Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH

Open Access

Enhanced mechanism to prioritize the cloud data privacy factors using AHP and TOPSIS: a hybrid approach

Mohammad Zunnun Khan[1*], Mohd Shoaib[2], Mohd Shahid Husain[3], Khair Ul Nisa[1,4] and Mohammad. Tabrez Quasim[1,4]

Abstract

Cloud computing is a new paradigm in this new cyber era. Nowadays, most organizations are showing more reliability in this environment. The increasing reliability of the Cloud also makes it vulnerable. As vulnerability increases, there will be a greater need for privacy in terms of data, and utilizing secure services is highly recommended. So, data on the Cloud must have some privacy mechanisms to ensure personal and organizational privacy. So, for this, we must have an authentic way to increase the trust and reliability of the organization and individuals The authors have tried to create a way to rank things that uses the Analytical Hieratical Process (AHP) and the Technique for Order Preference by Similarity to the Ideal Solution (TOPSIS). Based on the result and comparison, produce some hidden advantages named cost, benefit, risk and opportunity-based outcomes of the result.

In this paper, we are developing a cloud data privacy model; for this, we have done an intensive literature review by including Privacy factors such as Access Control, Authentication, Authorization, Trustworthiness, Confidentiality, Integrity, and Availability. Based on that review, we have chosen a few parameters that affect cloud data privacy in all the phases of the data life cycle. Most of the already available methods must be revised per the industry's current trends. Here, we will use Analytical Hieratical Process and Technique for Order Preference by Similarity to the Ideal Solution method to prove that our claim is better than other cloud data privacy models. In this paper, the author has selected the weights of the individual cloud data privacy criteria and further calculated the rank of individual data privacy criteria using the AHP method and subsequently utilized the final weights as input of the TOPSIS method to rank the cloud data privacy criteria.

Keywords Analytical Hieratical Process (AHP), Technique for Order Preference by Similarity to the Ideal Solution (TOPSIS), Cloud data privacy, Access control, Authorization, Authentication, Trustworthiness, Confidentiality, Integrity, Availability, Service Level Agreement (SLA)

Introduction

Cloud Computing is an internet-enabled technology that allows access and manipulates information stored on remote servers. Computing resources and related applications are now available for us as a service via the internet, which is increasing daily. This concept is familiar; we have already used cloud services such as Google Mail, Microsoft Office 365, and Google Docs. It is a well-known and undeniable fact that shortly, most government offices, business enterprises, and even individuals will increasingly rely on Cloud technologies. The cloud computing paradigm has vastly changed the way of information management, particularly in personal data processing. It is quite exciting for End customers to use cloud services without being experts in the underlying technology. This is one of the crucial features of cloud services, which has the advantage of lowering costs by sharing

*Correspondence:
Mohammad Zunnun Khan
zunnunkhan@gmail.com
Full list of author information is available at the end of the article

processing and storage resources in conjunction with an on-demand provisioning mechanism based on a pay-per-use business model [1]. These new capabilities heavily impacted the budget of IT infra and the related costs, but it is also a matter of concern for traditional security, privacy, and trust-related measures. In this study, privacy is referred to as the right of an individual, which is totally self-defined, or the right of an individual to "know what is known about them", be aware of publicly available information about them, and control over the communication of that information and to prevent its abuse. In other words, the right to privacy is linked to the right to self-determination, which is the right to preserve personal information. Every person has the right to be in charge of his or her data, whether it is personal, public, or work-related. End customers who utilize cloud services need to learn where the server is physically located or how personal data is processed. They also need to learn about the processes involved. The privilege of modifying data in the cloud services comes with the risk of losing access to it. For instance, putting personal data on a server someplace on the web may be a big problem for Privacy [2]. So, cloud computing brings up many privacy and security problems. Can one trust cloud providers? Can you count on cloud servers? What are the consequences of data loss? What about security and privacy? Will it be hard to switch from one cloud to another? In the online world, privacy issues are becoming more and more significant. Most people agree that taking privacy issues seriously boosts user confidence and economic growth [3]. However, putting personal information in the Cloud in a way that is safe, easy to maintain, and under control is a significant task for everyone involved, with both legal and business pressures [4]. The paper has been organized in following sections: 1. Introduction and its sub sections, 2. Literature Review: Cloud Privacy Issues, and its sub-sections "Weighted normalized decision matrix. Each condition must weight to add up to 1. Expertise and literature review can determine weights.". Challenges to Privacy in the Cloud Ecosystem, 4. Proposed Model of Cloud Data Privacy, 5. Evaluation and Discussion, 6. Major Contributions, 7. Effectiveness of Using AHP and TOPSIS in Proposed work, 8. Conclusion and Future directive

Importance of cloud computing

Cloud computing plays a crucial role in revolutionizing the structure of contemporary IT infrastructure. The significance of this resides in its ability to offer flexible and readily available access to a communal collection of computer resources, such as servers, storage, and applications, via the internet. Organizations' gain cost efficiency by only paying for the resources they utilise, so eliminating the necessity of making significant upfront investments. The versatility of cloud services facilitates adaptability, enabling enterprises to swiftly implement and expand applications. Real-time data availability promotes collaboration, stimulating innovation and facilitating global connectivity. Cloud computing enhances resilience and disaster recovery by redundantly storing data across numerous servers and geographic locations. Furthermore, it enables the implementation of cutting-edge technology such as artificial intelligence and big data analytics. In summary, cloud computing plays a crucial role in updating IT infrastructure, fostering innovation, and allowing organisations to quickly adjust to changing business needs. Cloud Computing could also be used in different sections of Current Cutting edge technolopgies of Modern era such as Smart Cities [5, 6], Smart Home Solutions [7], Traffic Security and Management [8], Firms those are working on Big Data technologies [9], etc.

Motivation

The requirement to protect sensitive data and ensure the confidentiality, integrity, and availability of cloud data drives cloud data privacy. Several considerations drive cloud data privacy emphasis:

1. **Security Concerns:** Cloud computing stores and processes data using third-party servers. This raises security worries regarding unauthorized access, data breaches, and more. Cloud data privacy is essential to reduce risks and protect sensitive data.
2. **Legal and regulatory compliance:** Different countries have established various Legal and regulatory compliance organizations that establish rules restricting personal and sensitive data processing and protection. Organizations employing cloud services must follow these regulations to prevent legal issues and maintain consumer trust.
3. **Trust and Client Comfort:** Users and organizations must trust that cloud data is managed responsibly and securely. Cloud service companies must create consumer and partner trust by committing to data protection.
4. **Data Ownership and Control:** Cloud customers must retain ownership and control over their data on third-party servers. Using strong data privacy controls, users have control over who sees, uses, and deletes their data.

5. **Business Continuity:** Cloud data privacy is crucial for company continuance. Organizations must ensure that their data is available and safe during cyberattacks, system breakdowns, and other unexpected events.
6. **Reputation Management:** Data breaches and privacy mishaps can damage a company's brand. Maintaining a good reputation and preventing reputational damage requires strong cloud data privacy practices.

Cloud data privacy is driven by security, compliance, trust, control, business continuity, reputation, and technology. Organizations and cloud service providers must actively address these aspects to store and process sensitive data securely and privately in the cloud.

