International Journal of Core Engineering & Management
Volume-7, Issue-12, 2024 ISSN No: 2348-9510

SECURING BIG DATA IN THE CLOUD COMPUTING ENVIRONMENTS: A SURVEY ON THREATS, VULNERABILITIES, AND DEFENSE MECHANISMS

Olamide Olaoye
Olamideolaoye1@gmail.com

Abstract

The combination of cloud computing with big data has revolutionized data processing, analytics, and storage by offering unmatched cost-effectiveness, scalability, and flexibility. But because cloud systems are remote and Big Data is large, diverse, and moving quickly, this convergence also brings with it serious security risks. This paper offers a thorough review of the most recent threats, vulnerabilities, and defense tactics to ensure the security of Big Data stored in the cloud. Data leaks, man-in-the-middle attacks, Distributed Denial of Service (DDoS) assaults, and insider threats are all classified as major security dangers. Additionally, it investigates critical weaknesses such misconfigured systems, insufficient access control, and unsafe APIs. Modern defense measures, including intrusion detection systems and cryptography approaches, are thoroughly examined in this work. Through the integration of knowledge from extant literature and practical case studies, this paper presents current best practices, addresses enduring issues, and suggests future research avenues to improve Big Data security in cloud systems.

Index Terms – Big Data, Cloud Computing, Data Security, Threats, Vulnerabilities, Defense Mechanisms, DDoS, Insider Threats, Encryption, Access Control, Intrusion Detection, RBAC, ABAC, Secure Cloud Architecture

I. INTRODUCTION

According to recent advancements, Big Data refers to datasets that are massive in size, continuously growing at an exponential rate, and characterized by their complexity and diversity. These data, which might be unstructured, semi-organized, or structured, are created and uploaded in massive amounts every day. Massive volumes of data are sent and received across networks, creating major problems for processing, administration, and storage. Traditional database systems cannot effectively manage Big Data because of its enormous amount and complexity[1]. The processing and storage of such data demand high-performance servers, which require substantial maintenance and operational costs.

To overcome these limitations, one viable remedy that has surfaced is cloud computing. With on-demand services, cloud computing makes it easier to store, analyses, and retrieve large amounts of unstructured data in real time, offering scalability, flexibility, and fault tolerance via diverse hardware and software infrastructures[2][3]. Today, it is widely adopted for both personal and enterprise-level applications. Major companies like Amazon, Microsoft, Google, IBM, Nokia, and Redbuds provide cloud-based services to users globally.

Cloud computing is not merely a trending tool for storing media files; it is critically used by governments, healthcare systems, financial institutions, and businesses for managing sensitive data. However, since third-party providers run cloud systems, protecting the integrity and security

of data kept there becomes crucial.
Numerous threats such as phishing, botnets, insider threats, DDoS attacks, and data loss have emerged as significant challenges in the cloud environment[4]. In order to combat these complex and dynamic attacks, traditional security measures like firewalls, IDS, and antivirus software are becoming less and less effective[5][6]. As a result, cloudsecurity ensuring that unauthorized access, data breaches, or service disruptions do not occur has become a fundamental concern for both individual users and organizations. Big Data technology can tackle a wide range of issues, regardless of their volume, pace, or origin. The use and administration of this ever-evolving technology involves several industries, consumers, and governmental organizations[7][8].

A. Structure of the paper

The structure of this paper is as follows: Section II A summary of large data in cloud computing settings. Section III explains the main weaknesses and dangers in large data cloud setups. section IV explores the defines Mechanisms and Security Solutions. Section V reviews relevant literature and case studies, and Section VI concludes with recommendations for more research.

II. OVERVIEW OF BIG DATA IN CLOUD COMPUTING ENVIRONMENTS

The phrase "big data" refers to information that is so extensive and intricate that it is difficult to manage with conventional data management tools and processing techniques. Because the information and data are utilized, it is crucial to safely retain data in order to detect trends and patterns, handle, and distribute large amounts of complicated data. Big Data's growth broadens its meaning and substance, particularly with regard to its acceptance by government and business[9]. The data itself, as well as the pertinent technology and knowledge to help produce, gather, store, manage, process, analyses, and use it, are now included in the original volume-based definition.

A. Characteristics of Big Data

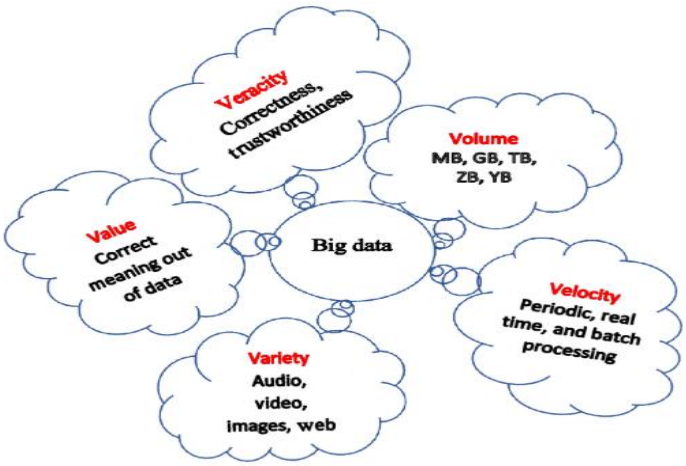

Fig. 1. Five Vs of Big Data

The three Vs of big data are variety, velocity, and volume. Because the new-generation architecture stores data in several formats, adding diversity, veracity, value, and velocity to the three Vs can make it five Vs. The five pillars of big data are depicted in Figure 1.

