Enhanced Multilevel Fuzzy Inference System for Risk Adaptive Hybrid RFID Access Control System

https://doi.org/10.3991/ijoe.v18i04.27485

Dima Suleiman[1](✉), Malek Al-Zewairi[2], Adnan Shaout[3]
[1] King Abdullah II School for Information Technology, The University of Jordan, Amman, Jordan
[2] Jordan Information Security and Digital Forensics Research Group, Amman, Jordan
[3] The University of Michigan, Dearborn, USA
d.suleiman@psut.edu.jo

Abstract—Risk-based access control systems are part of identity management systems used to accommodate environments with needs for dynamic access control decisions. The risk value is subjected to overestimation or underestimation since it is measured qualitatively, thus; causing uncertainty problems, which was apparent in a previously proposed hybrid risk adaptive (HRA) access control system. Conversely, Fuzzy Inference Systems can deal with the uncertainty of measures and control the outcomes more precisely; therefore, a multilevel fuzzy inference system (HRA-MFIS) was proposed to replace the risk assessment model in HRA. This paper continues to improve the previous model by introducing an enhanced multilevel fuzzy inference system (EHRA-MFIS), which utilizes user behaviour and time analysis to detect anomalous access behaviour. Moreover, it improves the hybrid adaptive risk calculation module by adding authentication, classification and the degree of user anomalous behaviour to the risk calculation algorithm. The results show that the proposed model has smoothed out the transition between the different risk levels and enhanced the system's overall security by considering the failed authorization attempts and failed authentication attempts, asset classification, and user behaviour when calculating the risk level.

Keywords—fuzzy logic, fuzzy inference system, access control, RFID, security, multilevel

1 Introduction

One of the security control systems is the access control system that can prevent unauthorized access of resources by keeping the access points secure. Risk-based access control systems can adapt to the dynamic changes that may require permission changes by updating these permission-based on several factors. The factors may be environmental, operational or situational [1][2]. Furthermore, risk adaptive access control models can be used to balance the benefits and the risks of granting or revoking permission [3].

Radio Frequency Identification (RFID) is a wireless, contactless device that consists of a reader and a tag that can be used in several applications such as personal identification, inventory tracking, e-shipment and gaming [4].

Fuzzy logic can be used in risk-based access control since Fuzzy Inference Systems (FIS) provide significant results with the systems that suffer from uncertainty in risk factors and the imprecise of the assessment process [5][6][7][8]. On the other hand, several problems may emerge because of using fuzzy. The first problem is the scalability that fuzzy inference-based access control uses, where the needed time to calculate the risk value is proportional to the number of variables—another problem related to the damages that the illegitimate users granted access due to underestimating the risk [9]. Also, the time required to deal with tens of parameters and hundreds of fuzzy rules will be high when complex relationships between variables exist.

In this research, an enhanced access control system, which utilizes user behaviour and time analysis to detect anomalous access behaviour and quantifies the risk value using a multilevel fuzzy inference system, is proposed (EHRA-MFIS). The proposed EHRA-MFIS system extends previous hybrid RFID risk adaptive access control systems [10][11] called HRA and HRA-MFIS, respectively. It uses the same systems proposed in [10] and [11]. However, the new model is based on multilayer fuzzy logic [12]. A new layer of fuzzy logic called anomaly FIS has been added. The input of the anomaly FIS is the user behaviour and the time, while the output is the anomaly degree. The anomaly degree fuzzy value and the output of the authorization FIS, the Failed Authorization in addition to the failed authentication and the Classification Level, are fed as input to risk FIS to produce the risk value.

The rest of this paper is organized as follows: the literature is covered in Section 2, while Section 3 provides a brief explanation of the previous models. The proposed model is discussed in Section 4. Section 5 evaluates the proposed model and compares it with the previous models. Finally, the conclusion is presented in section 6.

2 Literature review

Access control is used to control and prevent the access of unauthorized users to the systems and their resources to control the security. In this section, a summary of the related work for both risk-based and fuzzy-based access control is covered.

2.1 Risk-based access control methods

User access privileges remain rigid and static in the Role-Based Access Control (RBAC) model [13]. On the other hand, the model presented in [2] is based on RBAC, allowing dynamic privileges changes by modifying the rules to access remote labs following the VDI/VDE 2182 guideline. The access decision depends on the value of risk and trust. These values were calculated using clearance subject level, history of rewards and penalties and the sensitivity level.

A standard for Extensible Access Control Markup language (XACML) to express access control policies was proposed in [14]. XACML could not quantify the risk directly, and this problem was addressed in [15], where a Risk adaptive eXtensible Access Control Markup Language (RXACML) was proposed. In RXACML, the quantified risk was used to measure the sensitive access request risk. RXACML may cause several problems, such as evaluating unclear performance, managing the permission denied access, and combining the rules and policies results.

The risk of access control was measured using the risk, trust and access metrics as in [16]; also, access control was determined using the combination between the metrics of risk and the trust by proposing Access Control in Cloud Federation using Learning Automata (ACCFLA). The security level was divided into four values including {secret, top-secret, classified and unclassified}. The security level was determined by sorting the sensitivity values determined for each security level. Furthermore, to determine whether to grant the users rewards or penalties, the user's experience of utilizing resources must be determined.

The level of the risk was used to determine the model of a risk adaptive hybrid RFID access control, whether it is serverless or server-based access modes [10]. The risk value was determined based on five factors: time, classification level, number of failed authentications, clearance level, and number of failed authorizations.

A multi-keyed model enhanced the security by using dynamic symmetric encryption was proposed in [17]. Their work utilized the same structure, authentication and identification, which was proposed in [11]. The experimental results showed enhanced security; on the other hand, there was a delay in processing time.

2.2 Fuzzy logic access control methods

In order to increase the information sharing while keeping the accountability of the users, the fuzzy Multi-Level Security (MLS) was used in [18]. Using MLS helps facilitate the risk information flow and quantify the risk efficiently.

The risk can be classified according to the difference between the subject and object security levels. If the difference between them is high, then the risk will be classified as high, while if the difference between them is low, the risk will be low. The model of MLS that considered this classification of the security level was proposed in [9]. There are four categories of security labels, including secret, top-secret, classified and unclassified. Fuzzy logic was used to define the values of security categories to overcome the problems of overestimation and underestimation that may occur by using crisp values.

The access control of medical information in a cloud environment had a high risk assessed using fuzzy logic was proposed in [19]. The component of the fuzzy logic module consists of three input variables and one output variable. The input variables are the past risk, the data sensitivity and the action consequences severity, while the output variable is the risk. Each of the past risk and action consequences severity variables had three linguistic values: low, medium and high, whereas the data sensitivity had three values that were not sensitive, sensitive, or highly sensitive. On the other hand, the risk variable had five linguistic values: unacceptable high, high, moderate, low, and negligible. Trapezoidal and triangle are used as membership functions. Also,

Mamdani's fuzzy inference method is used with a total number of rules equal to 27, and finally, for the defuzzification, a centroid is used. The proposed fuzzy model was evaluated using a set of services such as SOAP-based web service, Amazon EC2 cloud service, and Health Level Seven (HL7) protocol for message transfer.

In [20], the risk value was calculated by modifying the risk assessment phase in the RIPRAN (Risk Project Analysis) methodology. The model consisted of two input variables: the number of sub-risk and the total value of sub-risks and one output variable, the total value of project risk. Also, the model variables had five linguistic values: very low, low, middle, high and very high. The membership function that was used is trapezoidal. Furthermore, Mamdani's is used with 25 rules.

