2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications

# A Fuzzy Modeling Approach for Risk-based Access Control in eHealth Cloud

Juan Li
Department of Computer Science
North Dakota State University
Fargo, USA
j.li@ndsu.edu

Yan Bai
Institute of Technology
University of Washington Tacoma
Tacoma, USA
yanb@uw.edu

Nazia Zaman
Department of Computer Science
North Dakota State University
Fargo, USA
nazia.zaman@my.ndsu.edu

***Abstract*— A number of recent studies have adopted risk assessment in access control for healthcare applications, but few of the work is specifically concerned with the risk assessment in the presence of uncertainties, such as uncertain values of risk factors, and consequences of imprecision. This paper presents a fuzzy modeling-based approach that accounts for uncertainty analysis when evaluating the risk. Three inputs—data sensitivity, action severity, and risk history—are modeled with fuzzy set and used to calculate the level of risk associated with healthcare information access in a cloud environment. Experiments were conducted and demonstrated that the approach can generate accurate and realistic outcomes in assessing current security risk and predicting the scope and impact of different risk factors. This would lead to a great change of access control from being active to being proactive to security breach, and enhance the security level of eHealth cloud applications.**

***Keywords— security, risk, access control, eHealth, cloud computing, fuzzy modeling***

## I. Introduction

eHealth applications over the cloud are being developed recently [7]. It allows medical professionals to coordinate amongst various medical departments, institutions, and other healthcare related businesses, and thus, optimizes patient flow and improves efficiency in the use of medical resources [5]. As compared to conventional methods, where institutions set up their own infrastructures, users of an eHealth cloud can significantly reduce fiscal expenditures [6]. Moreover, the healthcare cloud would provide scalable solutions that can easily expand and contract based on healthcare information and users' needs. However, eHealth cloud is facing privacy and security challenges. There is an urgent need for effective access control to protect highly sensitive healthcare information over a cloud computing environment [9, 11]. Recent approaches integrate risk management to handle healthcare information access [4, 12], but these methods have drawbacks. They use different factors to estimate risks, indicate risk levels that are either minor or major but otherwise are mainly qualitative. Furthermore, uncertainty of risk factors exists in most of these approaches. Fuzzy logic technique is an alternative technique that is becoming more frequently used to address the uncertainties and the qualitative aspects associated with risk assessment [8]. To the best of our knowledge, little fuzzy logic has been applied to risk-based access control in eHealth cloud applications. Hence, we adopt fuzzy theory to produce more accurate and realistic risk assessment that are linked to an effective control of healthcare information access in a cloud environment.

The rest of the paper is organized as the follows. In Section II, we survey the work that has been done on enhancing security and privacy of eHealth cloud. Section III describes our fuzzy logic model of risk assessment. Section IV discusses the proposed model for providing access control in cloud-assisted eHealth. We conclude our work with future work in Section V.

## II. Related Work

Although eHealth clouds offer new possibilities, they also pose a variety of security and privacy risks. There have been many works proposed to address the privacy and security problems in eHealth cloud. One category of works focuses on cryptographically enforced access control for outsourced data and attribute based encryption. To realize fine-grained access control, the traditional public key encryption (PKE) based schemes [17], [18] have been used. However, these works require encrypting multiple copies of a file using different users' keys, which may incur high key management overhead. To improve the scalability, one-to-many encryption methods such as ABE [19] are proposed. This potentially makes encryption and key management more efficient [20]. In a recent study [21], the authors propose a patient-centric framework for data access control to personal health record (PHR) stored in semi-trusted servers by leveraging attribute based encryption (ABE) techniques to encrypt each patient's PHR file. They divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users.

Another category of the research in security and privacy of eHealth cloud focus on network security and access control policies. For example, authors in [23] propose an Efficient and Secure Patient-centric Access Control (ESPAC) scheme which allows data requesters to have different access privileges based on their roles and then assigns different attribute sets to them. In [24], a sensor network architecture is proposed for collecting and accessing large amount of data generated by medical sensor networks. However, they do not address the client

978-0-7695-5022-0/13 $26.00 © 2013 IEEE
DOI 10.1109/TrustCom.2013.66

platform security appropriately [22]. To solve this problem, in [16], the authors present security architecture for establishing privacy domains in e-health infrastructures. This solution provides client platform security and appropriately combines this with network security concepts.

