Standardization of Cloud Security using Mamdani Fuzzifier

Shan e Zahra
Department of Computer Science
Faculty of Information Technology
Lahore Garrison University, Lahore, Pakistan

Muhammad Nadeem Ali
Department of Computer Science
Faculty of Information Technology
Lahore Garrison University, Lahore, Pakistan

Muhammad Adnan Khan
School of Computer Science
National College of Business Administration & Economics
Lahore, Pakistan

Sabir Abbas
Department of Computer Science
Faculty of Information Technology
Lahore Garrison University, Lahore, Pakistan

***Abstract*—Cloud health has consistently been a major issue in information technology. In the CC environment, it becomes particularly serious because the data is located in different places even in the entire globe. Associations are moving their information on to cloud as they feel their information is more secure and effectively evaluated. However, as a few associations are moving to the cloud, they feel shaky. As the present day world pushes ahead with innovation, one must know about the dangers that come along with cloud health. Cloud benefit institutionalization is important for cloud security administrations. There are a few confinements seeing cloud security as it is never a 100% secure. Instabilities will dependably exist in a cloud with regards to security. Cloud security administrations institutionalization will assume a noteworthy part in securing the cloud benefits and to assemble a trust to precede onward cloud. In the event that security is tight and the specialist organizations can guarantee that any interruption endeavor to their information can be observed, followed and confirmed. In this paper, we proposed ranking system using Mamdani fuzzifier. After performing different ranking conditions, like, if compliance is 14.3, Data Protection 28.2, Availability 19.7 and recovery is 14.7 then cloud health is 85% and system will respond in result of best cloud health services.**

Keywords*—CC; CS, FIS; FRBS; MIE, standards; compliance; data protection; availability and recovery

I. INTRODUCTION

Cloud Computing (CC) [1] has been envisioned as the next generation paradigm in computation. In the CC environment, both applications and resources are delivered on demand over the Internet as services. Cloud is an environment of the hardware and software resources in the data centers that provide diverse services over the network or the Internet to satisfy user's requirements [1], [2].

In CC, applications are given and overseen by the cloud server and information is likewise put away remotely in the cloud setup [1], [2]. Clients don't download and introduce applications all alone gadget or PC; all handling and capacity is kept up by the cloud server.

CC is a web based exercise of utilizing a framework of far off servers facilitated on the web to store, oversee, and handle information, instead of a neighborhood server or a PC [1], [3].

CC is the after effect of the development and appropriation of existing advances and models. The objective of distributed computing is to enable clients to take benefit from these advancements, without the requirement for profound learning about them or mastery with every one of them. The cloud reason for existing is to diminishing expenses, and help the clients concentrate on their center business as opposed to being hampered by IT hindrances [1], [3], [4].

For CC security [1], one must comprehend your security and administration prerequisites for a particular framework or potentially information store. Individuals who put security around cloud or customary frameworks don't comprehend what issues they are offering to fathom. Individuals need to outline them before all else [4].

One should likewise understand that the area of the information is a great deal more vital than representing access. By taking a gander at chances to break and how the information is gotten to. Once more, a large portion of the information breaks happen around discovering powerlessness, regardless of if it's cloud construct or in light of destinations [4]. At long last, weakness testing is an articulate necessity, regardless of in case you're trying the security of cloud-based or customary frameworks. Unsubstantiated frameworks are dangerous and unsecured frameworks.

Clients will soon think distinctively around the cloud and security as more public cloud-based frameworks and information stores are deployed. In any case, without the appropriate measure of arranging and great innovation, cloud-based stages can turn out to be more secure. There are such a large number of parameters on which the cloud security relies on upon; some being, consistence necessities, misfortune in administration, accessibility and unwavering quality, confirmation and approval, feasibility, information insurance,

get to controls, issue and data security administration, and so forth. As per our exploration we trust that by institutionalization of a couple of parameters the cloud security issue [4], [11] can be diminished. The main parameters that we are going to standardize are compliance, availability, data protection and recovery. By finding out the probability of these four parameters, the cloud could either be protected or perilous. In this paper, we proposed ranking system using Mamdani fuzzifier. After performing different ranking conditions, like, if compliance is 14.3, Data Protection 28.2, Availability 19.7 and recovery is 14.7 then cloud health is 85% and system will respond in result of best cloud health services.

