

Enhancing the Cloud-Based Security Using a Fuzzy Inference System

Sachin Kumar Vishnoi^{1*}, Dr. Ashish Saini², Kavita Paliwal³

¹ Research Scholar, Department of Computer Science & Engineering, Quantum University, Roorkee.

Email: vishnoisachin007@gmail.com

² Associate Professor, Department of Computer Science & Engineering, Quantum University, Roorkee.

Email: ashishsainigkv7@gmail.com

³ Research Scholar, Department of Electrical and Electronics Engineering, COER University, Roorkee.

Email: Kpali.246@gmail.com

Abstract. Cloud computing is a critical tool for storing and processing data, but it also offers huge security issues, such as data breaches, inadequate authentication, and lack of transparency. In this research, we present a security improvement model using fuzzy inference system (FIS) to address the major problems such as authentication vulnerability, data recovery, privacy risk, accountability and transparency. The model incorporates several security criteria and makes intelligent recommendations regarding risk mitigation. The presented solution improves cloud security by offering users a customizable and flexible means to manage the not-so-clear situations.

Keywords: cloud security, Fuzzy inference system, data privacy, authentication, and risk management.

1 Introduction

Cloud computing has transformed the way organizations store, process, and share data by offering on-demand access to configurable computing resources such as servers, storage, applications, and services. It provides essential benefits such as scalability, flexibility, broad network access, and cost effectiveness. NIST also stresses that cloud systems depend on measured service, where resource utilization is tracked and reported, hence generating an expectation of openness between providers and customers [2]. But security is still one of the biggest hurdles to cloud adoption. When users migrate data and services to the cloud, they generally lose direct control of infrastructure, access enforcement, storage location, and incident visibility. Already at the beginning of the research into clouds, it was stressed that cloud customers might be threatened not only by external attackers, but also by internal misuse, shared resource exposure, and flaws in provider-side controls [1]. The problem gets more apparent when security is considered as more than concealment. In real cloud systems, organizations are concerned about strong authentication, secure key management, reliable data recovery, privacy-preserving, accountability, and operational transparency. Research on cloud trustworthiness shows that clients are unable to trust cloud service providers if they cannot clearly understand the provider's security posture, compliance status, or actual processing of sensitive data. Another issue is the lack of visibility into many of the cloud security decisions. For example, authentication may be good but not perfect, privacy risk may be medium rather than high, and openness may differ between one provider (or service type) and another. This kind of ambiguity might be an issue for standard binary or rigid scoring methods. Fuzzy logic is most suitable for this case, as it is able to describe fuzzy inputs and also process them through rule-based inference to produce meaningful outputs for choice.

It has recently been proven that fuzzy inference algorithms may successfully help cloud service providers in trust evaluation and security preparedness analysis [13]. These limitations lead this study to present a cloud security model based on a fuzzy inference system (FIS) that incorporates key authentication, data recovery risk, data privacy, accountability, and transparency into a single assessment framework. The aim is not only to uncover cloud security vulnerabilities, but also to give an adaptive approach to estimate the total security risk in contexts where accurate assessments are challenging. This technique integrates several security variables into a structured fuzzy model to enhance the cloud security assessment and offer better decision-making for both cloud customers and cloud service providers.

2 Literature Review

Trust, privacy, transparency, access control, and risk assessment are some of the cloud security perspectives that have been researched extensively. This paper's most pertinent works are summarized in the following review.

2.1 Cloud security and trust foundational research: Armbrust et al. (2010) offered one of the earliest analyses of cloud computing and how security concerns were preventing its broader use. According to their explanation, there are internal and external security threats in the cloud environment, and businesses are still hesitant to transfer important workloads to a third party without full oversight [2]. "Mellow and Grrance (2012)" The National Institute of Standards and Technology (NIST) codified the key features and service models of cloud computing in their definition of cloud computing. Because it connects cloud operations with monitoring and reporting, their definition of measurable service is highly pertinent and lends direct support to the idea of transparency in cloud settings [3]. Subashini and Kavitha (2011) found that there are different security holes introduced by each service tier in the SaaS, PaaS, and IaaS architectures. Concerns about data security, network security, and access control remain, and their work is useful for categorizing cloud dangers according to service delivery models. Cloud security reviews that came after this one frequently reference this survey[4]. In a 2014 study, Fernandes, Soares, Gomes, Freire, and Inácio surveyed cloud security challenges and classified main dangers and protections, expanding on this subject. According to their findings, cloud security is multi-layered and affects many different areas, including identity management, virtualization security, data protection, and governance [5]

