang, N. Koceja, J. Zhan, G. Dozier, and D. Dipankar, "An artificial immune system for phishing detection," in *Evolutionary Computation (CEC), 2012 IEEE Congress on*, 2012: IEEE, pp. 1-7.

[5] J. P. Wahle, T. Ruas, S. M. Mohammad, and B. Gipp, "D3: A Massive Dataset of Scholarly Metadata for Analyzing the State of Computer Science Research," *arXiv preprint arXiv:2204.13384,* 2022.

[6] J. P. Wahle, T. Ruas, F. Kirstein, and B. Gipp, "How Large Language Models are Transforming Machine-Paraphrased Plagiarism," *arXiv preprint arXiv:2210.03568,* 2022.

[7] F. Kirstein, J. P. Wahle, T. Ruas, and B. Gipp, "Analyzing Multi-Task Learning for Abstractive Text Summarization," *arXiv preprint arXiv:2210.14606,* 2022.

[8] T. Ruas, J. P. Wahle, L. Küll, S. M. Mohammad, and B. Gipp, "CS-Insights: A System for Analyzing Computer Science Research," *arXiv preprint arXiv:2210.06878,* 2022.

[9] M. M. A. Zahra, M. J. Mohsin, and L. A. Abdul-Rahaim, "Artificial intelligent smart home automation with secured camera management-based GSM, cloud computing, and arduino," *Periodicals of Engineering and Natural Sciences (PEN),* vol. 8, no. 4, pp. 2160-2168, 2020.

[10] A. Ganne, "Cloud Computing And Security Model-A Brief Survey," *International Research Journal of Modernization in Engineering Technology …,* vol. 4, no. 11, 2022.

[11] A. Ganne, "Cloud Data Security Methods: Kubernetes vs Docker Swarm," *International Research Journal of Modernization in Engineering Technology,* vol. 4, no. 11, 2022.

[12] A. Ganne, "Emerging Business Trends in Cloud Computing," *International Research Journal of Modernization in Engineering Technology,* vol. 4, no. 12, 2022.

[13] A. Ganne, "Applying Azure To Automate Dev Ops For Small ML Smart Sensors," *International Research Journal of Modernization in Engineering Technology,* vol. 4, no. 12, 2022.

[14] Z. Xu, W. Liu, J. Huang, C. Yang, J. Lu, and H. Tan, "Artificial intelligence for securing IoT services in edge computing: a survey," *Security and communication networks,* vol. 2020, 2020.

[15] R. S. Chunduri and N. Mazher, "Sas Viya 4.0 Deployment in Cloud."

[16] R. S. Chunduri and N. Mazher, "SEIBEL IP. 22X DEPLOYMENT IN CLOUD SYSTEMS."

[17] V. Kanimozhi and T. P. Jacob, "Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing," *ICT Express,* vol. 7, no. 3, pp. 366-370, 2021.

[18] A. Grusho, M. Zabezhailo, A. Zatsarinnyi, and V. Piskovskii, "On some artificial intelligence methods and technologies for cloud-computing protection," *Automatic Documentation and Mathematical Linguistics,* vol. 51, no. 2, pp. 62-74, 2017.

[19] U. F. Mustapha, A. W. Alhassan, D. N. Jiang, and G. L. Li, "Sustainable aquaculture development: a review on the roles of cloud computing, internet of things and artificial intelligence (CIA)," *Reviews in Aquaculture,* vol. 13, no. 4, pp. 2076-2091, 2021.

[20] P. Radanliev *et al.*, "Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains," *Cybersecurity,* vol. 3, no. 1, pp. 1-21, 2020.

[21] S. Sood, S. Mehmi, and S. Dogra, "Artificial intelligence for designing user profiling system for cloud computing security: Experiment," in *2015 International Conference on Advances in Computer Engineering and Applications*, 2015: IEEE, pp. 51-58.

[22] J. P. Wahle, N. Ashok, T. Ruas, N. Meuschke, T. Ghosal, and B. Gipp, "Testing the generalization of neural language models for COVID-19 misinformation detection," in *International Conference on Information*, 2022: Springer, pp. 381-392.

[23] H. Susanto, L. F. Yie, D. Rosiyadi, A. I. Basuki, and D. Setiana, "Data security for connected governments and organisations: Managing automation and artificial intelligence," in *Web 2.0 and cloud technologies for implementing connected government*: IGI Global, 2021, pp. 229-251.

[24] U. A. Butt *et al.*, "A review of machine learning algorithms for cloud computing security," *Electronics,* vol. 9, no. 9, p. 1379, 2020.