The risk of different cyber security threats was assessed in [21]. The assessment was made using a multilevel fuzzy inference system, where three fuzzy controllers were used. The first controller used the potential capabilities, target and intent of the threat agent to calculate the overall capabilities of that threat. The second controller had three input variables, the first input was the vulnerabilities, the second input was action, and the last one was the success likelihood; the output of the second controller was the threat likelihood. The last controller took the input from the previous controllers and the impact of the threat as another input; the output of this controller was the scale of the risk.

A binary decision of whether to grant or deny access using FIS was proposed in [22]. Since the access decision is binary, Mamdani FIS was used because it is the most adaptable tool for binary decisions. A comparative study between the previously mentioned approaches is presented in Table 1.

Table 1. Comparisons of fuzzy logic risk access control and risk access control methods

Ref.	Access Control Method	Technique	Static / Dynamic	Benefits	Limitations
[22]	Fuzzy access control with binary decision	FIS	Dynamic	-	It cannot easily be used to handle sensitive data
[17]	Multilayer fuzzy logic risk adaptive MAC using	Multilayer fuzzy logic with Multi-keyed model	Dynamic	-	-
[11]	Multilayer fuzzy logic risk adaptive MAC	Multilayer fuzzy logic	Dynamic	Adapt the risk with dynamic, imprecise and uncertain factors, while decreasing the number of rules	-
[10]	Risk adaptive MAC	Alternate dynamically between server-based and serverless mode based on the level of risk	Dynamic	Scalability, and good performance	The entire space of scenarios of the risk is difficult to study
[21]	Fuzzy inference, multilevel security (MLS)	Three fuzzy controllers have been used	Dynamic	The model is more realistic and can deal with imprecise	-

				system measurements	
[16]	Risk and trust matrices	Dividing the security into four levels and calculating the trust values	Dynamic	Using the amount of experience on dealing with the resources to give penalties or rewards	-
[19]	fuzzy logic module	Using Mamdani's FIS and generating 27 rules	Dynamic	Improve security on real uncertain applications	Cannot incorporate context information in addition to trust limitations
[23]	Radio Frequency Identification (RFID)	Using offline and online access control without backend database	Dynamic	Low complexity and cost, high availability and security	Practical data transfer time cannot be achieved without a high data transfer rate. Cannot operate on multi authorization level
[2]	Trust and risk values	Use penalties, reward history, subject sensitivity, and clearance levels to calculate risk and trust values	Dynamic	There are no tunable parameters for calculating risk and trust values	Considering the subject past behaviour
[9]	Fuzzy inference, multilevel security (MLS)	Using the difference between object and subject security level the classify the risk to high or low	Dynamic	Provable correct solution	Overestimation or underestimation of the sensitivity of the documents
[15]	Extensible markup language	Using policies and rules for risk adaptation	Dynamic	Quantified risk is covered	Hard to combine the results of rules with policies, in case of denied access, it is hard to manage the risk
[25]	Extensible markup language	Using the enforcement point policy	Static	A framework that is powerful and standardizes	The quantified risk is not supported
[18]	Fuzzy inference, multilevel security (MLS)	Using quantified risk and risk tolerance to determine the action where the risk scale is divided into band	Dynamic	Keeping the accountability while increasing the sharing of information	The factors that affect the risk must be considered by tuning the parameters

3 Previous design

This research extends the previous work in [10], which proposed a risk adaptive hybrid system (HRA) based on RFID access control. The main idea was to keep the high availability and simplicity of the system by decreasing the restriction of security level control when the risk level is low [23]. On the other hand, when the risk level is high, a high level of authentication is required. The system used a new multi-modules subsystem in the enterprise subsystem [24] called the Risk Engine subsystem.

Risk Engine is used to implement the adaptive risk features of the access control system. This subsystem comprises three modules: Risk Analysis, Risk Rule, and Decision Making. The Risk Analysis module calculates the risk value using Equation (1). The calculation is based on five risk factors: the number of failed authentication attempts, the number of failed authorization, the level of location classification, the time indicator, and the user clearance. Furthermore, the risk policy is defined by the Risk Rule Module, which consists of a set of rules, the risk acceptable level, and the risk scale. Finally, the outputs of the previous modules are fed as input to the Decision Making Module, which is responsible for alternating between offline and online access modes and granting and revoking the permissions of accessing the system.

$$Risk = Max\left(\frac{\frac{Authentication_{Fail}}{Maximum_{Fail}}+\frac{Authorization_{Fail}}{Maximum_{Fail}}+\frac{Clearance}{Maximum_{Level}}+\frac{Classification}{Maximum_{Level}}+Time_{Indicator}}{Risk_{Factors}}\right) \quad (1)$$

In addition, the proposed model extends the HRA-MFIS model proposed in [11]. Their work used the fuzzy logic system to change the risk rule module. They used two layers of fuzzy inference systems: the authorization FIS and the risk FIS. The inputs of the authorization FIS are the clearance and classification levels. The inputs for the risk FIS are the authentication, classification level, and the authorization FIS output, which is the authorization.

4 Proposed design

Fuzzy logic can solve the problem of the imprecise value of the access control risk factors and their uncertainty. This paper proposes a new access control model (EHRA-MFIS) based on the previous model proposed by [11], which also uses multilayer fuzzy logic. Instead of using two FIS, the proposed model uses three FIS: authorization FIS, anomaly FIS, and risk FIS. The proposed EHRA-MFIS model makes enhancements in terms of efficiency and deals with the uncertainty of the risk value. More details about the new design are discussed in the following subsections.

4.1 Fuzzy system architecture

The risk access control is designed using the Fuzzy Logic Controller. The EHRA-MFIS consists of two layers of fuzzy logic where the first layer has two FIS: the authorization FIS and the anomaly FIS, while the second layer has the risk FIS. The system consists of six variables which are five inputs and one output. The number of rules of the proposed systems will be determined based on the number of values of each variable where the generated rules are stored in the knowledge-based system.

After generating the rules, the Mamdani model aggregates all generated rules in the three FIS. Finally, the Mean of Max (MOM) defuzzification converts the fuzzy values into crisp values. The proposed access control model architecture can be seen in Figure 1. The proposed model consists of two layers: the first layer consists of two FIS, the authorization FIS and the anomaly FIS, while the second layer consists of the risk FIS. The model is implemented using MATLAB. Table 2 shows the details of the FIS variables, their values, and the universe of discourse.

