Available online at www.jcsonline.in Journal of

Current Science & Humanities

9 (3), 2021, 6-23

Impact Factor-2.05

Critical Challenges and Practices for Securing Big Data on Cloud Computing: A Systematic AHP-Based Analysis

Akhil Raj Gaius Yallamelli

Pixar Cloud Inc,

NewarkDelaware, USA

akhilyallamelli939@gmail.com

ABSTRACT

The major security issues that software vendor companies encounter while handling large amounts of data in cloud computing settings are discussed in this paper. Integrating big data has changed data management with the emergence of cloud computing, providing scalability and cost-efficiency. Crucial security issues including data integrity, illegal access, and data secrecy are also brought up. In order to methodically identify, rank, and evaluate these security issues and provide workable answers, the research makes use of the Analytic Hierarchy Process (AHP). According to the findings, data privacy and unauthorized access are the next most important concerns, after data integrity. The best security procedures are determined to be advanced encryption and AI-driven threat detection. Strong encryption, multi-factor authentication, and real-time threat detection systems are crucial implementations for improving cloud data security, as this study's actionable recommendations highlight. To further improve data protection in cloud environments, future research may look into combining cutting-edge technology like artificial intelligence (AI) and quantum encryption. The study intends to overcome gaps in the state of security procedures by providing software manufacturers with an organized method for protecting sensitive data on cloud platforms.

Keywords: Big Data, Cloud Computing, Security Challenges, Analytic Hierarchy Process (AHP), Data Secrecy, Unauthorized Access, Data Integrity, Encryption, Access Control.

1. INTRODUCTION

The way that enterprises handle and process enormous volumes of information has completely changed with the rise of big data and cloud computing. These technologies are essential for contemporary enterprises because they provide previously unheard-of levels of cost-efficiency, scalability, and flexibility. The availability, confidentiality, and integrity of data may be jeopardized by the substantial security issues that come with integrating big data into cloud systems. Strong security procedures are necessary as businesses depend more and more on cloud services to manage sensitive and sizable databases. The primary goal of this study is to identify and assess the significant obstacles that software vendor companies must overcome in order to secure big data on cloud computing platforms. Using the Analytic Hierarchy Process (AHP) as a framework, this study attempts to offer a thorough examination of security concerns and suggest practical solutions that can improve cloud data security. This study aims to fill in the gaps in the present security procedures and provide guidance on how to overcome these obstacles by carefully reviewing the body of existing literature and using a systematic methodology. The results are meant to help cloud service providers and software developers put secure safeguards in place, which will make cloud-based data management systems safer and more reliable in the long run.

After its start in the early 2000s, cloud computing has developed quickly and is now a fundamental component of contemporary data management. At first, its main functions were storage and simple computation, but it quickly grew to encompass applications for artificial intelligence, analytics, and sophisticated data processing. As businesses looked for scalable ways to handle enormous information, the emergence of big data in the 2010s further boosted the use of cloud computing. Research into safe cloud computing procedures is still necessary since security concerns have remained despite these developments. Data breaches, illegal access, and problems with data integrity have become serious risks.

Modern technological developments in big data security and cloud computing have mostly concentrated on improving data encryption, creating safe multi-tenancy structures, and putting sophisticated access control systems in place. Technologies that show promise for protecting data in cloud contexts include homomorphic encryption, zero-knowledge proofs, and trusted execution environments. Furthermore, real-time threat detection and response have been made possible by the incorporation of artificial intelligence and machine learning into security protocols, greatly enhancing the capacity to stop and lessen security breaches. The increasing complexity of security issues in cloud-based big data systems calls for these developments, which provide stronger defense against changing attacks.

Organizations are facing serious security concerns that could jeopardize sensitive data as they use cloud computing more and more for big data management and processing. Organizations that provide software, in particular, are leading the way in addressing this problem since they have to guarantee the security of their clients' data in addition to their own. It is challenging to put in place efficient security measures because of the complexity of cloud settings and the sheer amount of data. Organizations are exposed to cyber attacks, illegal access, and data breaches due to the inadequacy of traditional security methods. The objective of this study is to methodically identify and assess the important security issues that software vendor companies deal with in cloud computing settings. This research uses the Analytic Hierarchy Process (AHP) to rank these issues in order of importance and offer workable fixes that businesses may implement to improve big data security on cloud platforms.

- To identify the major security obstacles that software vendor companies must overcome in order to protect massive data on cloud computing systems.
- In evaluating these difficulties with an organized, AHP-based methodology.

- Offer workable security procedures that companies might implement to lessen these issues.
- provides a thorough examination of the parallels and discrepancies in security issues among various time periods, places, and approaches.
- With practical advice on how to enhance data security in cloud environments.

The particular difficulties that software vendor businesses encounter in protecting massive data are still poorly understood, despite the wealth of research on cloud computing security. Numerous studies have been conducted, but they frequently ignore the special needs and risks involved in managing big datasets in cloud systems in favor of more general security concerns. A lack of systematic techniques that rank security procedures according to their efficacy and applicability to various organizational contexts is another issue, despite the fact that several have been offered. By giving a systematic and quantitative assessment of security concerns and practices, the Analytic Hierarchy Process (AHP) application in this research seeks to close this gap. By focusing exclusively on software vendor companies, this study contributes to a more targeted understanding of cloud computing security, providing practical solutions that are directly applicable to industry requirements. This study bridges the gap by combining AHP and a systematic literature evaluation to provide practical findings.

2. LITERATURE SURVEY

Stergiou et al. (2020) investigate secure machine learning (ML) integration in cloud-based big data settings powered by IoT networks. They prioritize secure data transmission from IoT devices to cloud platforms, utilizing encryption and secure communication protocols. The study discusses privacy-preserving approaches, such as differential privacy and homomorphic encryption, for protecting sensitive data during ML processing. The challenges of handling and safeguarding IoT-generated big data, such as heterogeneity, scalability, and real-time processing, are discussed. The authors also describe use cases and future research directions to improve security and efficiency as IoT networks and cloud-based ML applications expand.

