Karafan

Quarterly Scientific Journal of National University of Skills

Autumn 2024, Vol. 21, No. 3, p. 85-110

Journal Homepage: https://karafan.nus.ac.ir/?lang=en

doi:10.48301/KSSA.2024.445634.2848

# Designing a Fuzzy Expert System to Investigate the Impact of Biometric Indicators and Radio Waves on Authentication

Majid Motamedi[1*]

[1]Assistant Professor, Department of Industrial Management, Nowshahr Branch, Islamic Azad University, Nowshahr, Iran.

**ARTICLE INFO**

**Article Type:**
Original Research

**Received:** 03.06.2024
**Revised:** 04.28.2024
**Accepted:** 06.02.2024

**Keyword:**
Fuzzy Expert System
Biometrics
Radio Waves
Authentication

***Corresponding Author:**
Majid Motamedi
**Email:**
*mmoatamedy@gmail.com*

**ABSTRACT**

Due to the increasing importance of identity recognition to increase the security of organizations, the importance of identity recognition methods such as biometric indicators and radio waves is also increasing. The purpose of this research was to provide a systematic way of improving authentication based on radio waves and biometric index using a fuzzy expert system for use in the field of information and communication security (cyber security). In this research, the impact of biometric indicators and radio waves on the improvement of identity authentication was investigated, and finally, a fuzzy expert system was designed, which showed the impact on each of the components. The population studied in this research included experts in the field of biometric indicators and radio waves of Tehran municipality. The results of the research showed a correlation between all research variables, and considering the high correlation, it can be said that by managing the security of the components of radio waves, it is possible to improve authentication based on identification through radio waves. The expert system for improving authentication based on identification through radio waves and biometric index can help managers to make decisions related to the issues of improving authentication, lead to improving the efficiency of decision making in improving authentication through radio waves and biometric index, and also make it more effective.



**E-ISSN:** 2538-4430
**ISSN:** 2382-9796

## EXTENDED ABSTRACT

### Introduction

The speed of change, the high volume of data and information and the speed of its transfer has caused many challenges in organizations and made it necessary to control the flow of information, security, accuracy, and speed of processing and use it as best as possible for the benefit of the organization .In this regard, organizations are facing the challenge of identification, using different information sources, documents and independent, reliable and reliable data. Authentication is the process in which senders or receivers provide information to each other to ensure that they are who they claim to be. Today, authentication has abandoned the use of traditional authentication protocols, because in these algorithms, which are based on sending codes and passwords, the possibility of deception is very high. Currently, providing security in the physical layer of communication has been the focus of researchers. One of the security parameters in the physical layer is radio authentication, which uses the transmitter's inherent characteristics based on radio specifications. Authentication usually requires the existence of servers and appropriate infrastructures for message exchange between different components, on the other hand, information transmission in the RFID system is done through non-secure channels. Therefore, it makes it vulnerable to important and serious security threats. One of the methods widely used in identity recognition is biometrics. Biometrics refers to a technology for measuring and analyzing people's body characteristics to recognize a person's identity and automatic identification of a person using specific characteristics that include physiological or behavioural characteristics. Therefore, the use of RFID technology along with the use of biometric indicators can help organizations to improve security and correct authentication.

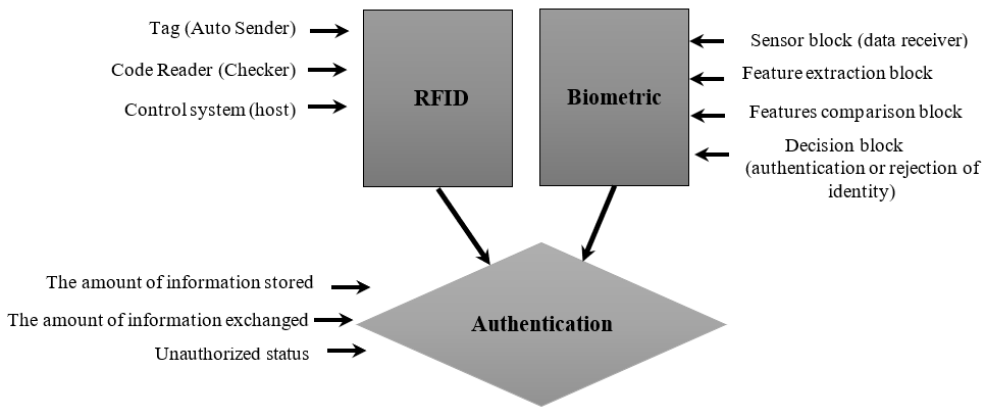



**Figure 1. Proposed authentication improvement model.**

Figure (1) shows the factors affecting the improvement of authentication based on RFID and biometric index, and the dimensions of authentication improvement and the important relationships between different aspects in relation to the problem under investigation. These variables and indicators extracted from the theoretical foundations were in the form

of a preliminary model which was evaluated by experts' opinions and with further analysis, the final research model was presented and entered into the research fuzzy inference system knowledge base.

## Methodology

The current research was applied in terms of purpose and descriptive survey in terms of data collection method. The statistical population of this research included experts in the field of network and information security in Tehran municipality. The content validity method was used to determine the validity of the proposed authentication improvement model and was confirmed based on the opinion of research experts. SPSS software was used to summarize and describe the data, and check the relationship of variables affecting the improvement of authentication. Then, the fuzzy expert system for improving authentication based on identification through radio waves and biometric index, under the title A+FEX, was presented for the first time in the research field related to the subject. Concepts and variables related to authentication based on identification through radio waves and biometric index were extracted from library sources and experts' opinions and then evaluated using expert opinions. After applying experts' opinions and making changes to the conceptual model of the research, it was entered into the knowledge base of the studied expert system. Finally, data analysis was carried out through the design of a fuzzy expert system using MATLAB software and the results were presented in the form of charts and tables.

## Results and discussion

Five steps were considered to design the fuzzy expert authentication system based on identification through radio waves and biometric index as follows:

1- Modelling the concepts of authentication based on identification through radio waves and biometric index to identify input and output variables and draw relationships between them.
2- Defining qualitative variables using linguistic adverbs and assigning numbers and fuzzy sets and membership functions to them.
3- Designing an expert system based on the definitions and designs made using MATLAB software; this stage includes the extraction of expert rules and their evaluation by experts and the creation of a database of fuzzy rules, as well as the design of an inference engine with access to fuzzy rules.
4- User interface design, and how to display options and use the designed expert system.
5- Choosing a method for De-fuzzification to convert fuzzy numbers and sets into a definite value to check the performance of the system.

The results of statistical analysis showed that according to the high correlation between the most important variables of identification through radio waves and authentication, it can be concluded that by considering the security of RFID components, it is possible to improve authentication based on identification through radio waves. Considering the high correlation between the most important indicators of the biometric index variable and the authentication variable, it can be concluded that by managing and considering the security

of the biometric index components, it is possible to improve biometric index-based authentication. Based on the results, using the outputs of the A+FEX system, it is possible to improve the status of authentication based on identification through radio waves and biometric index based on variables such as the security variable of the volume of information stored in RFID and the security variable of the volume of exchanged information. In RFID, the security variable of unauthorized items, the security variable of the amount of information stored in biometrics, and the security variable of unauthorized items in biometrics were analyzed.

## Conclusion

In this research, a fuzzy expert system was designed that provides guidelines to authentication experts. This research presents a systematic way to provide a method to improve authentication based on identification through radio waves and biometric index using a fuzzy expert system for use in the field of information and communication security (cyber security). The advantages of the presented authentication improvement expert system are helping the manager to make decisions related to authentication improvement issues, improving the efficiency of decision-making in authentication improvement and increasing its effectiveness.

کارافن
فصلنامه علمی دانشگاه ملی مهارت
پاییز ۱۴۰۳، دوره ۲۱، شماره ۳، ۱۱۰-۸۵
آدرس نشریه: https://karafan.nus.ac.ir/
doi:10.48301/KSSA.2024.445634.2848

# طراحی یک سیستم خبره فازی به‌منظور بررسی تأثیر شاخص‌های بیومتریک و امواج رادیویی بر احراز هویت

مجید معتمدی[1*]

۱- استادیار، گروه مدیریت صنعتی، واحد نوشهر، دانشگاه آزاد اسلامی، نوشهر، ایران.

**اطلاعات مقاله**

**نوع مقاله:** مقاله پژوهشی

**دریافت مقاله:** ۱۴۰۲/۱۲/۱۶
**بازنگری مقاله:** ۱۴۰۳/۰۲/۰۹
**پذیرش مقاله:** ۱۴۰۳/۰۳/۱۳

**کلید واژگان:**
سیستم خبره فازی
بیومتریک
امواج رادیویی
احراز هویت

***نویسنده مسئول:** مجید معتمدی
**پست الکترونیکی:**
*mmoatamedy@gmail.com*

**چکیده**

با توجه به افزایش روزافزون اهمیت تشخیص هویت به‌منظور افزایش امنیت سازمان‌ها، اهمیت روش‌های تشخیص هویت ازجمله شاخص‌های بیومتریک و امواج رادیویی نیز در حال افزایش است. هدف این تحقیق، ارائه یک راه نظام‌مند با هدف بهبود احراز هویت مبتنی بر امواج رادیویی و شاخص بیومتریک با استفاده از سیستم خبره فازی، به‌منظور استفاده در حوزه امنیت اطلاعات و ارتباطات (امنیت سایبری) است. در این تحقیق میزان تأثیر شاخص‌های بیومتریک و امواج رادیویی بر بهبود احراز هویت مورد بررسی قرار گرفت و در نهایت یک سیستم خبره فازی طراحی گردید که میزان این تأثیر را روی هریک از مؤلفه‌ها نشان می‌دهد. جامعه موردمطالعه این تحقیق، خبرگان در حوزه شاخص‌های بیومتریک و امواج رادیویی شهرداری تهران بودند. نتایج تحقیق بیانگر همبستگی بین تمامی متغیرهای تحقیق بود و با توجه به همبستگی بالا می‌توان گفت که با مدیریت امنیت مؤلفه‌های امواج رادیویی می‌توان به بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی دست یافت. سیستم خبره بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بیومتریک می‌تواند به مدیر برای تصمیم‌گیری در ارتباط با مسائل بهبود احراز هویت کمک کند و منجر به بهبود کارایی تصمیم‌گیری در بهبود احراز هویت از طریق امواج رادیویی و شاخص بایومتریک و نیز اثربخشی بیشتر آن گردد.

شاپای الکترونیکی: ۲۵۳۸-۴۴۳۰
شاپای چاپی: ۲۳۸۲-۹۷۹۶

## مقدمه

محیط امن از جمله نیازهای اصلی سازمان‌هاست و وجود آن را می‌توان ضامن بقا و پایداری جامعه سالم دانست [۱]. امروزه با پیشرفت تکنولوژی، امنیت اطلاعات و داده‌ها بیش از هر نوع امنیت دیگری مورد توجه می‌باشد [۲]. در عصر حاضر، سرعت تحولات، حجم بالای داده‌ها و اطلاعات و سرعت انتقال آن، سازمان‌ها را دچار معضلات متعددی کرده و نیاز به مهار جریان اطلاعات، امنیت، صحت، سرعت پردازش و استفاده هرچه بهتر از آن در جهت منافع سازمان ضرورتی غیرقابل انکار است. در این راستا سازمان‌ها با معضل هویت‌سنجی، با استفاده از منابع اطلاعاتی مختلف، مستندات و داده‌های مستقل، معتبر و قابل‌اتکا مواجه هستند [۳].