Literature review: cloud privacy issues

The current body of literature on cloud data privacy places significant emphasis on the difficulties presented by advancing technologies such as edge computing and artificial intelligence. Researchers stress the importance of implementing strong encryption methods and sophisticated access restrictions to protect sensitive data in cloud environments [10]. The use of privacy-preserving machine learning models is increasing in order to address issues around data analytics and processing. Furthermore, regulatory advancements, such as revised data protection legislation and global benchmarks, significantly influence the discussion on the privacy of cloud data [11]. With the rising trend of *organizations* adopting multi-cloud environments, there is a growing demand for *standardized* privacy frameworks to guarantee consistent security across various platforms. Continuous research and innovation in encryption techniques and privacy-enhancing technologies are crucial for dealing with the ever-changing nature of cloud data privacy [12].

With cloud computing, customers are provided with on-demand access to various computational tasks through the Internet, which is performed by a combination of hardware and software [13]. Cloud providers build massive server infrastructures and allow their customers to pool their resources [14]. Cloud computing refers to the on-demand availability of computing resources such as data storage and processing, without having physical instance of it in customer premises [15]. It's common parlance to refer to the multiple online labor markets that cater to different customers by using this term. Cloud computing [16] refers to the use of multiple sites throughout the web to complete a single task. Data storage, human resources, data collecting, and the ability to associate structures are only some of these assets' tools and resources. Cloud computing is a viable choice for customers and companies due to its low cost, numerous benefits, rapidity, productivity, efficiency, and security [2]. The right kind of math may be done in public or private. Public cloud services charge customers for access to a variety of online support resources. Private cloud companies restrict their support to a select clientele and offer only limited services. Organizations like this have shown to be valuable structures for enterprises. There is also a hybrid model that combines aspects of both public and private firms. Appropriate processing is an umbrella term for anything defined as the online dissemination of valuable information [17]. Three types of cloud computing companies are known by their acronyms: IaaS, PaaS, and SaaS [18].

The image of a cloud, often used to represent the Internet at the time, gave rise to the term "cloud computing". No matter what cloud organization is chosen, people will have different preferences. When a company uses a cloud service, it usually does not accept or maintain its accounting system [19]. Even though security problems are rare, many companies worry about cloud organizations [4]. How safe you think cloud computing is will depend on how safe your current systems are [20]. In-house structures managed by various people with different duties are more likely to leak than systems that a professional manages at a cloud provider dedicated to ensuring that the framework works. Customers who choose services sent over the Cloud can drastically cut the IT resources they need for their connections and get access to intelligent filtering and flexible effort-level working connections during the process.

As yet, there is no one definition of "cloud computing" that everyone agrees on. The National Institute of Standards and Technology (NIST, http://csrc.nist.gov) in the United States has this to say about it: "Cloud computing is a model for providing easy, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services) that can be quickly set up and taken down with minimal management effort or service provider interaction". As per the above quoted definition, the cloud bas model increases availability of resources and comprises three delivery models and four deployment models [13, 21]. It also has five fundamental features. The five most essential things in cloud computing are self-service on-demand, network access everywhere, location-independent resource pooling, quick elasticity, and measured service. All of these things are designed to make Cloud use smooth and clear. Rapid elasticity lets resources grow (or shrink) quickly [14, 16]. Measured services are primarily based on how the business model works. Cloud service providers control and optimize computer resources using automated technologies for resource

allocation, load balancing, and metering. Application/Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service are the three ways that Cloud services are delivered (see Fig. 1). (IaaS). In March 2009, ITU Technology Watch assessed the cloud computing trend [20]. People protect personal information in these three standard cloud service types [18]. Each model has its own benefits and risks, and it need to be selected on case to case basis on the type of cloud services as requested by consumer.

Lack of confidentiality as threats

It includes a threat to customer data from within the company, the risk of an assault from the outside, and worries about data security [22]. The second is the risk of an assault from the outside, which is becoming increasingly crucial for cloud apps in an open environment. This danger includes assaults on cloud users and apps through remote programming or attacks on their hardware. The third risk is that information could get out because of a problem with protected access. Once that happens, anything could happen from there.

Lack of integrity as threats

Data separation risks, powerless customer access management, and data quality risks are included [23]. Most importantly, data segregation risks, which combine the incorrect importance of secure borders, foolish Virtual Machine designs, and of-customer-side-based hypervisors. This is a complex problem in the cloud environment because it provides resources to clients, and if those resources change, data dependability may suffer. The helpless consumer access control comes next. It transmits many concerns and threats due to wasted access and character control, opening doors for aggressors who can destroy data resources.

Lack of availability as threats

It brings to mind the board's impact on development, the lack of connections, actual resource interference, and ineffective recovery processes. The first is advancement on the board, which includes client entry testing for different customers and institution adjustments. Any type of change in the Cloud infrastructure, content, and apps could make it harder to join the Cloud to its consumer. Next, companies reject structure data transfer restrictions, DNS affiliation enrolling the product, and assets [4]. Third, it bothers IT departments in large businesses, cloud users, and WAN expert associations. Fourth, the time and effectiveness with which a scene's event can be rebuilt are affected by recovery processes that do not operate properly (also known as "Deficient disappointment recovery").

Lack of authentication and identity as threats

Although there are various methods for client authentication and framework distribution, cryptography is by far the most well-known [1, 2]. Clients can be verified in several ways, including using a secret phrase, a security token, or a measurable identifier like a fingerprint. Using several cloud service providers (CSPs) might challenge enterprises relying on conventional cloud identity management approaches [2]. In this scenario, the flexibility of synchronizing character data with the mission is compromised. However, as the organization shifts toward a cloud-based strategy, several problems arise between traditional identification and the Cloud [3].

Lack of access control as threat

Access control allows cloud data owners to offer restrictive consent to reclaim their data. Only authorized users of a cloud service can access its contents. Information stored in the cloud for access control purposes is protected against modification and exposure to unauthorized users. Strong, unique passwords should be created for each client and should be changed often [4].

Lack of information integrity as a threat

Integrity in distributed computing guarantees the authenticity and completeness of the data. The integrity of information is not just related to the accuracy of information but also if it is trusted and relied upon [6]. Cloud services provide clients with data and associated resources. A standard level of trust between providers and clients is a beneficial approach to the issue of information reliability. Another line of action is eligible for approval, permission, and accounting oversight. To ensure fair use of resources, information access must undergo multiple checks.

Lack of availability of information in SLA as a threat

The unavailability of information is a severe issue in cloud systems. The Service Level Agreement (SLA) provides information about whether or not system assets are available to users. SLA management is essential for cloud services; it is helpful for both parties [7]. It is basically a negotiation between clients and service providers that helps to build trust. One approach to resource availability is to develop a support strategy for local resources similar to the most important information [8]. As a result, even after the resources are unavailable, the consumer can still get information about them.