Our work is more related to risk-based access control approaches. Risk is the potential harm that may arise from some present processes or from some future events. It is often mapped to the probabilities of undesirable events and related impact. Risk assessment is an effective tool used in decision making. It has recently been adopted in access control for healthcare applications. In [30], we provided a comprehensive study of access control on eHelath applications. Here, we review some representative techniques discussed in [30].

In [10], the authors augmented role-based access control with risk assessment. Risk of granting access is determined by the consequence of different actions. The consequence is measured by how availability, integrity and confidentiality would be affected. In [25], an attribute-based access control framework for risk-adaptive access control was presented. It provides access to resources accounting for operational needs, risk factors and situational factors, and allows for a variety of enforcement architectures and detailed implementation.

In [26], a more fine-grained risk-based role-based access control (RBAC) approach was proposed. It requires that each permission to be associated with a risk mitigation strategy. In deciding access request, user trustworthiness, the degree of competence of a user-role assignment, and the degree of appropriateness of a permission-role assignment were all considered. In [27], the authors focus on access control approaches usable for information sharing through large screens where several individuals are present at the same time. They outlined and evaluated a various approaches. The evaluation was based on criteria derived from risk analyses of a planned coordination system for the perioperative hospital environment. In [28], two dynamic risk-based decision methods for access control systems were proposed. Theoretical and simulation-based analysis and evaluation of both schemes prove that the proposed methods, not only allow exceptions under certain controlled conditions, but uniquely restrict legitimate access of bad authorized users. In [29], the proposed access control allowed information consumers (i.e. doctors) to make access decisions, while still being able to detect and control the over-accessing of patients' medical data by quantifying the related risk. In particular, the authors applied statistical methods and information theory techniques to quantify the risk of privacy violation. Additionally, occasional exceptions on information needs are granted. A prototype implementation and simulations on real-world medical history records were performed to demonstrate the effectiveness of the proposed approach.

## III. Fuzzy-based Risk Assessment for Cloud-Assisted eHelath

Risk assessment is an "assessment" of something hypothetical defined as "risk" , which must then be interpreted as "high", or "low", or "tolerable". Such assessment, whether qualitative or quantified, requires analyst's judgment, expert human knowledge and experience [1]. Quantification of risk in scalar values is subject to uncertainties for many reasons including difficulties in defining the likelihood and consequence severity and the mathematics of combining them [1]. In contrast, fuzzy logic techniques allow the use of degrees of truth to calculate results. It is tolerant of imprecisely defined data; it can model non-linear functions of arbitrary complexity; and it is able to build on top of the experience of experts. In healthcare systems, some patient information, such as test result, might be confidential, whereas another part, such as geographical information, might be unclassified. The latter, therefore, introduces a contain degree of vagueness regarding the patient information and the possible risks that a typical healthcare system might incur. In addition to vagueness, intuitive and experiences in modeling risk assessment in a healthcare system must be accommodated because human observation forms the basis of any risk assessment [2]. For example, we cannot precisely determine the likelihood of exposing databases files with patient information to outsiders, but we can estimate a value based on observations. Fuzzy logic ensures that we do not neglect human common sense, intuition, and experiences. Fuzzy logic and fuzzy set operations enable characterization of vaguely defined (or fuzzy) sets of likelihood and consequence severity and the mathematics to combine them using expert knowledge.

We, therefore, extend the results of our prior work on control of healthcare information access in a cloud environment [4], and introduce a fuzzy logic approach to deal with the uncertainty and imprecision of risk assessment and resulted decision making in access control. Three risk factors that determine the security level of the eHealth cloud, i.e., data sensitivity, action severity and risk history, are identified and selected in [4]. We incorporate them in the fuzzy model. To construct the fuzzy model, four major steps are involved.

The first step specifies key risk indicators and defines linguistic variables. We begin to determine problem input and output variables and their ranges in this step. For our problem, there are three key risk indicators defined as input: (1) the severity of a particular action's consequence. An action/task may incur the possibility of compromising confidentiality, integrity, or availability of the sensitive patient information. For example, a "view" operation may incur confidentiality risk, while a "delete" operation may incur higher risk because it compromise confidentiality, integrity, and availability. We can measure the severity of the consensuses using the normalized AIC score defined in our previous paper [4]; (2) the sensitivity of the data. Some patient information, such as clinical information, might be confidential, whereas another part, such as geographical information, might be not very sensitive; (3) The past risk score. Previous users' behavior patterns are stored and used as a factor to predict their future behavior. The output is the risk.