II. Literature Review

In a related research paper, it was expressed there are many cloud benchmarks and numerous in trial or draft organize. A few gauges are gone for particular points; a few measures are gone for the whole cloud biological community [1]. Particularly in the territory of data security administration framework gauges there is a surge of endeavors, frequently matched with affirmation programs, with a comparative objective ("to build confide in cloud suppliers") [11], [12], [15].

It is intriguing to see that a large portion of these ventures concentrate on rather nonexclusive prerequisites. What is more often than not out of extension are particular criteria, for example, a base level of accessibility, least reaction times to occurrences, a base arrangement of capacities for the authoritative interfaces, or at least obligation or duty regarding security breaks [1], [13], [14]. It was expressed that institutionalization here could make it simpler for clients to assess, look at and embrace cloud benefits by giving institutionalized interfaces.

III. Parameters for Security

A. Compliance

Consistence issues in cloud security emerge when one uses the cloud storage or administration. One is concerned how their data will be kept with reference to the rules, regulation and laws. To conquer consistence issues one ought to be very much aware of which sort of cloud administration he is utilizing [3], [14], [15]. Other than that, they must be extremely watchful about which information they are moving to the cloud. Consistence is one of the key parameters with regards to cloud security [1] notwithstanding; it can be traded off in a few circumstances. As in it can extend from very high to very low and still be viewed as secure now and again. This is however safety measures from the client's end.

In an association, they now and again choose to keep profoundly private data off of a cloud or want to keep it on an inside system with the goal that it is not under any hazard. They once in a while move it to a private cloud where they can without much of a stretch get to both physical and logical infrastructures.

The following thing to investigate once you know which information you will put on the cloud is to investigate the concurrences with your cloud supplier [1]. All in all, on the off chance that it is an inside cloud, would you say you will have inner consistence agendas? On the off chance that it's outer, you need to clearly relate to the supplier what kind of information exists on their cloud administrations, how will ensure it, how will back it up and how may you maintain whatever authority is needed to review the security and consistence structure that they work around your information?

B. Data Protection

In cloud security [3], information assurance is the most basic component. Protecting information on the cloud is a noteworthy need. Associations are uncertain by the prospect of presentation or the break of information and additionally the inaccessibility of information [4], [12].

In institutionalization, it is profoundly essential to keep this parameter secure, as without the security, many will quit utilizing the cloud. The real concern is the abuse of the vital information. It might be troublesome for the cloud benefit client to adequately check the information taking care of practices of the cloud supplier [3], [13]. Consequently, cloud specialist organizations are quick to keep their clients upbeat by keeping a standard in cloud security and keeping information ensured constantly [4].

C. Availability

Accessibility is the nearness of the cloud administrations. It is a standout amongst the most fundamental parameters in cloud security. Cloud security [2] depends intensely on accessibility and its standard ought to dependably be high or kept up as it without it cloud can't work legitimately. It is profoundly versatile and equipped for meeting wide variations [3].

D. Recovery

Recovery is additionally a critical parameter, as associations need to know how they can recoup from aggregate debacle. A specialist organization that does not copy the information over various locales is presented to an aggregate disappointment [4]. Cloud specialist co-ops need to disclose to one where precisely are they putting away the information, and what might happen to your information and administration in the event that one of its destinations respects a disaster. Does it have the inclination to do an entire repair, and to what extent will it take?

IV. Methodology

We proposed fuzzy rule [5] - [7] based scheme (FRBS) that is capable of choosing cloud health using Mamdani fuzzifier [6] system. The four input and one output fuzzy inference system (FIS) is proposed to calculate cloud health on the basis of fuzzy logic principle [1].