Challenges to privacy in the cloud ecosystem

The promise of delivering resources as a service has different types of customers, ranging from small-sized to large-sized organizations and government authorities to

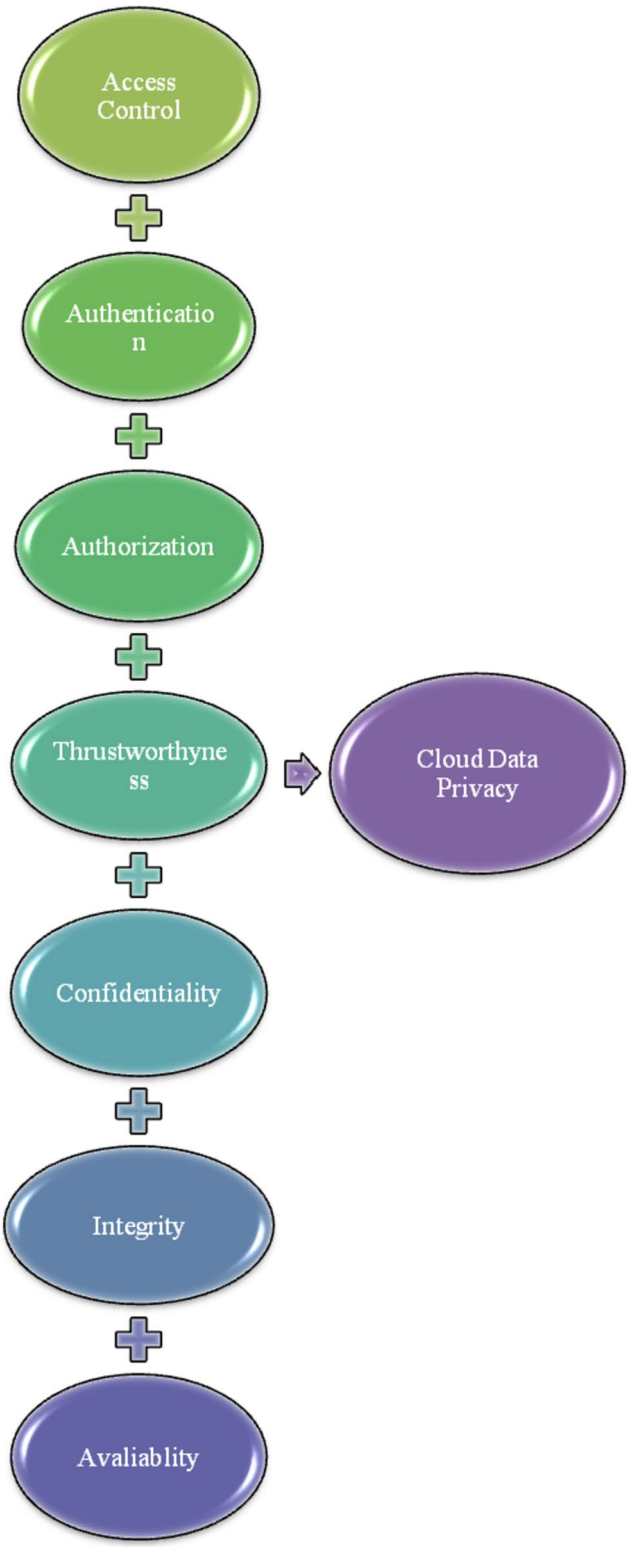

Fig. 1 Proposed model of cloud data privacy

end-users. Cloud services are expected to increase rapidly in the ICT sector, according to industry analysts [17]. Users generate an increasing amount of personal data. According to International Data Corporation, the "digital universe", or the amount of information and content created and stored digitally, will increase from approximately two zettabytes (ZB) in 2011 to more than seven ZB by 2015 [19]. This massive demand for personal data will boost the demand for cloud services, especially if cloud computing lives up to its promises of decreased prices for clients and the introduction of new business models for providers [15]. Among the most significant privacy issues for cloud computing are the following:

a) Providing Access Control on the available data in a cloud environment.
b) Providing Authorization for the set of user groups or individual
c) Achieving Authentication of each user
d) Cloud risk assessment complexity
e) Existence of New business models and enforcement of consumer privacy policies;
f) Regulatory compliance for all the parties.

Privacy criteria and its effect chart

Table 1 is used to decide the weight of privacy criteria of the Cloud. List of authors who have emphasized the criteria of Privacy one over another. In this table, the author has tried to gather all the most prominent privacy criteria from the recent literature and included articles in the last decade from different major databases.

Table 2, In this mentioned table we have tried to articulate the latest and significant contribution done in the field of Cloud data privacy.

Proposed model of cloud data privacy

The proposed model of cloud data privacy is based on the multi-criteria decision-making methodology. Here, we have used AHP and TOPSIS together to strengthen our claim. As the first step, we used AHP steps to set up assumed weights and check their consistency index and used the final weights of selected criteria in TOPSIS to correlate the model further. The figure below (Fig. 1) shows the relationship between different data privacy criteria and their relationship with the Cloud [33, 34].

Figure 1 shows the relationship between Cloud Data Privacy and its subsequent factors [35, 36]: Access control, Authentication, Authorization, Trustworthiness, Confidentiality, Integrity, and Availability. Here, the author has proposed a joint method, AHP-TOPSIS, to choose and rank the best service in a cloud environment to provide Data Privacy on the above-listed parameters [37, 38]. The below figure (Fig. 2) shows the Graphical Representation of Hybrid CP-AHP_TOPSIS model.

Proposed architecture (AHP-TOPSIS)

Figure 2

Cloud privacy using Analytical Hierarchy Process (CP_AHP)

Saaty's [21] Analytical Hierarchy Process is a powerful technique for handling qualitative and quantitative multi-criteria decision-making elements. The analytical Hierarchy Process (AHP) model is used as the decision-making process using sensitivity analysis on the following criteria and benchmarks. Pairing comparisons simplify computations and judgments. Multi-criteria decision-making yields compatibility and incompatibility conclusions [39]. The Analytical Hierarchy Process is one of the most inclusive systems for making decisions with various criteria since it formulates the problem hierarchically and considers quantitative and qualitative factors. Prioritize

Table 1 Weighted chart of different criteria of cloud privacy

Author (year)/Criteria	Access Control	Authorization	Authentication	Trust Worthiness	Confidentiality	Integrity	Availability
J. Schiffman (2010) [24]		Yes	Yes	Yes	Yes		Yes
Z. Mahmood (2011) [23]	Yes		Yes			Yes	Yes
Sun, Y (2014) [25]	Yes		Yes	Yes	Yes		Yes
Jakimoski, K. (2016) [26]		Yes	Yes			Yes	
Ning, J. (2017) [27]	Yes			Yes		Yes	
Roy, S. (2018) [28]	Yes	Yes		Yes		Yes	
Yang, C. (2020) [29]	Yes	Yes		Yes		Yes	Yes
Suresha, K. (2021) [30]	Yes		Yes		Yes	Yes	
Ahmadi, S (2022) [31]		Yes	Yes		Yes	Yes	
Qiwen Li, (2023) [32]		Yes	Yes		Yes	Yes	
Total	6	6	7	5	5	8	4