As we mentioned earlier, the inputs and the output constitute vague estimates rather than crisp values; such vague estimates defined general categories, as opposed to rigid, fixed collections. Valid ranges of the inputs are considered and divided into classes, or fuzzy sets. For example, the severity of the action consequence can range from "low" to "high". The sensitivity of the data can range from "not sensitive" to "highly sensitive" with other values in between. The passed risk score can range from “low” to “high”. The output is risk and is defined in fuzzy sets in five categories: Negligible, Low, Moderate, High, Unacceptable High. These categories have more flexible membership requirements that allow for partial membership to a category. The degree to which a value is a member of a category can be any value between 0 and 1. In fuzzy logic, these categories are called fuzzy sets. We cannot specify clear boundaries between classes. The degree of belongingness of the values of the variables to any selected classes is called the degree of membership [13]. Table I list the input and output variables and their ranges.

TABLE I. INPUT AND OUTPUT VARIABLES AND THEIR RANGE

| **Input variable: the severity of the action consequence, *a*** | | |
|---|---|---|
| Value | Notation | Range (normalized) |
| Low | L | 0, 0.4 |
| Medium | M | 0.35, 0.7 |
| High | H | 0.6, 1 |
| **Input variable: the sensitivity of the data, *s*** | | |
| Value | Notation | Range (normalized) |
| Not sensitive | NS | 0, 0.35 |
| Sensitive | S | 0.2, 0.5 |
| Highly Sensitive | HS | 0.45, 1 |
| **Input variable: past risk, *p*** | | |
| Value | Notation | Range (normalized) |
| Low | L | 0, 0.4 |
| Moderate | M | 0.3, 0.7 |
| High | H | 0.6, 1 |
| **Output variable: risk, *r*** | | |
| Value | Notation | Range (normalized) |
| Negligible | N | 0, 0.3 |
| Low | L | 0.1, 0.4 |
| Moderate | M | 0.2, 0.6 |
| High | H | 0.4, 0.8 |
| Unacceptable High | UH | 0.7, 1 |

The second step determines fuzzy sets. Each fuzzy set has a corresponding membership function that returns the degree of membership for a given value within a fuzzy set. Fuzzy sets can have a variety of shapes. In our system, we choose to use a triangle or a trapezoid, because they can often provide an adequate representation of the expert knowledge; and at the same time significantly simplifies the process of computation [3]. Figures 1-4 show how we can represent the inputs and outputs by means of membership functions.

Step 3 specifies fuzzy rules. Having specified the risk and its indicators, the logical next step is to specify how the risk varies as a function of the factors. Experts provide fuzzy rules that relate risk to various levels of indicators based on their knowledge and experience. In our system, there are three input and one output variables. For a three-by-one system (three inputs and one output), the representation of the rule metrics takes the shape of a 3*3*3 cube called FAM (fuzzy associative memory).