1) Volume
Data is always growing and comes from different sources. The Internet creates vast amounts of data worldwide. Indicates the volume of data produced hourly from various sources.

2) Velocity
Data is expanding rapidly and dramatically. The everyday addition of millions of linked devices results in increases in both volume and velocity. Evaluates how quickly information can be gathered, examined, and used.

3) Variety
Sensors, cell phones, and social networks may all provide data in a variety of forms. These technological advancements produce information in the forms of data logs, written word, spoken word, visual, and audio files[10]. To add to it, the data might be structured, semi-structured, or randomly organized.

4) Value
One of the main characteristics of large data is value. It concerns the process of dealing with data and transforming it into valuable insights.

5) Veracity
The quality, accuracy, and reliability of data are referred to as veracity. Thus, it is essential to ensure data integrity.

B. Cloud Computing Environment Architecture
The organised framework that permits the architecture of a cloud computing environment refers to the ability to tap into shared computer resources such as storage, databases, software, networking, and analytics whenever needed. Usually arranged according to service models. The terms PaaS, SaaS, and IaaS are interchangeable. To provide scalable and elastic IT services, the cloud architecture makes use of distributed computing, virtualisation, and automated provisioning. The physical infrastructure layer (hardware, data centres), the virtualisation layer (hypervisors, containers), the orchestration and management layer (for resource allocation, monitoring, and security), and the service delivery layer (APIs, user interfaces) are the fundamental layers of a cloud environment. High availability, effective resource use, and adaptable application deployment across public, private, or hybrid cloud models are all encouraged by this tiered approach. In data-intensive fields like big data analytics and industrial automation, a well-designed cloud architecture is crucial for guaranteeing system performance, security, and compliance. Figure 2 depicts the architecture of the cloud computing ecosystem.

International Journal of Core Engineering & Management
Volume-7, Issue-12, 2024 ISSN No: 2348-9510

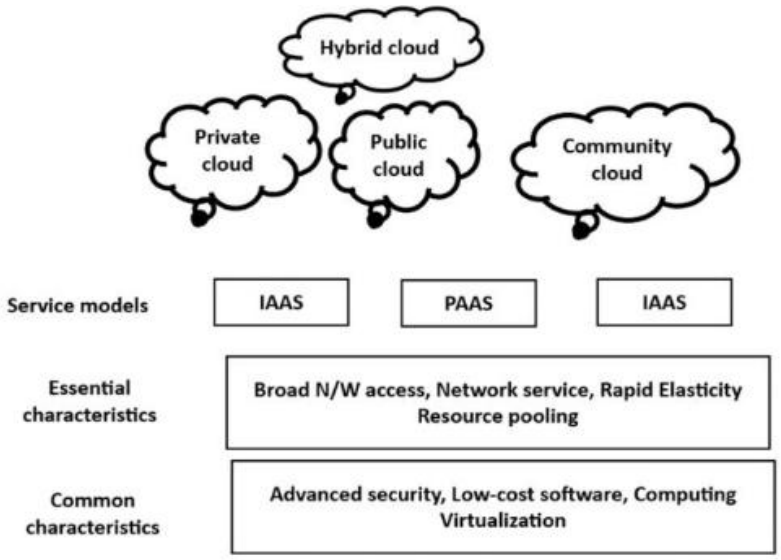

Fig. 2. Architecture of the Cloud Computing Ecosystem

C. Importance of Data Security in Big Data Cloud Computing Environment

There has been a rise in the use of Big Data cloud computing technologies due to the fast development of science and technology, which raises data security problems that directly jeopardise people's privacy and property protection[11]. The area of big data cloud computing is now preoccupied with data security. The intricacy of the large data cloud computing environment necessitates addressing practical concerns and data security challenges.

D. Security Issues in a Big Data Cloud Computing Environment

Cloud computing with big data and big data Technology that can host several programs has many benefits, include affordability, usability, and practical administration. However, a number of challenges remain, the primary one being data security. The following are some data security considerations.

1) Data Access Security Issues

In the framework development of Big Data cloud computing environments often have data access security vulnerabilities due to the prevalence of unauthorized access. External and internal threats are also included in this issue[12]. Big data cloud computing platforms are vulnerable to external security threats, which can compromise or corrupt data stored there. This is typically the result of customers' tardiness in implementing adequate security measures. Concerns about the safety of internal systems, on the other hand, are caused by internal personnel acting improperly, which results in the inability to function in compliance with cloud computing needs for huge data.