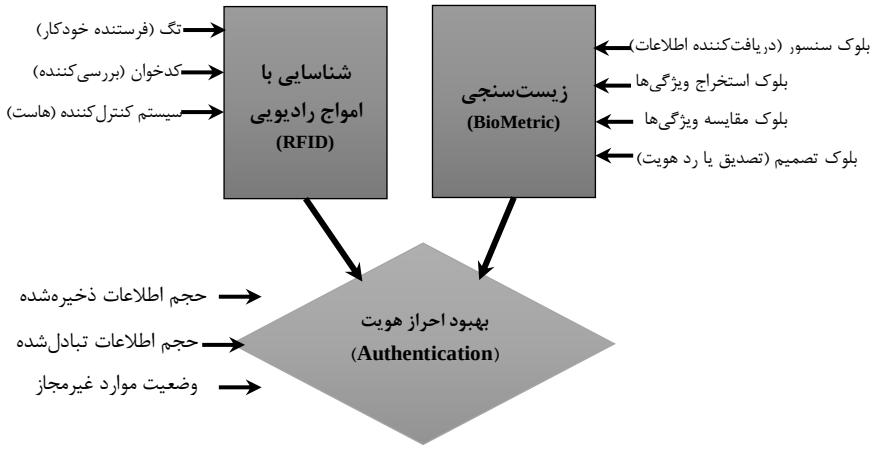
در سال‌های اخیر، به پژوهش درباره هویت توجه زیادی شده و جزو محبوب‌ترین مفاهیم در مطالعات سازمانی بوده است [۴]. احراز هویت به فرایندی گفته می‌شود که در آن ارسال‌کننده یا دریافت‌کننده اطلاعات برای یکدیگر اطلاعاتی را ارائه می‌کنند تا مطمئن شوند آنها همانی هستند که ادعا می‌کنند [۵; ۶]. هدف از سیستم احراز هویت، تبادل امن اطلاعات و یکپارچه‌سازی احراز هویت است [۷]. امروزه احراز هویت به‌کارگیری پروتکل‌های سنتی احراز هویت را کنار گذاشته‌اند زیرا در این الگوریتم‌ها که بر پایه ارسال کد و رمز هستند، احتمال فریب بسیار زیاد است. گزارش‌های زیادی در خصوص آسیب‌پذیری سازمان‌هایی که از شیوه سنتی استفاده می‌کنند منتشر شده است و هر روز شاهد آسیب-پذیری‌های بیشتر این سامانه‌ها هستیم. فناوری‌های احراز هویت سنتی معمولاً احراز هویت را بر اساس تأیید اطلاعات کاربر (برا مثال واردکردن رمز عبور) یا اطلاعات بیومتریک (برای مثال اثر انگشت) برای تأیید هویت انجام می‌دهند. با این حال، زمانی که این روش‌های احراز هویت صرفاً اعمال شوند، خطرات امنیتی وجود دارد. برایمثال، اگر رمز عبور به خطر بیفتد، بعید است که بر اساس رمز عبور مشخص شود که آیا کاربر قانونی است یا خیر [۸]. در حال حاضر تأمین امنیت در لایه فیزیکی ارتباطات مورد توجه محققان قرار گرفته است. یکی از پارامترهای تأمین امنیت در لایه فیزیکی، احراز هویت رادیویی است احراز هویت بر اساس مشخصات رادیویی از مشخصات ذاتی فرستنده استفاده می‌کند و احتمال فریب بسیار کاهش پیدا می‌کند [۹]. با پیشرفت چشم‌گیر فناوری مدارهای مجتمع در دهه‌های گذشته و در نتیجه، کاهش هزینه‌های استفاده از فناوری RFID[1]، شاهد رشد چشم‌گیر و به‌کارگیری سامانه‌های RFID در حوزه‌های مختلفی چون استفاده در ترابری و پشتیبانی قوای نظامی، بارکدهای الکترونیکی، بلیط‌های حمل‌ونقل عمومی و گذرنامه‌های الکترونیکی بوده‌ایم [۱۰]. RFID شامل یک تگ، بررسی‌کننده و یک کنترل‌کننده است [۱۱]. تگ یا دستگاه فرستنده خودکار، شامل یک مدار الکترونیکی است که به شی موردنظری که لازم است دارای یک کد شناسایی باشد، متصل می‌گردد. زمانی که تگ نزدیک یا در محدوده کدخوان قرار می‌گیرد، میدان مغناطیسی تولیدشده توسط کد خوان باعث فعال‌شدن تگ می‌گردد. در ادامه، تگ به‌طور پیوسته اقدام به ارسال داده از طریق پالس‌های رادیویی می‌کند. در نهایت داده توسط کدخوان دریافت و توسط نرم‌افزارهای مربوطه پردازش می‌گردد [۵; ۱۲]. احراز هویت معمولاً نیازمند وجود سرورها و زیرساخت‌های مناسب برای تبادل پیام میان اجزای مختلف است [۱۳]، از طرفی انتقال اطلاعات در سیستم RFID به‌تنهایی، از طریق کانال‌های غیرایمن صورت می‌گیرد. بنابراین آن را در برابر تهدیدهای امنیتی مهم و جدی آسیب‌پذیر می‌سازد [۱۴]. با توجه به افزایش روزافزون اهمیت و کاربرد تشخیص هویت، اهمیت روش‌های تشخیص هویت نیز روز به روز افزایش پیدا می‌کند. یکی از روش‌های که به‌طور گسترده در تشخیص هویت استفاده می‌شود، بیومتریک است [۱۵]. در این علم سعی می‌شود با توجه به مشخصات رفتاری یا فیزیولوژی انسان، هویت او تعیین شود [۳]. بیومتریک فناوری‌ای برای اندازه‌گیری و تحلیل مشخصات بدن افراد برای تشخیص هویت شخص، شناسایی اتوماتیک یک شخص با استفاده از ویژگی‌های اختصاصی که شامل مشخصات فیزیولوژیکی یا رفتاری است [۶; ۷]. از این‌رو

[1] Radio Frequency Identification

به‌کارگیری فناوری RFID در کنار استفاده از شاخص‌های بیومتریک می‌تواند به سازمان‌ها در زمینه ارتقای امنیت و بهبود احراز هویت صحیح کمک کند.

با توجه به مفاهیم فوق، هدف این تحقیق بررسی ارتباط شاخص‌های بایومتریک و امواج رادیویی بر بهبود احراز هویت، در راستای بهره‌مندی حوزه احراز هویت شهرداری تهران می‌باشد. بدین منظور یک سیستم خبره فازی برای بررسی این ارتباط طراحی می‌گردد. سیستم خبره فازی عبارت از یک برنامه هوشمند رایانه‌ای است که از دانش و رویه‌های استنتاج برای حل مسائلی استفاده می‌کند. منظور از سیستم خبره فازی در این تحقیق عبارت است از سیستم خبره‌ای که تقریب، عدم‌قطعیت و شرایط مرزی کیفی را از طریق مجموعه‌های فازی و توابع عضویت مربوطه، به نمایش می‌گذارد و توصیه‌هایی در مورد بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بایومتریک ارائه می‌دهد. در واقع یکی از دلایل استفاده از منطق فازی در این سیستم خبره، این است که فهم و پروسه تصمیم‌گیری انسان‌ها در بسیاری از موارد، کاملاً قطعی نیست و بسته به زمان و مکان آن، تا حدودی درست و تا حدودی نادرست است زیرا در تفکرات، استنتاجات و ادراکات متخصصان بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بایومتریک همیشه درجه معینی از فازی‌بودن وجود دارد [۱۶].

چهارچوب نظری تحقیق (شکل ۱)، عوامل مؤثر بر بهبود احراز هویت مبتنی بر RFID و شاخص بیومتریک و ابعاد بهبود احراز هویت و روابط مهم بین جنبه‌های مختلف را در ارتباط با مسئله تحت بررسی نشان می‌دهد. این متغیرها و شاخص‌های مستخرج از مبانی نظری به‌صورت یک مدل اولیه است که طبق نظرات خبرگان ارزیابی شدند و با تحلیل بیشتر آن، مدل نهایی پژوهش ارائه و وارد پایگاه دانش سیستم استنتاج فازی تحقیق شد.




**شکل ۱. مدل پیشنهادی بهبود احراز هویت.**

در حوزه شبکه رایانه‌ای مرتبط با پژوهش حاضر (شکل ۱)، احراز هویت بدین معناست که یک خدمات‌رسان بتواند تشخیص دهد کسی که تقاضایی را روی آن سیستم دارد شخص حقیقی است یا یک شیاد است تا بدین ترتیب به گیرنده پیام اطمینان داده شود که پیام از همان مبدأیی است که ادعا شده است. هر مکانیزمی که بتواند هویت واقعی یک فرد را بدون هیچ ابهامی، تأیید یا رد کند، سرویسی برای اصالت‌سنجی است. در واقع، احراز هویت، متغیر وابسته (هدف) پژوهش حاضر است که در برگیرنده مؤلفه‌هایی چون: حجم اطلاعات ذخیره‌شده، حجم اطلاعات تبادل‌شده و وضعیت موارد غیرمجاز است. در واقع، منظور از حجم اطلاعات ذخیره‌شده در پژوهش حاضر، کمّیت داده‌های موجود در

سیستم‌های شناسایی از طریق امواج رادیویی و همچنین داده‌های موجود در انواع شاخص‌های بیومتریک است که به‌منظور احراز هویت موردنیاز هستند. از طرفی، منظور از حجم اطلاعات تبادل‌شده در پژوهش حاضر، کمّیت داده‌های تبادل‌شده از طریق سیستم‌های شناسایی از طریق امواج رادیویی است که به‌منظور احراز هویت، بین تگ‌ها و سیستم هاست مرکزی RFID مبادله می‌شوند. از طرفی دیگر، منظور از وضعیت موارد غیرمجاز در پژوهش حاضر، انواع تهدیدهای امنیت سایبری هستند که ارتباطات و اطلاعات موجود در سیستم‌های شناسایی از طریق امواج رادیویی و همچنین داده‌های موجود در انواع شاخص‌های بایومتریک را تهدید می‌کنند.

منظور از زیست‌سنجی در پژوهش حاضر، هر خصوصیت فیزیولوژیکی یا ویژگی رفتاری منحصربه‌فرد و متمایزکننده، مقاوم و قابل سنجشی است که بتواند برای تعیین یا تأیید خودکار هویت افراد به‌کار رود. در واقع، متغیر شاخص بایومتریک دربرگیرنده مؤلفه‌هایی چون: بلوک سنسور (دریافت‌کننده اطلاعات)، بلوک استخراج ویژگی‌ها، بلوک مقایسه ویژگی‌ها و بلوک تصمیم (تصدیق یا رد هویت) است.

علت استفاده از متغیر شناسایی از طریق امواج رادیویی در این پژوهش، این است که این سیستم نسبت به سیستم‌های بارکدی، خواندن اطلاعات تعداد زیادی از اشیا به صورت یک‌باره و بدون دید مستقیم اتفاق می‌افتد، در صورتی که در بارکد اشیا باید یک به یک و در دید مستقیم خوانده شوند و شناسایی گردند. متغیر شناسایی از طریق امواج رادیویی دربرگیرنده مؤلفه‌هایی چون: تگ (فرستنده خودکار)، کدخوان (بررسی‌کننده) و سیستم کنترل‌کننده (هاست) است.

در جدول ۱ یافته‌های مرتبط‌ترین پژوهش‌های موجود در ادبیات نظری ارائه و با پژوهش حاضر مقایسه شده است. در پژوهش‌های گذشته یک مؤلفه به انتخاب محقق بر اساس تجربیات و مطالعات قبلی انتخاب و روشی برای به‌کارگیری آن به‌منظور بهبود نتایج احراز هویت ارائه گردید ولی در این تحقیق ابتدا اصلی‌ترین مؤلفه‌های تأثیرگذار بر نتایج احراز هویت تعیین و سپس میزان تأثیر هریک سنجیده شده است. همچنین در این پژوهش با طراحی سیستمی فازی بر مؤلفه‌های مؤثر بر احراز هویت ارزش‌گذاری می‌شود؛ این امر به محققان و مهندسان این عرصه این امکان را می‌دهد که با توجه به خروجی سیستم با صرف کمترین هزینه و زمان بر روی مؤثرترین مؤلفه‌ها، نتایج را بهبود بخشند و سیستمی کاراتر ارائه دهند که موارد فوق از جنبه‌های نوآوری این تحقیق هستند.