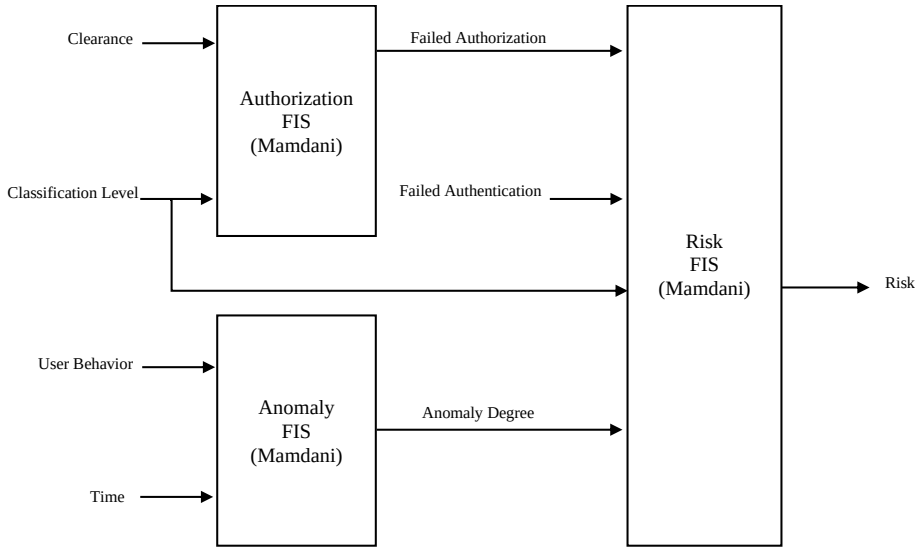

Fig. 1. Proposed EHRA-MFIS architecture

Table 2. Fuzzy input and output linguistics variables and values

Fuzzy Linguistic Variable	MFIS Level	Input / Output	Linguistic Value	Universe of Discourse
Clearance	L1	Input	{Unclassified, Public, Confidential, Secret, Top-Secret}	1 <= X <= 5
Classification	L1	Input		
User behaviour	L1	Input	{Intruder, Authorized}	0 <= X <= 1
Time	L1	Input	{Morning, Noon, Evening, Midnight}	0 <= X <= 2400
Anomaly Degree	L1	Output	{Low, Medium, High}	0 <= X <= 1
Authorization	L1	Output	{None, Low, Medium, High}	0 <= X <= 3
Authorization	L2	Input		

Authentication	L2	Input		
Classification	L2	Input	{Unclassified, Public, Confidential, Secret, Top-Secret}	1 <= X <= 5
Risk	L2	Output	{Insignificant, Very-Minor, Minor, Very-Low, Low, Moderate, High, Very-High, Major, Extreme}	0 < X <=100

4.2 Fuzzy linguistic variables

The proposed EHRA-MFIS model consists of five inputs: Clearance, Classification, User behaviour, Time, and Authentication (failed attempts). It also consists of one output which is the Risk value. The inputs of the authorization FIS are the Clearance and the Classification, while the output is the failed authorization level. On the other hand, the inputs of the anomaly FIS are user behaviour and time, while the output is the Anomaly Degree. The output of the authorization FIS, the anomaly FIS, the classification level, and the failed authentication attempts is fed as input to the risk FIS.

In authorization FIS, the values of the two membership variables (Clearance and Classification) are {unclassified, public, confidential, secret, and top secret} where each value is represented using Trapezoidal as shown in Figures 2, 3 and 4. The output of the authorization FIS is the fuzzy variable authorization that has four values {None, Low, Medium, High} which are also represented by Trapezoidal as shown in Figure 5. After determining the input and output variables and their values, we used the Mamdani model and maximum function for aggregation. Finally, for defuzzification, we used Mean of Max (MOM). The total number of rules resulting from the Authentication FIS is 18 rules shown in Table 3.

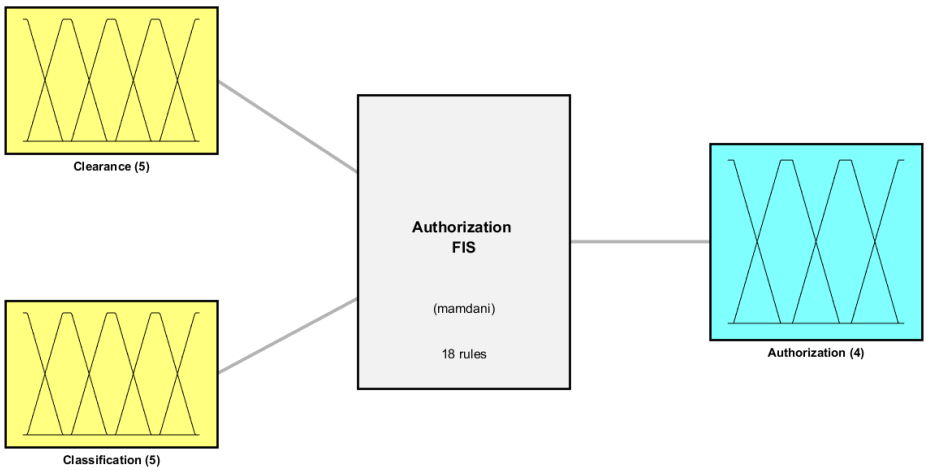

Fig. 2. Authorization FIS: 2 inputs, 1 output and 18 rules

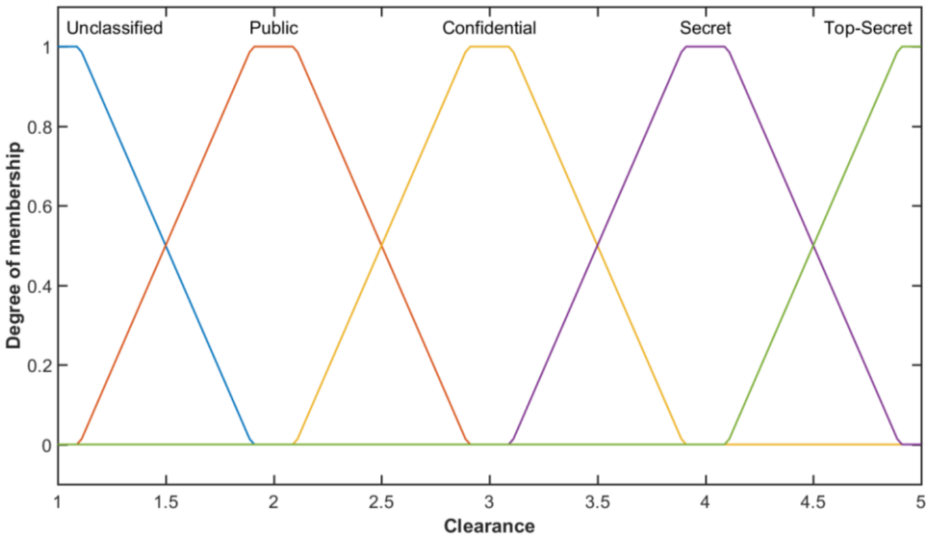

Fig. 3. Authorization FIS: Clearance membership function (input)

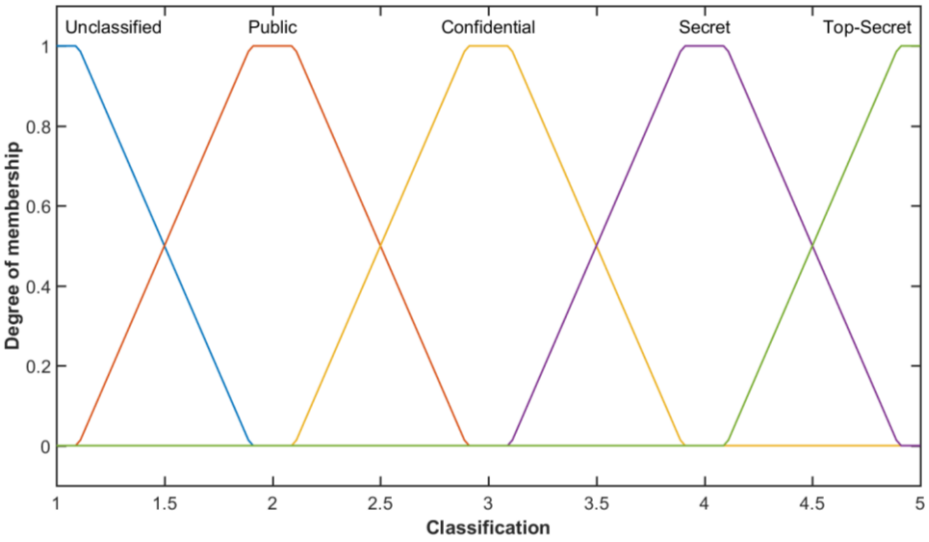

Fig. 4. Authorization FIS: Classification membership function (input)