2) Data Isolation Security Issues

A significant concern with Data isolation and security are key components of large data cloud computing. The majority of utilization occurs during the sharing procedure[13]. Currently, the majority of the clients of large data cloud computing are all, with a significant percentage coming from business organizations[14]. In particular, government entities constantly need resources that

are open to sharing. In this instance, it is challenging to encrypt the data since the isolation wall does not require external computers to cross. Because of the environment's lack of security, malicious attackers might corrupt and disclose data.

3) Data Destruction Security Issues

In order to maintain data security and conserve storage space, there may be instances in the big data cloud computing environment where certain data deletions are necessary. If it was not possible to reduce the time it took to remove data or if it was not entirely eliminated, there may be data leaks and unauthorized usage.

4) Data Integrity Security

The term "data integrity" describes the integrity of data as it is being operated and stored. Cloud computing for massive amounts of data invariably employs dynamic processes for its backend software. Practically ensuring data security and integrity is difficult because of both internal and external enemies.

5) Data Privacy Security

The backend applications of big data cloud computing are intricate. It increases terminal systems' network susceptibility by giving network intruders easy access to attackable situations, which are carried out by use of network access services.

III. THREATS AND KEY VULNERABILITIES IN BIG DATA CLOUD ENVIRONMENTS

Big data cloud environments face significant security risks due to their distributed, large-scale, and multi-tenant architecture. Common threats include data breaches, unauthorized access, insider attacks, and DDoS attacks. These are often enabled by vulnerabilities such as weak access controls, insecure APIs, misconfigurations, and lack of proper encryption[15][16]. The integration of diverse data sources and third-party services further increases the attack surface. Without effective security measures, these threats can compromise data confidentiality, integrity, and availability, making it essential to identify and address them proactively. The cloud environment is still unsafe for data outsourcing due to a number of security flaws and assaults.

A. Distributed Denial of Service (DDoS) attack

The DDoS assault is the most prevalent. In reality, a DoS assault serves as its foundation. DoS attacks are a kind of cyberattack where the attacker sends a lot of pointless packets or requests to try to stop the victim's machine from providing services. These requests cause the victim system to become overloaded with processing them, which prevents it from being able to assist the authorized user[17]. This often occurs when the volume of requests received surpasses the system's capacity. These are also known as bandwidth depletion since they waste the system's bandwidth. DDoS assaults are a type of cyberattack that is becoming more and more prevalent. Attackers employ these attacks to prevent other individuals from using services by supplying network users with unauthorized and interrupted services. Figure 3 depicts a DDoS attack's life cycle.

International Journal of Core Engineering & Management
Volume-7, Issue-12, 2024 ISSN No: 2348-9510

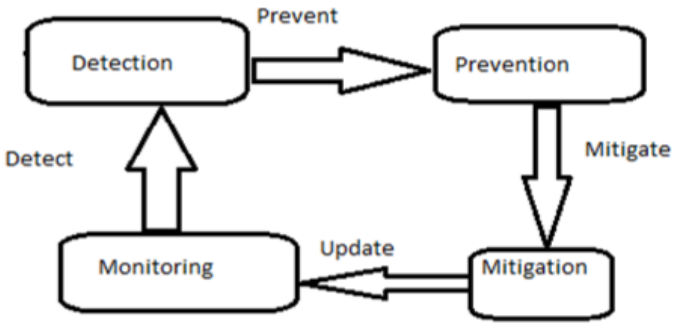

Fig. 3. Attack Life Cycle of DDoS

such attacks can lead to significant operational downtime, data ingestion failure, and service unavailability[18]. The elastic nature of cloud resources may provide some resilience, but sophisticated DDoS attacks can still overwhelm systems and incur high financial and operational costs.

B. Man-in-the-Middle (MITM) Attacks

A man-in-the-middle (MITM) attack occurs when an attacker secretly transmits and changes communications between two parties that believe they are having a direct discussion. When a malicious actor starts a conversation between a user and an app without permission, it's referred to as an MITM assault. A schematic of men-in-the-middle assault ideology is shown in Figure 4.

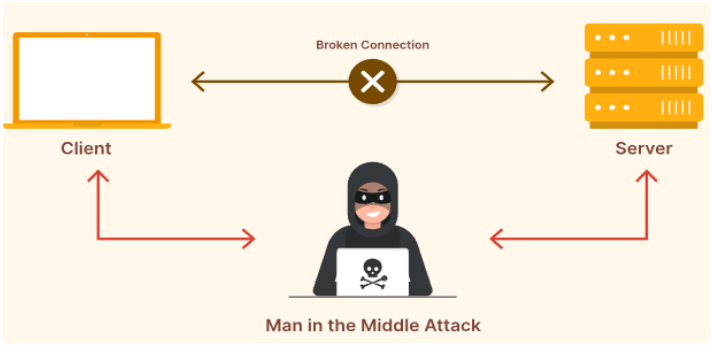

Fig. 4. Men-In-The-Middle Attack Ideology Schematic

In a big data pipeline, sensitive information such as authentication tokens, control commands, or raw datasets can be intercepted if communication is not adequately encrypted[19]. MITM attacks can lead to data manipulation, unauthorized access, or replay attacks, undermining data integrity and confidentiality.