2.2 Comprehensive studies on privacy and security in the cloud: In their 2014 study, Khalil, Khreishah, and Azeem categorized vulnerabilities, assaults, and reaction strategies in cloud computing, as well as their overall security and privacy. Their research demonstrated the need to address data privacy, data integrity, and confidentiality simultaneously rather than sequentially [6]. When Liu et al. (2015) performed their investigation of cloud security and privacy issues, they highlighted that the provider's capacity to protect sensitive data and provide security assurances has a major effect on the amount of confidence that users have in the cloud. This has all to do with them since openness and accountability are two traits that are taken into consideration in this research [7]. By Singh, A., and Chatterjee, S. (indexed in 2017/2016). An analysis of cloud security issues, threats, and potential remedies. The results indicate the necessity for models that can assess cloud risk in different and dynamic operating environments [8]. Tabrizchi and Kuchaki Rafsanjani (2020) study the cloud security problems and conclude that while there are breakthroughs in the encryption, access control, and virtualization security, the real adoption is still confronted with open issues in privacy, trust and secure administration. Their assessment indicates that contemporary AI approaches such as fuzzy logic may be viable answers to these unresolved difficulties [9]. In a review of service-based cloud security models Khoda Parast et al. (2022) argue that owing to the vast number of cloud services, a uniform security policy is impracticable. Therefore, adaptive evaluation approaches such as fuzzy inference that may utilize multiple signals for different service kinds are even more significant [10]. According to the research of Butt et al. (2023), cloud security today is a mixture of risk-aware decision-making, monitoring, trust management, and preventative measures. According to their research, cloud security assessments should be dynamic and multifactor instead of static and one-size-fits-all [11].

2.3 Integrity and transparency in cloud computing: Rashdi et al. (2016) developed a conceptual framework for accountability in cloud computing, stating that cloud security is not complete without tools to explain duties, policy enforcement, and proof of compliance. Their work is very important to this study as accountability is one of the stated aims of the suggested paradigm[12]. Ismail et al. (2020) addressed cloud security transparency by establishing a framework and enabling an audit procedure to evaluate cloud service providers against pre-defined customer needs. They stated that much earlier work had considered the transparency conceptually, but without providing a specific means to attain it. This gives obvious motivation for integrating transparency as an explicit factor in cloud security evaluation[13].

2.4 Fuzzy logic-based and trust-based cloud security models: Rizvi et al. (2020) suggested a fuzzy inference approach for determining the security preparedness of cloud service providers. Their technique produced a quantifiable security score to rank up providers and highlighted the effectiveness of fuzzy logic in trust measuring because of the uncertainty and ambiguity involved. This research is one of the greatest arguments for adopting FIS in the present work[14]. John et al. (2024) proposed an analytical approach using fuzzy inference for the evaluation of trust in a cloud service provider. The model they developed included security, privacy, performance, dynamicity, and data integrity and sought to offer a consistent trust evaluation pattern among providers. This paper illustrates that fuzzy

systems are still very important for current cloud trust and service assessment[15]. Akhtar et al. (2024) proposed a method for evaluation of trustworthiness of clouds through compliance and feedback, especially for the deployment of digital twins. They used compliance, user feedback, auditor rating and measurement accuracy to illustrate that trust may be boosted when security evidence is more visible and structured. This is in line with the present paper's focus on accountability and transparency[16].

3 Objectives, Research Gap, and Methodology Proposed

This research aims to improve the security of clouds by addressing the key issues linked to the risks of authentication, data recovery, privacy threats, accountability, and transparency. Despite the existence of several security approaches and surveys, much of the available research focuses on specific areas of security and lacks a holistic framework to deal with uncertainty in real world cloud systems. Furthermore, the integration of trust-related elements, such as openness and accountability, with technical indicators in a comprehensive evaluation model has not been well studied. In this research, a Fuzzy Inference System (FIS) based model is proposed to address this gap by integrating several security criteria into a single decision-making model. The model input parameters include authentication strength, data sensitivity, privacy risk and transparency level. A thorough cloud security risk assessment is produced by processing the input parameters using fuzzification, rule-based inference and defuzzification. Such cloud security evaluation is more flexible, adaptable and accurate than the old inflexible ones.

4 Proposed Methodology

4.1 System Overview

The proposed model is based on a Fuzzy Inference System (FIS) that considers several unforeseen elements to assess the possible risks associated with cloud computing. FIS is able to accommodate partial truth values, unlike the binary models often used. This makes it a good candidate for usage in complex and dynamic cloud systems.