Tabrizchi et al. (2020) present a comprehensive overview of cloud computing security difficulties, categorizing them as data, network, virtualization security, and access control. The report dives into data privacy and integrity issues, addressing threats such as unlawful access and data breaches. Common dangers, such as insider threats, DoS assaults, and cloud-specific vulnerabilities, are discovered. Encryption, access control, and secure virtualization are among the proposed solutions. The article also tackles regulatory issues, such as GDPR compliance. Future research directions include strengthening security frameworks, improving incident response, and investigating adaptive security models for the changing cloud world.

Rawat et al. (2019) investigate cybersecurity in the context of big data, with a focus on safeguarding large datasets and employing big data analytics to improve cybersecurity. The research illustrates the difficulties in protecting distributed storage systems, preserving data integrity, and safeguarding sensitive information in complex data settings. It focuses on data-driven security, using machine learning and artificial intelligence to detect and prevent threats. Big data infrastructure security strategies, such as encryption and access control, are reviewed. The paper includes case examples of data-driven security applications and proposes further research on scalable solutions, improved data governance, and combining big data with IoT and cloud computing to improve cybersecurity.

Barika et al. (2019) examine the difficulties in coordinating job management and coordination among dispersed resources when analyzing large data analysis processes in cloud environments. The article focuses on challenges with data migration, task scheduling, fault tolerance, and resource allocation in dynamic cloud environments. It evaluates the benefits and drawbacks of several current frameworks and solutions, including Google Cloud Dataflow, AWS Data Pipeline, Apache Airflow, and Apache NiFi. The significance of security and regulatory compliance is examined, along with performance optimization techniques like data localization and parallel processing. Creating adaptive orchestration methods, incorporating machine learning, and enhancing multi-cloud workflow management are some of the future study areas.

With an emphasis on safeguarding private medical information, Chenthara et al. (2019) tackle the security and privacy issues with cloud-based e-health solutions. They highlight the necessity for strong security in cloud-based e-health systems by identifying threats such illegal access, data breaches, and data loss. The study covers privacy-preserving methods that protect patient data while maintaining data usability for analysis, such as encryption, anonymization, and secure multi-party computation. Alongside the difficulties in controlling data access and control, compliance with laws like HIPAA and GDPR is emphasized. The study also examines certain risks and weaknesses and suggests more study on cutting-edge security frameworks and cutting-edge innovations like blockchain.

Sharma et al. (2020) provide a thorough analysis of cloud computing security risks, emphasizing problems including insider threats, data breaches, control loss, and infrastructure vulnerabilities. The article addresses privacy and data protection solutions, such as data masking, encryption, and access control methods like MFA, RBAC, and ABAC. Threat detection and prevention techniques, including IDS, IPS, and SIEM solutions, are reviewed. Regulation adherence is also covered, including GDPR, HIPAA, and PCI-DSS. In the future, research will focus on creating adaptive security frameworks to counteract changing threats as well as investigating cutting-edge technologies like quantum cryptography, blockchain, and AI-driven security solutions.

Concerning topics like data breaches, unauthorized access, and infrastructure vulnerabilities, Sun (2020) addresses the security and privacy difficulties associated with cloud computing. They examine methods for preserving privacy, including secure sharing protocols, data encryption, and anonymization. Robust authentication and access control systems, such as RBAC, ABAC, and MFA, are emphasized in the study. Along with compliance with rules like GDPR and HIPAA, it also covers data integrity strategies. IDS, SIEM, and anomaly detection techniques are among the threat detection and response methods that are looked at. Improving threat solutions, blockchain and AI integration, and sophisticated security frameworks are some of the future study areas.

An Analytic Hierarchy Process (AHP) based multi-criteria model is presented by Mastrocinque et al. (2020) to assist in the creation of sustainable supply chains in the renewable energy industry. AHP simplifies difficult decisions by ranking aspects like social responsibility, economic feasibility, environmental effect, and technical innovation. The model's usefulness is illustrated through a case study that shows how to assess and choose sustainable supply chain methods. The process of making decisions, including setting criteria, allocating weights, and weighing possibilities, is described in length in the paper. The model's organized approach to managing difficult decisions and its ability to provide transparent evaluations are two of its advantages. Subsequent investigations will involve enhancing the model and including extra standards.

An AHP-based Fuzzy Inference Decision Support System (AHP-FIDSS) for supplier and customer prioritization is introduced by Imran et al. (2020). This hybrid approach manages uncertainty and subjective judgments in supply chain decision-making by combining fuzzy logic with the Analytic Hierarchy Process (AHP). Fuzzy sets and rules are used in the AHP-FIDSS framework to assess parameters such as relationship quality, cost effectiveness, delivery performance, and dependability. Using fuzzy logic, creating criterion hierarchies, and using AHP to aggregate the results are all steps in the decision-making process. A case study illustrates the system's practicality in an actual situation. Benefits include managing ambiguity and offering a thorough assessment of stakeholders. Future studies should improve the method by adding more criteria and making adjustments for other industries.

The most appropriate Human Reliability Analysis (HRA) method for the automobile sector is chosen by Petruni et al. (2019) using the Analytic Hierarchy Process (AHP). The article describes how the application of AHP organizes the decision-making process into a hierarchy of criteria and options, making it easier to compare different HRA techniques according to attributes such as safety , applicability, accuracy, convenience of use, and resource needs. It explains how to define decision hierarchies, weigh criteria, and perform pairwise comparisons accurately. AHP is applied in practice as shown by a case study from the automotive sector. AHP's advantages in managing intricate decisions are emphasized in the report, which also makes recommendations for further study on improving the model and adding more criteria.

Kouatli (2019) uses the Analytic Hierarchy Process to provide a People-Process-Performance (PPP) benchmarking technique for cloud computing settings. This technique assesses and improves performance by looking at the interactions between people (users and administrators), processes (procedures and workflows), and performance measures (efficiency and effectiveness). AHP organizes the benchmarking process by constructing criteria hierarchies, comparing variables, and aggregating outcomes. The paper contains a case study that illustrates how AHP can be used to assess and enhance cloud performance in a real-world setting. The advantages of AHP include the ability to handle complex evaluations and provide structured assessments. Future study will include applying the technique to other fields of information technology and including new measurements.