C. Insiders Threat

Intentionally or purposefully using an organization's resources in a way that would be damaging to the organization is known as an insider. This includes contractors, previous or present business partners, and other trustworthy personnel. Networks, computer systems, and private firm information are all directly accessible to insiders. Insider threats have the potential to cause the loss of sensitive information and intellectual property[20]. Malicious insiders may exfiltrate data, sabotage analytics workflows, or exploit vulnerabilities for personal or competitive gain. Unlike

external attackers, insiders often bypass traditional security controls, making detection and mitigation more challenging.

D. Malicious Insiders

It might be more difficult to stop security risks that are intrinsic to the cloud environment. Any insider or employee with administrative access can copy any sensitive data to a storage device[21]. A dissatisfied ex-employee, system administrator, business associate, or outside contractor might potentially steal the data. Background checks and data access controls can mitigate some of these dangers.

E. Advanced Persistent Threats (APTs)

One of the information security dangers that organizations are now facing with the quickest rate of growth is APT. They target private organizations' sensitive data and are executed by the most skilled and well-funded attackers[22][23]. It infiltrates cloud environments through sophisticated means such as spear-phishing or zero-day exploits and establishes long-term unauthorized access. In big data systems, APTs may remain undetected for extended periods, silently collecting valuable data or observing system behavior for future exploitation.

F. Insecure Interfaces and Application Program Interfaces (APIs):

Insecure VM, APIs, and interfaces can potentially pose a risk to the cloud computing environment. To access cloud services, the user makes use of virtual machines, APIs, and other software interfaces. These points of contact provide supply, administration, and activity monitoring, making them crucial components[24]. As a result, security holes at these sites lead to improper access controls, illegal authentication, encryption violations, etc. Weak API credentials, inadequate key management, operating system (OS) flaws, unpatched software, and hypervisor problems are the causes of these risks.

G. Hypervisor Vulnerabilities

The hypervisor, which manages VM in cloud environments, represents a critical attack surface. Vulnerabilities at the hypervisor level can enable attackers to perform cross-tenant attacks, escaping from one virtual machine to another. In multi-tenant big data environments, such breaches can compromise the confidentiality and isolation of data across different clients or departments.

IV. DEFENSE MECHANISMS AND SECURITY SOLUTIONS

A complex strategy including cryptographic approaches to secure large amounts of information systems for use in cloud computing, IDS, models for controlling access, and privacy-preserving frameworks.

A. Data Encryption Security Technology

Cloud computing for massive amounts of data makes use of data encryption as one of its data security measures. This security protection technology's primary purpose is to guarantee data privacy and security. For the system platform to avoid several data security problems, the data encryption technology must be completely optimized. Conventional data encryption techniques and the latest cloud server configurations are typically included in data encryption processing.

One essential tool for ensuring data security, integrity, and secrecy is encryption. It is essential for safeguarding data while it is being computed, in transit, and at rest, especially in multi-tenant cloud architectures where unauthorized access or breaches can have severe consequences[25][26]. Among emerging encryption approaches, homomorphic encryption (HE) has garnered significant attention for its ability to allow computations on data that is encrypted without requiring decryption.

B. Data Sharing Security Technology

One significant technology type to enhance data security during data transmission is data-sharing security protection technology. The three basic components of shared encryption technology are as follows. First, encryption technology for cloud servers. After the data is downloaded from the cloud, the cloud server encryption technology can use public key encryption to retransmit to the cloud[25]. This operation mode is relatively complicated and the efficiency is relatively low. Second, technique for proxy re-encryption. To finish the data transmission procedure, this encryption technology must be sent via a triple relationship, starting with the authorized individual and ending with the agent and accepted potential. Multiple procedures must be involved in the entire data transmission process.

C. Intrusion Detection

These methods assist the victim in detecting defending against DDoS attacks and keeping the system from crashing[27]. There are two primary categories into which intrusion detection systems fall. The first is a system for detecting network intrusions, and the other is the Host-Based IDS.

1) Network Intrusion Detection System as a Service (NIDSaaS)

A system that examines the network traffic entering the system. It is installed at a crucial network point or focus, where it monitors all network-connected devices' inbound and outbound traffic. The NIDS has just been made available as NASAs on the OpenStack cloud.

2) Host-Based Intrusion Detection System (HIDS)

A device that monitors important operating system files. It functions on all network devices and has connections to both the company's intranet and the internet[28]. The HIDS can identify anomalous network packets in malicious transmission. It also detects malicious traffic that comes from the host. Other IDS type subsets exist. The most common types are specification-based detection, anomaly detection, and signature detection[29].

D. Access Control Mechanisms

Access control refers to the limitation of access to a certain location or resource. A person's capacity to access resources or data is determined by a set of conditions. The variety of services and the ever-changing nature of the cloud make access control methods essential[30]. To guarantee that each attempt by specific users to access the object is predicated on the access credentials granted by the system, access control measures are employed. Figure 5 provides an illustration of an access control system.