**جدول ۱. مقایسه یافته‌های مرتبط‌ترین پژوهش‌های موجود در ادبیات نظری با پژوهش حاضر.**

| هدف تحقیق | منبع | مقایسه یافته‌های پژوهش | | | | | |
|---|---|---|---|---|---|---|---|
| | | احراز هویت | RFID | بایومتریک | سیستم خبره | منطق فازی | اعتبارسنجی سیستم |
| ارائه روشی برای بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بیومتریک | این تحقیق | * | * | * | * | * | * |
| طرح احراز هویت ایمن مبتنی بر بلاکچین در سیستم‌های هواشناسی | [۱۳] | * | | | | | |
| ارائه یک سیستم کنترل دسترسی احراز هویت سه‌عاملی با استفاده از RFID، اثر انگشت، رمز و کد | [۱۷] | * | * | * | | | * |
| احراز هویت دوطرفه در اینترنت اشیا | [۱۸] | * | | * | | | |
| سیستم احراز هویت ترکیبی دانش‌آموز با استفاده از RFID Reader و بیومتریک چهره با استفاده از تکنیک‌های یادگیری عمیق | [۱۹] | * | * | * | | | |

| هدف تحقیق | منبع | مقایسه یافته‌های پژوهش | | | | |
|---|---|---|---|---|---|---|
| | | احراز هویت | RFID | بایومتریک | سیستم خبره منطق فازی | اعتبارسنجی سیستم |
| طراحی و اجرای سیستم کنترل دسترسی RFID بر اساس ویژگی‌های بیومتریک چندگانه | [۱۵] | * | * | * | | |
| روشی برای ارزیابی مخاطره امنیتی در سیستم‌های سایبر- فیزیکی با اطلاعات ناقص | [۲۰] | * | | * | | |
| احراز هویت اطلاعات بیومتریک کاربر بر اساس RFID | [۸] | * | * | * | | |
| استفاده از بیومتریک های متعدد دست، برای احراز هویت کاربر، مقاوم در برابر حمله با استفاده از COTS RFID | [۲۱] | * | * | * | | |
| احراز هویت و کنترل دسترسی در اینترنت اشیا مبتنی بر الگوریتم زنجیره‌ای هش و اثر انگشت بهبودیافته | [۲] | * | | * | | |
| پیاده‌سازی احراز هویت دو عاملی بر اساس RFID و تشخیص چهره با استفاده از الگوریتم LBP در سیستم کنترل دسترسی | [۲۲] | * | * | * | | |
| ضعف‌های پروتکل احرازهویت SPRSو ارائه یک پروتکل بهبودیافته برای سامانه‌های RFID | [۲۳] | * | * | | | |
| ارائه سیستم احراز هویت اینترنتی براساس سیستم شناسایی صدا و موبایل | [۲۴] | * | * | * | | |
| تحلیل محرمانگی و امنیت پروتکل احراز هویت دوسویه در سامانه‌های RFID مبتنی بر توابع چکیده‌ساز | [۱۲] | * | * | | | |
| تصدیق امضای پویا و احراز هویت مبتنی بر استخراج نقاط غالب پایدار و تقطیع الگوهای امضا | [۱۶] | * | | * | | * |
| عوامل مؤثر بر توسعه فناوری شناسایی از طریق فرکانس‌های رادیویی (RFID) در مدیریت زنجیره تأمین الکترونیکی، مطالعه موردی: شرکت ایران‌خودرو | [۲۵] | | | * | * | |
| تحلیل امنیتی پروتکل Seas: یک پروتکل احراز هویت در سیستم‌های RFID | [۲۶] | * | * | | | * |
| طراحی سیستمی یکپارچه با هدف بهینه‌سازی احراز هویت، مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بایومتریک در تعاملات تجارت الکترونیک | [۷] | * | * | * | | * |
| ارائه یک سیستم احراز هویت مبتنی بر صفت بیومتریک پنهان | [۲۷] | * | | * | | * |
| ارائه یک سیستم احراز هویت بیومتریک استوار بر اساس اثر انگشت و رمزگذاری | [۲۸] | * | | * | | * |
| ارائه یک سیستم احراز هویت دو عاملی با استفاده از شناسایی فرکانس رادیویی و فناوری علامت‌گذاری | [۲۹] | * | * | * | | * |

## روش تحقیق

پژوهش حاضر از نظر هدف، کاربردی و از نظر روش گردآوری داده‌ها توصیفی- پیمایشی است. جامعه مورد آماری این تحقیق شامل خبرگان حوزه امنیت شبکه و اطلاعات و افراد شاغل در بخش فناوری اطلاعات و افراد فعال در حوزه شاخص‌های بیومتریک و امواج رادیویی در شهرداری تهران می‌باشد. به‌منظور کسب داده‌های موردنظر تحقیق از ابزار

پرسش‌نامه و اسناد مرتبط با احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بایومتریک در شهرداری تهران استفاده شد (جدول ۲)، همچنین برای ارزیابی قواعد سیستم خبره از نظرات خبرگان استفاده شد. برای تعیین اعتبار مدل پیشنهادی بهبود احراز هویت از روش اعتبار محتوا استفاده شد و روایی مدل پیشنهادی، بر اساس نظر خبرگان تحقیق تأیید گردید. پایایی ابزار اندازه‌گیری نیز با استفاده از روش آلفای کرونباخ تأیید شد.

**جدول ۲. شاخص‌های اندازه‌گیری تأثیر مؤلفه‌های شناسایی از طریق امواج رادیویی و شاخص زیست‌سنجی بر بهبود احراز هویت.**

| شاخص‌ها | سؤالات |
|---|---|
| متغیر شناسایی از طریق امواج رادیویی (RFID) | ۱ تا ۶ |
| متغیر شاخص زیست‌سنجی (Biometrics) | ۷ تا ۱۴ |
| متغیر احراز هویت | ۱۵ تا ۲۰ |

به‌منظور خلاصه‌سازی و توصیف داده‌ها و بررسی ارتباط متغیرهای مؤثر بر بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بیومتریک از آزمون همبستگی و نرم‌افزار SPSS استفاده شد. سپس سیستم خبره فازی بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بیومتریک، تحت عنوان A+FEX[1] برای اولین‌بار در حوزه پژوهشی مرتبط با موضوع ارائه گردید. در این پژوهش، یک سیستم خبره فازی طراحی گردید که به متخصصان احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بیومتریک، رهنمودهایی را ارائه می‌دهد. مفاهیم و متغیرهای مرتبط با احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بیومتریک، از منابع کتابخانه‌ای استخراج شدند و سپس با استفاده از نظرات خبرگان ارزیابی شد و بعد از اعمال نظرات خبرگان و انجام تغییراتی مدل مفهومی پژوهش، وارد پایگاه دانش سیستم خبره مورد مطالعه شد. در نهایت تجزیه و تحلیل اطلاعات از طریق طراحی سیستم خبره فازی با استفاده از نرم‌افزار Matlab انجام شد و نتایج به‌دست‌آمده در قالب نمودارها و جداول ارائه گردید.

## نتایج و بحث

جدول مربوط به اطلاعات توصیفی متغیرها و شاخص‌های پژوهش شامل متغیر شناسایی از طریق امواج رادیویی، دربرگیرنده مؤلفه‌هایی چون: تگ (فرستنده خودکار)، کدخوان (بررسی‌کننده) و سیستم کنترل‌کننده (هاست)، متغیر شاخص بایومتریک، دربرگیرنده مؤلفه‌هایی چون: بلوک سنسور (دریافت‌کننده اطلاعات)، بلوک استخراج ویژگی‌ها، بلوک مقایسه ویژگی‌ها و بلوک تصمیم (تصدیق یا رد هویت) و متغیر وابسته پژوهش یعنی احراز هویت، دربرگیرنده مؤلفه‌هایی چون: حجم اطلاعات ذخیره‌شده، حجم اطلاعات تبادل‌شده و وضعیت موارد غیرمجاز، نشان می‌دهد که داده‌های این تحقیق از نظر تقارن و تجمع در وضعیت مطلوبی هستند زیرا آماره چولگی تمامی شاخص‌های مذکور، منفی یا صفر شده است که به معنای انتخاب گزینه زیاد در بین پاسخ‌های خبرگان حوزه مورد مطالعه است.

[1] Improving Authentication Fuzzy Expert System (A+FEX)

**جدول ۳. اطلاعات توصیفی مربوط به متغیرهای پژوهش.**

| میانگین وزنی | شاخص‌های پژوهش | حداقل | حداکثر | میانگین | انحراف معیار | چولگی | | متغیرهای پژوهش |
|---|---|---|---|---|---|---|---|---|
| | | | | | | خطای استاندارد | آماره | |
| ۴.۲۸۰ | اهمیت امن‌بودن مؤلفه «تگ (فرستنده خودکار)» | ۲ | ۵ | ۴.۴۲ | ۸۵۰. | ۳۰۹. | ۱.۶۱۸- | متغیر شناسایی از طریق امواج |
| | امکان مدیریت کردن امنیت مؤلفه «تگ (فرستنده خودکار)» | ۲ | ۵ | ۴.۴۳ | ۸۹۰. | ۳۰۹. | ۱.۵۸۳- | |
| | اهمیت امن بودن مؤلفه «کدخوان (بررسی‌کننده)» | ۲ | ۵ | ۴.۰۰ | ۱.۱۶۴ | ۳۰۹. | ۸۰۰.- | |
| | امکان مدیریت کردن امنیت مؤلفه «کدخوان (بررسی‌کننده)» | ۲ | ۵ | ۳.۹۵ | ۱.۰۳۲ | ۳۰۹. | ۷۵۹.- | |
| | اهمیت امن‌بودن مؤلفه «سیستم کنترل‌کننده (هاست)» | ۳ | ۵ | ۴.۶۰ | ۶۱۶. | ۳۰۹. | ۱.۲۹۵- | |
| | امکان مدیریت کردن امنیت مؤلفه سیستم کنترل‌کننده (هاست) | ۲ | ۵ | ۴.۲۸ | ۸۴۶. | ۳۰۹. | ۱.۱۰۸- | |
| ۴.۲۹۳ | اهمیت امن‌بودن مؤلفه بلوک سنسور (دریافت‌کننده اطلاعات) | ۲ | ۵ | ۴.۳۳ | ۹۱۴. | ۳۰۹. | ۱.۲۷۴- | متغیر شاخص زیست‌سنجی (Biometrics) " |
| | امکان مدیریت کردن امنیت مؤلفه بلوک سنسور دریافت‌کننده اطلاعات | ۲ | ۵ | ۴.۴۳ | ۸۹۰. | ۳۰۹. | ۱.۵۸۳- | |
| | اهمیت امن‌بودن مؤلفه بلوک استخراج ویژگی‌ها | ۳ | ۵ | ۴.۵۰ | ۶۷۶. | ۳۰۹. | ۱.۰۱۹- | |
| | امکان مدیریت کردن امنیت مؤلفه بلوک استخراج ویژگی‌ها | ۳ | ۵ | ۴.۴۵ | ۶۷۵. | ۳۰۹. | ۸۴۰.- | |
| | اهمیت امن‌بودن مؤلفه بلوک مقایسه ویژگی‌ها | ۲ | ۵ | ۴.۱۸ | ۶۹۳. | ۳۰۹. | ۷۴۱.- | |
| | امکان مدیریت کردن امنیت مؤلفه بلوک مقایسه ویژگی‌ها | ۲ | ۵ | ۴.۳۵ | ۸۸۰. | ۳۰۹. | ۱.۲۲۴- | |
| | اهمیت امن‌بودن مؤلفه «بلوک تصمیم (تصدیق یا رد هویت) | ۲ | ۵ | ۴.۱۷ | ۹۶۰. | ۳۰۹. | ۸۲۲.- | |
| | امکان مدیریت کردن امنیت مؤلفه بلوک تصمیم (تصدیق یا رد هویت) | ۲ | ۵ | ۳.۹۳ | ۱.۱۶۳ | ۳۰۹. | ۶۷۰.- | |
| ۴.۲۰۳ | اهمیت امن‌بودن مؤلفه حجم اطلاعات ذخیره‌شده | ۲ | ۵ | ۳.۹۰ | ۱.۰۶۹ | ۳۰۹. | ۶۵۷.- | متغیر احراز هویت |
| | امکان مدیریت کردن امنیت مؤلفه حجم اطلاعات ذخیره‌شده | ۲ | ۵ | ۴.۴۲ | ۸۶۹. | ۳۰۹. | ۱.۴۱۷- | |
| | اهمیت امن‌بودن مؤلفه حجم اطلاعات تبادل‌شده | ۲ | ۵ | ۴.۲۰ | ۱.۰۳۸ | ۳۰۹. | ۱.۰۷۵- | |
| | امکان مدیریت کردن امنیت مؤلفه حجم اطلاعات تبادل‌شده | ۲ | ۵ | ۴.۵۳ | ۷۹۱. | ۳۰۹. | ۱.۹۱۹- | |
| | اهمیت امن‌بودن مؤلفه وضعیت موارد غیرمجاز | ۲ | ۵ | ۳.۸۵ | ۱.۱۱۷ | ۳۰۹. | ۵۹۹.- | |
| | امکان مدیریت کردن امنیت مؤلفه وضعیت موارد غیرمجاز | ۲ | ۵ | ۴.۳۲ | ۸۹۲. | ۳۰۹. | ۱.۱۲۴- | |