In this method, we have picked Four parameters with respect to cloud security; compliance, data Protection, availability and recovery. We flipped around these parameters considering that they are the more vital than other and sorted them in principles. The brief description of fuzzy rule based scheme is given below. We used Mat-lab 7.12.0 fuzzy system [7] toolbox in designing of FRBS [1].

A. Fuzzy Sets

We used a number of fuzzy sets [6], [8], [9] to cover input-output spaces. The four input variables compliance, data Protection, availability and recovery with one output variable Cloud health are already shown in Fig. 1, 2, 3, 4 and 5. There are 5, 5 fuzzy sets [5], [8] used for the variables: Compliance and data Protection and 3, 3 fuzzy sets [10], [11], [15] used for variable Availability and Recovery.

B. Fuzzifier

We used triangular fuzzifier [5], [6] with "AND" respectively.

C. Rule Base

The rule base [6], [7] contains total 264 output rules. The rules are shown in Fig. 1.

D. Inference Engine

We used Mamdani Inference Engine (MIE) [6] in order to map the four inputs to one output shown in Fig. 6.

E. De-Fuzzifier

We used center average De-fuzzifier [6], [7]. Fig. 8, 9 and 10 represents rule surface of above FRBS.

F. Compliance

Cloud specialist co-ops might be novel, yet it is realized that most directions hold the client of the administration, at last, in charge of the security and veracity of corporate and client information, notwithstanding when it is held by the specialist organization [14], [15]. Customary specialist organizations capitulate to outside reviews and security guarantees, giving their clients data on the exact controls that were assessed. A distributed computing supplier that is unwilling or not able to do this is signaling that clients can just utilize them for the most minor capacities. (Surveying the Security Risks of CC) [14], [15]. We have taken five membership functions: very high, high, medium, low and very low using Mamdani fuzzy logics [5], [8] as shown in Fig. 1.

G. Data Protection

The administration of methodological, basic and lawful measures is so as to accomplish the objectives of information security (protection, trustworthiness and accessibility), straightforwardness, intervene ability and transportability, and in addition consistence with the applicable legitimate system. To measure data protection effect in cloud health we have taken five membership functions: very high, high, medium, low and very low using Mamdani fuzzifier [5], [8], [11], [14] as shown in Fig. 2.

H. Availability

In different papers, it is demonstrated regardless of whether the standard is public and open, with reference to get to. They have recognized three levels:

1) Fully open

Open counsel for drafts (like W3C, IETF, OASIS, and so forth.), and open access to conclusive renditions for a little expense.

2) Partially open

Consultation is shut/enrolment, yet there is open access to the standard.

3) Closed

Consultations are not open to the general population, and the standard is not public either. There is a significant expense [2].

Accessibility is typically secured by authorization at a general level. Accessibility is a key administration level goal, as it characterizes whether the cloud administration can really be utilized, and it is commonly important to determine numeric esteems for accessibility to make significant revelations that are valuable for cloud benefit clients. The topic of what "usable" means is a mind boggling matter, which relies on upon the cloud benefit concerned. An administration can be up and accessible, however it can perform so ineffectively that it will be considered adequately unusable. So also, the administration can be up, however it might react with blunders for legitimate necessities. To measure availability effect in cloud health we have taken three membership functions [6]fully open, partially open and closed using Mamdani fuzzifier [6], [8] as shown in Fig. 3.

I. Recovery

Most cloud suppliers have the money related assets to reproduce content in numerous areas as a matter of course. Along these lines repetition and freedom is expanded from disappointment and gives a level of disaster recovery. Clients of the cloud supplier ensure those measures are conformed to [13], [14]. At times, when delicate information and money related information are prepared, the client need to ensure significantly firmer information safety efforts with regards to the capacity of information, correspondence or transmission of information, information disaster recuperation and ahead transmission [13], [14]. To measure recovery effect in cloud health we have taken three membership functions [5], [8], [11], [15] low, medium and high using Mamdani fuzzifier as shown in Fig. 4.