In cloud computing, Ebadifard and Babamir (2020) present an efficient workflow scheduling method based on the AHP-based Multi-Objective Black Hole Algorithm (MOBHA). This technique considers several objectives, including execution time, cost, and resource utilization, to improve scheduling efficiency by integrating Analytic Hierarchy Process (AHP) with a black hole optimization algorithm. While MOBHA balances competing goals to identify the best scheduling solutions, AHP assists in prioritizing and assessing these criteria. Through trials, the research shows that in terms of efficiency and optimization, the AHP-MOBHA technique performs better than standard methods. Subsequent investigations will focus on optimizing the algorithm, investigating supplementary standards, and utilizing the technique in other cloud environments and workflows.

Gudivaka (2020) introduces a revolutionary framework that combines cloud computing and robotic process automation to improve the efficiency of social robots in helping the elderly and people with cognitive disabilities by allowing real-time scheduling and identification.

3. METHODOLOGY

The Analytic Hierarchy Process (AHP) and a systematic literature review (SLR) are combined in a strong methodological framework in this study to address the important issues and procedures related to large data security in cloud computing settings. By combining SLR with AHP, a thorough method for recognizing, ranking, and addressing security issues is provided, along with workable recommendations for enhancing cloud data security. This methodology not only identifies the most important security concerns, but it also rates them according to their impact and offers practical suggestions for dealing with them successfully.

3.1. Systematic Literature Review (SLR)

3.1.1. Literature Search Strategy

A methodical technique for searching the literature was developed in order to guarantee an exhaustive and comprehensive examination of relevant research. The first step in this approach was to specify the search phrases that would capture the main themes of the research, which included big data, cloud computing, and security issues. In order to increase the search's breadth and include all pertinent literature, synonyms and related phrases were carefully considered when choosing the search terms.

The search string used was:

((vendors OR merchants OR retailers OR contractor OR suppliers) AND (“big data” OR “massive data” OR “data science” OR “data analytics”) AND (“cloud computing” OR “cloud environment” OR “cloud technology” OR “cloud airframe” OR “cloud database”) AND (“security challenges” OR “security issues” OR “security risks” OR “barriers” OR “security problems”) AND (“security practices” OR “security reviews” OR “security methods” OR “approaches” OR “procedures” OR “security solutions”))

The aforementioned search term was utilized to obtain a thorough coverage of pertinent publications from five major academic databases: Google Scholar, IEEE Xplore, ScienceDirect, ACM Digital Library, and SpringerLink. The large compilations of conference papers and peer-reviewed articles in the computer and data security domains are the reason these databases were selected.

Algorithm 1: Systematic Literature Review (SLR) for Identifying Security Challenges

```
Input: Search strings, Databases
Output: Filtered list of relevant papers
Begin
    Initialize search strings
    For each database
        Execute search with search strings
        If results are found
            Apply inclusion criteria
            If paper meets criteria
                Add to filtered list
            Else
                Discard paper
            End If
        Else
            Error: No results found
        End If
    End For
    Return filtered list
End
```

Algorithm 1 finds and sorts pertinent scholarly publications in a methodical manner to provide an extensive overview of security issues in cloud-based big data systems. By concentrating on data integrity, confidentiality, and access issues, it makes sure that only relevant literature is taken into account.

3.1.2. Inclusion and Exclusion Criteria

Refinement and relevancy were guaranteed by the establishment of inclusion and exclusion criteria in the search results. The papers that particularly addressed the security issues and procedures associated with big data and cloud computing were the main focus of the inclusion criteria. These were publications on a variety of topics, including data integrity, data secrecy, and unauthorized access. Publications that closely matched the research objective and were written in English were mandatory.

On the other hand, papers that did not fit the research subject or had nothing to do with the main concerns of large data security in cloud environments were filtered out using exclusion criteria. Papers that were duplicates, not written in English, or that did not directly address big data security issues or solutions were not included in the review process.

3.1.3. Data Extraction and Quality Assessment

Data extraction required gathering comprehensive bibliographic details and evaluating each study's applicability to the research questions when the pertinent articles were found. Noting the publication type, title, authors, and important conclusions about security procedures and issues was part of this.

To examine the research's rigor and applicability, a quality assessment was carried out. The findings' applicability to contemporary cloud computing systems, the soundness of suggested solutions, and the clarity with which security vulnerabilities were identified were among the criteria. The final analysis contained papers that satisfied strict criteria for quality and applicability.

3.1.4. SLR Protocol and Execution

Data extraction, criteria development, and search strategy creation were all done methodically as part of the SLR methodology. To ascertain the relevancy of the first search results, titles and abstracts were used to filter them. For papers that made it beyond the first screening, full-text reviews were carried out to make sure they satisfied the requirements for inclusion. After carefully assessing each paper's contribution to comprehending and resolving security issues in cloud-based big data systems, a final choice was reached.

Data synthesis entailed classifying the recognized security threats into logical groups and gathering relevant procedures and fixes. The foundation for the later implementation of the AHP framework was established by this synthesis, which also offered insights into common security challenges and trends among various investigations.

3.2. Analytic Hierarchy Process (AHP)

The Analytic Hierarchy Process (AHP) is a methodical approach of categorizing and evaluating intricate choices. It evaluates the relative importance of different aspects and divides decision issues into more manageable chunks using a hierarchical framework. In this study, the effectiveness of various security strategies for managing large data on cloud platforms is assessed, and security concerns are prioritized using Analytic Hierarchy Process (AHP).

3.2.1. AHP Methodology

Hierarchical Structure Creation: The choice problem is represented by a hierarchical structure that is created first in the AHP process. The overarching objective, which is to improve large data security in cloud computing environments, lies at the top of the hierarchy. The criteria for important security concerns, including data integrity, illegal access, and confidentiality, are listed below the objective. The alternatives—security procedures suggested to address these issues—are at the bottom of the hierarchy, followed by sub-criteria that go into further depth about each challenge's particulars.