International Journal of Core Engineering & Management
Volume-7, Issue-12, 2024 ISSN No: 2348-9510

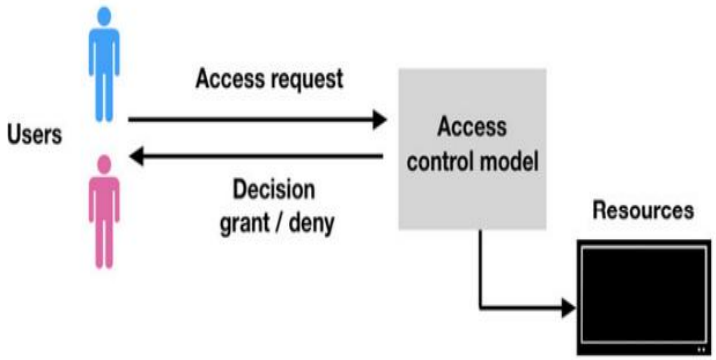

Fig. 5. Access Control Mechanism Scenario

The highest possible degree of availability, privacy, scalability, and integrity should be guaranteed to users of cloud-based systems[31]. However, creating and putting into place an access control system is a crucial and difficult task for cloud computing systems[32]. Effective access control systems stop illegal disclosure of data, tampering, and misuse, especially in multi-tenant big data environments.

1) Role-Based Access Control (RBAC)

The access control method known as RBAC first appeared in the 1970s. According to RBAC, users are categorized into several roles, and it is because of these roles that the required authorizations, constraints, and permissions are carried out[33]. The RBAC's main structure is as follows: role searches permission assignment (PA) determines each role's system rights and assigns administrative permissions to these roles according to user assignment[34][35]. Permissions are passed down to users according to their position within an organization. RBAC is very simple to deploy and streamlines access management in large-scale applications. However, in dynamic large data systems with intricate and changing access needs, it can become inflexible and challenging to maintain.

2) Attribute-Based Access Control (ABAC)

In contrast to RBAC, attributes rather than roles are used to guarantee user controls, or access rights. Therefore, user characteristics are crucial when using ABAC. These attributes have the ability to access the user's general characteristics, like age, height, and personal traits, and they can be modified based on this data[36][37]. ABAC supports fine-grained policies that are essential for securing big data in cloud systems, where users may access data across different platforms, geographies, and organizational boundaries. Its dynamic policy evaluation makes it suitable for modern distributed environments, although it may incur additional computational complexity.

V. LITERATURE REVIEW

This section examines current studies on protecting big data in cloud computing settings. It emphasizes the primary risks, weaknesses and defines strategies covered in the literature, including encryption methods, insider threats, and data breaches. A comparative summary of the examined studies is given in Table I, which also highlights key problems, potential fixes, and future lines of inquiry.

Kaur, Dhiman and Singh (2023) examine the issues with, and solutions to, safeguarding massive data in cloud instances. Data privacy, data availability, data authentication, data location, data storage, and data integrity are among the critical security issues highlighted by the study's comprehensive literature review. By reviewing relevant publications, it identifies research limitations and gaps in the areas of cloud computing and huge data security. The article delves into several security-related subjects, such as data obfuscation, access control, and encryption. In order to secure data in cloud settings, this review article gives helpful information on security challenges and current methods for securing large data in the cloud[38].

Zhou et al. (2023) Based on demand, Computer resources are distributed effectively using cloud computing. Because of this, it is now a practical option for AI and big data analytics, which find extensive use across several fields of study. Cloud infrastructures are particularly vulnerable to threats due to their reliance on third-party providers. Data security in some industries, including scientific research, continues to be a significant worry when transferring operations to the cloud. They outline a secure cloud architecture that allows for workflow scheduling and packaging while preserving the safety of its computation, logic, and data when it is at rest, in transit, and in use[39].

Dzulhikam and Rana (2022) explains the current problems with cloud computing for analytics on large datasets and provides a critical assessment of the contemporary CSP's cloud computing ecosystem. A safe, expandable, and widely available platform for massive data dispersed management systems is provided by cloud computing. Since many of the cloud services and deployment tactics offered by CSP are focused on client expectations, cloud computing has several attractive features for its consumer market. Additionally, cloud computing can do real-time big data analytics and store and manage enormous volumes of data, providing clients with useful information and trends[40].

Fataftah and Isong (2022) finds security issues and solutions by carefully reviewing cloud computing and big data research corpus. Using predetermined inclusion and exclusion criteria, a large number of pertinent publications were gathered, evaluated, and ultimately included. Data authentication, data backup or recovery, data integrity, data availability, data location, and data storage are all defined in the article. They also found several useful measures, such as audits and compliance on a regular basis, intrusion prevention systems that are network-based, access restrictions that are fine-grained, and robust data encryption[41].

Sandhu (2022) The concept, category, and features of big data, as well as an examination of several cloud providers, including Google Cloud, Amazon Web providers, International Business Machines cloud, Hortonworks, and MapR. on addition, they compare a number of big data frameworks that operate on the cloud. Data security, heterogeneity, distributed database storage, and data visualization are some of the many words used to characterize the challenges researchers face. Powerful storage of massive amounts of data is now possible with cloud computing services. They do away with some necessities, such a specific area and the ongoing maintenance of expensive computer gear and software[42].