V. Simulation and Results

In this paper, Mat-lab 7.12.0 fuzzy system [6] toolbox and triangular fuzzifier with "AND" operation has been used. There are four parameters: Compliance, Data Protection, Availability and Recovery that are being utilized to rank any cloud security given by various specialist co-ops. These are the following Ranges and Membership functions:

In Table I, all the ranges and membership functions of the parameters are shown.

TABLE I. RANGES AND MEMBER FUNCTIONS OF CLOUD HEALTH

Parameters	Member Functions	Ranges
Compliance	Very low	0-5.5
	Low	5.2-10
	Medium	8-13
	High	12-20
	Very High	20>
Data Protection	Very low	0-5.5
	Low	5-8
	Medium	8-15
	High	12-20
	Very High	19-30
Availability	Fully Open	0-5.8
	Partially open	5-14
	Closed	12-20
Recovery	Low	0-5
	Medium	4-10
	High	8-15

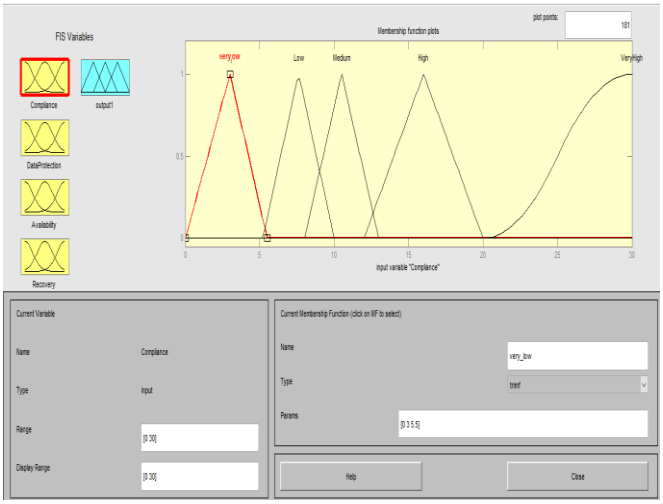

Fig. 1. Fuzzy sets for input variable compliance.

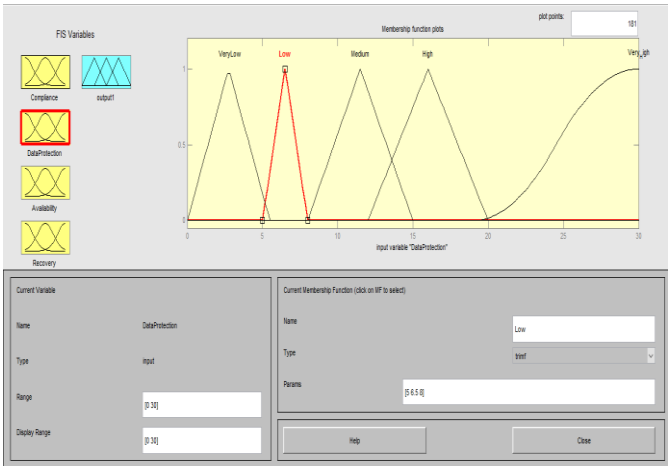

Fig. 2. Fuzzy sets for input variable data protection.

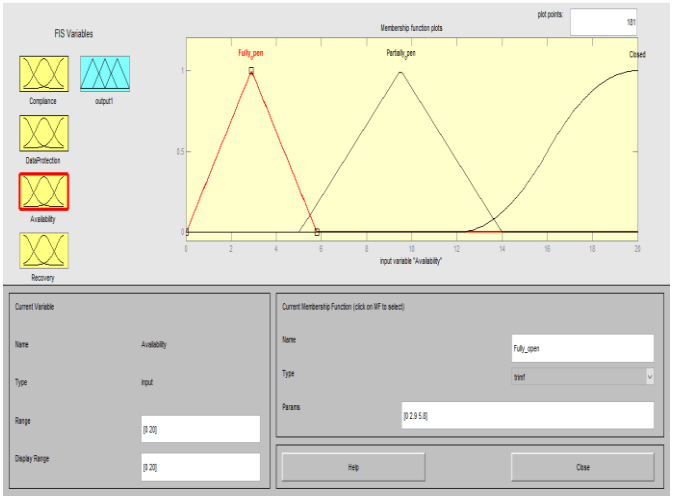

Fig. 3. Fuzzy sets for input variable availability.