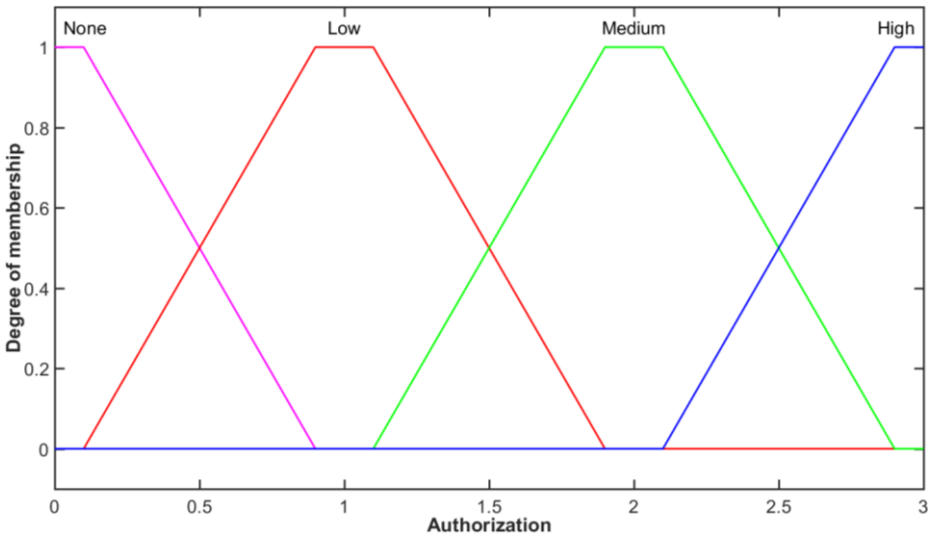

Fig. 5. Authorization FIS: Authorization membership function (output)

Table 3. Fuzzy rules of authorization FIS

Rules
Clearance = Unclassified & Classification = Unclassified → Authorization = None
Clearance = Unclassified & Classification = Public → Authorization = Low
Clearance = Unclassified & Classification = Confidential → Authorization = Medium
Clearance = Unclassified & Classification = Secret → Authorization = High
Clearance = Unclassified & Classification = Top-Secret → Authorization = High
Clearance = Public & Classification = Unclassified → Authorization = None
Clearance = Public & Classification = Public → Authorization = None
Clearance = Public & Classification = Confidential → Authorization = Low
Clearance = Public & Classification = Secret → Authorization = Medium
Clearance = Public & Classification = Top-Secret → Authorization = High
Clearance = Confidential & Classification = Unclassified → Authorization = None
Clearance = Confidential & Classification = Public → Authorization = None
Clearance = Confidential & Classification = Confidential → Authorization = None
Clearance = Confidential & Classification = Secret → Authorization = Low
Clearance = Confidential & Classification = Top-Secret → Authorization = Medium
Clearance = Secret & Classification = Not Top-Secret → Authorization = None
Clearance = Secret & Classification = Top-Secret → Authorization = Low
Clearance = Top-Secret → Authorization = None

In anomaly FIS, there are two member variables: User behaviour and time, as shown in Figure 6. The values of the User behaviour are {Intruder, Authorized} while the values of the time are {Morning, Noon, Evening, Midnight}. The user behaviour values

are represented using the Gaussian membership function, as shown in Figure 7. In addition, the Triangle membership function represents the values of the time, as shown in Figure 8. Furthermore, the Triangle membership function is used to represent the values of the Anomaly degree output which has three values {Low, Medium, High} as shown in Figure 9. Also, in anomaly FIS, Mamdani is used for aggregation and MOM is used for defuzzification. The total number of rules resulting from the anomaly FIS is eight, as shown in Table 4.

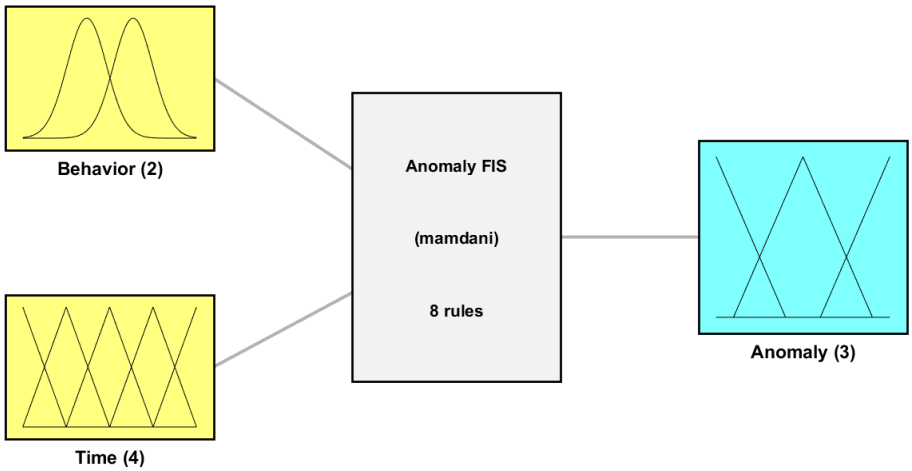

Fig. 6. Anomaly FIS: 2 inputs, 1 output and 8 rules

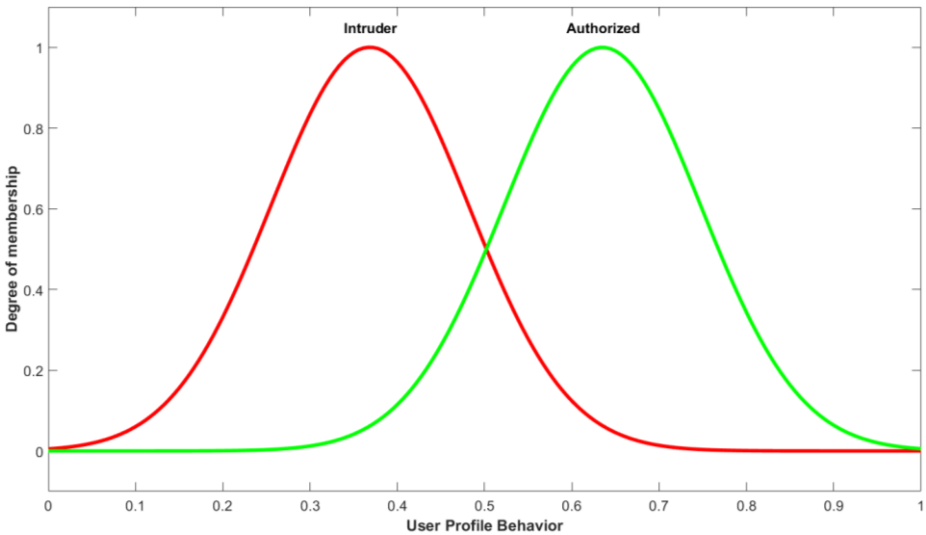

Fig. 7. Anomaly FIS: behaviour function (input)