Table 2 Major contributions in field of cloud privacy in past decade

Author (year)/Criteria	Factors of Data Privacy	Methodology used	Advantages of the proposed model
J. Schiffman (2010) [24]	Authorization, Authentication, Trustworthiness, Confidentiality, Availability, Integrity	Verifying a Multi-layer System	Mulit layer system help to achive privacy in better way
Z. Mahmood (2011) [23]	Access Control, Authentication, Integrity	A hybrid technique is proposed for data confidentiality and integrity	Confidentiality and integrity are used efficiently
Sun, Y (2014) [25]	Access Control, Authentication, Trustworthiness, Confidentiality, Availability	Privacy-preserving multi keyword ranked search approach	Access Control, Authentication, are assured and ranking has been given
Jakimoski, K. (2016) [26]	Authorization, Authentication, Integrity	Proposed security technique for confidentiality in cloud computing	Confidentially, Access Control are highlighted
Ning, J. (2017) [27]	Access Control, Trustworthiness, Integrity	Proposed system is resistant to key leakage attacks	Trustworthiness, Integrity are important to assure data privacy and avoid attacks
Roy, S. (2018) [28]	Access Control, Authorization, Trustworthiness, Integrity	Proposed fine-grained access control over cloud-based multi-server data along with a provably	One of the major advantage is On-demand access control to the cloud services
Yang, C. (2020) [29]	Access Control, Authorization, Trustworthiness, Integrity Availability	Proposed a cloud data deletion protocol to solve the behavior of tampering users by tampering with data deletion results when cloud server is not trusted	Used to avoid tempering of data that assures Confidentiality, Integrity, Availability, Authenticity
Suresha, K. (2021) [30]	Access Control, Authentication, Confidentiality, Integrity Availability	Proposed a system that uses attribute based encryption technique, threshold secret sharing and multi-authority access control mechanism	Attributed based encryption technique has been used
Ahmadi, S (2022) [31]	Authorization, Authentication, Confidentiality, Integrity	Highlighted Privacy-Preserving Cloud Computing	Authorization, Authentication has been higileghted
Qiwen Li, (2023) [32]	Authorization, Authentication, Confidentiality, Integrity	Homomorphic encryption technique	Using Authentication, Confidentiality, Integrity addresses Homoporpic encryption

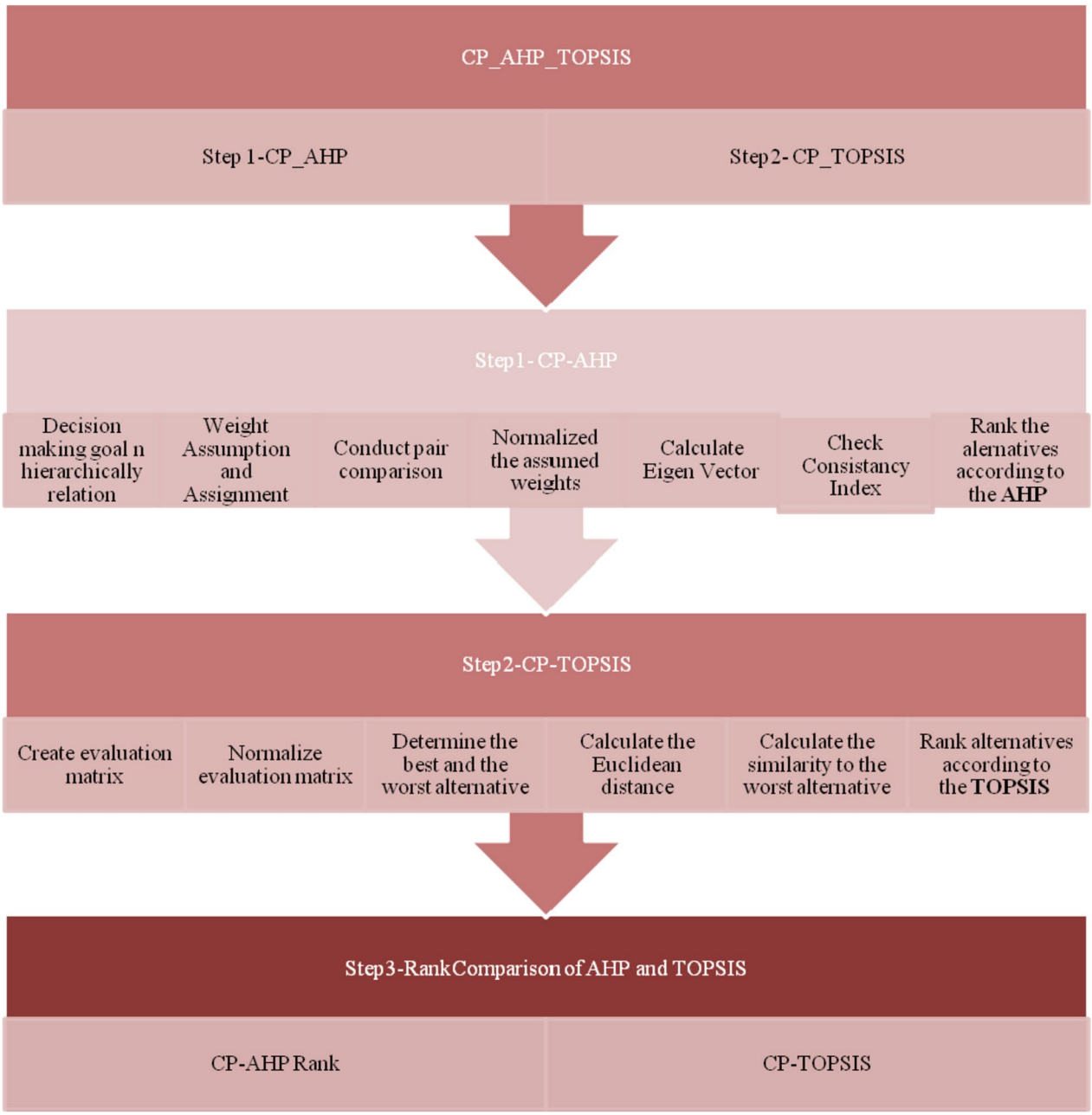

Fig. 2 Representation CP_AHP and CP_TOPSIS method

the issue. Next, assign nominal values to each hierarchy level and generate a pair-wise comparison judgment matrix.

Goal of decision-making

We are hierarchically presenting the decision issue and goal. Indicators and choices make decisions. Figure 3 shows the group's hierarchy for the understudied problem.