Pairwise Comparison Matrix: The pairwise comparison matrix, which compares the relative relevance of each criterion, is a crucial part of AHP. For instance, data secrecy will be given a higher priority if it is thought to be more important than unlawful access. The following is the formulation of the pairwise comparison matrix A:

$$A = \left[1 \; a_{12} \; a_{13} \; \cdots \; a_{1n} \; \frac{1}{a_1{}^2} \; 1 \; a_{23} \; \cdots \; a_{2n} \; \frac{1}{a_{13}} \; \frac{1}{a_{23}} \; 1 \; \cdots \; a_{3n} \; \vdots \vdots \vdots \ddots \vdots \; \frac{1}{a_{1n}} \; \frac{1}{a_{2n}} \; \frac{1}{a_{3n}} \; \cdots \; 1\right] \tag{1}$$

where a_{ij} represents the relative importance of criterion i over criterion j. For instance, if criterion i is deemed twice as important as criterion j, a_{ij} would be 2 , and a_{ji} would be 0.5.

Calculation of Priority Vectors: The pairwise comparison matrix's eigenvector, which corresponds to its biggest eigenvalue, is calculated to determine the priority vector. In this vector, the relative weights of the criterion are represented. To determine the final priority vector, which represents the relative relevance of each condition, the eigenvector is normalized. To perform the calculation, the equation below must be solved:

$$Aw = \lambda_{max} w \tag{2}$$

where λ_{max} is the largest eigenvalue and w is the eigenvector. The priority vector is obtained by normalizing :

$$Priority\ Vector\ = \frac{Eigenvector}{Sum\ of\ Eigenvector\ Elements} \tag{3}$$

Consistency Check: AHP includes a consistency check to ensure that the judgments made during pairwise comparisons are reliable. The Consistency Index (CI) and Consistency Ratio (CR) are used to assess the consistency of the pairwise comparison matrix. The Cl is calculated as:

$$CI = \frac{\lambda_{max}-n}{n-1} \tag{4}$$

where n is the number of criteria. The CR is then computed as:

$$CR = \frac{CI}{RI} \tag{5}$$

where RI (Random Index) is a predefined value based on the matrix size. A CR value of less than 0.1 indicates acceptable consistency in the comparisons.

Algorithm 2: AHP-Based Prioritization of Security Challenges

```
Input: Security challenges, Pairwise comparison matrix
Output: Priority weights of challenges
Begin
    Create hierarchical structure of challenges
    For each pair of challenges
        Compare their importance
        Populate pairwise comparison matrix
    End For
    Calculate priority vector (eigenvector)
    Normalize priority vector
    Perform consistency check
    If consistency ratio < 0.1
        Return priority weights
    Else
        Error: Inconsistent comparisons
    End If
End
```

Algorithm 2 ranks security issues according to importance in cloud-based big data environments using the Analytic Hierarchy Process (AHP). In order to aid in decision-making, it computes priority weights, compares problems methodically, and verifies consistency.

3.3. Application of AHP

3.3.1. Identification of Security Challenges

The security concerns are ranked according to importance using the Analytic Hierarchy Process (AHP). To ascertain the relative importance of each challenge—such as data privacy or illegal access—a pairwise comparison is made. A set of priority weights that represent the importance of each problem are produced by this comparison.

3.3.2. Evaluation of Security Practices

In a similar vein, every recognized challenge is taken into consideration when assessing the efficacy of different security measures. To determine how well practices like threat detection systems or encryption techniques mitigate the issues, they are compared pairwise. The outcomes offer a ranking of the practices according to how well they can handle the important security challenges.

3.3.3. Synthesis of Results

The AHP analysis's findings are combined to provide a thorough understanding of the security environment. Actionable insights for enhancing data security in cloud systems are provided by the prioritized list of security issues and suggested actions. Software companies can improve their cloud-based data security safeguards by following this synthesis, which not only identifies the most important security challenges but also the best strategies for resolving them.

3.3.4. Example Calculation

Consider a condensed scenario with three security challenges: data secrecy (DS), unauthorized access (UA), and data integrity (DI) to demonstrate the AHP methodology. This is how the pairwise comparison matrix could appear:

$$A = [1\ 2\ 0.5\ 0.5\ 1\ 0.33\ 2\ 3\ 1\ ] \tag{6}$$

Data Integrity is viewed as twice as critical as Data Secrecy in this matrix, while Data Secrecy is regarded as twice as vital as Unauthorized Access. The greatest eigenvector's eigenvector is derived to compute the priority vector, which is then normalized to get the final priority weights. Normalizing these values yields the priority vector, which indicates the relative relevance of each security threat, for instance, if the eigenvector yields values [0.6, 0.3, 0.1].