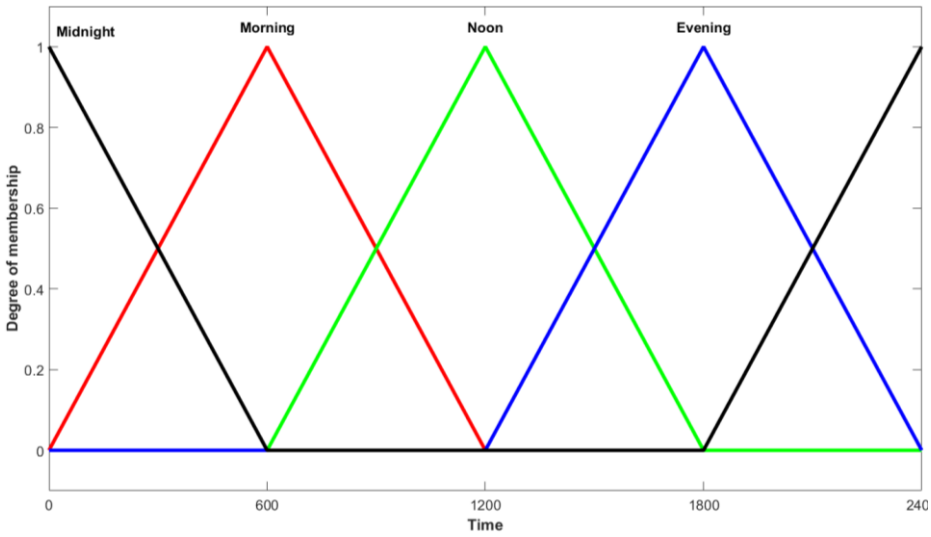

Fig. 8. Anomaly FIS: Time Function (Input)

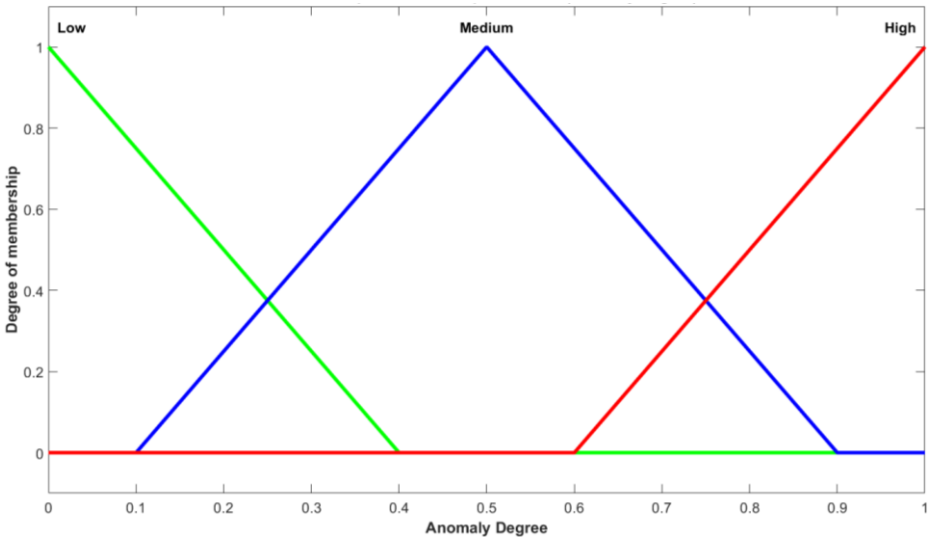

Fig. 9. Anomaly FIS: Anomaly degree (output)

Table 4. Fuzzy rules of anomaly FIS

Rules
Behaviour = Intruder & Time = Morning → Anomaly = Low
Behaviour = Intruder & Time = Noon → Anomaly = Medium
Behaviour = Intruder & Time = Evening → Anomaly = High
Behaviour = Intruder & Time = Midnight → Anomaly = High
Behaviour = Authorized & Time = Morning → Anomaly = Low

Behaviour = Authorized & Time = Noon → Anomaly = Low
Behaviour = Authorized & Time = Evening → Anomaly = Medium
Behaviour = Authorized & Time = Midnight → Anomaly = High

The Authorization level layer and Anomaly level layer outputs are fed as inputs to the Risk layer. The other two inputs are the Classification level and the authentication. The classification level is the same as the one that was one of the inputs of the Authentication level. The values of the authentication membership variable are {none, low, medium, high} shown in Figure 10. Finally, the output of the proposed EHRA-MFIS model is the risk level layer which may have one of the tenth values {Insignificant, Very-Minor, Minor, Very-Low, Low, Moderate, High, Very-High, Major, Extreme} as shown in Figure 11. Again, in this layer, Mamdani is used for aggregation and MOM is used for the defuzzification process, as shown in Figure 12.

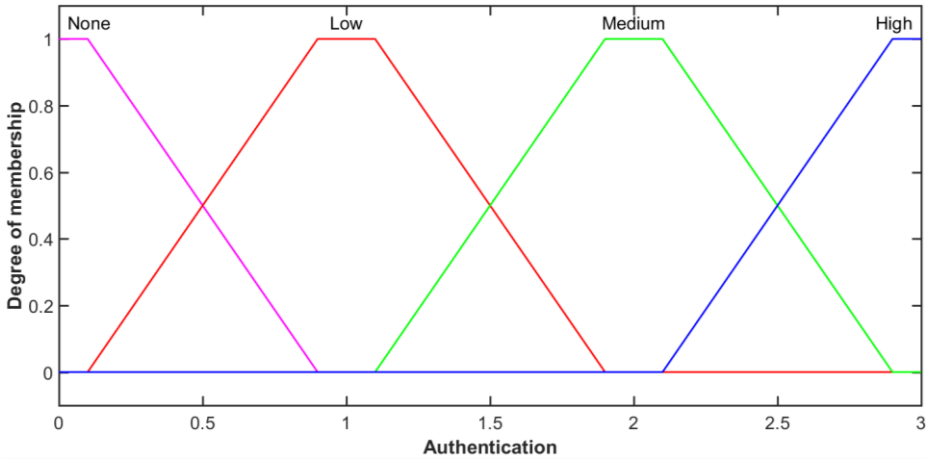

Fig. 10. Risk FIS: Authentication membership function (input)

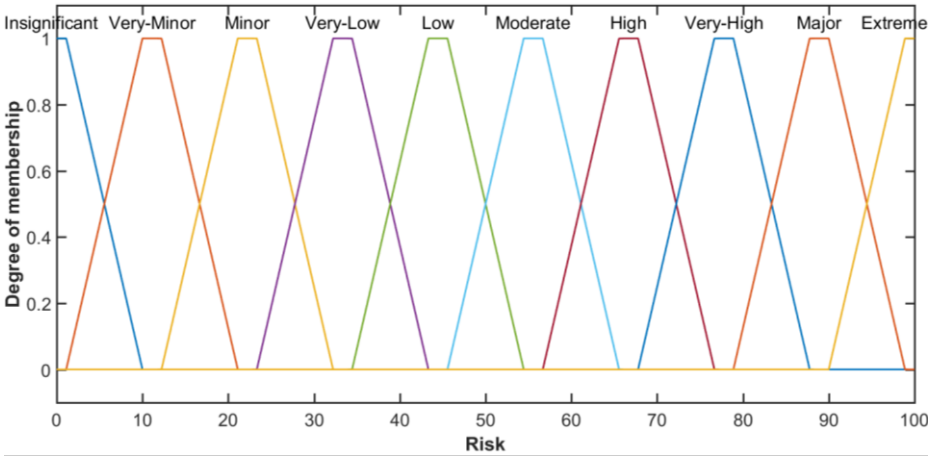

Fig. 11. Risk FIS: Risk membership function (output)