Pair-wise comparison

In order to conduct a paired comparison, a questionnaire or literature review should be used to collect opinions and/or feedback from researchers, engineers,

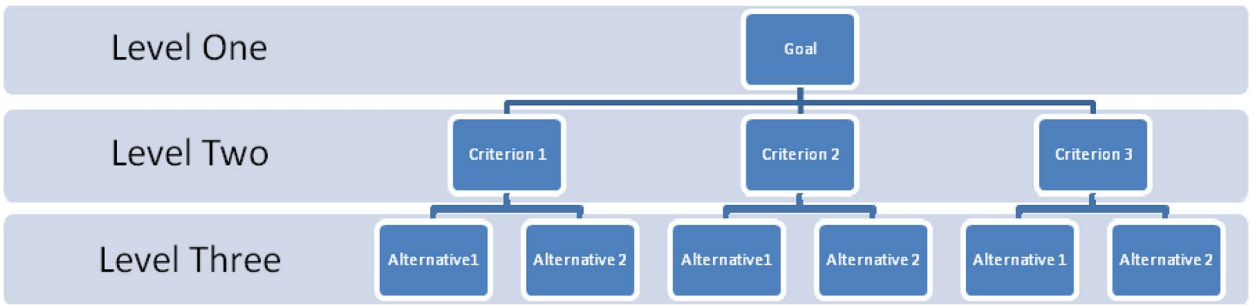

Fig. 3 General correlation among goals, alternatives, and criteria

Table 3 Sample AHP questionnaires

Scale of Importance	Importance Level Indicator
1	Equal Importance
2	Equal to Moderate Importance
3	Moderate Importance
4	Moderate to Strong Importance
5	Strong Importance
6	Strong to Very Strong Importance
7	Very Strong Importance
8	Very Strong to Extreme Importance
9	Extreme Importance

consumers, Etc. Each decision maker input their preferred amount for each member and then used their geometrical average to turn individual assessments into group judgments for each paired comparison. One indicates that the two elements are equal. However, number nine indicates that one member in a pair-wise matrix is essential. Table 3 shows the pair-wise scale and numerical importance.

How critical are the following security criteria in comparison.

Data analysis involves these processes. Review data is used to extract matrix A, the pair-wise comparison matrix. M's major right Eigenvector is w.

If m_{ik}. $m_{kj} = m_{ij}$ is not validated for every k, j, and i, Eigenvector is chosen [19].

The pair comparisons matrix cannot be used to normalize Wi if the matrix is incompatible or inconsistent. AHP formula normalized the expected weights.

Eigenvector approach for positive and reversed matrices:

$$e^r = (1, 1, \ldots\ldots, 1)$$
$$w = \lim_{n\to\infty}\left(\frac{A^k.e}{e^r.A^k.e}\right)$$

To decide on an incompatible matrix, the calculation must be repeated numerous times to get a convergence among the set of results. Then, the following formula converts raw data into understandable absolute values and normalized weight w = (w1, w2, w3… wn):

$$Aw = \lambda max.w, \qquad where\ \lambda max \geq n$$
$$\lambda max = \sum \frac{\text{ajwj}-\text{n}}{\text{w1}}$$
$$\text{A} = \{\text{aij}\}\ \text{with aij} = 1/\text{aij}$$

A: pair-wise comparison
w: normalized weight vector
λmax: A's matrix eigen value
aij: numerical comparison between i and j. Next, to validate the AHP results, the consistency ratio (CR) is determined using the formula CR = CI/RI, where the consistency index (CI) is assessed using the following formula:

$$C.I. = \frac{\boldsymbol{\lambda max} - \boldsymbol{n}}{\boldsymbol{n} - 1} -$$

Cloud privacy using TOPSIS (CP_TOPSIS)

TOPSIS is one of the popular multi-criteria decision analysis methods. It compares options using a pre-specified criterion. TOPSIS uses multi-criteria decision-making. TOPSIS picks between the least Euclidean distance from the ideal answer and the most significant distance from the negative ideal solution.

1. Make an M-by-N matrix. "Evaluation matrix" describes this matrix.

$$(a_{ij})M * N$$

2. Normalize evaluation matrix:

$$a_{ij} = \frac{a_{ij}}{\sqrt{\sum_{i=1}^{M}(a_{ij})^2}}$$

3. Weighted normalized decision matrix. Each condition must weight to add up to 1. Expertise and literature review can determine weights.

$$X_{ij} = a_{ij} * w_j$$
$$w_j = \frac{w_j}{\sum_{j=1}^{N} w_j}$$
$$\sum_{j=1}^{N} w_j = 1$$

4. Each criterion's best and worst alternatives:

$$X_j^b = max_{i=1}^{M} X_{ij}$$
$$X_j^w = min_{i=1}^{M} X_{ij}$$

5. Computing the Euclidean distance between the target and best/worst alternatives of cloud privacy:

$$S_i^b = \sqrt{\sum_{j=1}^{N}\left(X_{ij} - X_j^b\right)^2}$$
$$S_i^w = \sqrt{\sum_{j=1}^{N}\left(X_{ij} - X_j^w\right)^2}$$

Choose the best and worst for each criterion.

Calculate the Euclidean distance between the target and best/worst alternatives.

Compare each possibility against the worst.

TOPSIS-rank alternatives.

6. Compare each possibility against the worst.

$$S_i = \frac{d_i^w}{d_i^w + d_i^b}$$

We compute a score for each cloud privacy alternative based on distances obtained in fifth step.

7. Rank the cloud privacy alternatives according to the obtained TOPSIS score in descending order.

The best one will score the lowest and top our list.

Evaluation and discussion

The table below (Table 4) shows the assumed weights given by the author in the proposed model based on the reviews and the effectiveness of the relationship among different privacy criteria.

The table below (Table 5) is used to Normalize the assumed weights based on the AHP formula below.

Below Table 6 is a Revised Normalization Matrix Employ pair-wise comparisons. Compare pairs. Pairwise comparisons compare the relative relevance, preference, or likelihood of two elements (objectives) to another. (the goal). Pair-wise comparisons determine priority. Decision items at each hierarchy level are compared pair-wise, and the reciprocal matrix is completed;

The matrix dimension affects RI (1.69). Table 7 is an accepted indicator of the anticipated weights of the second stage. Consistency ratios below 0.10 indicate acceptable comparison results.

Table 4 Assumed weights of different criteria

Criteria	Access Control	Authorization	Authentication	Trust Worthiness	Confidentiality	Integrity	Availability
Access control	1	5	4	3	2	3	2
Authentication	0.2	1	5	2	3	4	5
Authorization	0.25	0.2	1	5	6	5	4
Trust Worthiness	0.3333333	0.5	0.2	1	6	7	6
Confidentiality	0.5	0.3333333	0.1666667	0.1666667	1	8	9
Integrity	0.3333333	0.25	0.2	0.1428571	0.125	1	9
Availability	0.5	0.2	0.25	0.1666667	0.1111111	0.1111111	1
Aggregate Assigned Weight	3.12	7.48	10.82	11.48	18.24	28.11	36.00

Table 5 Normalized pair-wise matrix

	Access Control	Authorization	Authentication	Trust Worthiness	Confidentiality	Integrity	Availability	Criteria Weight
Access control	0.05	0.24752475	0.18648019	0.14263074	0.10434783	0.27146397	0.85510689	0.16133498
Authentication	0.01	0.04950495	0.23310023	0.09508716	0.15652174	0.36195196	2.13776722	0.09753506
Authorization	0.0125	0.00990099	0.04662005	0.23771791	0.31304348	0.45243994	1.71021378	0.02300701
Trust Worthiness	0.01666667	0.02475248	0.00932401	0.04754358	0.31304348	0.63341592	2.56532067	0.51572383
Confidentiality	0.025	0.01650165	0.00777001	0.00792393	0.05217391	0.72390391	3.847981	0.66875063
Integrity	0.01666667	0.01237624	0.00932401	0.00679194	0.00652174	0.09048799	3.847981	0.57002137
Availability	0.025	0.00990099	0.01165501	0.00792393	0.0057971	0.01005422	0.42755344	0.07112639