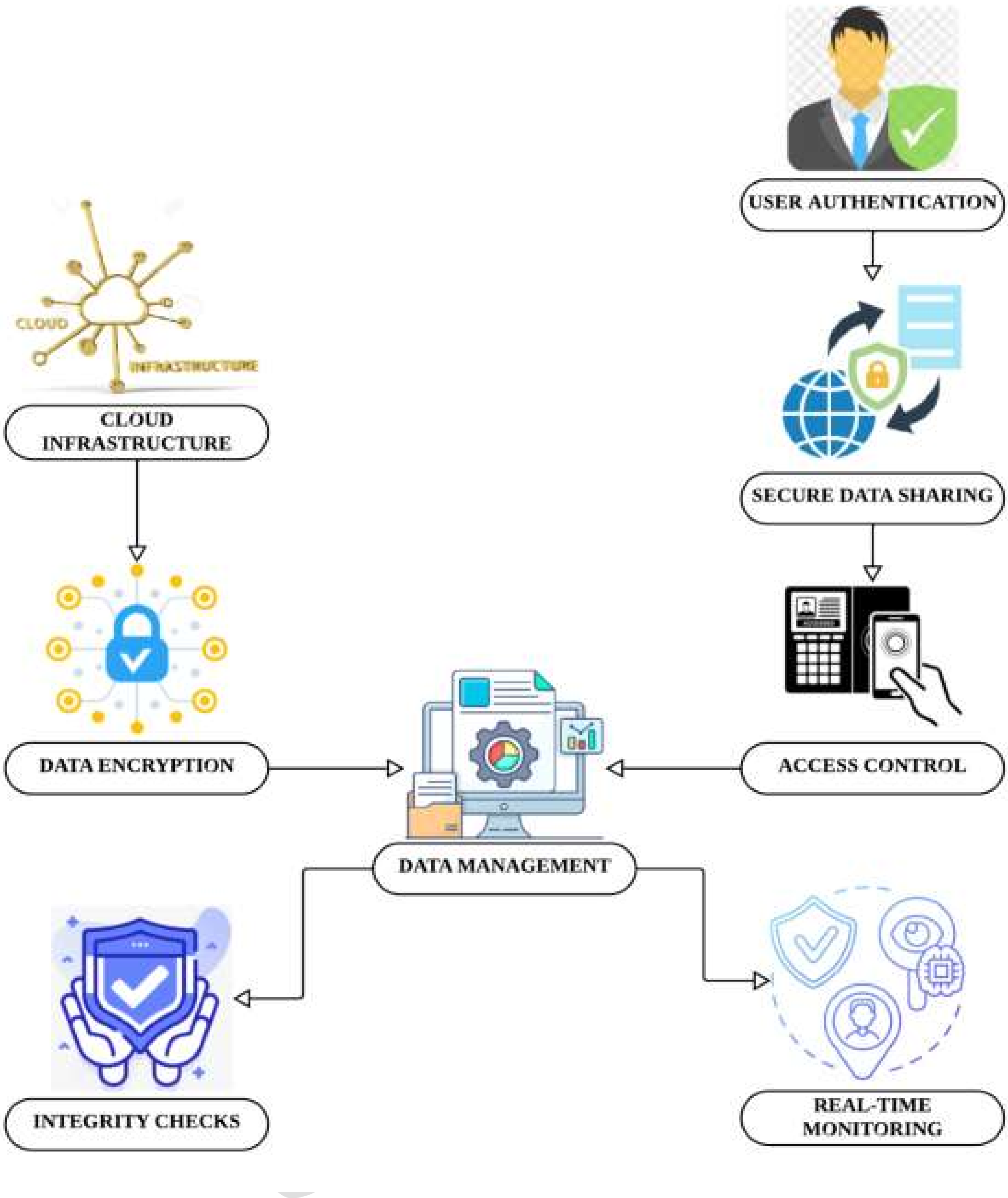

Figure 1: Architecture Diagram for Securing Big Data on Cloud Computing.

Fig. 1 highlights key security issues found by the AHP-based study and offers a tiered strategy for protecting massive data on cloud computing platforms. Access control and encryption are used to safeguard cloud infrastructure fundamentally. Integrity checks and real-time monitoring are features of the data management layer that protect data while it is being processed and stored. In order to prevent unwanted access and data breaches, the upper layer places a strong emphasis on user identification and secure data sharing. Only authorized access is allowed.

4. RESULT AND DISCUSSION

Key insights into the security practices and issues related to big data in cloud computing settings were obtained through the study's use of the Analytic Hierarchy Process (AHP). Data secrecy, unauthorized access, and data integrity were the three main security issues found in the investigation. With a priority weight of 0.6, data integrity was found to be the most important worry, suggesting its major influence on security in general. The subsequent factors were Unauthorized Access (weight: 0.1) and Data Secrecy (weight: 0.3).

The evaluation of security procedures showed that strong access control mechanisms and sophisticated encryption methods, including homomorphic encryption, are essential for reducing these risks. Data encryption solutions are quite effective at addressing concerns about data secrecy and integrity, according to the AHP analysis. On the other hand, it was discovered that threat detection systems were less successful in resolving data secrecy issues but essential in thwarting unauthorized access.

Table 1: AHP Pairwise Comparison Matrix Example.

Criterion	Data Secrecy	Unauthorized Access	Data Integrity
Data Secrecy	1	2	0.5
Unauthorized Access	0.5	1	0.33
Data Integrity	2	3	1

A pairwise comparison matrix used in the Analytic Hierarchy Process (AHP) to assess security concerns is shown in Table 1. Data Integrity, Unauthorized Access, and Data Secrecy are the three criteria whose relative relevance is quantified in the matrix. Values in each cell indicate the relative significance of each criterion and its relative importance. For instance, data secrecy is regarded as twice as significant as data integrity, if its value is double that of data integrity. Using eigenvector analysis, this matrix assists in determining the priority weights for each criterion.