به‌منظور بررسی نرمال‌بودن توزیع داده‌های پژوهش از آزمون کولموگروف- اسمیرنوف شد و نتایج بیانگر نرمالبودن داده‌ها بود. سپس برای بررسی ارتباط بین متغیر تابع (وابسته) و متغیرهای مستقل، با توجه به داده‌های نرمال از ضریب همبستگی پیرسون استفاده گردید. نتایج آزمون ضریب همبستگی نشان دا بین اهمیت امن‌بودن مؤلفه تگ (فرستنده خودکار) و امکان مدیریت کردن امنیت مؤلفه وضعیت موارد غیرمجاز، رابطه مثبت و معنی‌داری وجود دارد (ضریب همبستگی = ۰.۷۱۷). بین اهمیت امن‌بودن مؤلفه حجم اطلاعات ذخیره‌شده و امکان مدیریت‌کردن امنیت مؤلفه کدخوان (بررسی‌کننده) رابطه مثبت و معنی‌داری وجود دارد (ضریب همبستگی= ۰.۹۶۳). بین امکان مدیریت کردن امنیت مؤلفه سیستم کنترل‌کننده (هاست) و اهمیت امن‌بودن مؤلفه حجم اطلاعات تبادل‌شده، ارتباط مثبت و معنی‌دار وجود دارد (ضریب همبستگی = ۰.۴۶۳). با توجه به همبستگی بالای بین مهم‌ترین شاخص‌های متغیر شناسایی از طریق امواج رادیویی و احراز هویت می‌توان گفت با مدیریت امنیت مؤلفه‌های RFID می‌توان به بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی دست یافت. از طرفی دیگر، بین اهمیت امن‌بودن مؤلفه بلوک استخراج ویژگی‌ها و امکان مدیریت کردن امنیت مؤلفه وضعیت موارد غیرمجاز، رابطه مثبت و معنی‌داری وجود دارد (ضریب همبستگی = ۰.۶۳۲). بین

اهمیت امن‌بودن مؤلفه حجم اطلاعات ذخیره‌شده و امکان مدیریت کردن امنیت مؤلفه بلوک تصمیم (تصدیق یا رد هویت)، ارتباط مثبت وجود دارد (ضریب همبستگی = ۰.۶۰۸). بین اهمیت امن‌بودن مؤلفه بلوک سنسور (دریافت‌کننده اطلاعات) و اهمیت امن‌بودن مؤلفه حجم اطلاعات تبادل‌شده، ارتباط مثبت وجود دارد (ضریب همبستگی = ۰.۸۵۷). بین اهمیت امن‌بودن مؤلفه حجم اطلاعات ذخیره‌شده و اهمیت امن‌بودن مؤلفه بلوک مقایسه ویژگی‌ها، ارتباط مثبت وجود دارد (ضریب همبستگی = ۰.۵۹۹). در واقع با توجه به همبستگی بالای بین مهم‌ترین شاخص‌های متغیر شاخص بایومتریک و متغیر احراز هویت می‌توان نتیجه‌گیری کرد که با مدیریت کردن امنیت مؤلفه‌های شاخص بیومتریک می‌توان به بهبود احراز هویت مبتنی شاخص بایومتریک دست یافت.

## طراحی سیستم خبره فازی احراز هویت

سیستمی که یک نگاشت از ورودی به خروجی را با استفاده از منطق فازی فرموله می‌کند به نام سیستم استنتاج فازی شناخته می‌شود. سیستم استنتاج فازی همچنین به نام سیستم مبتنی بر قواعد نیز نامیده می‌شود زیرا این سیستم‌ها از تعدادی عبارت «اگر- آن‌گاه» ساخته شده است. وقتی چنین سیستم‌هایی در نقش کنترلی ظاهر می‌شوند به آنها کنترل‌کننده‌های فازی می‌گویند. نقطه شروع ساخت یک سیستم فازی به‌دست‌آوردن مجموعه‌ای از قواعد اگر-آن‌گاه فازی از دانش افراد خبره یا دانش حوزه موردبررسی می‌باشد. مرحله بعدی ترکیب این قواعد در یک سیستم واحد است. سیستم‌های فازی مختلف از اصول و روش‌های متفاوتی برای ترکیب این قواعد استفاده می‌کنند. مشکل اصلی در رابطه با سیستم‌های فازی خالص این است که ورودی‌ها و خروجی‌های آن مجموعه‌های فازی هستند. در حالی که در سیستم‌های مهندسی، ورودی‌ها و خروجی‌ها متغیرهایی با مقادیر حقیقی می‌باشند. برای حل این مشکل، تاکاگی-سوگنو و کانگ، نوع دیگری سیستم‌های فازی معرفی کرده‌اند که ورودی‌ها و خروجی‌های آن متغیرهایی با مقادیر واقعی هستند. مشکلات عمده سیستم فازی عبارتند از: ۱) بخش آن‌گاه قاعده یک فرمول ریاضی است و بنابراین چهارچوبی را برای نمایش دانش بشری فراهم نمی‌کند. ۲) این سیستم دست ما را برای اعمال اصول مختلف منطق فازی باز نمی‌گذارد و در نتیجه انعطاف‌پذیری سیستم‌های فازی در این ساختار وجود ندارد، برای حل این مشکلات ما از نوع سومی از سیستم‌های فازی یعنی سیستم‌های فازی با فازی‌سازها و غیرفازی‌سازها استفاده می‌کنیم. به‌منظور استفاده از سیستم‌های فازی خالص در سیستم‌های مهندسی، یک روش ساده، افزودن یک فازی ساز در ورودی که متغیرهای با مقادیر حقیقی را به یک مجموعه فازی تبدیل می‌کند و یک غیرفازی‌ساز که یک مجموعه فازی را به یک متغیر با مقدار حقیقی در خروجی تبدیل می‌کند، می‌باشد. نتیجه یک سیستم فازی با فازی‌ساز و غیرفازی‌ساز این است که سیستم فازی، معایب سیستم فازی خالص و سیستم فازی را می‌پوشاند. با توجه به کاربرد سیستم خبره فازی طراحی‌شده در پژوهش‌های [۱۶; ۲۸; ۳۰; ۳۱]، مراحل پنج‌گانه‌ای برای طراحی سیستم خبره فازی احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بایومتریک درنظر گرفته شد که عبارتند از:

۱- مدل‌سازی مفاهیم حوزه احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بایومتریک به‌منظور شناسایی متغیرهای ورودی و خروجی و ترسیم روابط بین آنها

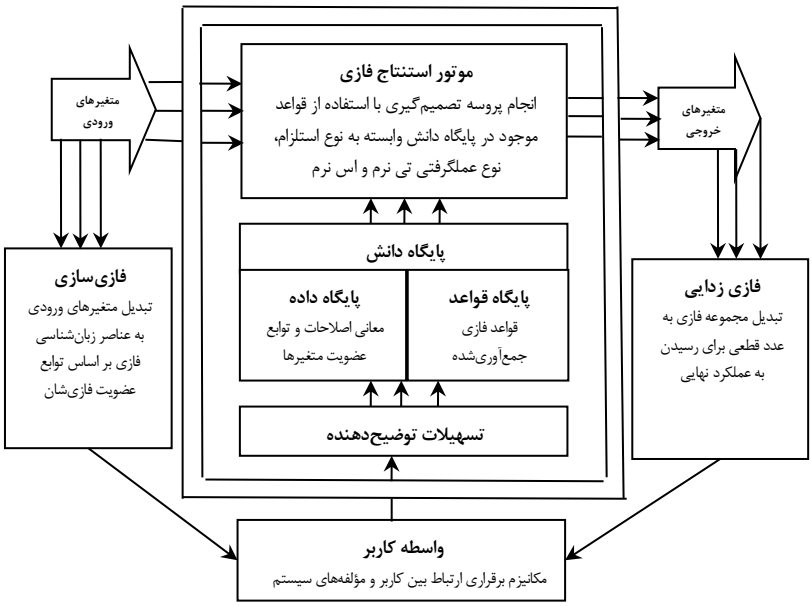
۲- تعریف متغیرهای کیفی با استفاده از قیدهای زبانی و تخصیص اعداد و مجموعه‌های فازی و توابع عضویت به آنها

۳- طراحی سیستم خبره اساس تعاریف و طراحی‌های صورت‌گرفته با استفاده از نرم‌افزار متلب: این مرحله شامل استخراج قواعد خبرگی و ارزیابی آنها توسط خبرگان و ایجاد پایگاه قواعد فازی و همچنین طراحی موتور استنتاج دارای دسترسی به قواعد فازی می‌باشد.

۴- طراحی رابط کاربر و نحوه نمایش گزینه‌ها و چگونگی استفاده از سیستم خبره طراحی‌شده

۵- انتخاب یک روش برای فازی‌زدایی به‌منظور تبدیل اعداد و مجموعه‌های فازی به مقدار قطعی به‌منظور بررسی واقعی عملکرد سیستم.

ساختار سیستم خبره فازی طراحی‌شده در این تحقیق با اقتباس از اجزا و ساختارهای موجود در پژوهش‌های [۱۶؛ ۲۸؛ ۳۰؛ ۳۱]، در شکل (۲) به نمایش گذاشته شده است.



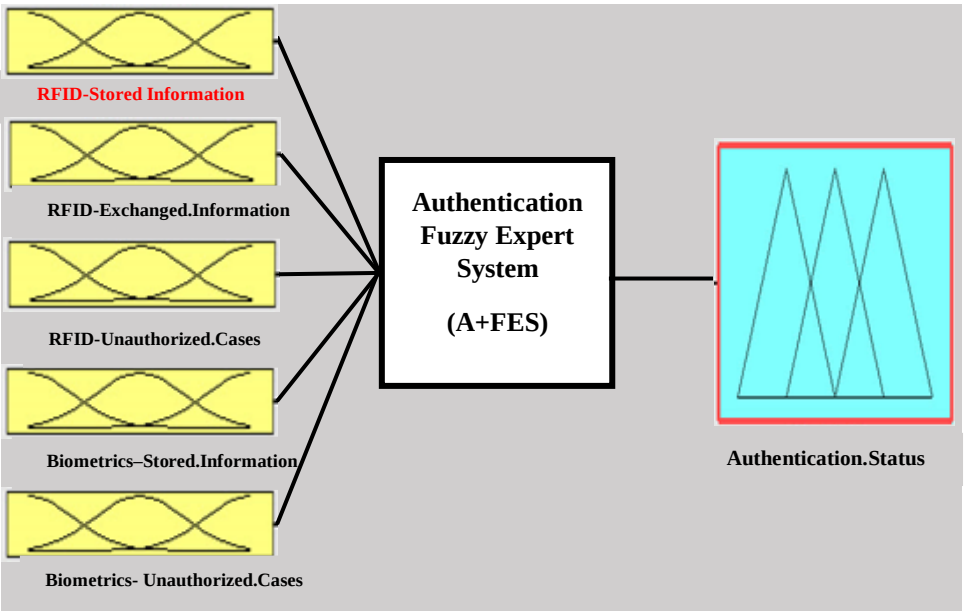

**شکل ۲. ساختار سیستم خبره فازی تحقیق.**

در پژوهش حاضر، به‌منظور ارائه روشی برای بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بایومتریک با استفاده از سیستم خبره فازی می‌توان گفت که سیستم A+FEX، سیستمی است که اطلاعات ورودی آن می‌تواند به صورت نادقیق باشند، یعنی اطلاعات ورودی یک سیستم فازی به‌صورت مجموعه‌های فازی یا اعداد فازی هستند. از سوی دیگر پردازش‌های یک سیستم فازی می‌تواند به‌صورت نادقیق انجام شود. یکی از معروف‌ترین و کاربردی‌ترین پردازش‌های نادقیق در سیستم‌های فازی، استفاده از پایگاه قوانین فازی است. در پایگاه قوانین فازی هر قانون با ساختار اگر – آن‌گاه تعریف می‌شود. با توجه به کاربرد سیستم خبره فازی طراحی‌شده در این تحقیق در پایان مراحل پنج‌گانه‌ای برای طراحی سیستم خبره فازی بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بیومتریک در نظر گرفته شد که عبارتند از:

**مرحله اول: شناسایی متغیرهای ورودی و خروجی سیستم**

پس از نهایی‌شدن مدل مفهومی سیستم خبره تحقیق، اقدام به تعریف متغیرهای ورودی و خروجی سیستم خبره شد. متغیرهای پنج‌گانه ورودی سیستم A+FEX عبارتند از: متغیر امن‌بودن حجم اطلاعات ذخیره‌شده در RFID، متغیر امن‌بودن حجم اطلاعات تبادل‌شده از طریق RFID، متغیر امن‌بودن وضعیت موارد غیرمجاز در RFID، متغیر امن‌بودن حجم اطلاعات ذخیره‌شده در بایومتریک و متغیر امن‌بودن وضعیت موارد غیرمجاز در بایومتریک. متغیر خروجی سیستم مذکور عبارت است از متغیر بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بایومتریک

که دارای پنج وضعیت (متغیرهای زبانی خبرگان حوزه امنیت اطلاعات و ارتباطات) است. با توجه با مدل مفهومی تحقیق و نیز اعمال نظرات خبرگان به‌منظور ارزیابی آن مدل، می‌توان متغیرهای ورودی و خروجی سیستم خبره را به شرح شکل ۳ بیان کرد.



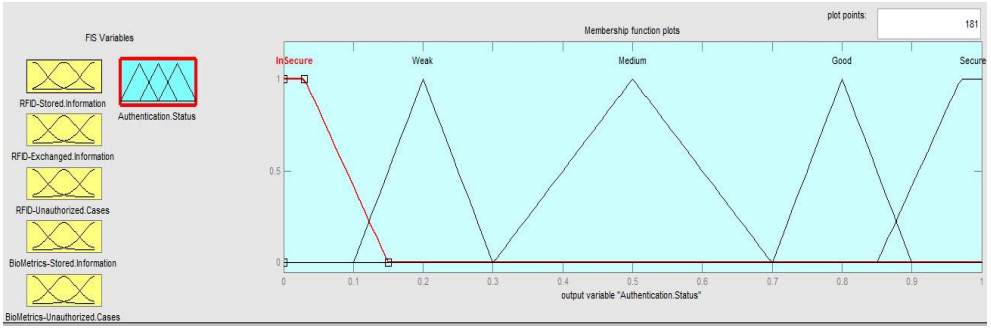

**شکل ۳. مدل متغیرهای ورودی ماژول بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بایومتریک.**

### مرحله دوم: تعریف متغیرهای کیفی با استفاده از قیدهای زبانی و تخصیص اعداد و مجموعه‌های فازی و توابع عضویت به آنها

جدول ۴ و شکل ۴ متغیرهای زبانی، مقادیر فازی و نیز توابع عضویت اعداد مثلثی و ذوزنقه‌ای مرتبط با متغیرهای ورودی و خروجی سیستم خبره تحقیق را درون طیف‌های سه تایی و پنج‌تایی، به نمایش می‌گذارند.

**جدول ۴. متغیرهای زبانی مرتبط با متغیر خروجی ماژول بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بایومتریک.**

| متغیر زبانی | معادل انگلیسی | توابع عضویت اعداد مثلثی و ذوزنقه‌ای |
|---|---|---|
| ناامن | Insecure | (۰ ۰ ۰/۰۳ ۰/۱۵) |
| ضعیف | Weak | (۰/۱ ۰/۲ ۰/۳) |
| متوسط (معمولی) | Medium | (۰/۳ ۰/۵ ۰/۷) |
| خوب | Good | (۰/۷ ۰/۸ ۰/۹) |
| امن | Secure | (۰/۸۵ ۰/۹۷ ۱ ۱) |




**شکل ۴. افرازبندی متغیر خروجی سیستم خبره تحقیق – مقادیر فازی مرتبط با متغیرهای زبانی (توابع عضویت اعداد مثلثی و ذوزنقه‌ای).**

### مرحله سوم: طراحی پایگاه دانش سیستم خبره

این مرحله شامل استخراج قواعد خبرگی و ارزیابی آنها توسط خبرگان و ایجاد پایگاه قواعد فازی می‌باشد. پایگاه قواعد فازی مجموعه‌ای از قواعد اگر- آن‌گاه است که قلب سیستم A+FEX محسوب می‌شود زیرا سایر اجزا سیستم فازی برای پیاده‌سازی این قواعد به شکل مؤثر و کارا استفاده می‌شوند. در اینجا احتمال وقوع حالت‌های مختلف بین متغیرهای اصلی سیستم خبره یکسان درنظر گرفته شده است. نقطه شروع ساخت یک پایگاه دانشی مبتنی بر قاعده در یک سیستم فازی، به‌دست‌آوردن مجموعه‌ای از قواعد اگر/ آن‌گاه فازی از دانش افراد خبره یا دانش حوزه مورد بررسی می‌باشد، مرحله بعدی، ترکیب این قواعد در یک سیستم واحد است. نحوه تولید قواعد پایگاه دانش ماژول اصلی سیستم A+FEX بر اساس مراحل ذیل می‌باشد:

الف: محاسبه وزن هرکدام از متغیرهای اصلی با استفاده از نظرات خبرگان: با توجه به جدول مربوط به وزن نهایی آیتم‌های اندازه‌گیری کننده وزن هر کدام از متغیرهای اصلی، می‌توان آنها را به شرح جدول ۵ مشاهده کرد:

**جدول ۵. اطلاعات مربوط به وزن هرکدام از متغیرهای اصلی.**

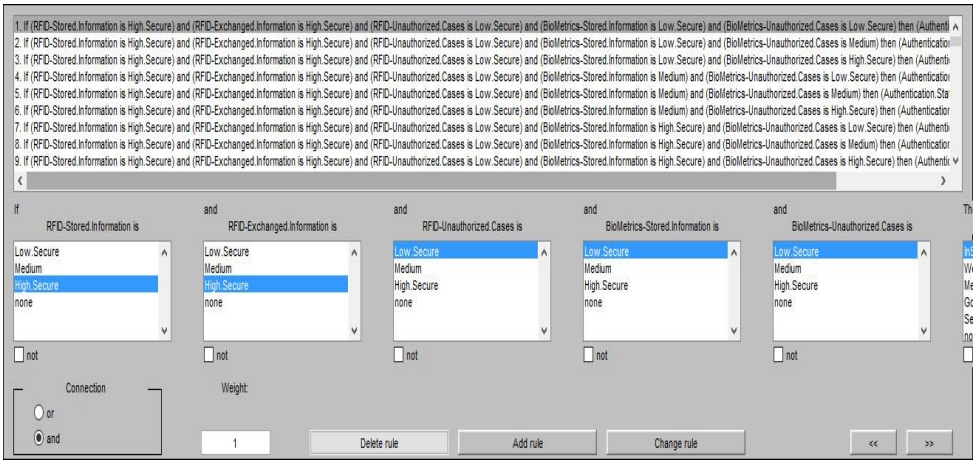
| متغیرهای پژوهش | میانگین وزنی متغیر * میانگین وزنی شاخص مورد بررسی | وزن متغیر ورودی | وزن نهایی متغیر ورودی |
|---|---|---|---|
| متغیر امن‌بودن حجم اطلاعات ذخیره‌شده در RFID | ۴.۲۸۰ * ۴.۴۲ | ۱۸.۹۱۸ | ۰.۲۰۰ |
| متغیر امن‌بودن حجم اطلاعات تبادل‌شده از طریق RFID | ۴.۲۸۰ * ۴.۵۳ | ۱۹.۳۸۸ | ۰.۲۰۶ |
| متغیر امن‌بودن وضعیت موارد غیرمجاز در RFID | ۴.۲۸۰ * ۴.۳۲ | ۱۸.۴۹۰ | ۰.۱۹۵ |
| متغیر امن‌بودن حجم اطلاعات ذخیره‌شده در بایومتریک | ۴.۲۹۳ * ۴.۴۲ | ۱۸.۹۷۵ | ۰.۲۰۲ |
| متغیر امن‌بودن وضعیت موارد غیرمجاز در بایومتریک | ۴.۲۹۳ * ۴.۳۲ | ۱۸.۵۴۶ | ۰.۱۹۷ |
| مجموع | | ۹۴.۳۱۷ | ۱۰۰٪ |

ب: محاسبه مقدار متغیر خروجی بر اساس وزن هرکدام از متغیرها: با توجه به وزن هرکدام از متغیرهای ورودی سیستم خبره می‌توان بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بایومتریک را در حالت‌های مختلف ارزشیابی کرد. در اینجا احتمال وقوع حالت‌های مختلف بین متغیرهای اصلی سیستم خبره، یکسان درنظر گرفته شده‌اند. در واقع پس از مصاحبه با خبرگان حوزه موردبررسی می‌توان بر اساس شرایط جدول ۶ به تولید قواعد فازی اقدام کرد:

**جدول ۶. نحوه محاسبه وزن حالت‌های ممکن برای تولید قاعده در پایگاه دانش سیستم خبره.**

| حالت‌های ممکن برای تولید قاعده | وزن هر متغیر * مقدار فازی متغیر زبانی | وزن حالت مفروض |
|---|---|---|
| اگر متغیر امن‌بودن حجم اطلاعات ذخیره‌شده در RFID ضعیف باشد | ۰.۱۵ * ۰.۲ | ۰.۰۳۰ |
| و متغیر امن‌بودن حجم اطلاعات تبادل‌شده در RFID نرمال باشد | ۰.۵ * ۰.۲۰۶ | ۰.۱۰۳ |
| و متغیر امن‌بودن وضعیت موارد غیرمجاز در RFID خوب باشد | ۰.۸۵ * ۰.۱۹۵ | ۰.۱۶۸ |
| و متغیر امن‌بودن حجم اطلاعات ذخیره‌شده در بایومتریک خوب باشد | ۰.۸۵ * ۰.۲۰۲ | ۰.۱۷۲ |
| و متغیر امن‌بودن وضعیت موارد غیرمجاز در بایومتریک نرمال باشد | ۰.۵ * ۰.۱۹۷ | ۰.۰۹۹ |
| آن‌گاه<br>وضعیت بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بایومتریک در چه سطحی قرار دارد؟ | مجموع اوزان متغیرها برای محاسبه وزن حالت مفروض:<br>۰.۵۷۲ (وضعیت متوسط (معمولی)) | |

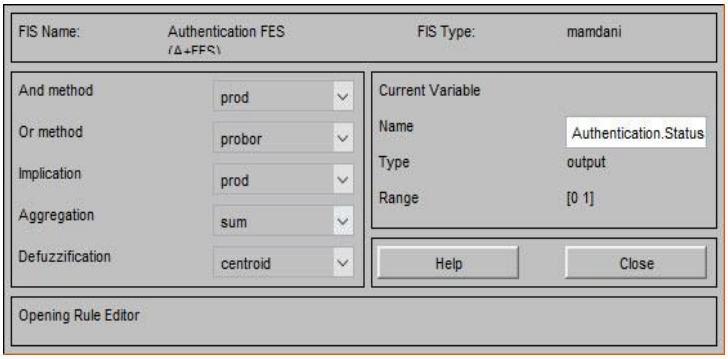
با توجه به توابع عضویت متغیرهای زبانی توسط خبرگان موجود در جدول ۵، ۰.۵۷۲ در بازه تعریف‌شده برای متغیر زبانی متوسط (معمولی) تعریف شده است بنابراین وضعیت بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بایومتریک در حالت فوق، در سطح متوسط (معمولی) قرار دارد. سایر قواعد پایگاه دانش این سیستم خبره نیز به این ترتیب تولید شدند. در نهایت تعداد قواعد فازی ماژول بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بیومتریک سیستم A+FEX به دلیل وجود پنج متغیر اصلی که هرکدام سه حالت دارند، برابر با ۲۴۳ است. در شکل (۵) پایگاه‌های قواعد فازی ماژول سیستم A+FEX نشان داده شده است.