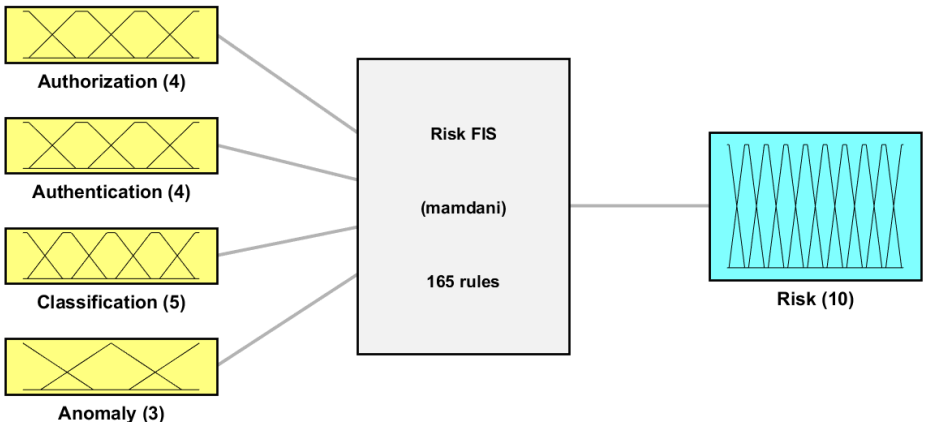

Fig. 12. EHRA-MFIS Risk FIS: 4 inputs, 1 output, and 165 rules

5 Evaluation

This section provides a brief description of the proposed EHRA-MFIS access control model. After that, we evaluate and discuss the results of the proposed model. Finally, comparisons between it and the previous models have been performed. The proposed model was designed using Matlab Fuzzy Logic Toolbox. Each FIS model is implemented separately; since Matlab does not support the multilayer fuzzy system.

Firstly, both the authorization FIS and anomaly FIS are evaluated; after that, the risk FIS is engaged to give an access decision based on the authorization and anomaly FISs. The output of the authorization FIS is the failed authorization which indicates the degree of failed authorization and if it occurs or not. Furthermore, failed authorization occurs when lower-level clearance tries to access higher-level classification. On the other hand, the second input of risk FIS, the failed authentication, occurs when invalid identifications such as fingerprint or passcode are used.

5.1 Risk visualization

Firstly, we studied the effect of changing the anomaly and the classification values on the risk, where the authentication and authorization values are set to "None", then to "High", and the results are shown in Figures 13, 14 respectively, using risk heat maps. In Figure 13, the authentication and authorization values were set to the lowest (i.e., "None"). In this case, the risk value varies from insignificant to high. The risk value is insignificant when the object is unclassified, and the anomalous behaviour is at its lowest value. On the other hand, when the object is classified as top-secret, and the anomalous behaviour is high, the risk value is high.

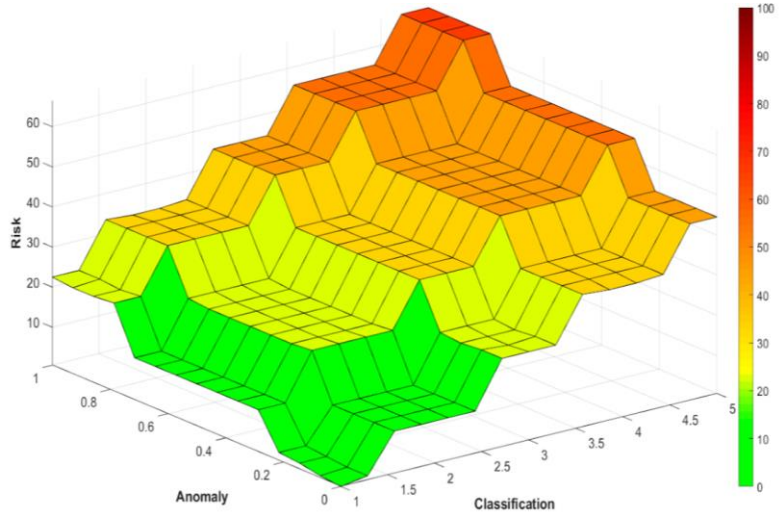

Fig. 13. Risk heat map where the authentication and the authorization value are "None"

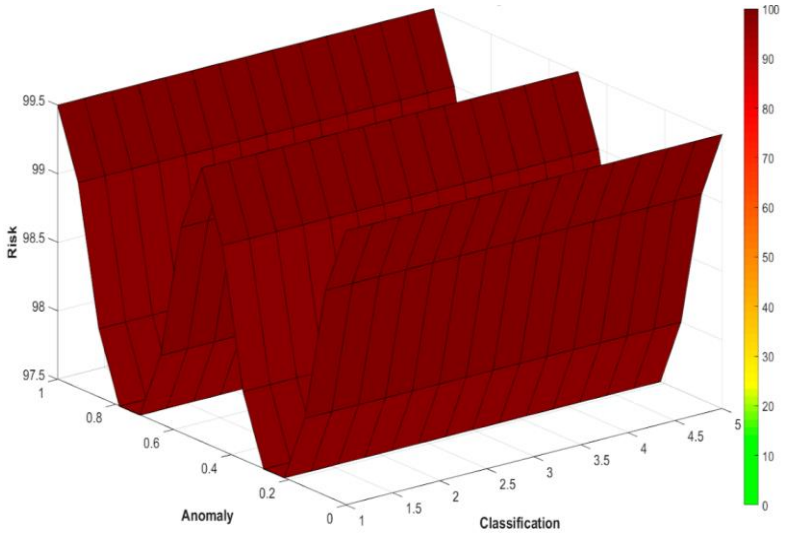

Fig. 14. Risk heat map where the authentication and authorization value is "High"

In Figure 14, both the authentication and the authorization values were set to "high". In this case, the risk value is always set to "extreme"; regardless of the degree of anomaly or the classification level.

Secondly, we studied the impact of the change in authentication and authorization on the risk value, where the classification level is at its highest value (i.e., top-secret). Three use cases were developed: 1) when the anomaly degree is at its lowest value (i.e., a= 0.0). 2) when the anomaly degree is medium (i.e., a=0.5). 3) when the anomaly

degree is at the highest value possible (i.e., a=1). The results are shown in Figures 15-17, respectively, using risk heat maps to show the change in risk value.

The first case covers the risk when the required access classification is top-secret - that is, the highest- and there is no apparent anomalous behaviour. In this case, the risk value varies from low to critical, mainly based on the authentication failure where it dictates the risk value when the authorization level is < 2.25, as shown in Figure 15.

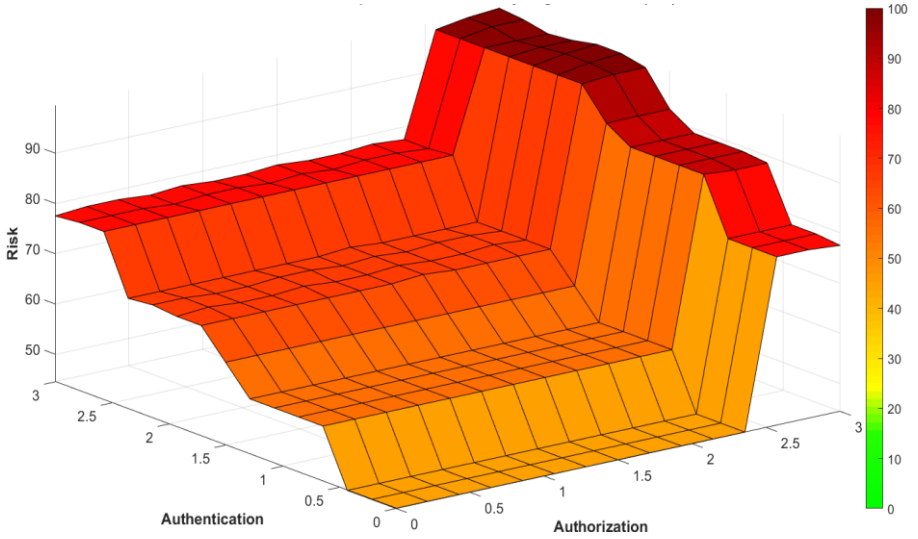

Fig. 15. Risk heat map where the classification level is "Top-Secret" and the Anomaly degree is "Low" (a=0.0)

In Figure 16, the second case where the access behaviour is considered moderately anomalous (i.e., medium, a=0.5) and the access classification level is at the highest level (i.e., top-secrete). Based on the access authentication and authorization values, the access risk value ranges from moderate to extreme, where the latter occurs when authentication fails with high certainty and the authorization level is at the highest degree.

