scientific reports

Check for updates

OPEN

Multiple biometric authentication for online banking system based on multiple fuzzy approach

Nazirah Mohammed Anwar[1], Sharifah Sakinah Syed Ahmad[1], Nasreen Kausar[2], Željko Stević[3] & Yaé U. Gaba[4]✉

Online banking continues to grow in popularity due to its convenience, but banks face significant challenges in ensuring secure customer identity verification. Traditional authentication methods such as PINs, passwords, and one-time passwords have shown limitations, especially in the wake of the COVID-19 pandemic, which accelerated the demand for seamless and contactless solutions. Voice biometrics have emerged as a reliable alternative, offering enhanced fraud protection and a more user-friendly experience. In Malaysia, this technology enables customer verification without the need for PINs or security questions. This study proposes an advanced authentication approach that integrates keystroke dynamics and voice biometrics within a multi-factor authentication framework. By leveraging artificial intelligence and fuzzy logic, the system aims to deliver heightened security and a smoother user experience. The goal is to provide Malaysian online banking users with a safer and more secure digital environment.

Keywords Fuzzy rules based, Multi-factor authentication, Fuzzy expert knowledge, Keystroke behaviour

With more clients accepting online banking, it is becoming more popular and pervasive. They are convenient and cost-effective for both financial institutions and customers, but they are susceptible to user authentication concerns, as well as the danger of identity theft and financial fraud.

Because of the lack of face-to-face communication, identifying the genuine user is both crucial and difficult. Biometrical technologies are becoming ever more common and profound in banking information technologies, both in physical interaction with points such as Automated Teller Machines (ATMs) and in electronic systems that are operable remotely (remote electronic banking, such as online banking, mobile banking, and phone banking), because they provide an opportunity to solve many of the security difficulties[1] they might pose for user authentication in online banking as biometric authentication systems[2]. These technologies are intended to mitigate the negative consequences of cyber-criminal conduct[3], such as the theft of log-in credentials and money fraud fingerprint films that deceive fingerprint sensors and stolen passcodes[4]. This is how the critical requirement for more accurate user identity validation[5] when using online banking is addressed, and how it is demonstrated as a direct manner of reducing data theft.

We are nearly unable to remain anonymous in these times, consequently, ongoing advancements in digital security and access verification measures are required. Artificial intelligence is one of the most advanced advances in computing today, and it can be effectively utilized in security and communication in a multimedia system. In computer science, security and safe communication are major trends. Physiological biometrics verify a person's identity by using their iris scans, fingerprints, or face traits[6]. Behavioural biometrics may identify patterns in a user's speech, keystrokes, and other characteristics[7]. A few specialized systems have been created to provide secure communication, especially when it comes to mobile communication, where high user expectations must be met by existing architectures. When more than two user authentication methods are combined, such as biometric information, a smartphone or token, and password knowledge, the process is known as multiple factor authentication, or MFA[8]. Therefore, one of the ways to solve the user identity problem and strengthen the user authentication method is to implement many biometric together in one authentication, as in this research biometric as keystroke behaviour and voice verification, are two biometrics authentications method used for single login. In terms of implementation, voice identity is a relatively inexpensive solution when compared

[1]Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, UTeM, Melaka, Malaysia. [2]Department of Mathematics, Faculty of Arts and Science, Balikesir University, 10145 Balikesir, Turkey. [3]Department of Mobile Machinery and Railway Transport, Faculty of Transport Engineering, Vilnius Gediminas Technical University, 10223 Vilnius, Lithuania. [4]Research and Innovation Centre (AIMS RIC), African Institute for Mathematical Sciences, Rue KG590 ST 1, P.O Box: 6428, Kigali, Rwanda. ✉email: yaeulrich.gaba@gmail.com

to sophisticated procedures and devices for iris verification. Several financial institutions have recently added multifactor authentication (MFA) to their security systems to thwart sophisticated attacks and provide a higher level of protection for sensitive operations[9]. MFA incorporates various modalities of user authentication, including what the user is (biometric data), what the user possesses (a smartphone or token), and what they know (a password)[10].

This study proposed a better user authentication method, especially for the online transaction signing by implementing the multiple biometric authentication as keystroke behaviour and Voice Biometric in Multi-Factor Authentication with Fuzzy Rules Based using the Mamdani Technique, in Fuzzy Logic. Fuzzy logic systems offer alternatives to the difficulty of mathematically modelling complex non-linear circumstances, and fuzzy logic fits the mathematical modelling demands of a process or system. Fuzzy logic-based systems can provide effective results when supplemented with indefinite linguistic knowledge, as can humans. In fuzzy logic, information is expressed in linguistic expressions such as big, tiny, extremely, few, and so on, rather than numerical values. When a system's behaviour is frequently governed by rules or requires extremely complicated non-linear processes, fuzzy logic techniques are frequently used in this research[11]. Fuzzy logic can be the best for the risk evaluation as it can set for the input parameters[12]. This research discussed the problem of the current existing user authentication method and proposed a better verification method based on artificial intelligence methods for Multi-Factor Authentication and compares the existing online banking authentication with the proposed authentication method using the Fuzzy Expert Knowledge.