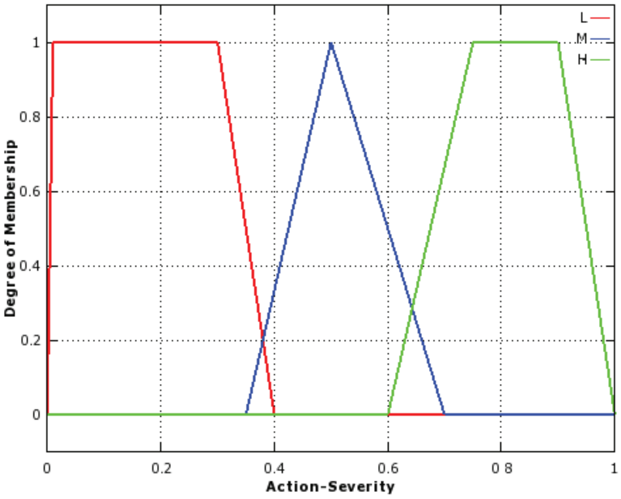

Fig. 1. Fuzzy Sets of Severity of Action Consequence

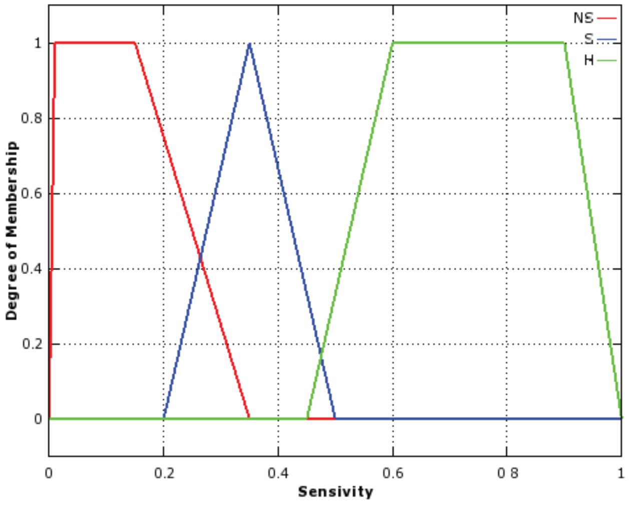

Fig. 2. Fuzzy Sets of Data Sensitivity

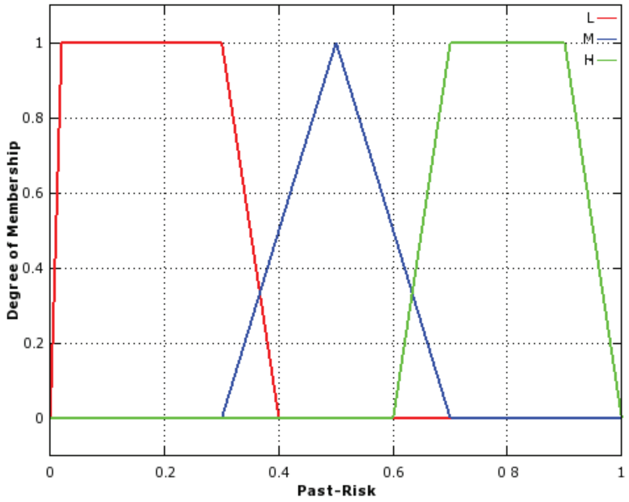

Fig. 3. Fuzzy Sets of Past Risk

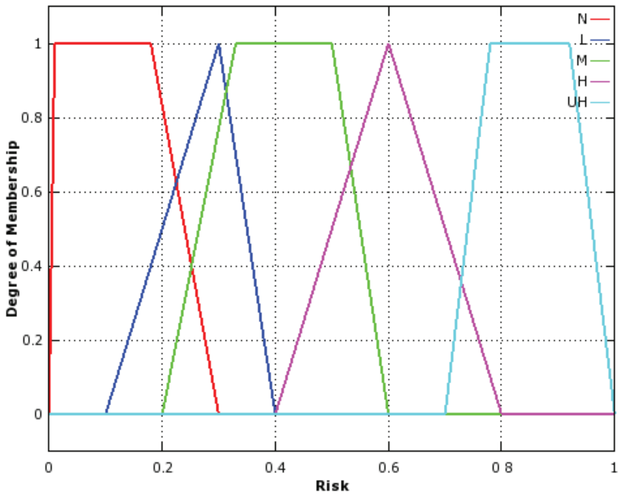

Fig. 4. Fuzzy Sets of Risk

We can first make use of a very basic relation between the past risk score *p*, and the risk *r*, assuming that other input variables are fixed. This relation can be expressed in the following form: if *p* increases, then *r* will not decrease. Thus we could write the following three rules:

1) If (*p* is *L*) then (r is *L*)
2) If (p is *M*) then (r is *M*)
3) If (p is *H*) then (r is *H*)

Then we can develop the 3*3 FAM that will represent the rest of the rules in a matrix form as shown in Fig. 5. Meanwhile, a detailed analysis of the system may enable us to derive 27 rules that represent complex relationships between all variables used in the system. Table II contains these rules.