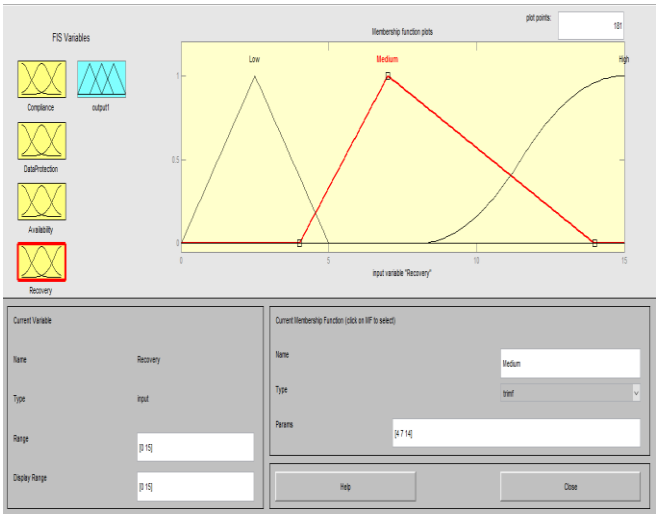

Fig. 4. Fuzzy sets for input variable recovery.

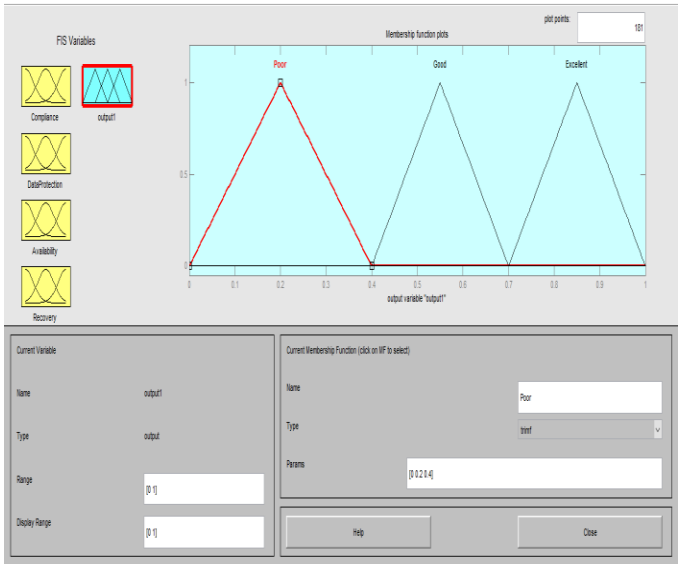

Fig. 5. Fuzzy sets for output variable cloud security.

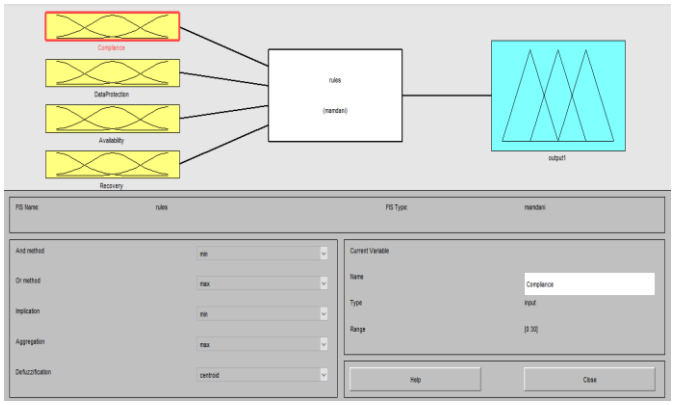

Fig. 6. Mamdani fuzzy rule base system.