Table 6 Reversed normalization matrix

Criteria Weight	0.05176523	0.01303364	0.002126997	0.044938591	0.036671779	0.02027744	0.001975733	0.170789411	
	Access control	**Authentication**	**Authorization**	**Trust Worthiness**	**Confidentiality**	**Integrity**	**Availability**	**Weighted Sum Value**	**Ratio**
Access control	0.00258826	0.00322615	0.000396643	0.006409625	0.00382662	0.005504594	0.001689463	0.023641355	0.456703329
Authentication	0.00051765	0.00064523	0.000495803	0.004273083	0.005739931	0.007339459	0.004223657	0.023234815	1.782680657
Authorization	0.00064707	0.00012905	9.91607E-05	0.010682708	0.011479861	0.009174324	0.003378926	0.03559109	16.73302721
Trust Worthiness	0.00086275	0.00032261	1.98321E-05	0.002136542	0.011479861	0.012844053	0.005068389	0.032734045	0.632355788
Confidentiality	0.00129413	0.00021508	1.65268E-05	0.00035609	0.00191331	0.014678918	0.007602583	0.026076635	0.580272657
Integrity	0.00086275	0.00016131	1.98321E-05	0.00030522	0.000239164	0.001834865	0.007602583	0.011025725	0.300659673
Availability	0.00129413	0.00012905	2.47902E-05	0.00035609	0.00021259	0.000203874	0.000844731	0.003065253	0.151165656
								0.155368919	16.73302721

Table 7 The acceptance matrix

Criteria Count	**7**
Eigen value	16.7330272
Consistency Index	1.6221712
Consistency Ratio	0.09982592
Check If (CR < 0.10)	TRUE

TOPSIS implementation

The above table (Table 8) is used to establish the relationships In the table (Table 8), Fuzzy criteria weight has been decided on pre-calculated AHP weights.

Table 9 helps determine each metric j for each privacy criteria i is normalized between 0 and 1. Higher values are better metrics.

Table 10: After weighting each metric, we must normalize them to sum to 1. Next, produce the multiplication of each normalized metric from the second step by its weight.

Table 8 Fuzzy weights of criteria

Criteria weights of CP_AHP	0.05176523	0.01303364	0.002126997	0.044938591	0.036671779	0.02027744	0.001975733
	Access control	**Authentication**	**Authorization**	**Trust Worthiness**	**Confidentiality**	**Integrity**	**Availability**
Access control	1.4	1.59	1.79	2.4	3.6	1.89	2.23
Authentication	3.35	4.24	5.26	2.21	3.12	4.6	1.689
Authorization	5.15	6.5	7.3	5.15	4.2	3.7	2.432
Trust Worthiness	1.6	2.59	2.78	4.2	6.3	1.89	2.23
Confidentiality	3.1	3.92	4.98	3.21	2.13	4.1	1.689
Integrity	5.6	6.1	3.7	2.5	4.9	5.6	2.432
Availability	2.3	3.43	5.21	7.28	6.21	2.2	3.12

Table 9 Normalization matrix

	Access control	Authentication	Authorization	Trust Worthiness	Confidentiality	Integrity	Availability
Access control	**0.22218**	**0.200711**	**0.195117**	**0.393672**	**0.566845**	**0.30491**	**0.6016**
Authentication	**0.531646**	**0.535229**	**0.573361**	**0.362507**	**0.491266**	**0.742108**	**0.455651**
Authorization	**0.817306**	**0.820515**	**0.79573**	**0.844755**	**0.66132**	**0.596913**	**0.656094**
Trust Worthiness	**0.242508**	**0.336379**	**0.408917**	**0.718247**	**0.76266**	**0.262748**	**0.6016**
Confidentiality	**0.469859**	**0.509115**	**0.732521**	**0.548946**	**0.257852**	**0.569983**	**0.455651**
Integrity	**0.848777**	**0.792245**	**0.544242**	**0.427528**	**0.59318**	**0.778513**	**0.656094**
Availability	**1**	**1**	**1**	**1**	**1**	**1**	**1**

Table 10 Weighted normalized decision matrix

	Access control	Authentication	Authorization	Trust Worthiness	Confidentiality	Integrity	Availability
Access control	**0.011501**	**0.002616**	**0.000415**	**0.017691**	**0.020787**	**0.006183**	**0.001189**
Authentication	**0.027521**	**0.001138**	**0.00122**	**0.016291**	**0.018016**	**0.015048**	**0.000969**
Authorization	**0.042308**	**0.001745**	**0.001693**	**0.037962**	**0.024252**	**0.012104**	**0.001396**
Trust Worthiness	**0.812401**	**1.426248**	**2.150905**	**1.587325**	**2.379499**	**1.208642**	**1.016102**
Confidentiality	**1.574027**	**0.001083**	**3.85306**	**1.21317**	**0.804497**	**2.621921**	**0.000969**
Integrity	**2.843404**	**0.001685**	**2.862715**	**0.944837**	**1.850721**	**3.581161**	**0.001396**
Availability	**3.1**	**3.92**	**4.98**	**3.21**	**2.13**	**4.1**	**1.689**

Table 11 Max and min values of each criterion

V+	0.042308	0.002616	0.001693	0.037962	0.024252	0.015048	0.001396
V-	0.011501	0.001138	0.000415	0.016291	0.018016	0.006183	0.000969

Table 12 The Euclidean distance

Si+	Si-
0.038108	0.003446
0.027015	0.018327
0.00307	0.038663
4.200107	4.221154
5.095575	5.116397
5.736476	5.763151
9.138368	9.163057

Table 13 Comparison of AHP and TOPSIS ranking

	TOPSIS	TOPSIS Ranking	AHP	AHP Ranking
Access control	**0.042308**	6	0.05176523	5
Authentication	0.002616	**3**	0.01303364	**3**
Authorization	0.001693	2	0.044938591	6
Trust Worthiness	0.024252	**5**	0.036671779	**4**
Confidentiality	0.015048	**4**	0.001975733	**1**
Integrity	0.001396	**1**	0.02027744	**2**
Availability	**1.689**	7	0.170789411	7

In Table 11, We wish to identify the maximum and minimum criterion metrics for all privacy factors.

Table 12 shows the geometric distance between each cloud privacy for different criteria and the best/worst value of such metrics.

The above table (Table 13) compares both CP_AHP and CP_TOPSIS ranking based on criteria final weights obtained by the computation. The minimum weights have a low ranking, and the maximum weights have a high ranking.