**شکل ۵. نحوه تولید قواعد فازی درون پایگاه دانش ماژول «بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بایومتریک».**

### مرحله چهارم طراحی موتور استنتاج سیستم A+FEX

در این مرحله روش Centroid برای فازی‌زدایی به‌منظور تبدیل اعداد و مجموعه‌های فازی به مقدار قطعی به‌منظور بررسی واقعی عملکرد سیستم انتخاب شده است. شکل ۶، موتور استنتاج سیستم A+FEX را به نمایش می‌گذارد:

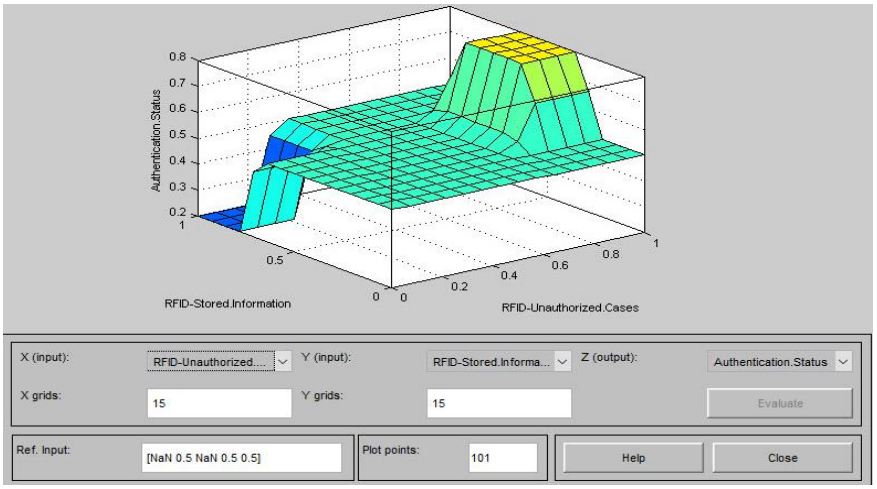



**شکل ۶. موتور استنتاج سیستم A+FEX.**

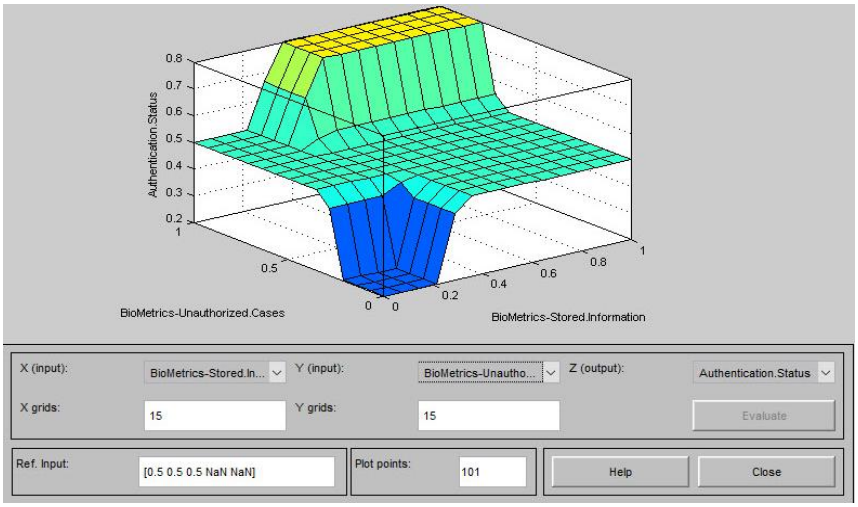
با استفاده از نرم‌افزار MATLAB می‌توان به استنتاج مبتنی بر قواعد پرداخت. در واقع مهم‌ترین دلیل استفاده از موتور استنتاج ممدانی (به جای سوگنو) این است که در موتور استنتاج سوگنو قسمت انتخاب نوع استلزام و سبک تجمیع قواعد فازی (به‌منظور گردآوری قواعد فازی برای استنتاج و نتیجه‌گیری) غیرفعال شده است. برای انتخاب نوع استلزام در نرم‌افزار MATLAB از Prod استفاده می‌شود زیرا عملگر Min مجموعه فازی خروجی را کوتاه و ناقص می‌کند. غیرفازی‌ساز موجود در سیستم A+FEX، خروجی فازی را تبدیل به یک عدد قطعی می‌کند. در قسمت غیرفازی‌ساز نرم‌افزار MATLAB از روش مرکزی استفاده می‌شود زیرا این غیرفازی‌ساز به کاهش پیچیدگی مسئله و نیز زمان کمتری برای محاسبات کمک می‌کند. در اینجا به دلیل متصل‌شدن قواعد فازی سیستم با استفاده از عملگر And، در نرم‌افزار MATLAB سبک تجمیع قواعد فازی Sum را انتخاب می‌کنیم. دراین‌صورت مجموع دقیق‌تر هر مجموعه خروجی قواعد درنظر گرفته می‌شوند نه حداکثر آن‌ها.

**مرحله پنجم: شرح چگونگی استفاده از سیستم خبره طراحی‌شده و تحلیل خروجی‌های آن**

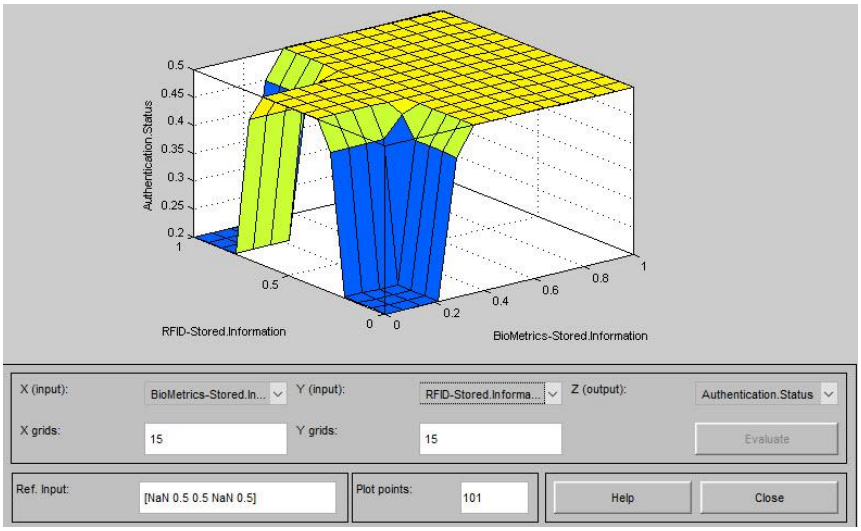
به‌منظور بررسی دقیق تأثیر متغیرهای ورودی بر متغیر خروجی سیستم A+FEX، می‌توان از ابزار واسط کاربری گرافیکی نرم‌افزار جعبه ابزار فازی نرم‌افزار MATLAB یعنی Surface viewer استفاده کرد. در اینجا باید تأثیر متغیرهای ورودی را به صورت دو به دو بر روی متغیر خروجی بررسی کرد. شکل (۷-۸ و ۹)، به حساسیت متغیر خروجی سیستم A+FEX یعنی بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بیومتریک بر اساس متغیرهای ورودی سیستم، در قسمت Surface viewer نرم‌افزار MATLAB می‌پردازد:




**شکل ۷. تحلیل حساسیت متغیر خروجی سیستم بر اساس متغیرهای متغیر امن‌بودن حجم اطلاعات تبادل‌شده در RFID و متغیر امن‌بودن وضعیت موارد غیرمجاز در RFID.**




**شکل ۸. تحلیل حساسیت متغیر خروجی سیستم بر اساس متغیرهای متغیر امن‌بودن حجم اطلاعات ذخیره‌شده در بایومتریک و متغیر امن‌بودن وضعیت موارد غیرمجاز در بیومتریک.**




**شکل ۹. تحلیل حساسیت متغیر خروجی سیستم بر اساس متغیرهای متغیر امن بودن حجم اطلاعات ذخیره شده در RFID و متغیر امن بودن حجم اطلاعات ذخیره شده در بایومتریک.**

به منظور تحلیل رفتار متغیر خروجی سیستم بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بایومتریک A+FEX می‌توان به تحلیل خروجی‌های سیستم A+FEX به‌صورت عددی (دقیق) و زبانی پرداخت. شکل ۱۰، به تحلیل رفتار متغیرهای ورودی و خروجی ماژول سیستم A+FEX می‌پردازد.


**شکل ۱۰. تحلیل رفتار متغیر خروجی در ماژول بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بیومتریک به صورت عددی و زبانی بر اساس ۵ متغیر ورودی.**

در اینجا، با استفاده از خروجی‌های سیستم A+FEX می‌توان وضعیت بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بایومتریک را بر اساس متغیرهایی چون متغیر امن‌بودن حجم اطلاعات ذخیره‌شده در RFID، متغیر امن‌بودن حجم اطلاعات تبادل‌شده در RFID، متغیر امن‌بودن وضعیت موارد غیرمجاز در RFID، متغیر امن‌بودن حجم اطلاعات ذخیره‌شده در بیومتریک و متغیر امن‌بودن وضعیت موارد غیرمجاز در بیومتریک مورد تحلیل قرار داد.

### ارزیابی نهایی پاسخ‌های سیستم خبره (اعتبارسنجی سیستم)

پس از طراحی سیستم خبره تحقیق، خروجی‌ها و جواب‌های سیستم خبره این تحقیق در یک ابزار گردآوری اطلاعات جداگانه با نظرات ۱۸ نفر از خبرگان مذکور مقایسه شدند که نتیجه آن را می‌توان در جدول ۷ مشاهده کرد:

**جدول ۷. نظرات خبرگان در مورد وضعیت بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بایومتریک.**

| قواعد سیستم خبره | حداقل | حداکثر | میانگین پاسخ‌های خبرگان | انحراف معیار |
|---|---|---|---|---|
| Rule.۳ | ۱ | ۲ | ۱/۲۲ | ۰.۴۲۸ |
| Rule.۴۵ | ۲ | ۳ | ۲/۷۲ | ۰.۴۶۱ |
| Rule.۷۹ | ۲ | ۴ | ۲/۷۸ | ۰.۵۴۸ |
| Rule.۸۶ | ۱ | ۲ | ۱/۶۷ | ۰.۴۸۵ |
| Rule.۱۰۳ | ۱ | ۳ | ۱/۶۷ | ۰.۵۹۴ |
| Rule.۱۴۰ | ۲ | ۴ | ۲/۷۸ | ۰.۶۴۷ |
| Rule.۱۵۷ | ۲ | ۴ | ۳ | ۰.۶۸۶ |
| Rule.۲۱۹ | ۲ | ۴ | ۲/۹۴ | ۰.۵۳۹ |
| Rule.۲۲۴ | ۲ | ۴ | ۳/۳۹ | ۰.۶۹۸ |
| Rule.۲۳۵ | ۲ | ۴ | ۲/۶۷ | ۰.۵۹۴ |

با توجه به اطلاعات توصیفی موجود در جدول ۶ می‌توان به مقایسه خروجی‌های سیستم خبره این تحقیق یعنی A+FEX با میانگین نظرات خبرگان پرداخت. از آن‌جایی که نظرات خبرگان بر اساس طیف ۵ تایی لیکرت (۱ تا ۵) بیان شده‌اند از این‌رو به‌منظور آزمودن فرض بالا می‌توان از درصد اختلاف بین خروجی‌های سیستم خبره این تحقیق یعنی A+FEX با میانگین نظرات خبرگان به شرح جدول ۸ استفاده کرد:

**جدول ۸. اطلاعات مربوط به مقایسه خروجی‌های سیستم A+FEX با میانگین نظرات خبرگان.**

| تفاوت نهایی | نسبت اختلاف | میانگین پاسخ‌های خبرگان | خروجی‌های سیستم خبره | قواعد سیستم خبره |
|---|---|---|---|---|
| ۰/۰۶۴۷۵ | ۰/۰۵۵ = ۴ / ۰/۲۲ | ۱/۲۲ | ۱ | Rule.۳ |
| | ۰/۰۶۷۵ = ۴ / ۰/۲۸ | ۲/۷۲ | ۳ | Rule.۴۵ |
| | ۰/۰۵۵ = ۴ / ۰/۲۲ | ۲/۷۸ | ۳ | Rule.۷۹ |
| | ۰/۰۸۲۵ = ۴ / ۰/۲۲ | ۱/۶۷ | ۲ | Rule.۸۶ |
| | ۰/۰۸۲۵ = ۴ / ۰/۲۲ | ۱/۶۷ | ۲ | Rule.۱۰۳ |
| | ۰/۰۵۵ = ۴ / ۰/۲۲ | ۲/۷۸ | ۳ | Rule.۱۴۰ |
| | ۰ = ۴ / ۰ | ۳ | ۳ | Rule.۱۵۷ |
| | ۰/۰۱۵ = ۴ / ۰/۰۶ | ۱/۹۴ | ۲ | Rule.۲۱۹ |
| | ۰/۱۵۲۵ = ۴ / ۰/۶۱ | ۱/۳۹ | ۲ | Rule.۲۲۴ |
| | ۰/۰۸۲۵ = ۴ / ۰/۲۲ | ۱/۷۸ | ۲ | Rule.۲۳۵ |

نتایج جدول ۸ نشان می‌دهد اختلاف نهایی بین خروجی‌های سیستم خبره تحقیق یعنی A+FEX و میانگین نظرات خبرگان معنی‌دار نیست و برابر با ۰/۰۶۴۷۵ است. از آن‌جایی که دلیل کافی برای پذیرش فرض صفر وجود ندارد؛ فرض مقابل پذیرفته می‌شود یعنی بین میانگین نظرات خبرگان و خروجی‌های سیستم A+FEX تفاوت معناداری وجود ندارد.

نتایج تحلیل‌های آماری جدول ۳ نشان می‌دهد بر اساس نظرات و تجربه حرفه‌ای خبرگان حوزه امنیت اطلاعات و ارتباطات (امنیت سایبری)، متغیر شناسایی از طریق امواج رادیویی با میانگین موزون (۴.۲۸۰) اهمیت بیشتری از متغیر شاخص بایومتریک با میانگین موزون (۴.۲۹۳) دارد. با توجه به اهمیت بالای شاخص بایومتریک (میانگین موزون بیشتر

از RFID)، کارت‌های RFID به‌تنهایی برای محرمانگی کفایت نمی‌کنند و نیاز است به مواردی چون: اهمیت امن‌بودن مؤلفه بلوک سنسور (دریافت‌کننده اطلاعات)، امکان مدیریت‌کردن امنیت مؤلفه بلوک سنسور (دریافت‌کننده اطلاعات)، اهمیت امن‌بودن مؤلفه بلوک استخراج ویژگی‌ها، امکان مدیریت‌کردن امنیت مؤلفه بلوک استخراج ویژگی‌ها، اهمیت امن‌بودن مؤلفه بلوک مقایسه ویژگی‌ها، امکان مدیریت‌کردن امنیت مؤلفه بلوک مقایسه ویژگی‌ها، اهمیت امن‌بودن مؤلفه بلوک تصمیم (تصدیق یا رد هویت) و امکان مدیریت‌کردن امنیت مؤلفه بلوک تصمیم (تصدیق یا رد هویت) نیز توجه ویژه شود تا بتوان به بهبود احراز هویت کمک کرد. از طرفی دیگر، همان‌طور که در آزمون همبستگی بین متغیرهای پژوهش مشاهده شد، بین اهمیت امن‌بودن مؤلفه تگ (فرستنده خودکار) و امکان مدیریت‌کردن امنیت مؤلفه وضعیت موارد غیرمجاز، رابطه مثبت و معنی‌داری وجود دارد زیرا ضریب همبستگی پیرسون بین آنها برابر با (۰.۷۱۷) شده است. رابطه بین اهمیت امن‌بودن مؤلفه حجم اطلاعات ذخیره‌شده و امکان مدیریت‌کردن امنیت مؤلفه کدخوان (بررسی‌کننده) بر اساس ضریب همبستگی برابر با (۰.۹۶۳) شده است. همچنین، ضریب همبستگی بین امکان مدیریت‌کردن امنیت مؤلفه سیستم کنترل‌کننده (هاست) و اهمیت امن‌بودن مؤلفه حجم اطلاعات تبادل‌شده برابر با (۰.۴۶۳) است. در واقع با توجه به همبستگی بالای بین مهم‌ترین شاخص‌های متغیر شناسایی از طریق امواج رادیویی و احراز هویت می‌توان نتیجه‌گیری کرد که با درنظرگرفتن امنیت مؤلفه‌های RFID می‌توان به بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی دست یافت.

همچنین نتایج نشان داد میزان میانگین موزون متغیر وابسته احراز هویت (۴.۲۰۳) تعیین شد. از طرفی، اهمیت امن‌بودن مؤلفه سیستم کنترل‌کننده (هاست) با میانگین (۴.۶۰) به‌عنوان مهم‌ترین مؤلفه در متغیر شناسایی از طریق امواج رادیویی، اهمیت امن‌بودن مؤلفه بلوک استخراج ویژگی‌ها با میانگین (۴.۵۰) به‌عنوان مهم‌ترین مؤلفه در متغیر شاخص بایومتریک و در نهایت امکان مدیریت‌کردن امنیت مؤلفه حجم اطلاعات تبادل‌شده با میانگین (۴.۶۰) به‌عنوان مهم‌ترین مؤلفه در متغیر احراز هویت مشخص شدند. از طرفی، اهمیت امن‌بودن مؤلفه سیستم کنترل‌کننده (هاست) در سیستم RFID می‌تواند به‌عنوان بستری برای بلوک استخراج ویژگی‌های اشخاص در شاخص بایومتریک باشد و با توجه به اهمیت بالای این دو مؤلفه در مدیریت‌کردن امنیت مؤلفه حجم اطلاعات تبادل‌شده و احراز هویت می‌توان نتیجه گرفت که شاخص‌های بایومتریک با رویکرد ترکیبی با شناسایی از طریق امواج رادیویی می‌تواند در احراز هویت بهبود ایجاد کند. برای انجام تحلیل‌های فازی به‌منظور بهبود وضعیت احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بایومتریک می‌توان از شکل‌های (۷-۸ و ۹) استفاده کرد. از طرفی دیگر، بین اهمیت امن‌بودن مؤلفه بلوک استخراج ویژگی‌ها و امکان مدیریت‌کردن امنیت مؤلفه وضعیت موارد غیرمجاز رابطه مثبت و معنی‌داری وجود دارد زیرا ضریب همبستگی پیرسون بین آنها برابر با (۰.۶۳۲) شده است. رابطه بین اهمیت امن‌بودن مؤلفه حجم اطلاعات ذخیره‌شده و امکان مدیریت‌کردن امنیت مؤلفه بلوک تصمیم (تصدیق یا رد هویت) با ضریب همبستگی (۰.۶۰۸) تأیید شده است. همچنین، ضریب همبستگی بین اهمیت امن‌بودن مؤلفه بلوک سنسور (دریافت‌کننده اطلاعات) و اهمیت امن‌بودن مؤلفه حجم اطلاعات تبادل‌شده برابر با (۰.۸۵۷) است. رابطه بین اهمیت امن‌بودن مؤلفه حجم اطلاعات ذخیره‌شده و اهمیت امن‌بودن مؤلفه بلوک مقایسه ویژگی‌ها با ضریب همبستگی (۰.۵۹۹) تأیید شده است. در واقع با توجه به همبستگی بالای بین مهم‌ترین شاخص‌های متغیر شاخص بایومتریک و متغیر احراز هویت می‌توان نتیجه‌گیری کرد که با مدیریت و درنظرگرفتن امنیت مؤلفه‌های شاخص بایومتریک می‌توان به بهبود احراز هویت مبتنی بر شاخص بیومتریک دست یافت.

بر اساس نتایج جدول ۸ اختلاف نهایی بین خروجی‌های سیستم خبره این تحقیق یعنی A+FEX و میانگین نظرات خبرگان معنی‌دار نیست و برابر (۰/۰۶۴۷۵) است بنابراین بین میانگین نظرات خبرگان و خروجی‌های سیستمA+FEX تفاوت معناداری وجود ندارد. از طرفی دیگر، با توجه به شکل ۹، با استفاده از خروجی‌های سیستم A+FEX می‌توان وضعیت بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بیومتریک را بر اساس متغیرهایی چون

متغیر امن‌بودن حجم اطلاعات ذخیره‌شده در RFID، متغیر امن‌بودن حجم اطلاعات تبادل‌شده در RFID، متغیر امن‌بودن وضعیت موارد غیرمجاز در RFID، متغیر امن‌بودن حجم اطلاعات ذخیره‌شده در بیومتریک و متغیر امن‌بودن وضعیت موارد غیرمجاز در بیومتریک مورد تحلیل قرار داد؛ برای مثال:

اگر:

- متغیر امن‌بودن حجم اطلاعات ذخیره‌شده در RFID ضعیف باشد
- و متغیر امن‌بودن حجم اطلاعات تبادل‌شده در RFID در وضعیت نرمال باشد
- و متغیر امن‌بودن وضعیت موارد غیرمجاز در RFID خوب باشد
- و متغیر امن‌بودن حجم اطلاعات ذخیره‌شده در بایومتریک خوب باشد
- و متغیر امن‌بودن وضعیت موارد غیرمجاز در بایومتریک نرمال باشد

آن‌گاه:

وضعیت بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بیومتریک در سومین سطح خود یعنی متوسط (معمولی) قرار دارد.

به بیانی دقیق‌تر، با استفاده از سیستم خبره طراحی‌شده در این تحقیق می‌توان وضعیت بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بیومتریک را به‌صورت عددی و دقیق‌تر نیز بررسی کرد:

اگر:

- متغیر امن‌بودن حجم اطلاعات ذخیره‌شده در RFID ضعیف، یعنی دقیقاً ۰.۱۵ باشد
- و متغیر امن‌بودن حجم اطلاعات تبادل‌شده در RFID در وضعیت نرمال، یعنی دقیقاً ۰.۵ باشد
- و متغیر امن‌بودن وضعیت موارد غیرمجاز در RFID خوب، یعنی دقیقاً ۰.۸۵ باشد
- و متغیر امن‌بودن حجم اطلاعات ذخیره‌شده در بایومتریک خوب، یعنی دقیقاً ۰.۸۵ باشد
- و متغیر امن‌بودن وضعیت موارد غیرمجاز در بایومتریک نرمال، یعنی دقیقاً ۰.۵ باشد

آن‌گاه

وضعیت بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بایومتریک در سطح متوسط یعنی دقیقاً ۰.۵۷۲ قرار دارد.