1. If (Compliance is very_low) and (Data_Protection is Low) then (output1 is Poor) (1)
2. If (Compliance is very_low) and (Data_Protection is High) then (output1 is Good) (1)
3. If (Compliance is very_low) and (Data_Protection is VeryLow) then (output1 is Poor) (1)
4. If (Compliance is very_low) and (Data_Protection is Medium) then (output1 is Good) (1)
5. If (Compliance is very_low) and (Data_Protection is Very_High) then (output1 is Good) (1)
6. If (Compliance is High) and (Data_Protection is Low) then (output1 is Poor) (1)
7. If (Compliance is High) and (Data_Protection is High) then (output1 is Good) (1)
8. If (Compliance is High) and (Data_Protection is VeryLow) then (output1 is Poor) (1)
9. If (Compliance is High) and (Data_Protection is Medium) then (output1 is Good) (1)
10. If (Compliance is High) and (Data_Protection is Very_High) then (output1 is Excellent) (1)
11. If (Compliance is Medium) and (Data_Protection is Low) then (output1 is Poor) (1)
12. If (Compliance is Medium) and (Data_Protection is High) then (output1 is Good) (1)
13. If (Compliance is Medium) and (Data_Protection is VeryLow) then (output1 is Good) (1)
14. If (Compliance is Medium) and (Data_Protection is Medium) then (output1 is Good) (1)
15. If (Compliance is Medium) and (Data_Protection is Very_High) then (output1 is Good) (1)
16. If (Compliance is Low) and (Data_Protection is Low) then (output1 is Poor) (1)

Fig. 7. Rule base for deciding cloud health

Fig. 7 shows that the rules of the system are shown where all the possibilities were made using the four parameters; compliance, data protection, availability and recovery.

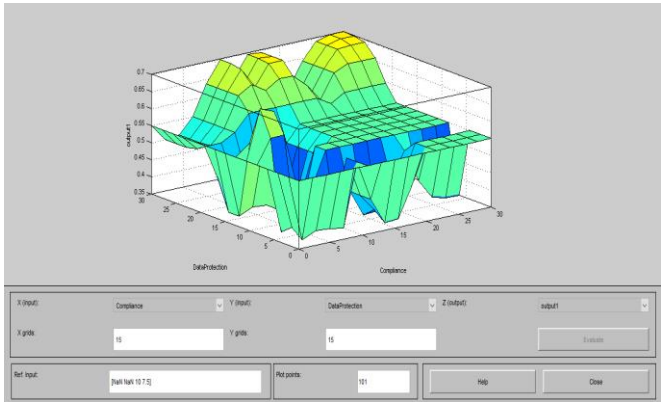

Fig. 8. Rule surface of data protection and compliance.

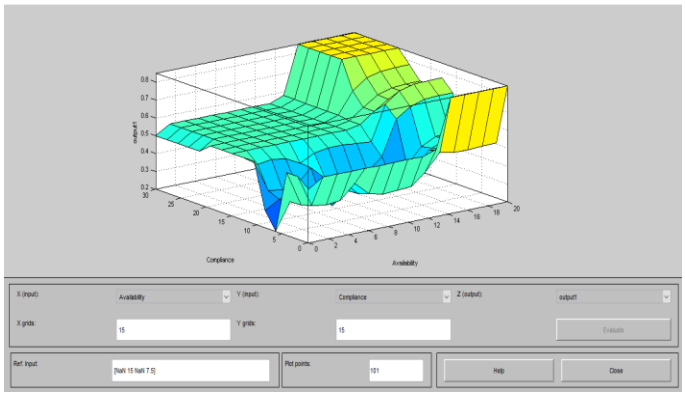

Fig. 9. Rule surface of compliance and availability.

A. Rule Viewer

In this proposed system, all the possibilities were made using the four parameters; compliance, data protection, availability and recovery. Their security statuses were toggled from very high, high, medium, low to very low and in result, cloud security be shown when it was very high, high, medium low or very low depending on the importance of the parameters in the experiment. The ranges given above were all tested one by one and as a result data protection and availability proved to be the most important as security depends on them massively. Recovery and compliance are important parameters too however not as important as the other two. Fig. 8, 9 and 10 depicts the surface view or the data under observation according to the standards of the four parameters.