Wang, Wang and Xue (2021) providing a synopsis of the fundamental concepts, defining features, and cutting-edge pieces of big data cloud computing. Data security concerns have received increased focus due to the rise of large data cloud computing. Concerning data transit, sharing, isolation, integrity, deletion, and access, as well as privacy management, security concerns are detailed. To improve data security in the big data cloud environment and decrease risks, a virtualization architecture and related tactics are ultimately proposed[43].

International Journal of Core Engineering & Management
Volume-7, Issue-12, 2024 ISSN No: 2348-9510

TABLE I. SUMMARY ON SECURITY CHALLENGES AND DEFENSE MECHANISMS IN BIG DATA CLOUD ENVIRONMENTS

Reference	Study On	Approach	Key Findings	Challenges	Future Direction
Kaur, Dhiman and Singh (2023)	Cloud computing security for big data	Literature review	identifies the following important issues: location, storage, integrity, privacy, availability, secrecy, and data authentication. Suggests remedies such as obfuscation, access control, and encryption.	Location of data, confidentiality, availability, integrity, and authenticity	Robust integrated security frameworks
Zhou et al. (2023)	Secure architecture for cloud-based workflows	Secure cloud architecture proposal	offers an architecture that ensures the safety of compute, logic, and data when it is being used, being sent, and being at rest.	Risks from outsourced environments, especially in biomedical research	Adoption of secure cloud frameworks across domains
Dzulhikam and Rana (2022)	Cloud computing for big data analytics	Critical review	Explores CSPs and benefits of scalability and accessibility. Real-time analytics highlighted.	Scalability, accessibility, security challenges	Enhanced real-time data processing techniques
Fataftah and Isong (2022)	Data security in the cloud especially with massive datasets	Comprehensive literature survey	Highlights security challenges and identifies solutions like fine-grained access control, strong encryption.	Integrity, confidentiality, availability, data location	Regular audits and advanced compliance strategies
Sandhu (2022)	Big data frameworks on cloud services	Comparative analysis	Compares cloud services; identifies challenges in database storage, data visualization, heterogeneity.	Distributed storage, heterogeneity, visualization	Improved framework compatibility and visualization tools
Wang, Wang and Xue (2021)	Cloud-based big data technologies	Overview of technologies	Discusses data quality and privacy issues; proposes virtualization architecture.	Data access, isolation, destruction, sharing	Enhanced privacy controls and virtualization strategies

VI. CONCLUSION AND FUTURE WORK

As businesses rely more and more on cloud infrastructure to handle large and complicated datasets, protecting big data has become essential in cloud computing systems. The main risks, weaknesses, and current defences related to cloud-based big data security have all been thoroughly reviewed in this study. DDoS assaults, insider threats, insecure APIs, and data integrity problems are among the concerns that have been identified. As a result, several security options have been investigated, including intrusion detection systems, encryption, and RBAC and ABAC. Despite notable advancements, several challenges remain unresolved. The inherently dynamic and distributed nature of cloud computing, coupled with the scale, velocity, and heterogeneity of Big Data, demands more adaptive, intelligent, and resilient security frameworks. Furthermore, maintaining data privacy, achieving regulatory compliance, and securing multi-tenant environments continue to pose significant hurdles.

Future work should emphasize the development of AI-driven and context-aware Security technologies that allow for autonomous reaction and real-time threat detection. Promising research directions include the implementation of technologies that protect privacy, such is homomorphic encryption and safe multi-party computing, and federated learning. Moreover, the establishment of standardized, scalable, and to promote confidence and guarantee the robustness of cloud environments cost-effective security techniques are essential for big data applications.

REFERENCES

1. V. C. Storey and I.-Y. Song, "Big Data Technologies and Management: What Conceptual Modeling Can Do," Data Knowl. Eng., vol. 108, pp. 50–67, Mar. 2017, doi: 10.1016/j.datak.2017.01.001.
2. F. R. Damayanti, K. A. Elmizan, Y. F. Alfredo, Z. N. Agam, and A. Wibowo, "Big Data Security Approach in Cloud: Review," Proc. 2018 Int. Conf. Inf. Manag. Technol. ICIMTech 2018, no. September, pp. 428–431, 2018, doi: 10.1109/ICIMTech.2018.8528112.
3. Abhishek and P. Khare, "Cloud Security Challenges: Implementing Best Practices for Secure SaaS Application Development," Int. J. Curr. Eng. Technol., vol. 11, no. 06, pp. 669–676, Nov. 2021, doi: 10.14741/ijcet/v.11.6.11.
4. S. Murri, "Data Security Environments Challenges and Solutions in Big Data," Int. J. Curr. Eng. Technol., vol. 12, no. 6, pp. 565–574, 2022.
5. S. Riaz, A. H. Khan, M. Haroon, S. Latif, and S. Bhatti, "Big data security and privacy: Current challenges and future research perspective in cloud environment," in Proceedings of 2020 International Conference on Information Management and Technology, ICIMTech 2020, 2020. doi: 10.1109/ICIMTech50083.2020.9211239.
6. G. Modalavalasa and S. Pillai, "Exploring Azure Security Center : A Review of Challenges and Opportunities in Cloud Security," ESP J. Eng. Technol. Adv., vol. 2, no. 2, pp. 176–182, 2022, doi: 10.56472/25832646/JETA-V2I2P120.
7. Y. B. Reddy, "Big Data Security in Cloud Environment," in Proceedings - 4th IEEE International Conference on Big Data Security on Cloud, BigDataSecurity 2018, 4th IEEE International Conference on High Performance and Smart Computing, HPSC 2018 and 3rd IEEE International Conference on Intelligent Data and Securit, 2018. doi: 10.1109/BDS/HPSC/IDS18.2018.00033.
8. A. Goyal, "Scaling Agile Practices with Quantum Computing for Multi-Vendor Engineering Solutions in Global Markets," Int. J. Curr. Eng. Technol., vol. 12, no. 06, Jun.