Finally, the most extreme case, where the access classification level is the highest (i.e., top-secrete) and the access behaviour is considered anomalous to a high degree of certainty (i.e., high, a=1), is presented in Figure 17. In this case, the risk value ranges between High and Extreme based on the clearance level (i.e., authorization) and the level at which the authentication failed.

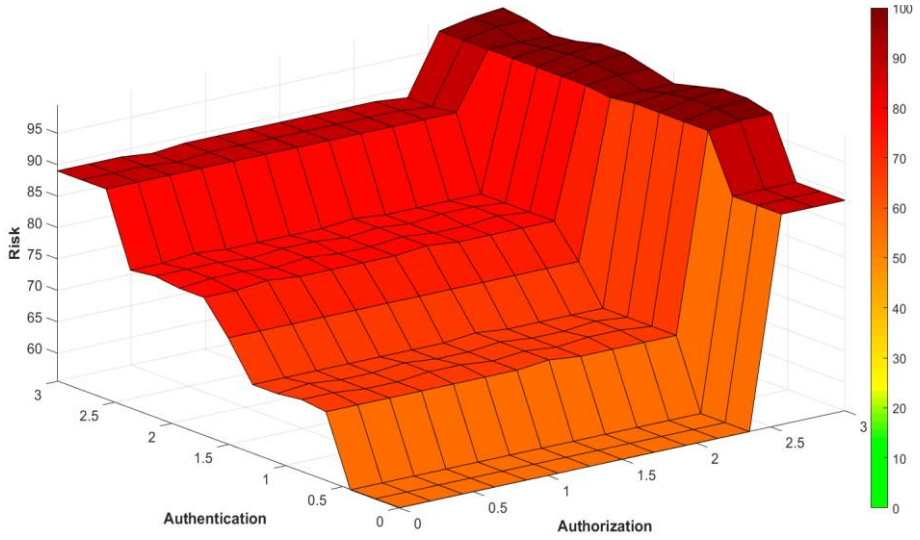

Fig. 16. Risk heat map where the classification level is "Top-Secret" and the Anomaly degree is "Medium" (a=0.5)

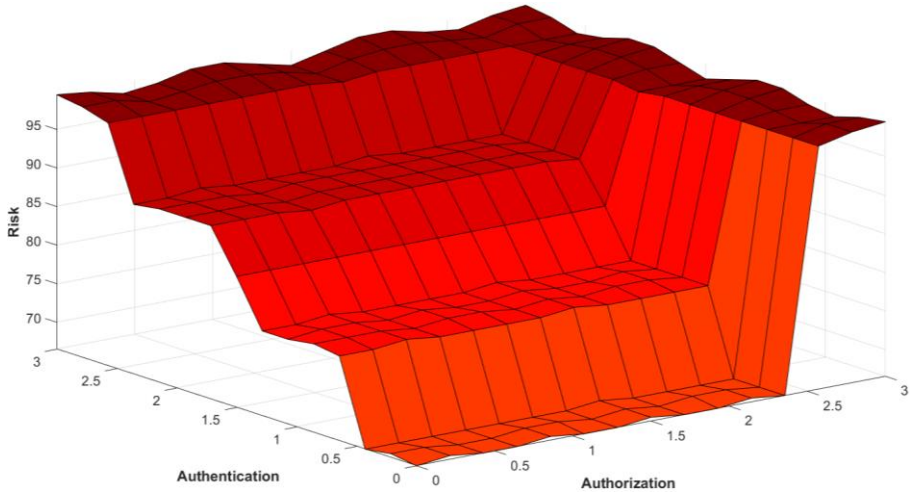

Fig. 17. Risk heat map where the classification level is "Top-Secret" and the Anomaly degree is "High" (a=1)

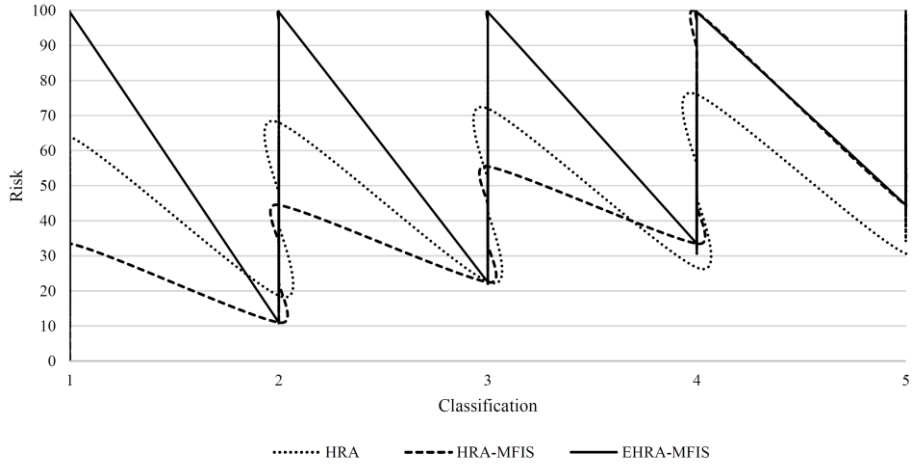

Fig. 18. Comparison between HRA, HRA-MFIS and EHRA-MFIS, where 1: Unclassified, 2: Public, 3: Confidential, 4: Secret, 5: Top-Secret

5.2 Comparison with previous models

As shown in Figure 18, when comparing the three risk-based systems (i.e., HRA, HRA-MFIS, and EHRA-MFIS), one can conclude that the newly proposed EHRA-MFIS system provides a smoother transition between the different risk levels as well as improved security by introducing the degree of anomalous behaviour as an input to the system. Furthermore, EHRA-MFIS cover the risk at a more significant range than HRA and HRA-MFIS at each classification level; thus, being more inclusive than the other two models. The addition of the anomalous FIS allows the proposed model to calculate the risk value more precisely by considering the user behaviour while calculating the risk value.

6 Conclusion

In this research, an enhanced multilayer fuzzy system, namely EHRA-MFIS, was proposed for risk access control systems. Fuzzy logic provided significant results when dealing with imprecise and uncertain risk values. The proposed EHRA-MFIS model consists of two layers. The first layer has two FIS: authorization and anomaly FISs. On the other hand, the second layer consists of risk FIS. The proposed system results showed that the uncertainty of the risk value was addressed using dynamic factors. The difference between this model and the previous model is the anomaly FIS added to the first layer. This addition enhanced the smooth transition between the risk levels and improved the overall security of the access control system.