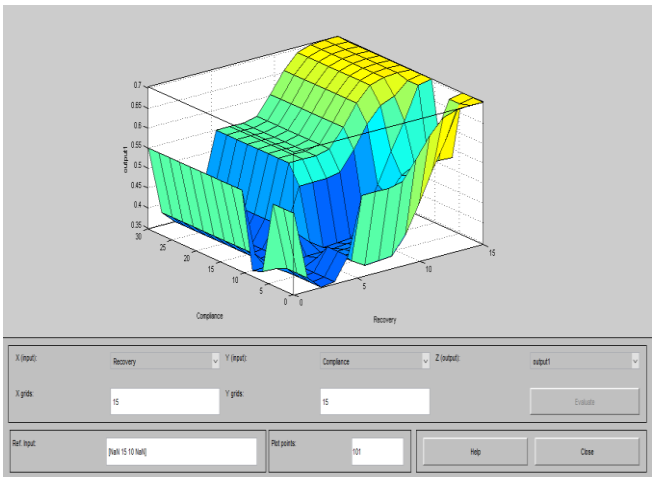

Fig. 10. Rule surface of compliance and recovery.

Fig. 11 shows that if compliance is 0, Data Protection 1.62, Availability 3.79 and recovery is 0.808 then cloud health is 0.2.

Fig. 12 shows that if compliance is 29.7, Data Protection 18.7, Availability 9.24.79 and recovery is 7.96 then cloud health is 0.55.

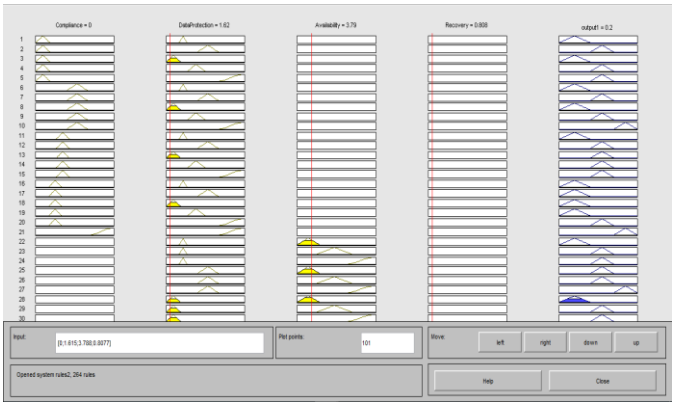

Fig. 11. Rule viewer when cloud health is poor.

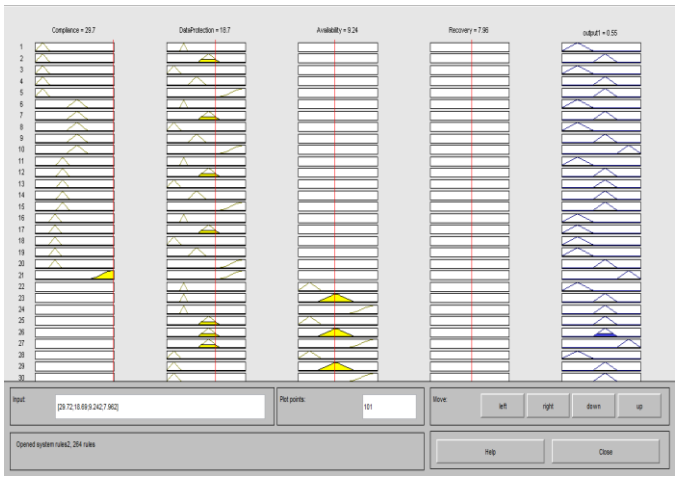

Fig. 12. Rule viewer when cloud health is good.

Fig. 13. Rule viewer when cloud health is excellent.

Fig. 13 shows that if compliance is 14.3, Data Protection 28.2, Availability 19.7 and recovery is 14.7 then cloud health is 0.85.