2022, doi: 10.14741/ijcet/v.12.6.10.
9. C. Yang, Q. Huang, Z. Li, K. Liu, and F. Hu, "Big Data and cloud computing: innovation opportunities and challenges," Int. J. Digit. Earth, vol. 10, no. 1, pp. 13–53, 2017, doi: 10.1080/17538947.2016.1239771.
10. L. Rabhi, N. Falih, A. Afraites, and B. Bouikhalene, "Big Data Approach and its applications in Various Fields: Review," Procedia Comput. Sci., vol. 155, no. 2018, pp. 599–605, 2019, doi: 10.1016/j.procs.2019.08.084.
11. Z. Wang, N. Wang, X. Su, and S. Ge, "An empirical study on business analytics affordances enhancing the management of cloud computing data security," Int. J. Inf. Manage., vol. 50, 2019, doi: 10.1016/j.ijinfomgt.2019.09.002.
12. M. Farsi, M. Ali, R. A. Shah, A. A. Wagan, R. Kharabsheh, and A. Farouk, "Cloud computing and data security threats taxonomy: A review," J. Intell. Fuzzy Syst., vol. 38, no. 3, pp. 2517–2527, Jan. 2020, doi: 10.3233/JIFS-179539.
13. V. Kolluri, "A Detailed Analysis Of Ai As A Double- Edged Sword: Ai-Enhanced Cyber Threats Understanding And Mitigation,"," Int. J. Creat. Res. THOUGHTS, vol. 8, pp. 5800–5804, 2020.
14. Y. Fuguang, "Research on campus network cloud storage open platform based on cloud computing and big data technology," J. Intell. Fuzzy Syst., vol. 38, pp. 1–9, 2019, doi: 10.3233/JIFS-179483.
15. M. Ali, S. Malik, Z. Khalid, M. M. Awan, and S. Ahmad, "Security Issues , Threats And Respective Mitigation In Cloud Computing – A Systematic Review," Int. J. Sci. Technol. Res., vol. 9, no. 08, pp. 474–484, 2020.
16. S. S. S. Neeli, "Critical Cybersecurity Strategies for Database Protection against Cyber Attacks," J. Artif. Intell. Mach. Learn. Data Sci., vol. 1, no. 1, 2023.
17. M. Amitha and D. M. Srivenkatesh, "DDoS Attack Detection in Cloud Computing Using Deep Learning Algorithms," Int. J. Intell. Syst. Appl. Eng., vol. 11, no. 4, pp. 82–90, 2023.
18. R. Goyal, R. Manoov, P. Sevugan, and P. Swarnalatha, "Securing the Data in Cloud Environment Using Parallel and Multistage Security Mechanism," Adv. Intell. Syst. Comput., vol. 1057, no. January, pp. 941–949, 2020, doi: 10.1007/978-981-15-0184-5_80.
19. A. Mallik, A. Ahsan, M. M. Z. Shahadat, and J. C. Tsou, "Man-in-the-middle-attack: Understanding in simple words," Int. J. Data Netw. Sci., vol. 3, no. 2, pp. 77–92, 2019, doi: 10.5267/j.ijdns.2019.1.001.
20. S. Kabade and A. Sharma, "Intelligent Automation in Pension Service Purchases with AI and Cloud Integration for Operational Excellence," pp. 725–735, 2023, doi: 10.48175/IJARSCT-14100J.
21. T. A. A. Abdullah Aljumah, "Cyber security threats, challenges and defence mechanisms in cloud computing," IET Journals, vol. 14, no. 7, pp. 1185–1191, 2020.
22. F. J. Abdullayeva, "Advanced Persistent Threat attack detection method in cloud computing based on autoencoder and softmax regression algorithm," Array, vol. 10, no. March, 2021, doi: 10.1016/j.array.2021.100067.
23. S. Singamsetty, "Fuzzy-Optimized Lightweight Cyber-Attack Detection For Secure Edge-Based Iot," J. Crit. Rev., vol. 6, no. 07, pp. 1028–1033, 2019, doi: 10.53555/jcr.v6:i7.13156.
24. A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities," IEEE Commun. Surv. Tutorials, vol. 21, no. 2, pp. 1851–1877, 2019, doi:

10.1109/COMST.2019.2891891.
25. Z. Tang, "A Preliminary Study on Data Security Technology in Big Data Cloud Computing Environment," in Proceedings - 2020 International Conference on Big Data and Artificial Intelligence and Software Engineering, ICBASE 2020, 2020. doi: 10.1109/ICBASE51474.2020.00013.
26. S. Chatterjee, "Risk Management in Advanced Persistent Threats (APTs) for Critical Infrastructure in the Utility Industry," Int. J. Multidiscip. Res., vol. 3, no. 4, pp. 1–10, 2021.
27. V. S. Thokala, "Scalable Cloud Deployment and Automation for E-Commerce Platforms Using AWS, Heroku, and Ruby on Rails," Int. J. Adv. Res. Sci. Commun. Technol., pp. 349–362, Oct. 2023, doi: 10.48175/IJARSCT-13555A.
28. S. A. Varma and K. G. Reddy, "A Review of DDoS Attacks and its Countermeasures in Cloud Computing," 2021 5th Int. Conf. Inf. Syst. Comput. Networks, ISCON 2021, no. July, 2021, doi: 10.1109/ISCON52037.2021.9702388.
29. V. Pillai, "Anomaly Detection for Innovators: Transforming Data into Breakthroughs," Lib. Media Priv. Ltd., 2022.
30. S. Chatterjee, "Integrating Identity and Access Management for Critical Infrastructure : Ensuring Compliance and Security in Utility Systems," Int. J. Innov. Res. Creat. Technol., vol. 8, no. 2, pp. 1–8, 2022.
31. A. R. Khan, "Access control in cloud computing environment," ARPN J. Eng. Appl. Sci., vol. 7, no. 5, pp. 613–615, 2012.
32. R. El Sibai, N. Gemayel, J. Bou Abdo, and J. Demerjian, "A survey on access control mechanisms for cloud computing," Trans. Emerg. Telecommun. Technol., vol. 31, no. 2, pp. 1–21, 2020, doi: 10.1002/ett.3720.
33. G. Karataş and A. Akbulut, "Survey on access control mechanisms in cloud computing," J. Cyber Secur. Mobil., vol. 7, no. 3, pp. 1–36, 2018, doi: 10.13052/jcsm2245-1439.731.
34. M. J. Persis Jessintha and R. Anbuselvi, "An Analysis on Access Control Mechanisms in Cloud Environment," vol. 3, no. 07, pp. 1–4, 2015.
35. A. Gogineni, "Multi-Cloud Deployment with Kubernetes: Challenges, Strategies, and Performance Optimization," Int. Sci. J. Eng. Manag., vol. 1, no. 02, 2022.
36. S. Shah and M. Shah, "Deep Reinforcement Learning for Scalable Task Scheduling in Serverless Computing," Int. Res. J. Mod. Eng. Technol. Sci., vol. 3, no. 12, pp. 1845–1852, Jan. 2025, doi: 10.56726/IRJMETS17782.
37. A. Kushwaha, P. Pathak, and S. Gupta, "Review of optimize load balancing algorithms in cloud," Int. J. Distrib. Cloud Comput., vol. 4, no. 2, pp. 1–9, 2016.
38. A. Kaur, A. Dhiman, and M. Singh, "Comprehensive Review: Security Challenges and Countermeasures for Big Data Security in Cloud Computing," in 2023 7th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech), 2023, pp. 1–6. doi: 10.1109/IEMENTech60402.2023.10423449.
39. N. Zhou, F. Dufour, V. Bode, P. Zinterhof, N. J. Hammer, and D. Kranzlmüller, "Towards Confidential Computing: A Secure Cloud Architecture for Big Data Analytics and AI," in 2023 IEEE 16th International Conference on Cloud Computing (CLOUD), 2023, pp. 293–295. doi: 10.1109/CLOUD60044.2023.00042.
40. D. Dzulhikam and M. E. Rana, "A Critical Review of Cloud Computing Environment for Big Data Analytics," in 2022 International Conference on Decision Aid Sciences and Applications (DASA), 2022, pp. 76–81. doi: 10.1109/DASA54658.2022.9765168.

41. F. Fataftah and B. Isong, "Security Issues and Possible Solutions in Cloud Computing and Big Data: A Review," in 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET), 2022, pp. 1–6. doi: 10.1109/ICECET55527.2022.9872548.
42. A. K. Sandhu, "Big data with cloud computing: Discussions and challenges," Big Data Min. Anal., vol. 5, no. 1, pp. 32–40, 2022, doi: 10.26599/BDMA.2021.9020016.
43. F. Wang, H. Wang, and L. Xue, "Research on Data Security in Big Data Cloud Computing Environment," in 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 2021, pp. 1446–1450. doi: 10.1109/IAEAC50856.2021.9391025.