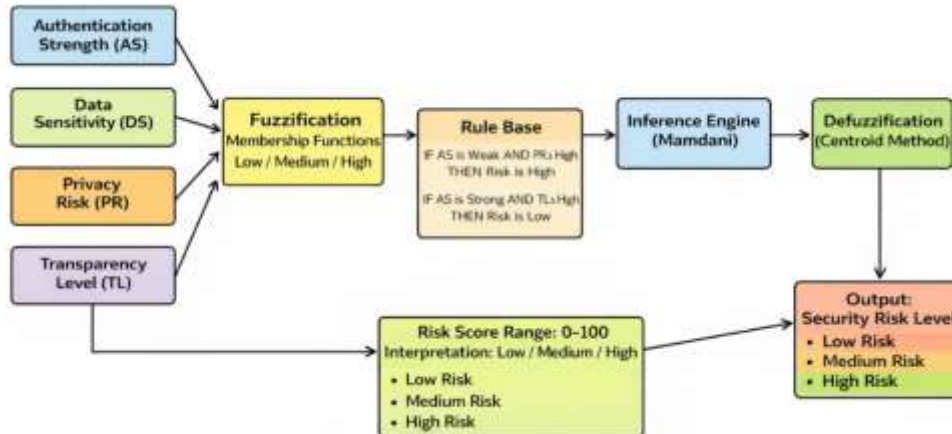


Fig. 1. Proposed Fuzzy Inference System (FIS) Model for Cloud Security Assessment

4.2 Input Parameters

The following 4 imperative safety aspects:

- Authentication Strength (AS): Determines how reliable the user verification is by measurement
- Data Sensitivity (DS): This identifies the value of the data that has been saved.
- Privacy Risk (PR): refers to the possibility that user data might be exposed.
- The Transparency Level (TL): signifies the degree to which cloud operations are apparent.

Each parameter is expressed using linguistic variables:

Parameter	Linguistic Values
AS	Weak, Medium, Strong
DS	Low, Medium, High
PR	Low, Medium, High
TL	Low, Medium, High

4.3 Fuzzification

Input values are transmuted into fuzzy sets via membership functions (triangular/trapezoidal). Example: AS = 60 → partly Moderate and Strong.

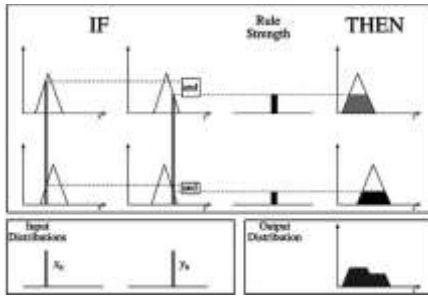


Fig. 2. Fuzzification.

4.4 Rule-Based Design

A collection of IF–THEN rules is developed to represent expert knowledge.

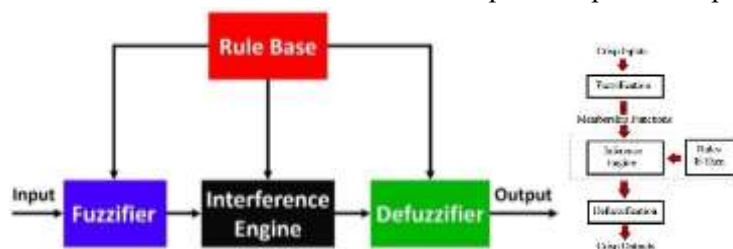


Fig 2: Fuzzy Inference System Architecture

- IF AS is Weak AND PR is Elevated → Risk is Elevated
- IF AS is robust AND PR is minimal AND TL is elevated → Risk is minimal.
- If DS is High and PR is Medium, then the Risk is Medium.

The total number of rules may vary from 20 to 50, depending on the intricacy.

4.5 Mechanism of Inference

There is an application of the Mamdani inference technique that provides for the integration of rules using min-max operations. Results in the creation of a single collection that has confusing outputs.

The process of defuzzification: An accurate value may be obtained from a fuzzy output by the use of the centroid technique. According to the FIS modeling, the final result is a Security Risk Assessment Score ranging from 0 to 100, which is then classed as Low, Medium, or High.

Modeling the Financial Information System (FIS) Mathematically: The Fuzzy Inference System is mathematically expressed by applying the centroid (center of gravity) defuzzification approach to improve the analytical power of the model that has been proposed at this time:

$$y = \frac{\sum_{i=1}^n \mu_i(x) \cdot z_i}{\sum_{i=1}^n \mu_i(x)} \quad (1)$$

Where:

- $\mu_i(x)$ = membership degree of input.
- z_i = output value of each rule.
- y = final crisp output.