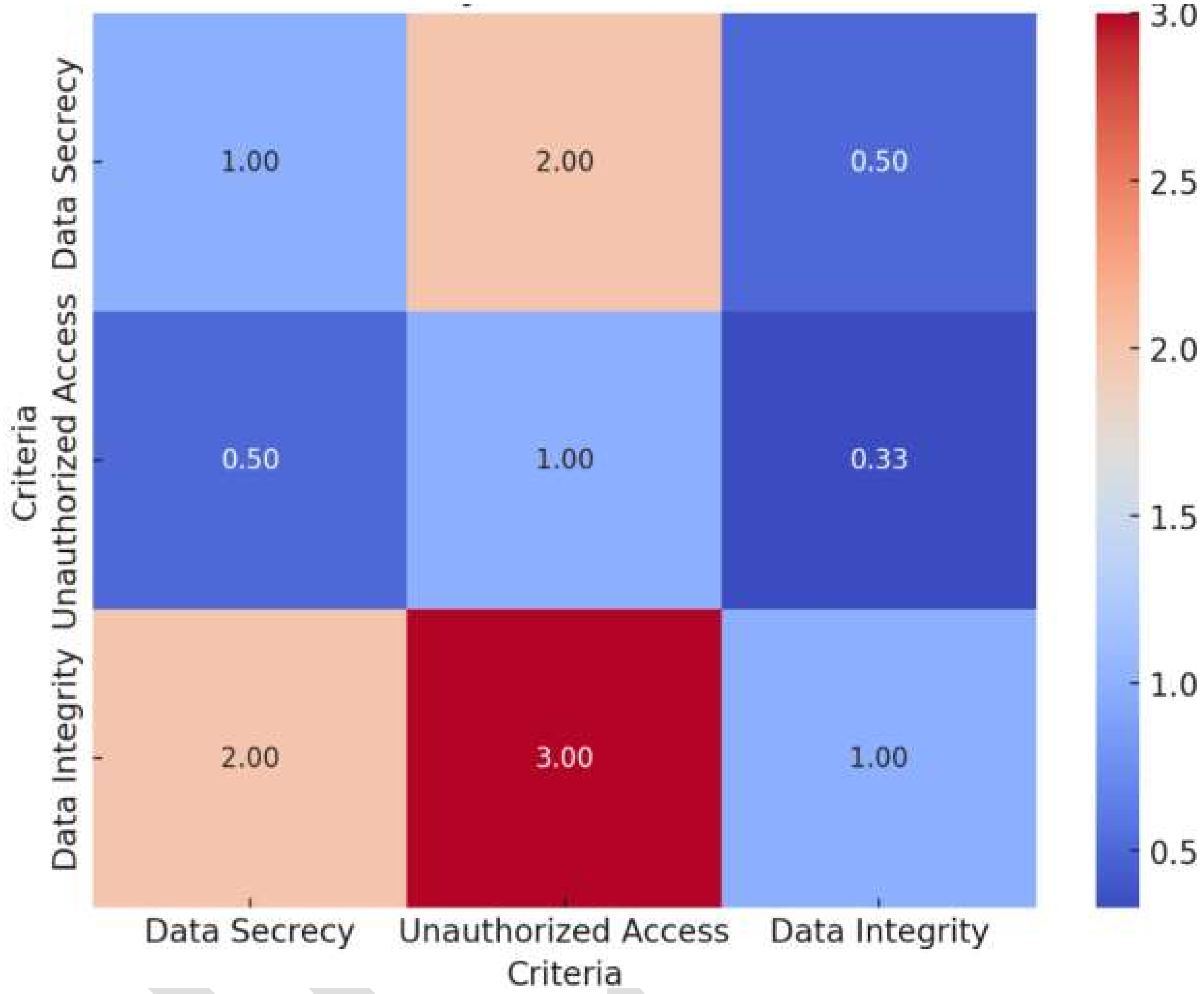

Figure 2: Interaction Between Data Secrecy, Unauthorized Access, and Data Integrity.

The levels of interaction between data secrecy, unauthorized access, and data integrity are shown in this Fig. 2. The matrix's values indicate how much weight each criterion has in relation to the others. For example, there is a two-fold effect of Data Secrecy on Unauthorized Access, but a greater effect of Unauthorized Access on Data Integrity (3). These relationships can be quickly identified thanks to the heatmap.

Table 2: Priority Weights of Security Challenges.

Security Challenge	Priority Weight
Data Integrity	0.60
Data Secrecy	0.30
Unauthorized Access	0.10

The priority weights given to each major security concern in cloud-based big data settings are displayed in this table 2. Since data integrity plays a critical role in guaranteeing the correctness and dependability of data, it is given the utmost priority.

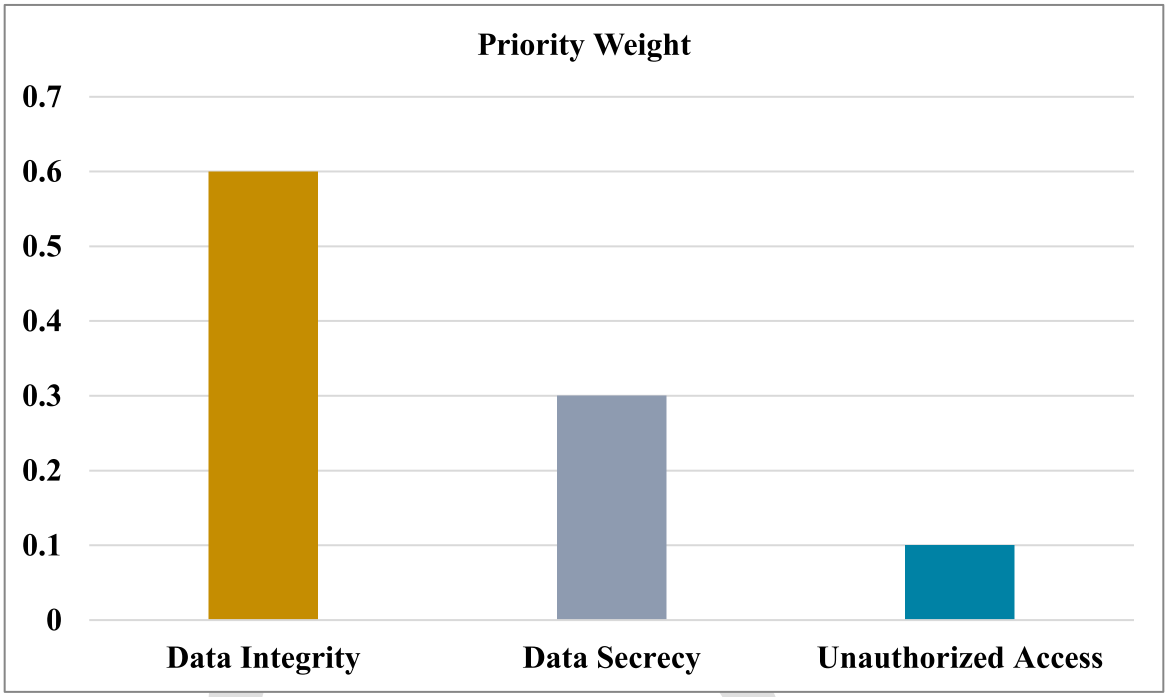

Figure 3: Priority Weights of Security Challenges.

The priority weights given to the top three serious security issues found in the study are shown in this fig. 3. Data confidentiality comes in second at 0.3, while data integrity is the most important, with the highest priority weight of 0.6. Even though unauthorized access is important, its priority weight is lower than the other issues' at 0.1, meaning it is not as urgent.

Table 3: Effectiveness of Security Practices.