7 References

[1] Ahmed, A., & Zhang, N. (2009). Towards the realisation of context-risk-aware access control in pervasive computing. Telecommunication Systems, 45(2-3), 127–137. https://doi.org/10.1007/s11235-009-9240-3

[2] D. Uckelmann et al., "Guideline to Safety and Security in Federated Remote Labs," Int. J. Onl. Eng., vol. 17, no. 04, p. 39, Apr. 2021. https://doi.org/10.3991/ijoe.v17i04.18937

[3] Shaikh, R. A., Adi, K., Logrippo, L., & Mankovski, S. (2011). Risk-based decision method for access control systems. In 2011 Ninth Annual International Conference on Privacy, Security and Trust (PST) (pp. 189–192). http://doi.org/10.1109/PST.2011.5971982

[4] Benssalah, M., Djeddou, M., & Drouiche, K. (2014). Security enhancement of the authenticated RFID security mechanism based on chaotic maps. Security and Communication Networks. https://doi.org/10.1002/sec.946

[5] Y. Bai, J. Xu, Y. Bai, and J. Xu, (2018), "Access Control Scheme Based on Fuzzy Identity in Opportunistic Network", 8th International Congress of Information and Communication Technology (ICICT-2018). https://doi.org/10.1016/j.procs.2018.04.278

[6] S. Rizvi, J. Mitchell, A. Razaque, M. R. Rizvi, and I. Williams, (2020) "A fuzzy inference system (FIS) to evaluate the security readiness of cloud service providers," Journal of Cloud Computing 9(1). https://doi.org/10.1186/s13677-020-00192-9

[7] X. Huang and W. Xu, "Method of Information Security Risk Assessment Based on Improved Fuzzy Theory of Evidence," Int. J. Onl. Eng., vol. 14, no. 03, p. 188, Mar. 2018. https://doi.org/10.3991/ijoe.v14i03.8422

[8] K. Almohammadi, "Conceptual Framework Based On Type-2 Fuzzy Logic Theory for Predicting Childhood Obesity Risk," Int. J. Onl. Eng., vol. 16, no. 03, p. 95, Mar. 2020. https://doi.org/10.3991/ijoe.v16i03.12701

[9] Ni, Q., Bertino, E., & Lobo, J. (2010). Risk-based Access Control Systems Built on Fuzzy Inferences. In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (pp. 250–260). New York, NY, USA: ACM. https://doi.org/10.1145/1755688.1755719

[10] Al-Zewairi, M., Alqatawna, J.' far, & Atoum, J. (2015). Risk adaptive hybrid RFID access control system. Security and Communication Networks, 8(18), 3826–3835. https://doi.org/10.1002/sec.1303

[11] M. Al-Zewairi, D. Suleiman, and A. Shaout, "Multilevel Fuzzy Inference System for Risk Adaptive Hybrid RFID Access Control System," in 2016 Cybersecurity and Cyberforensics Conference (CCC), 2016, pp. 1–7. https://doi.org/10.1109/CCC.2016.9

[12] Shaout, A., & Al-Shammari, M. (1998). Fuzzy logic modeling for performance appraisal systems: A framework for empirical evaluation. Expert Systems with Applications, 14(3), 323–328. https://doi.org/10.1016/S0957-4174(97)00085-7

[13] Ferraiolo, D. F., Kuhn, D. R., & Chandramouli, R. (2003). Role-Based Access Control. Norwood, MA, USA: Artech House, Inc.

[14] Alqatawna, J., Rissanen, E., & Sadighi, B. (2007). Overriding of Access Control in XACML. In Eighth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'07) (pp. 87–95). https://doi.org/10.1109/POLICY.2007.31

[15] Chen, C., Han, W., & Yong, J. (2010). Specify and enforce the policies of quantified risk adaptive access control. In 2010 14th International Conference on Computer Supported Cooperative Work in Design (CSCWD) (pp. 110–115). https://doi.org/10.1109/CSCWD.2010.5471991

[16] Behnaz Seyed Taheri, Mostafa Ghobaei Arani, & Mehrdad Maeen. (2014). ACCFLA: Access Control in Cloud Federation using Learning Automata. International Journal of Computer Applications, 107(6), 30–40. https://doi.org/10.5120/18758-0028

[17] M. Al-Zewairi and S. Hamdan and M. Al-Fayoumi, (2017), "Enhanced Multi-keyed Risk Adaptive Hybrid RFID Access Control System", ACIT'2017 The International Arab Conference on Information Technology.

[18] Cheng, P. C., Rohatgi, P., Keser, C., Karger, P. A., Wagner, G. M., & Reninger, A. S. (2007). Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control. In 2007 IEEE Symposium on Security and Privacy (SP' 07) (pp. 222–230). https://doi.org/10.1109/SP.2007.21

[19] Li, J., Bai, Y., & Zaman, N. (2013). A Fuzzy Modeling Approach for Risk-Based Access Control in eHealth Cloud. In 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (pp. 17–23). http://doi.org/10.1109/TrustCom.2013.66

[20] Doskočil, R. (2015). An Evaluation of Total Project Risk Based on Fuzzy Logic. Verslas: Teorija Ir Praktika, 15(2), 23–31. http://doi.org/10.3846/btp.2016.534

[21] Hany Sallam. (2015). Cyber Security Risk Assessment Using Multi Fuzzy Inference System. International Journal of Engineering and Innovative Technology, 4(8), 13–19.

[22] D. D. Regateiro, Ó. M. Pereira, and R. L. Aguiar (2019), "BDFIS: Binary Decision Access Control Model Based On Fuzzy Inference Systems", The 31st International Conference on Software Engineering and Knowledge Engineering. 503-508. https://doi.org/10.18293/SEKE2019-039

[23] Al-Zewairi, M., Alqatawna, J., & Al-Kadi, O. (2011). Privacy and Security for RFID Access Control Systems: RFID Access Control Systems without backend database (pp. 272–277). Presented at the 2011 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT), Amman, Jordan: IEEE. http://doi.org/10.1109/AEECT.2011.6132520

[24] Karygiannis, T., Eydt, B., Barber, G., Bunn, L., & Phillips, T. (2007). Guidelines for Securing Radio Frequency Identification (RFID) Systems. National Institute of Standards and Technology Special Publication. https://doi.org/10.6028/NIST.SP.800-98

[25] S. Godik and T. Moses, "eXtensible Access Control Markup Language (XACML)," ACM Standardview - STANDARDVIEW, 2003.

8 Authors

Dima Suleiman received her BSc degree in 2002 and MSc degree in 2004 in Computer Science from the University of Jordan. In 2020, she received her PhD degree from Princess Sumaya University for Technology in Computer Science. In 2005, she started her academic journey at Jordan University as a full-time instructor until now. Her research interests are in Artificial Intelligent, Algorithms, Natural Language Processing, Data Science, machine learning and Data Mining (email: d.suleiman@psut.edu.jo).

Malek Al-Zewairi is a senior manager and a subject-matter expert for Professional Development at PwC's Academy Middle East. He has over ten years of experience in information security, digital forensics, incident response and ethical hacking. During his career, he worked in several fields of information security, including security operation, auditing, training, consultation and academia. Malek is a certified trainer for various certification bodies. In 2021, he received his PhD degree in Computer Science

from Princess Sumaya University for technology, focusing on intelligence and security informatics (email: m.alzewairi@jisdf.org).

Adnan Shaout is a full professor in the Electrical and Computer Engineering Department at the University of Michigan – Dearborn. At present, he teaches courses in embedded systems, cloud computing, software engineering methods, fuzzy logic and engineering applications and computer engineering (hardware and software) (email: shaout@umich.edu).

Article submitted 2021-10-11. Resubmitted 2021-12-21. Final acceptance 2022-01-09. Final version published as submitted by the authors.