Lastly, we encode the fuzzy model and tune the system. Probably this is the most laborious step to evaluate and tune the system to let it meet the requirements specified at the beginning. To build our fuzzy expert system, we use Octave Fuzzy Logic Toolkit [14], a mostly MATLAB-compatible fuzzy logic toolkit for Octave. It provides a systematic framework for computing with fuzzy rules and graphical user interfaces.

| | | | | |
|---|---|---|---|---|
| s | | | | |
| HS | H | UH | UH | |
| S | M | M | H | |
| NS | N | N | L | |
| | L | M | H | a |

Fig. 5. FAM Matrix

TABLE II. RULE LIST

| Rule | Input | | | Output |
|---|---|---|---|---|
| | ***a*** | ***s*** | ***p*** | ***r*** |
| 1 | L | NS | L | N |
| 2 | M | NS | L | N |
| 3 | H | NS | L | N |
| 4 | L | S | L | L |
| 5 | M | S | L | L |
| 6 | H | S | L | L |
| 7 | L | HS | L | M |
| 8 | M | HS | L | M |
| 9 | H | HS | L | M |
| 10 | L | NS | M | N |
| 11 | M | NS | M | N |
| 12 | H | NS | M | L |
| 13 | L | S | M | M |
| 14 | M | S | M | M |
| 15 | H | S | M | H |
| 16 | L | HS | M | H |
| 17 | M | HS | M | UH |
| 18 | H | HS | M | UH |
| 19 | L | NS | H | L |
| 20 | M | NS | H | M |
| 21 | H | NS | H | H |
| 22 | L | S | H | UH |
| 23 | M | S | H | UH |
| 24 | H | S | H | UH |
| 25 | L | HS | H | UH |
| 26 | M | HS | H | UH |
| 27 | H | HS | H | UH |

The fuzzy Logic Toolbox can generate surface to help us analyze the system's performance. We can generate a three-dimensional output surface by varying any two of the inputs and keeping other inputs constant. Then we can observe the performance of our three-input one-output system on two three-dimensional plots. Figures 6-8 represent the three-dimensional plots of the system.

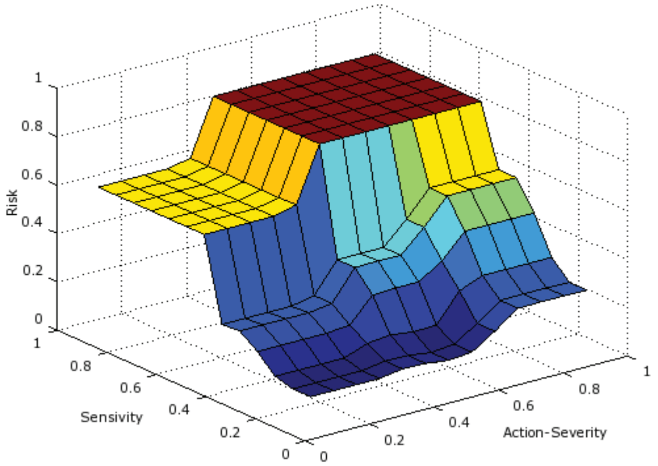

Fig. 6. Three-dimensional Plots of Inference Rules in Terms of Sensitivity and Severity

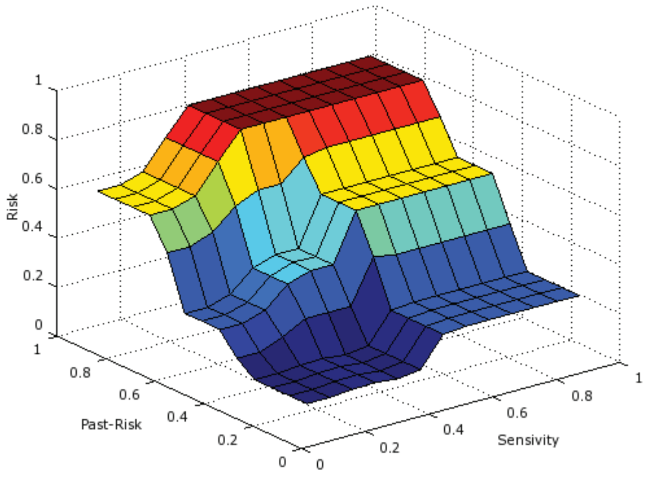

Fig. 7. Three-dimensional Plots of Inference Rules in Terms of Past Risk and Sensitivity