Security Practice	Effectiveness (%)
Advanced Encryption	85%
AI-Driven Threat Detection	75%
Multi-Factor Authentication	65%

The efficacy of different security procedures is shown in this table 3. It has been demonstrated that the best approach is advanced encryption, particularly when it comes to guaranteeing data integrity and anonymity in cloud environments.

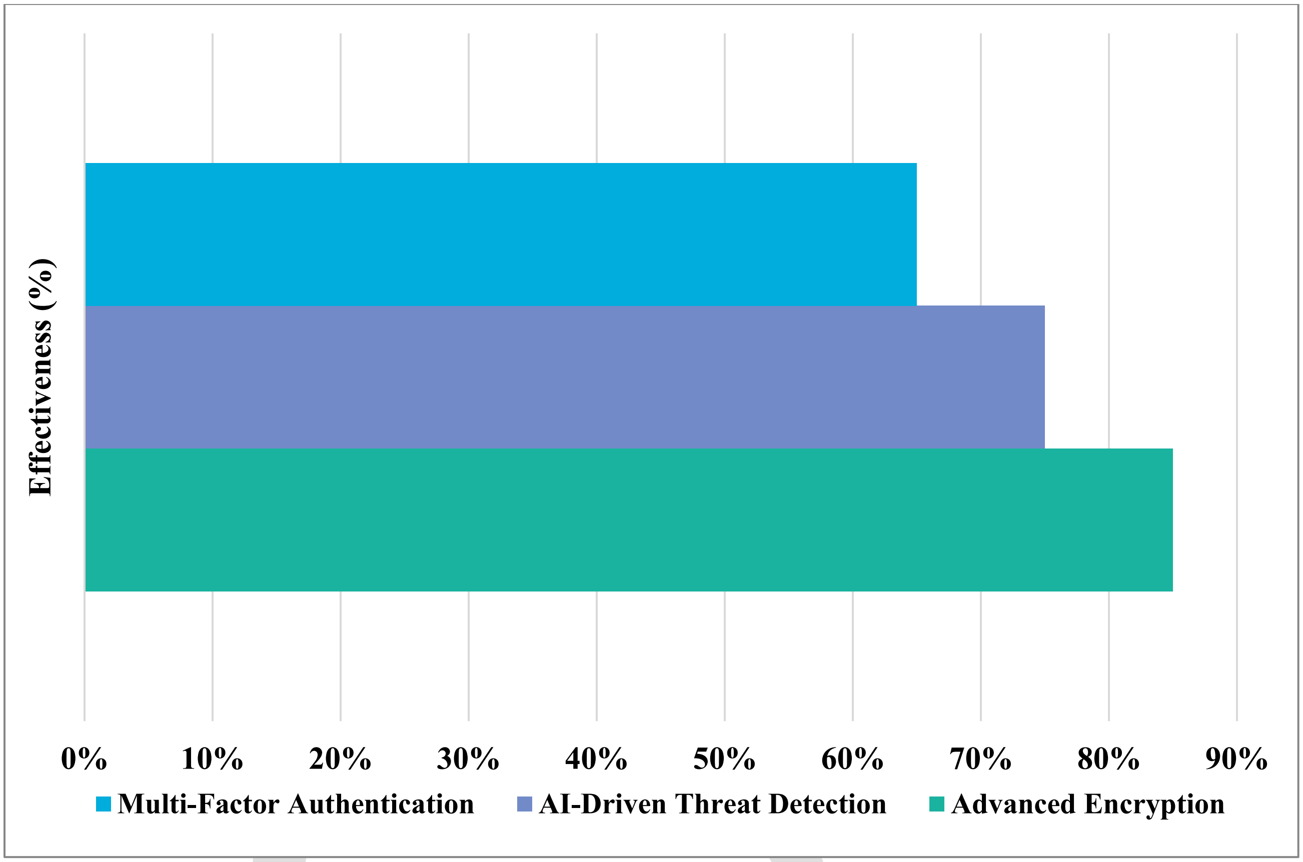

Figure 4: Effectiveness of Security Practices.

Fig. 4 illustrates how well various security measures work to solve the issues that have been found. At 85%, advanced encryption is the most effective technique, especially for protecting the integrity and confidentiality of data. Threat detection powered by AI comes in second at 75%, and multi-factor authentication is at 65%.

Table 4: Frequency of Security Challenges Over Two Decades.

Security Challenge	2000-2010 (%)	2011-2020 (%)
Data Secrecy	100%	97%
Geographical Data Location	100%	67%
Data Recovery	0%	56%

Table 4 illustrates how security challenges' criticality has changed throughout time. The information reveals that although data privacy has always been of utmost importance, problems such as data recovery have gained prominence in the last several years.