VI. CONCLUSION

CC is a promising and rising innovation for the up and coming age of IT applications. The obstruction and obstacles toward the quick development of CC are information security and protection issues. Diminishing information stockpiling and preparing cost is an obligatory prerequisite of any association, while examination of information and data is dependably the most essential assignments in every one of the associations for basic leadership. So no associations will exchange their information or data to the cloud until the point when the trust is worked between the cloud specialist co-ops and buyers. In this research paper, four parameters are listed and their standards relevant for CC security, and we explained how the standards can be set to achieve optimum security in cloud services. They have been classified by standards according to their characteristics, and the reason to standardize these parameters is also explained. We conclude with some general remarks. Ranking based services for selecting the most appropriate methods from given numbers of providers. We proposed ranking system using Mamdani Fuzzifier. After performing different ranking conditions, like, if compliance is 14.3, Data Protection 28.2, Availability 19.7 and recovery is 14.7 then cloud health is 85% and system will respond in result of best cloud health services.

REFERENCES

[1] "Cloud Security Alliance," a non Profit Cloud Evangelists Group, [Online]. Available: http://cloudsecurityalliance.org/.

[2] M. X. L. R. L. a. X. S. Barua, "ESPAC: Enabling Security and Patient-centric Access Control for eHealth in cloud computing," International Journal of Security and Networks 6, pp. 67-76, 2011.

[3] D.-G. M. Z. Y. Z. a. Z. X. Feng, "Study on cloud computing security," Journal of software 22, vol. 1, pp. 71-83, 2011.

[4] B. R. a. A. R. Kandukuri, "Cloud security issues In Services Computing," in IEEE International Conference on, pp. 517-520, 2009.

[5] G. a. B. Y. Klir, "Fuzzy sets and fuzzy logic. Vol. 4. New Jersey: Prentice hall, 1995", New Jersey: Prentice hall, vol. 4, 1995.

[6] Shahzad, "Fuzzy Approach Based Two Layered Block Coded Adaptive MC-CDMA system with FT/ST," Recent Sci, E-ISSN, vol. 5, no. 3, pp. 50-57, 2016.

[7] S. M. a. C. Y. C. CHEN, "A new weighted fuzzy rule interpolation method based on GA-based weights-learning techniques," in International Conference on Machine Learning, Qingdao, Shandong, China, 2010.

[8] S. M. a. K. Y. K. CHEN, "Fuzzy interpolative reasoning for sparse fuzzy rule-based systems based on α-cuts and transformation techniques," IEEE Transaction on Fuzzy System, vol. 16, no. 6, 2008.

[9] P. P. B. V. C. K. H. a. S. M. J. BONISSONE, "Industrial application of fuzzy logic at general electric," IEEE Transaction on Industrial Application, vol. 38, no. 3, pp. 450-456, 1995.

[10] Y. C. C. S. M. a. L. C. J. CHANG, "A new fuzzy interpolative reasoning method based on the areas of fuzzy sets," in IEEE International Conference on System, Manufacturing and Cybern, 2007.

[11] T. S. K. a. S. L. Mather, Cloud security and privacy: an enterprise perspective on risks and compliance., " O'Reilly Media, Inc.", 2009.

[12] R. E. a. Z. L. A. BELLMAN, "Decision making in a fuzzy environment," Management Scince, vol. 17, pp. 141-164, 1970.

[13] J. C. K. J. M. K. R. a. P. N. R. BEZDEK, "Fuzzy models and algorithms for pattern recognization and image processing," Boston, MA: Kluwer, 1999.

[14] S. M. a. C. Y. C. CHEN, "A new method for weighted fuzzy inter-polative reasoning based on weights-learning techniques," in IEEE International Conference on Fuzzy Systems, Barcelona, Spain, 2010.

[15] S. M. K. Y. K. C. Y. C. a. J. S. P. CHEN, "Weighted fuzzy interpolative reasoning based on weighted incremental transformation and weighted ratio transformation techniques," IEEE Transaction on Fuzzy System, vol. 17, no. 6, pp. 1412-1427, 2009.