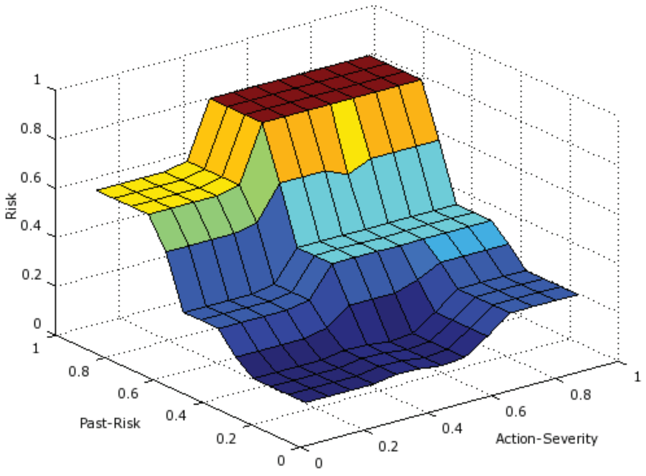

Fig. 8. Three-dimensional Plots of Inference Rules in Terms of Past Risk and Severity

## IV. USING THE FUZZY SYSTEM TO DETERMINE RISKS

The use of fuzzy model developed in Section III to determine risks in eHelath consists of four main steps: Fuzzification, Rule Evaluation, Aggregation, and Defuzzification. Fig. 9 shows the diagram of our fuzzy logic model for a cloud-assisted eHealth system. In the following, we use an example to illustrate how to use the system to evaluate the risk and then make access control decisions. Suppose there is a request for viewing a patient's biographical information. Related to this action, there are three input variable values: the consequence severity of this particular action a1 (0.38), information sensitivity s1 (0.4) and the past risk score of the user, p1 (0.25).

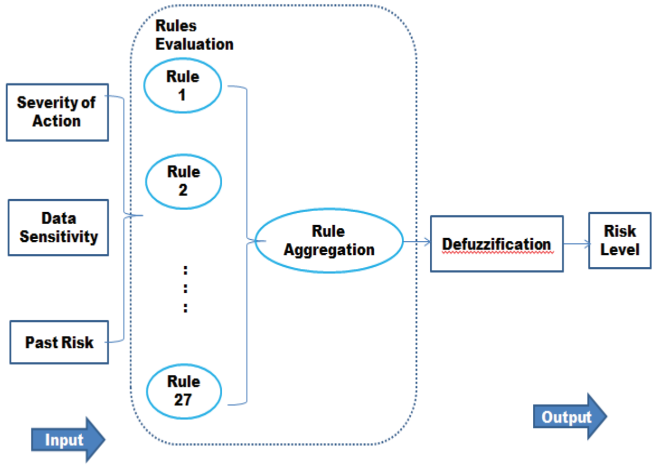

Fig. 9. Diagram of our Fuzzy System

*Step 1: Fuzzification:* The first step is to take the crisp input, *a1*, *s1*, *p1*, and determine the degree to which these inputs belong to each of the appropriate fuzzy set. For example, the crisp input *a1* (severity of action, rated as 38%) corresponds to the membership functions A1 and A2 (low, medium) to the degrees of 0.35 and 0.1 respectively, the crisp input *s1* (sensitivity, rated as 34%) maps the membership functions S1 and S2 (not sensitive, sensitive) to the degree of 0.08 and 0.87 respectively and the crisp input p1 (past risk score, rated as 22%) maps the membership functions P1 of degree 1. In this manner, each input is fuzzified over all the membership functions used by the fuzzy rules.

*Step 2: Rule evaluation:* The second step is to take the fuzzified input *u* (*a*=A2) = medium, u (*s*=S2) = sensitive, u (*p*=P1) = low and apply them to the following fuzzy rule.

<u>Rule 1</u>: If *a1* is low and *s1* is not_sensitive and *p1* is low then risk_score is negligible.

<u>Rule 2</u>: If *a1* is low and *s1* is sensitive and *p1* is low then risk_score is low.

<u>Rule 3</u>: If *a1* is medium and *s1* is not_sensitive and *p1* is low then risk_score is negligible.

<u>Rule 4</u>: If *a1* is medium and *s1* is sensitive and *p1* is low then risk_score is low.

*Step 3: Aggregation of the rule outputs:* Aggregation is the process of unification of the outputs of all rules. In other words, we take the membership functions of all rule consequents previously clipped or scaled and combine them into a single fuzzy set. Thus, the input of the aggregation process is the list of clipped or scaled consequent membership functions, and the output is one fuzzy set for each output variable. If we aggregate the output of the 4 rules mentioned above we will have an aggregated fuzzy output as in Fig. 10 which is low ([0.1 0.4]).