## نتیجه‌گیری

این تحقیق یک راه نظام‌مند به‌منظور ارائه روشی برای بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بیومتریک با استفاده از سیستم خبره فازی، برای استفاده در حوزه امنیت اطلاعات و ارتباطات (امنیت سایبری) ارائه می‌دهد. مزایای سیستم خبره بهبود احراز هویت مبتنی ارائه‌شده عبارت از کمک به مدیر برای تصمیم‌گیری در ارتباط با مسائل بهبود احراز هویت و بهبود کارایی تصمیم‌گیری در بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بایومتریک و توجه بیشتر به اثربخشی آن است. با توجه به معیارهایی نظیر توسعه دانش درباره مسائل بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بایومتریک با استفاده از منطق فازی و نیز نبود یک سیستم به‌منظور ارائه توصیه‌هایی به مدیر برای تصمیم‌گیری در مورد مسائل بهبود احراز هویت می‌توان به اهمیت و ضرورت انجام این تحقیق اشاره کرد. به‌منظور بهبود در احراز هویت نیاز است که به مواردی از قبیل: اهمیت امن‌بودن مؤلفه تگ (فرستنده خودکار)، امکان مدیریت‌کردن امنیت مؤلفه تگ (فرستنده خودکار)، اهمیت امن‌بودن مؤلفه کدخوان (بررسی‌کننده)، امکان مدیریت‌کردن امنیت مؤلفه کدخوان (بررسی‌کننده)، اهمیت امن‌بودن مؤلفه سیستم کنترل‌کننده (هاست)، امکان مدیریت‌کردن امنیت مؤلفه سیستم کنترل‌کننده (هاست)، اهمیت امن‌بودن مؤلفه بلوک سنسور (دریافت‌کننده اطلاعات)، امکان مدیریت‌کردن امنیت مؤلفه بلوک سنسور (دریافت‌کننده اطلاعات)، اهمیت امن‌بودن

مؤلفه بلوک استخراج ویژگی‌ها، امکان مدیریت‌کردن امنیت مؤلفه بلوک استخراج ویژگی‌ها، اهمیت امن‌بودن مؤلفه بلوک مقایسه ویژگی‌ها، امکان مدیریت‌کردن امنیت مؤلفه بلوک مقایسه ویژگی‌ها، اهمیت امن‌بودن مؤلفه بلوک تصمیم (تصدیق یا رد هویت)، امکان مدیریت‌کردن امنیت مؤلفه بلوک تصمیم (تصدیق یا رد هویت)، اهمیت امن‌بودن مؤلفه حجم اطلاعات ذخیره‌شده، امکان مدیریت‌کردن امنیت مؤلفه حجم اطلاعات ذخیره‌شده، اهمیت امن‌بودن مؤلفه حجم اطلاعات تبادل‌شده، امکان مدیریت‌کردن امنیت مؤلفه حجم اطلاعات تبادل‌شده، اهمیت امن‌بودن مؤلفه وضعیت موارد غیرمجاز، امکان مدیریت‌کردن امنیت مؤلفه وضعیت موارد غیرمجاز، توجه ویژه‌ای شود. مهم‌ترین محدودیت‌های پژوهش را می‌توان مشکلات موجود در حین انجام کار، از قبیل نبود یک مدل مشابه به‌منظور بررسی بهبود احراز هویت مبتنی بر شناسایی از طریق امواج رادیویی و شاخص بیومتریک دانست که با استفاده از یافته‌های آن بتوان متغیرهای پژوهش را به‌صورت جامع‌تری تحلیل کرد.

## References


[1] Dorostan, R., Zabihi, H., Asgharzadeh, A., & Gorji Poshti, M. (2021). Explaining the Components of Feeling Safe in Crime Prevention in Urban Design (Case Study: Rajai Main Street, Karaj). *Quarterly Scientific Journal of National University of Skills*, *18*(Special Issue 1), 77-93. https://doi.org/10.48301/kssa.2021.130678

[2] Askari, E., & Motamed, S. (2021). Authentication and Access Control in IoT Based on Hash Chain Algorithm and Improved Fingerprint with emphasis on its military applications. *Iranian Journal of Marine technology*, *8*(4), 1-13. https://doi.org/10.22034/ijmt.2021.526748.1669

[3] Gholizadeh, M. H., Esmaili, M., Ebrahimpour, M., & Moradi, M. (2023). Strategic Analysis of Blockchain Technology to Facilitate the KYC for the Social Security Organization Costumers Based on Actor-Network Theory. *Sciences and Techniques of Information Management*, *9*(1), 279-310. https://doi.org/10.22091/stim.2021.6920.1581

[4] Bahrami, S., Zabardast, M. A., & Salimi, J. (2021). Study of the factors affecting the process of formation and development of professional identity of faculty members. *Quarterly Scientific Journal of National University of Skills*, *17*(Special Issue), 13-26. https://doi.org/10.48301/kssa.2021.128452

[5] Patel, U. A., & Priya, S. (2014). Development of a student attendance management system using RFID and face recognition: a review. *International Journal of Advance Research in Computer Science and Management Studies*, *2*(8), 109-119. https://www.academia.edu/9421523/Development_of_a_Student_Attendance_Management_System_Using_RFID_and_Face_Recognition_A_Review

[6] Tronci, R., Giacinto, G., & Roli, F. (2009). Designing multiple biometric systems: Measures of ensemble effectiveness. *Engineering Applications of Artificial Intelligence*, *22*(1), 66-78. https://doi.org/10.1016/j.engappai.2008.04.007

[7] Peiravi, N., & Jafari, S. (2009, May 24). *Identity verification integration model design, with the help of biometric index and RFID to participate in electronic interactions* [Conference session]. The Second Conference on Electronic City, Tehran, Iran. https://civilica.com/doc/71903/

[8] Peng, N., Liu, X., & Zhang, S. (2021). RF-Ubia: User Biometric Information Authentication Based on RFID. In Z. Liu, F. Wu, & S. K. Das (Eds.), *Wireless Algorithms, Systems, and Applications* (pp. 135-146). Springer International Publishing. https://doi.org/10.1007/978-3-030-86130-8_11

[9] Naseri, A., & Tabatabaei Manesh, S. R. (2020). Providing an algorithm for authentication of radio transmitters Based on power amplifier nonlinear behavior. *Journal of Command and Control*, *4*(2), 84-101. http://ic4i-journal.ir/article-1-202-en.html

[10] Chothia, T., & Smirnov, V. (2010). A Traceability Attack against e-Passports. In R. Sion (Ed.), *Financial Cryptography and Data Security* (pp. 20-34). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-14577-3_5

[11] Erguler, I. (2015). A potential weakness in RFID-based Internet-of-things systems. *Pervasive and Mobile Computing*, *20*, 115-126. https://doi.org/10.1016/j.pmcj.2014.11.001

[12] Alavi, S. M., Abdul Maleki, B., & Bagheri, K. (2014). Analysis of confidentiality and security of two-way authentication protocol in RFID systems based on abstracting functions. *Electronic and Cyber Defense*, *2*(2), 23-31. https://ecdj.ihu.ac.ir/article_208219.html?lang=en

[13] Salami, Y., & Hosseini, S. (2023). BSAMS: Blockchain-Based Secure Authentication Scheme in Meteorological Systems. *Nivar*, *47*(120-121), 181-197. https://doi.org/10.30467/nivar.2023.415722.1260

[14] Abdollahi, A., Sajadieh, M., & Yazdani, M. R. (2023). LRAPM: A Lightweight RFID Authentication Protocol for MIoT Systems. *Technovations of Electrical Engineering in Green Energy System*, *1*(4), 71-89. https://doi.org/10.30486/teeges.2022.1968457.1039

[15] Liu, J., Zou, X., Lin, F., Han, J., Xu, X., & Ren, K. (2021, July 07-10). *Hand-Key: Leveraging Multiple Hand Biometrics for Attack-Resilient User Authentication Using COTS RFID* [Conference session]. 41st International Conference on Distributed Computing Systems, District of Columbia, USA. https://doi.org/10.1109/ICDCS51616.2021.00103

[16] Elahi, S. B., Rashidi, M., & Sadeghi, M. (2015). Designing fuzzy expert system for chief privacy officer in government and businesses E-transactions. *Journal of information technology management*, *7*(3), 511-530. https://doi.org/10.22059/jitm.2015.54073

[17] Valentine, N. H., Akaerue, E. I., Etido, M. G., & Davies-Ekpo, C. S. (2024). A 3-factor authentication access control system using RFID, fingerprint, token and code. *Multimedia Tools and Applications*, *83*(15), 43635-43647. https://doi.org/10.1007/s11042-023-17325-2

[18] Mahmoudi-Nasr, P., & Kimia, H. (2022). A Mutual Authentication Method for Internet of Things. *Signal and Data Processing*, *19*(2), 73-86. https://doi.org/10.52547/jsdp.19.2.73

[19] Meivel, S., Praghadeesh, C., Ravinder, A., & Sibisaran, D. (2022, May 09-11). *Hybrid Student Authentication System Using RFID Reader and Face Biometrics Using Deep Learning Techniques* [Conference session]. 2022 International Conference on Applied Artificial Intelligence and Computing, Salem, India. https://doi.org/10.1109/ICAAIC53929.2022.9792810

[20] Sepehrzadeh, H. (2022). A Method for Assessing the Security Risk in Cyber-Physical Systems with Incomplete Information Using Bayesian Game Theory. *Quarterly Scientific Journal of National University of Skills*, *19*(1), 495-521. https://doi.org/10.48301/kssa.2022.320681.1909

[21] Leyu, Z., Xinyou, Z., Yunjia, F., Shuyao, L., Jun, B., & Xijia, H. (2021, December 17-19). *Design and Implementation of RFID Access Control System Based on Multiple Biometric Features* [Conference session]. 18th International Computer Conference on Wavelet Active Media Technology and Information Processing, Chengdu, China. https://doi.org/10.1109/ICCWAMTIP53232.2021.9674127

[22] Wahyudono, B., & Ogi, D. (2020, November 19-20). *Implementation of Two Factor Authentication based on RFID and Face Recognition using LBP Algorithm on Access Control System* [Conference session]. 2020 International Conference on Information and Communication Technology for Smart Society, Bandung, Indonesia. https://doi.org/10.1109/ICISS50791.2020.9307564

[23] Mardani, M., Abdolmaleki, B., & Bagheri, K. (2015). Weaknesses of SPRS Authentication Protocol and Present a Developed Protocol for RFID Systems. *Electronic and Cyber Defense*, *3*(3), 39-48. https://ecdj.ihu.ac.ir/article_200092.html?lang=en

[24] Ren, H., Song, Y., Yang, S., & Situ, F. (2016, August 23-25). *Secure smart home: A voiceprint and internet based authentication system for remote accessing* [Conference session]. 11th International Conference on Computer Science & Education, Nagoya, Japan. https://doi.org/10.1109/ICCSE.2016.7581588

[25] Sanayei, A., Sobhanmanesh, F., Sobhanmanesh, F., & Ghazifard, A. (2011). The Factors Influencing the Development of Radio Frequency Identification Technology in E-Supply Chain Management (Case study: Iran Khodro Industrial Group (IKCO)). *New Marketing Research Journal*, *1*(1), 41-70. https://nmrj.ui.ac.ir/article_17573.html?lang=en

[26] Safkhani, M., Bagheri, N., & Naderi, M. (2011). Cryptanalysis of SEAS: An RFID Authentication Protocol. *Electronics Industries*, *2*(3), 77-92. https://ei.sinaweb.net/article_591480.html?lang=en

[27] Kulkarni, S., Raut, R. D., & Dakhole, P. K. (2016). A Novel Authentication System Based on Hidden Biometric Trait. *Procedia Computer Science*, *85*(35), 255-262. https://doi.org/10.1016/j.procs.2016.05.229

[28] Murillo-Escobar, M. A., Cruz-Hernández, C., Abundiz-Pérez, F., & López-Gutiérrez, R. M. (2015). A robust embedded biometric authentication system based on fingerprint and chaotic encryption. *Expert Systems with Applications*, *42*(21), 8198-8211. https://doi.org/10.1016/j.eswa.2015.06.035

[29] Ting, S. L., & Tsang, A. H. C. (2013). A two-factor authentication system using Radio Frequency Identification and watermarking technology. *Computers in Industry*, *64*(3), 268-279. https://doi.org/10.1016/j.compind.2012.11.002

[30] Ustundag, A., Kılınç, M. S., & Cevikcan, E. (2010). Fuzzy rule-based system for the economic analysis of RFID investments. *Expert Systems with Applications*, *37*(7), 5300-5306. https://doi.org/10.1016/j.eswa.2010.01.009

[31] Wen, W. (2010). An intelligent traffic management expert system with RFID technology. *Expert Systems with Applications*, *37*(4), 3024-3035. https://doi.org/10.1016/j.eswa.2009.09.030