This calculation confirms precise accretion of fuzzy productions into a sole sanctuary risk worth.

4.6 Membership Function Design

Each input parameter is defined using triangular or trapezoidal membership functions.

Example:

1. Authentication Strength:	2. Privacy Risk:
• Weak (0–40)	• Low, Medium, High (overlapping ranges).
• Medium (30–70)	
• Strong (60–100)	

These place on top regions consent a plane evolution amid sanctuary stages and progress conclusion correctness.

4.7 Rule Table (Important for Evaluation)

A structured rule base is developed as shown below:

AS	PR	TL	Output Risk
Weak	High	Low	High
Weak	Medium	Medium	High
Medium	Medium	Medium	Medium
Strong	Low	High	Low
Strong	Medium	High	Low
Medium	High	Low	High

This rule table helps in the systematic evaluation of cloud security conditions.

5 Results and Discussion

5.1 Experimental Configuration

The suggested Fuzzy Inference System (FIS) model is tested using simulated cloud security situations. Each input parameter (Authentication Strength (AS), Data Sensitivity (DS), Privacy Risk (PR), and Transparency Level (TL)) was assigned values in the range of 0–100 and divided into fuzzy sets (Low, Medium, High). 10 distinct test cases were examined to examine system behavior under different scenarios.

5.2 Extended Test Case Evaluation

TEST CASE	AS	DS	PR	TL	RISK SCORE	RISK LEVEL
1	20	80	90	30	85	High
2	30	70	80	40	78	High
3	50	60	60	50	55	Medium
4	60	40	50	70	48	Medium
5	80	30	20	80	25	Low
6	75	50	30	70	35	Low
7	40	80	70	40	72	High
8	65	60	50	60	52	Medium
9	90	20	10	90	15	Low
10	55	50	65	45	60	Medium

5.3 Graphical Analysis

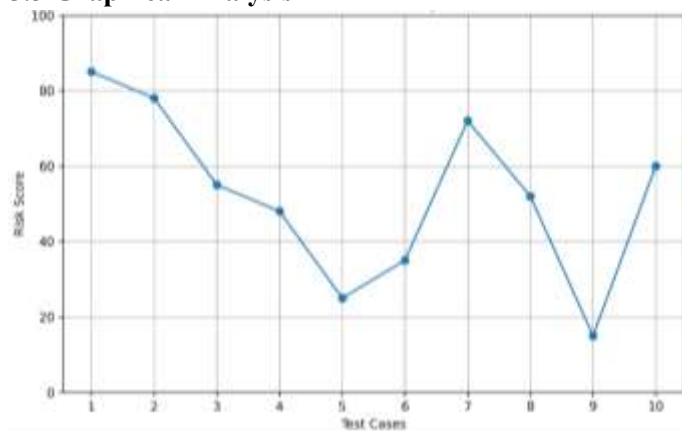


Fig. 3. Risk score versus test cases for the proposed FIS model

Also, the proposed Fuzzy Inference System was evaluated using a simulation implemented in Python in fig.3. To study the system behavior under different cloud security settings, the input test cases were numerically modeled, and the risk ratings that resulted were reported. The simulation results show that the risk score increases with the decrease of the authentication strength and increase of the privacy risk, and vice versa with the increase of the authentication strength and transparency. The defined test cases were used to run a Python-based simulation to support the analytical

assessment. A line graph was used to illustrate the calculation of the risk scores from the presented FIS framework, which helped to analyze the change in scores for different cloud security scenarios. The results of the simulation indicate that the model performs consistently and has shown that it is able to correctly assess cloud hazard categories.

Observation:

Risk score is highest when: - Authentication is weak - Privacy risk is high - Transparency is low	Risk score is lowest when: - Authentication is strong - Privacy risk is low - Transparency is high
--	---

5.4 Performance Analysis

An important feature in reducing the effect of uncertain inputs is the modularity of the FIS model. This approach enables smooth transitions between the risk categories, that in turn helps to reduce the danger of sudden misclassification. But this is contrary to the rigid threshold based approaches as demonstrated in Figure 4.