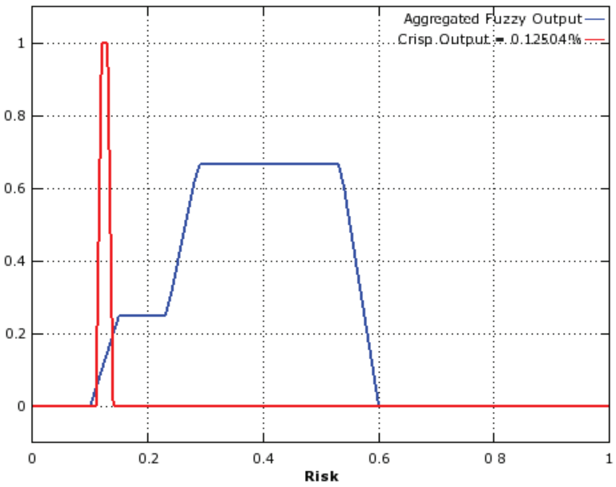

Fig. 10. Aggregated Fuzzy output and Crisp output (considering sensitivity and past-risk)

*Step 4: Defuzzification:* The final output of a fuzzy system has to be a crisp number. The input for the defuzzification process is the aggregate output fuzzy set and the output is a single number. We adopt the most popular method, centroid technique to defuzzifize the output. For example, crisp output z is 0.12504. It means for instance, that the risk involved in our system is 0.12504 percent, which is very low. The risk score determines whether access should be granted or not. If access is granted, the server provides the client with the information client requested.

Our eHealth cloud system architecture consists of clients that communicate with their server located in the cloud (i.e, using Amazon EC2). Health Level Seven (HL7) [15] is used for message transfer in order to achieve interoperability between different healthcare systems and applications. We implement our fuzzy access control model as SOAP-based web service in the Amazon Web Service (AWS) cloud environment.

The above example shows that the fuzzy approach can generate accurate and realistic outcomes in assessing current security risk and forecasting the scope and impact of different risk factors.

## V. CONCLUSION

In this work, a fuzzy-based system is designed to evaluate the risk of healthcare information access. A risk score associated with data sensitivity, action severity, and risk history is determined as a fuzzy value, which is used to determine appropriate controls of healthcare information access in a cloud environment.

Risk-aware access control often uses the knowledge of humans, which is qualitative and inexact. Current risk assessment in eHealth applications are even more complicated because there are no prior data to use in estimating the outcome of the risk factors such as annual loss expected and probability of occurrence breach in eHealth applications. It is very difficult to provide assurance for the risk analysis and justify security measures incorporated. Our approach leverages fuzzy modeling of risk factors and addresses their uncertainties in real applications, which improves the performance of risk assessment methodologies and provides an effective security management. We plan to extend the fuzzy approach to incorporate different trust factors and/or context information for offering a comprehensive access control in eHealth domain.

## REFERENCES.

[1] N. D. Mahant, "Risk Assessment is Fuzzy Business – Fuzzy Logic Provides the Way to Assess Off-site Risk from Industrial Installations", Risk 2004, No. 206.

[2] E. Smith and J. Eloff, "Cognitive Fuzzy Modeling for Enhanced Risk Assessment in Health Care Institution", IEEE Intelligent Systems and Their Applications. March/ April 2000, pp.69-75.

[3] M. Negnevitsky, "Artificial Intelligence. A Guide to Intelligent Systems", Addison-Wesley 2002.

[4] M. Sharma, Y. Bai, S. Chung, and L. Dai, "Using Risk in Access Control for Cloud-Assisted eHealth", In Proceedings of the 2012 IEEE 14th International Conference on High Performance Computing and Communications (HPCC 2012), Liverpool, UK, June 2012, pp.1047-1052.

[5] M. Meglic M and et.al, "Feasibility of an eHealth Service to Support Collaborative Depression Care: Results of a Pilot Study", Journal of Medical Internet Research, Dec. 2010; 12(5):e63.

[6] J. Lin and et.al., "Fine-grained Data Access Control Systems with User Accountability in Cloud Computing", in Proceedings of 2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), Indianapolis, IN, Nov/Dec 2010, pp. 89-96.

[7] R. Wooten, R. Klink, F. Sinek, Y. Bai, and M. Sharma, "Design and Implementation of a Healthcare Social Cloud System", In Proceedings of the 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid 2012), May 2012, Ottawa, Canada, pp.805-810.