Figure 4, is used to show the comparative graph of the original score of all the criteria named Access control, Authentication, Authorization, Trust Worthiness, Confidentiality, Integrity, and Availability with Si+ and Si- comparison of all the seven criteria, Si+ is to find the optimal result by checking in a maximum of individual criteria

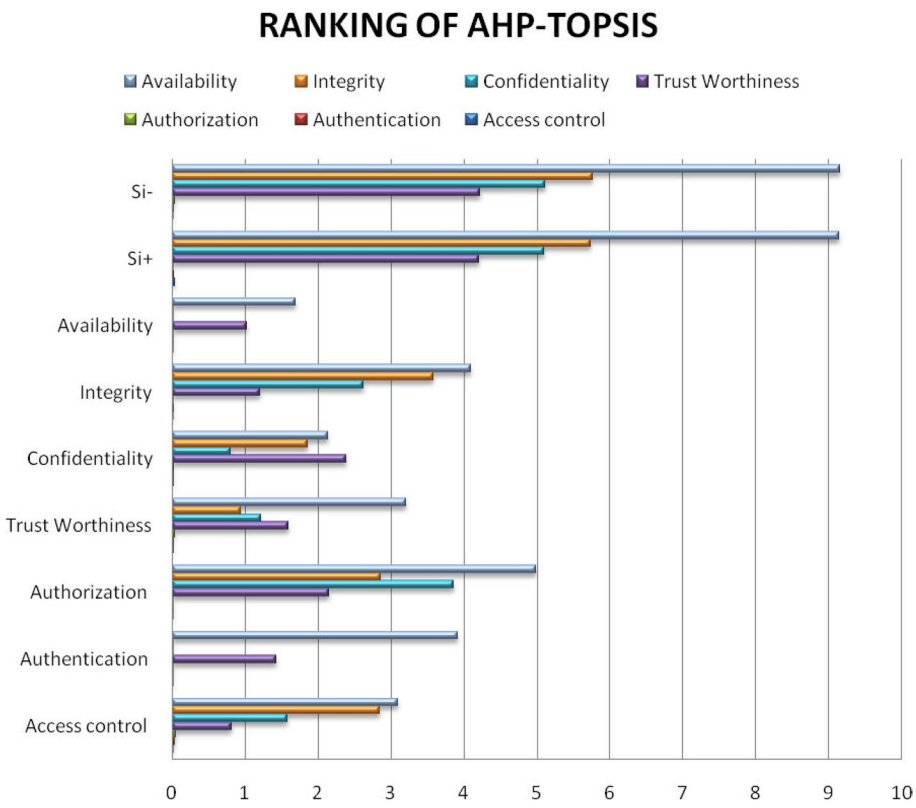

Fig. 4 Ranking chart of AHP-TOPSIS

in horizontal span and Si- is to find the optimal result by accruing a minimum of individual criteria in horizontal span.

Major contributions

In this paper, the significant findings are as follows.

- Ranking methods are crucial to determine the effectiveness of individual parameters [40].
- Other authors who have contributed to this field primarily focused on C.I.A., but other factors such as Access Control, Authentication, and Authorization are also critical to enhancing Data Privacy.
- Hybrid CP_AHP and CP_TOPSIS help to validate the criteria twice.
- It could be used further on different parameters of privacy.
- In the proposed model, Authorization ranked first, Integrity ranked second, and Authentication ranked third.

Effectiveness of using AHP and TOPSIS in proposed work

When we implement the combined approach of Analytic Hierarchy Process (AHP) and Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) cloud data privacy models, it could be beneficial for us in the following ways:

1. Multi-criteria decision-making (MCDM) methods AHP and TOPSIS allow us to weigh multiple criteria simultaneously. Considerations for cloud data privacy include authorization, authentication, access control, compliance with rules, etc. These methods assist in evaluating and comparing options using these criteria.
2. AHP and TOPSIS offer an organized, quantitative approach to decision-making. You can make better decisions about implementing the cloud data privacy model by weighing factors and comparing alternatives.

3. AHP establishes the relative relevance of the criteria. In cloud data privacy, some criteria may be more important than others. For instance, regulatory compliance may be more important than other aspects, and AHP reflects this.
4. AHP and TOPSIS enable a thorough assessment of cloud data privacy model elements. This comprises technological, cost, scalability, and usability factors. This holistic review can improve decision-making and balance.
5. AHP effectively handles subjective judgments by involving specialists in decision-making. This is crucial in data privacy since criteria may be subjective. AHP permits these opinions to influence decision-making.
6. AHP and TOPSIS offer sensitivity analysis to determine how changes in criteria weights or evaluations affect the conclusion. This helps modify the cloud data privacy paradigm to changing needs.
7. AHP ensures logical consistency in the decision matrix. This prevents decision model discrepancies, making decision-making more dependable.
8. AHP and TOPSIS simplify communication by providing a systematic and visual approach to complex decision-making processes. This helps stakeholders comprehend and accept decisions.
9. AHP and TOPSIS improve cloud data privacy model decision-making by providing a systematic, quantitative, and complete approach. It supports prioritization, subjective judgments, and adaptation in a fast-changing context.

Conclusion and future directive

We built a model using the chosen criteria and showed that CP_AHP and CP_TOSIS are the one of the finest ways to rank each criterion based on their assumed weights. This lets the user or organization look at each cloud privacy criterion's risks, costs, and benefits before choosing one. This could be beneficial for the industry to obtain the best-suited criteria matrix for the scale of the proposed work. We can also give generic guidelines for designing privacy-oriented cloud services with features such as optimal cost, least risk, and maximum benefit per the industry's and users' requirements. The guidelines will be the new benchmark for industry personnel. After this claim, anyone can further prepare the framework using the above-suggested parameters to address an organization's individual or customized needs. The framework extension could be based on one or more of the following benchmarks: risk, cost, and benefit.

Acknowledgements
The authors are thankful to the Deanship of Graduate Studies and Scientific Research at University of Bisha for supporting this work through the Fast-Track Research Support Program.

Authors' contributions
Mohammad Zunnun Khan- Conceptualization of the paper theme, Mohd Shoaib- Worked on Review and Data Collections, Mohd Shahid Siddiqui- Worked on Making model, Khair Ul Nisa- worked on Visualization, Md Tabrez Quasim- Worked on Results and discussion.

Funding
This paper has no funding.

Availability of data and materials
We have used fuzzy data set based on Literature review.

Declarations

Ethics approval and consent to participate
This paper does not include animal or human data, hence it is not applicable.

Competing interests
The authors declare no competing interests.

Author details
[1]Department of Information Science and Cybersecurity, College of Computing and Information System, University of Bisha, P.O. Box 551, Bisha, Saudi Arabia. [2]Department of Computer Engineering, Zakir Husain College of Engineering and Technology, Aligarh Muslim University, Aligarh, India. [3]College of Computing and Information Sciences, University of Technology and Applied Sciences, Ibri, Sultanate of Oman. [4]Department of Computer Science and Artificial Intelligence, College of Computing and Information System, University of Bisha, P.O. Box 551, Bisha, Saudi Arabia.