- Handles multiple parameters simultaneously
- Produces realistic and human-like decision outputs
- Reduces misclassification in borderline cases

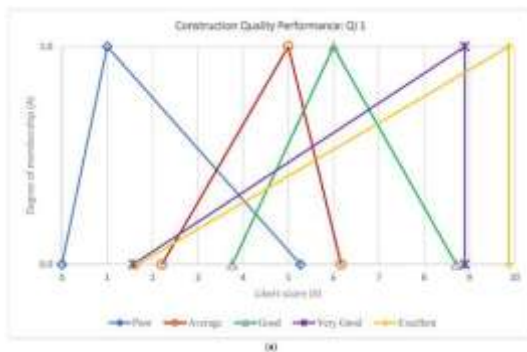


Fig. 4. Graphical Analysis

5.5 Model Comparison

Parameter	Traditional Model	FIS Model
Decision Style	Binary (Rigid)	Fuzzy (Flexible)
Accuracy	Medium	High
Handling Uncertainty	Poor	Excellent
Adaptability	Low	High

5.2 Evaluation

AS	DS	PR	TL	Output Risk
Weak	High	High	Low	High
Medium	Medium	Medium	Medium	Medium
Strong	Low	Low	High	Low

The FIS model is highly adaptable in managing any unknown inputs. We compare this to rigid threshold-based systems which do not enable a smooth transition between risk categories. As a result, this method reduces the amount of sudden categorization errors inside the system. The results clearly show that a single criterion or a strict methodology cannot be used to properly assess cloud security. The proposed FIS-based method is able to address a large number of security aspects and to offer an overall risk assessment. Openness and accountability are included as components for assessment, making the paradigm far more robust and adaptable to real-world cloud systems. The model was evaluated with some simulated cloud situations under varied input conditions.

6. Conclusion

This research deals with some of the key challenges, such authentication, threats associated with data recovery, privacy, accountability and openness. Moreover, a cloud security model based on Fuzzy Inference System is proposed. The provided approach enhances a traditional security evaluation for the following reasons: Components of fuzzy logic: Taking Care of Unpredictable Things. A decision making framework that takes into account a number of diverse risk concerns, retaining outcomes that are both adaptive and interpretable. The findings of the research suggest that the FIS model increases the accuracy of the evaluation of the security of cloud and contributes to the decision-making process. Next, we will implement this in real time and combine it with machine learning methods. This greatly improves both automation and accuracy.

References

1. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.H., Konwinski, A., Zaharia, M.: Above the clouds: A Berkeley view of cloud computing. Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley (2009)
2. Armbrust, M., Fox, A., Griffith, R., et al.: A view of cloud computing. Communications of the ACM 53(4), 50–58 (2010)
3. Mell, P., Grance, T.: The NIST definition of cloud computing. NIST Special Publication 800-145, National Institute of Standards and Technology (2011)
4. Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications 34(1), 1–11 (2011)
5. Fernandes, D.A.B., Soares, L.F.B., Gomes, J.V., Freire, M.M., Inácio, P.R.M.: Security issues in cloud environments: a survey. International Journal of Information Security 13(2), 113–170 (2014)
6. Khalil, I.M., Khreishah, A., Azeem, M.: Cloud computing security: a survey. Computers 3(1), 1–35 (2014)
7. Liu, Y., et al.: A survey of security and privacy challenges in cloud computing. Wireless Networks 22, 203–221 (2015)
8. Singh, S., Chatterjee, K.: A survey on cloud computing security: issues, threats, and solutions. Journal of Network and Computer Applications 75, 200–222 (2016)
9. Tabrizchi, H., Kuchaki Rafsanjani, M.: A survey on security challenges in cloud computing. The Journal of Supercomputing 76, 9493–9532 (2020)
10. Khoda Parast, F., et al.: Cloud computing security: a survey of service-based models. Computers & Security 113, 102580 (2022)
11. Butt, U.A., et al.: Cloud security threats and solutions: a survey. Wireless Personal Communications 130, 101–125 (2023)
12. Al Rashdi, Z.A., et al.: A conceptual framework for accountability in cloud computing. Procedia Computer Science 94, 74–81 (2016)
13. Ismail, U.M., et al.: A unified framework for cloud security transparency and audit. Journal of Information Security and Applications 54, 102594 (2020)
14. Rizvi, S., et al.: A fuzzy inference system (FIS) to evaluate the security readiness of cloud service providers. Journal of Cloud Computing 9(1), 1–17 (2020)
15. John, J., et al.: Trust value evaluation of cloud service providers using fuzzy inference based analytical process. Scientific Reports 14, 69134 (2024)
16. Akhtar, S.I., et al.: Compliance and feedback based model to measure cloud trustworthiness for hosting digital twins. Journal of Cloud Computing 13, 90 (2024)