[8] Zeng, J., M. An, and N. J. Smith., "Application of a Fuzzy Based Decision Making Methodology to Construction Project Risk Assessment", International Journal of Project Management 25 (6): 589–600, 2007.

[9] M. Barua, X.Liang, R. Lu, and X.Shen, "ESPAC: Enabling Security and Patient-centric Access Control for eHealth in cloud computing", International Journal of Security and Networks, 6 (2), pp. 67-76 (2011).

[10] N. N. Diep, L. X. Hung, Y. Zhung, S. Lee, Y.-K. Lee, and H. Lee, "Enforcing Access Control Using Risk Assessment," in Proceedings of the Fourth European Conference on Universal Multiservice Networks, Toulouse, France, February 2007, pp. 419-424.

[11] N. Mohamed, E. AbuKhousa, J. Al-Jaroodi, "e-Health Cloud: Opportunities and Challenges", Future Internet, Vol. 4(3), 2011, pp.621-645.

[12] Q. Wang and H. Jin "Quantified Risk-Adaptive Access Control for Patient Privacy Protection in Health Information Systems", the 6th ACM Symposium on Information, Computer and Communications Security, Hong Kong, China, Mar. 2011.

[13] W.-H. Au and K.C.C. Chan, Classification with Degree of Membership: A Fuzzy Approach, in: Proc. of the 1stIEEE Int'l Conf. on Data Mining, San Jose, CA, 2001, pp. 35–42.

[14] Octave Fuzzy Logic Toolkit:http://sourceforge.net/projects/octave-fuzzy

[15] Health Level Seven International: http://www.hl7.org/

[16] H. Lohr, A.-R. Sadeghi, and M. Winandy, "Securing the e-health ¨ cloud," in Proceedings of the 1st ACM International Health Informatics Symposium, ser. IHI '10, 2010, pp. 220–229.

[17] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in CCSW '09, 2009, pp. 103–114.

[18] C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," in Journal of Computer Security, 2010.

[19] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in CCS ’06, 2006, pp. 89–98.

[20] M. Li, W. Lou, and K. Ren, “Data security and privacy in wireless body area networks,” IEEE Wireless Communications Magazine, Feb. 2010.

[21] Li M., Logan Yu S., Zheng Y., Ren K., and Lou W. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. Parallel and Distributed Systems, 2012, Issue: 99:1.

[22] A. Sunyaev, J. M. Leimeister, and H. Krcmar. Open security issues in german healthcare telematics. In HEALTHINF 2010 - Proceedings of the 3rd International Conference on Health Informatics, pages 187{194. INSTICC, 2010.

[23] Mrinmoy Barua, Xiaohui Liang, Rongxing Lu, and Xuemin Shen. 2011. ESPAC: Enabling Security and Patientcentric Access Control for eHealth in cloud computing. Int. J. Secur. Netw. 6, 2/3 (November 2011), 67-76.

[24] A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal. “Secure and Scalable Cloud-based Architecture for e-Health Wireless Sensor Networks”. In Proc. of the 21st International Conference on Computer Communication Networks (ICCCN). Munich, Germany. 2012.

[25] S. Kandala, R. Sandhu, and V. Bhamidipati, “An Attribute Based Framework for Risk-Adaptive Access Control Models”, the 6th International Conference on Availability, Reliability and Security, Vienna, Austria, Aug. 2011.

[26] L. Chen and J. Crampton “Risk-Aware Role-Based Access Control”, the 7th International Workshop on Security and Trust Management, Copenhagen, Denmark, Jun. 2011.

[27] M. B. Line, I. A. Tøndel, and E. A. Gjære,“A Risk-Based Evaluation of Group Access Control Approaches in a Healthcare Setting”, the 6th International Conference on Availability, Reliability and Security, Vienna, Austria, Aug. 2011.

[28] R. A. Shaikh, K. Adi, and L Logrippo,“Dynamic Risk-based Decision Methods for Access Control Systems”, Computers & Security, vol. 31, Nr. 4 (2012), pp. 447-464.

[29] Q. Wang and H. Jin “Quantified Risk-Adaptive Access Control for Patient Privacy Protection in Health Information Systems”, the 6th ACM Symposium on Information, Computer and Communications Security, Hong Kong, China, Mar. 2011.

[30] Y. Bai, L. Dai, and J. Li, “Issues and Challenges in Securing eHealth Systems”, International Journal of E-Health and Medical Communications,IGIGlobal.(Forthcoming)