Received: 10 September 2023 Accepted: 30 January 2024
Published online: 14 February 2024

References

1. Golden BL, Wang Q (1990) An alternative measure of consistency. In: Golden BL, Wasil A, Harker PT (eds) Analytic hierarchy process: applications and studies. Springer Verlag, New-York, pp 68–81
2. Jalaliyoon N, Bakar NA, Taherdoost H (2012) Accomplishment of critical success factor in organization; using analytic hierarchy process. Int J Acad Res Manag 1(1):1–9. Helvetic Editions Ltd
3. Van Blarkom GW, Borking JJ (2003) Handbook of privacy and privacy-enhancing technologies - the case of intelligent software agents. Retrieved from e-Europe: ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/DPP/CWA15263-00-2005-Apr.pdf
4. Federal Trade Commission (2010) Protecting consumer privacy in an era of rapid change: a proposed framework for businesses and policymakers. Retrieved from www.ftc.gov/os/2010/12/101201privacyreport.pdf
5. Quasim MT, Nisa KU, Khan MZ et al (2023) An internet of things enabled machine learning model for Energy Theft Prevention System (ETPS) in Smart Cities. J Cloud Comp 12:158. https://doi.org/10.1186/s13677-023-00525-4
6. Quasim MT, Mobarak MM, Nisa KU, Meraj M, Khan MZ (2023) Blockchain-based Secure health records in the healthcare industry. In: 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India. pp 545–549. https://doi.org/10.1109/ICOEI56765.2023.10125802
7. Quasim MT, Khan MA, Algarni F, Alshahrani MM (2021) Fundamentals of smart cities. In: Khan MA, Algarni F, Quasim MT (eds) Smart cities: a data analytics perspective. Lecture notes in intelligent transportation and infrastructure. Springer, Cham. https://doi.org/10.1007/978-3-030-60922-1_1

8. Alnahari W, Quasim MT (2021) Privacy concerns, IoT devices and attacks in smart cities. In: 2021 International Congress of Advanced Technology and Engineering (ICOTEN). pp 1–5. https://doi.org/10.1109/ICOTEN52080.2021.9493559
9. Halima NB, Alluhaidan AS, Khan MZ et al (2023) A service-categorized security scheme with physical unclonable functions for internet of vehicles. J Big Data 10:178. https://doi.org/10.1186/s40537-023-00865-7
10. Gupta R, Gupta I, Singh AK, Saxena D, Lee CN (2022) An iot-centric data protection method for preserving security and privacy in cloud. IEEE Syst J. 17(2):2445–2454
11. Gupta R, Saxena D, Gupta I, Singh AK (2022) Differential and triphase adaptive learning-based privacy-preserving model for medical data in cloud environment. IEEE Netw Lett 4(4):217–221
12. Gupta R, Singh AK (2022) A differential approach for data and classification service-based privacy-preserving machine learning model in cloud environment. N Gener Comput 40(3):737–764
13. Brands S (2000) Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. MIT Press, Cambridge. https://doi.org/10.7551/mitpress/5931.001.0001
14. Cavoukian A, Abrams ST (2010) Privacy by design: essential for organizational accountability and strong business practices. Retrieved from www.globalprivacy.it/Allegati_Web/57C2B8AA758546A0B76D5668F5CF5E16.pdf
15. The Danish Data Protection Agency (2010) Processing of sensitive personal data in a cloud solution. Retrieved from www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/
16. ENISA (2009) Cloud computing information assurance framework. Retrieved from ENISA: www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework
17. ENISA (2009) Cloud computing security risk assessment. Retrieved from www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment
18. ENISA (2011) Security & resilience in governmental clouds. Retrieved from www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-governmental-clouds
19. Enterprise Privacy Group (2008) Privacy by design: an overview of privacy enhancing technologies. Retrieved from www.ico.gov.uk/upload/documents/pdb_report_html/pbd_pets_paper.pdf
20. Gartner (2010) Worldwide cloud services market to surpass $68 billion in 2010. Retrieved from www.gartner.com/it/page.jsp?id=1389313
21. Saaty TL (1980) The analytic hierarchy process: planning, priority setting, resources allocation. McGraw-Hill, London
22. Alluhaidan AS, Khan MZ, Halima NB, Tyagi S (2023) A diversified context-based privacy-preserving scheme (DCP2S) for internet of vehicles. Alex Eng J 77:227–237. https://doi.org/10.1016/j.aej.2023.06.073. ISSN 1110-0168
23. Mahmood Z (2011) Cloud computing: characteristics and deployment approaches. 2011 IEEE 11th International Conference on Computer and Information Technology, p 121–126
24. Schiffman J, Moyer T, Vijayakumar H, Jaeger T, McDaniel P (2010) Seeding clouds with trust anchors. In: Proceedings of the 2010 ACM workshop on Cloud computing security workshop. pp 43–46
25. Sun Y, Zhang J, Xiong Y, Zhu G (2014) Data security and privacy in cloud computing. Int J Distrib Sens Netw 10(7):190903
26. Jakimoski K (2016) Security techniques for data protection in cloud computing. Int J Grid Distrib Comput 9(1):49–56
27. Ning J, Cao Z, Dong X, Liang K, Ma H, Wei L (2017) Auditable σ-time outsourced attribute-based encryption for access control in cloud computing. IEEE Trans Inf Forensics Secur 13(1):94–105
28. Roy S, Das AK, Chatterjee S, Kumar N, Chattopadhyay S, Rodrigues JJ (2018) Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications. IEEE Trans Industr Inf 15(1):457–468
29. Yang C, Tan L, Shi N, Xu B, Cao Y, Yu K (2020) AuthPrivacyChain: a blockchain-based access control framework with privacy protection in cloud. IEEE Access 8:70604–70615
30. Suresha K, Vijayakarthick P, Dhanasekaran S, Murugan BS (2021) WITHDRAWN: threshold secret sharing and multi-authority based data access control in cloud computing
31. Ahmadi S, Salehfar M (2022) Privacy-preserving cloud computing: ecosystem, life cycle, layered architecture and future roadmap. arXiv preprint arXiv:2204.11120
32. Li Q, Gao R, Xia Y (2023) Encrypted data-driven predictive cloud control with disturbance observer. ArXiv. /abs/2301.00322
33. Goldberg I, Wagner D, Brewer E (1997) Privacy-enhancing technologies for the Internet, p 103–109. https://doi.org/10.1109/CMPCON.1997.584680
34. IDC (2008) IT cloud services forecast. Retrieved from http://blogs.idc.com/ie/?p=224
35. IDC (2010) IDC predictions 2011: welcome to the new mainstream. Retrieved from www.idc.com/research/predictions11/downloads/IDCPredictions2011_WelcometotheNewMainstream.pdf
36. IBM (2015) Identity mixer. Retrieved from www.zurich.ibm.com/security/idemix/
37. ITU-T Technology Watch Report (2009) Distributed computing: utilities, grid & clouds. Retrieved from www.itu.int/dms_pub/itu-t/oth/23/01/T23010000090001PDFE.pdf
38. Shahid Husain M, Zunnun Khan M, Siddiqui T (2023) Big data concepts, technologies, and applications, 1st edn. Auerbach Publications. https://doi.org/10.1201/9781003441595
39. Lee MC (2007) A method of performance evaluation by using the analytic network process and balanced score card. In: International conference on convergence information technology
40. Singh AK, Gupta R (2022) A privacy-preserving model based on differential approach for sensitive data in cloud environment. Multimed Tools Appl 81(23):33127–33150

Publisher's Note