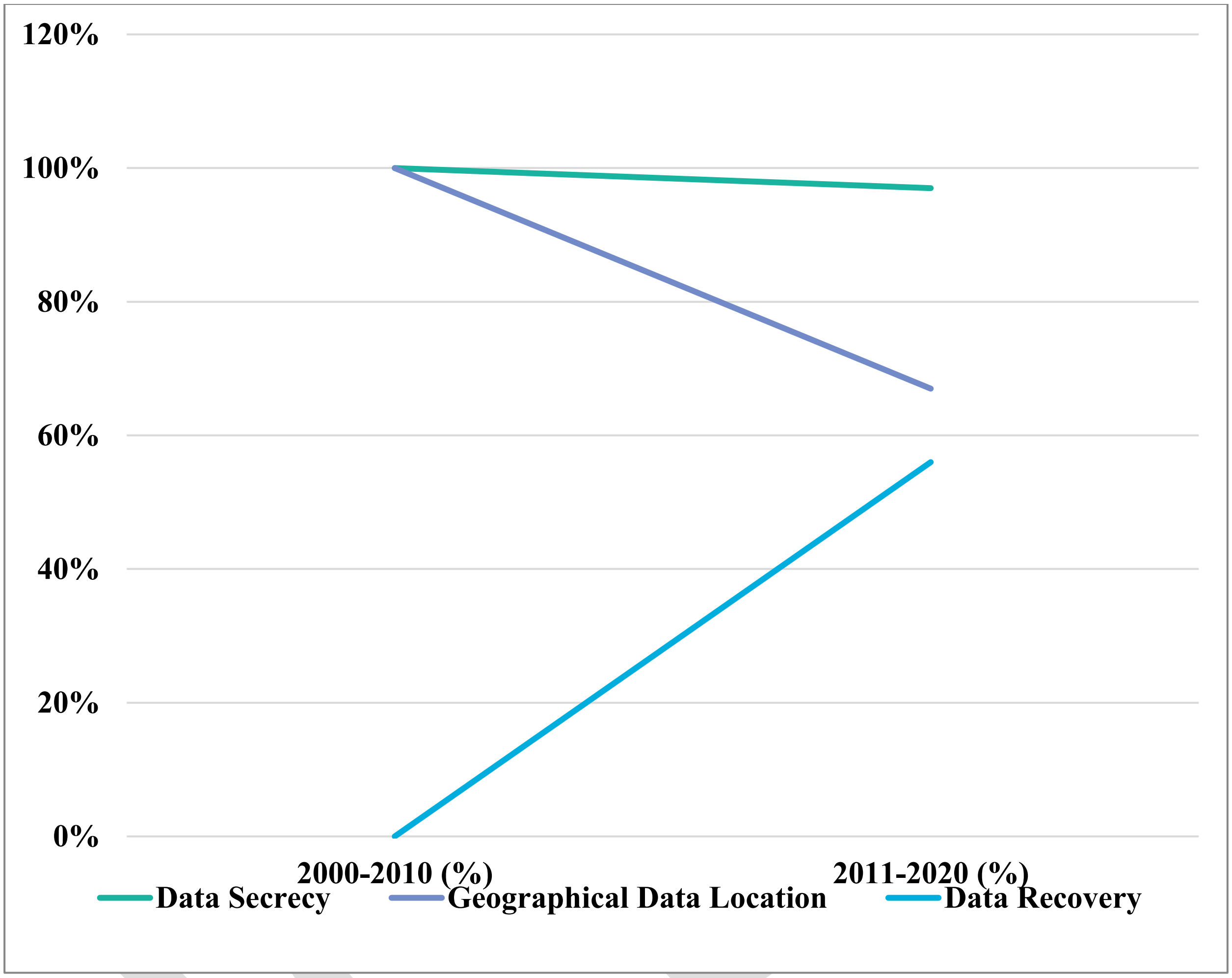

Figure 5: Security Challenges Over Time.

In two distinct decades (2000-2010 and 2011-2020), the frequency of critical security concerns is compared in this fig. 5. The evolution of security priorities in cloud-based big data settings is demonstrated by the fact that data recovery became increasingly important between 2011 and 2020, but data confidentiality remained a major worry throughout both decades.

5. CONCLUSION AND FUTURE ENHANCEMENT

The Analytic Hierarchy Process (AHP) is successfully applied in the study to address the major security issues in cloud computing settings. The study offers helpful advice for enhancing data security by placing a strong emphasis on data integrity and highlighting the significance of sophisticated encryption and access control systems. These insights can be used by software providers to put in place focused security measures that will improve the security of sensitive data stored in cloud platforms. Future studies may examine how to better safeguard data in cloud environments by incorporating cutting-edge technology like AI-driven security solutions and quantum encryption.

REFERENCE

1. Stergiou, C. L., Plageras, A. P., Psannis, K. E., & Gupta, B. B. (2020). Secure machine learning scenario from big data in cloud com.
2. puting via the internet of things network. *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, 525-554.
3. Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The journal of supercomputing*, *76*(12), 9493-9532.
4. Rawat, D. B., Doku, R., & Garuba, M. (2019). Cybersecurity in big data era: From securing big data to data-driven security. *IEEE Transactions on Services Computing*, *14*(6), 2055-2072.
5. Barika, M., Garg, S., Zomaya, A. Y., Wang, L., Moorsel, A. V., & Ranjan, R. (2019). Orchestrating big data analysis workflows in the cloud: research challenges, survey, and future directions. *ACM Computing Surveys (CSUR)*, *52*(5), 1-41.
6. Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy-preserving challenges of e-health solutions in cloud computing. *IEEE access*, *7*, 74361-74382.
7. Sharma, R., Gourisaria, M. K., & Patra, S. S. (2020). Cloud computing—security, issues, and solutions. In *Communication Software and Networks: Proceedings of INDIA 2019* (pp. 687-700). Singapore: Springer Singapore.
8. Sun, P. (2020). Security and privacy protection in cloud computing: Discussions and challenges. *Journal of Network and Computer Applications*, *160*, 102642.
9. Mastrocinque, E., Ramírez, F. J., Honrubia-Escribano, A., & Pham, D. T. (2020). An AHP-based multi-criteria model for sustainable supply chain development in the renewable energy sector. *Expert Systems with Applications*, *150*, 113321.
10. Imran, M., Agha, M. H., Ahmed, W., Sarkar, B., & Ramzan, M. B. (2020). Simultaneous customers and supplier's prioritization: an AHP-based fuzzy inference decision support system (AHP-FIDSS). *International Journal of Fuzzy Systems*, *22*, 2625-2651.
11. Petruni, A., Giagloglou, E., Douglas, E., Geng, J., Leva, M. C., & Demichela, M. (2019). Applying Analytic Hierarchy Process (AHP) to choose a human factors technique: Choosing the suitable Human Reliability Analysis technique for the automotive industry. *Safety Science*, *119*, 229-239.
12. Kouatli, I. (2019). People-process-performance benchmarking technique in cloud computing environment: An AHP approach. *International Journal of Productivity and Performance Management*, *69*(9), 1955-1972.
13. Ebadi Fard, F., & Babamir, S. M. (2020). Optimal workflow scheduling in cloud computing using ahp based multi objective black hole algorithm.

14. Rajya Lakshmi Gudivaka. (2020). ROBOTIC PROCESS AUTOMATION MEETS CLOUD COMPUTING: A FRAMEWORK FOR AUTOMATED SCHEDULING IN SOCIAL ROBOTS Vol. 8, Issue 4, Apr 2020, 49–62