Literature review

The banking sector in Malaysia is robust and well-developed, with a high level of financial inclusion. As of 2023, about 90% of the population is banked[13]. The banking sector contributes significantly to Malaysia's GDP. The finance industry has shown resilience, with stable credit growth and low non-performing loan (NPL) ratios[14]. Strong labour market conditions and proactive policies have helped maintain low NPL ratios, which are expected to remain under 2%. Biometric authentication methods such as facial recognition, fingerprint scans, and voice recognition are increasingly used in banking for secure identity verification[15]. Biometric systems can improve security and protect assets, providing insights into the application of biometrics in banking environments[16.] However, scammers regularly try to infiltrate social media accounts, personal bank accounts, and e-mail accounts[2]. Considering sensitive data is accessible through online banking services, effective and trustworthy security measures must be implemented. Strong authentication is critical to provide the finest security and[17] phishing is the practice of sending e-mails to recipients acting as legal financial companies and asking for confidential data such as usernames and passwords. Hacking may allow you to swipe money from an e-account. These hackers have previously attacked many banks' websites and collected enormous sums of money using their technological prowess; e-transactions rely entirely on internet banking[18]. Nonetheless, the rise of severe cyber threats has shown that passwords alone are insufficient to prevent unauthorized access to user accounts[19]. Strong authentication is required to guarantee high anonymity and security[20].

The typical banking transaction is evolving in today's environment, from utilizing a bank book to using a computer. As a result of technological advancements, typical banking transactions are switching from utilizing a bank book over the counter to do online transactions[21]. Secure online financial transactions are a major priority in today's banking system[22]. Several security issues have been reported in the news. The security problem began in August 1995, with attackers hacking into their system[23] resulting in a $10 million loss estimate. It was the first successful intrusion by a hacker into the system containing the $10 million unlawfully transferred cash, with $400,000 still missing[4]. Three individuals were apprehended by British authorities in August 2000 in connection with a scheme to defraud the Egg Banking System[23]. A hacking incident cost an Arkansas fire alarm firm more than $110,000 in April 2010[4]. Hackers gained access to the company's computer system and stole the company's online banking passwords, as well as draining the payroll account. Someone had confirmed two bundles of finance instalments, one for $45,000 and the other for $67,000, over the last few days. Melanie Eakel, CEO of JE Frameworks Inc., was informed by the bank a few days later about the Web Address used to process the payments, as well as the username and password for online banking[6]. Because of the reported financial thefts, it is evident that the online banking system needs to be strengthened even via mobile devices[10]. Many sorts of studies on banking security have been published by experts and academics, particularly in the context of user authentication methods.

To execute keyboard dynamics-based user authentication, employ one of three prominent speech biometrics algorithms 1) Gaussian Mixture Model with Universal Background Model (GMM-UBM), 2) identity vector (I-vector) method to user modelling or 3) deep machine learning technique. Unlike most existing keystroke biometrics systems, which exclusively employ data from actual users during training, the suggested methods incorporate data from a broad pool of background users to improve the model's discriminative capabilities. These methods make no assumptions about the data's underlying probability distribution and may be implemented in real-time. Although these approaches were initially created for speech analysis, our trials employing these algorithms on the publicly available CMU keyboard dynamics dataset revealed a considerable reduction in the equal mistake rate[24].

Extensive worldwide research has greatly helped to clarify current online banking authentication techniques, biometrics applied in banking settings, existing hazards, forms of hacking, and fuzzy logic applied in banking. Previous research has shed important light on the weaknesses and dangers online banking systems experience, the efficiency of certain authentication techniques, and the advantages and limits of several biometric technologies. Furthermore, studies on fuzzy logic have shown its ability to manage uncertain and imprecise data, so it is a useful instrument for banking risk assessment and decision-making and some highlights the use of fuzzy logic to analyse user behaviour and detect anomalies[25], which can be relevant to your research on risk evaluation in online banking[26]. Using these insights helps banks create more sophisticated and safe authentication mechanisms,

therefore improving the general dependability and security of online banking systems. However, in this research, we will focus on the Multimodal Biometrics Authentication with double fuzzy approaches. This study mainly focuses on how to construct the secured authentication by implementing MFA with Multilayer of Fuzzy Logic but not deeply focusing on each of the biometrics methods and their assessment as the method studies were done before[14]. For example, the Voice Activity Detection Using Fuzzy Entropy was calculated and evaluated by using the accuracy of voice detected in percentage[3] and the accuracy of User Authentication Method Based on MKL for Keystroke[27].

The keystroke biometric will be authenticated and verified using the Fuzzy Rule-Based, and the output from the first stage will be applied to the second stage together with the Voice detection's output using another Fuzzy Rule-Based for risk evaluation of the fraud detection. In the final stage of the research, we will compare the existing authentication system in Online Banking with the proposed authentication system using the Fuzzy approach.

Problem statements

1. Single authentication method, might sometime forget the login details, ending up by using the common credentials which easily got attacked by the fraudsters.
2. Physiological biometrics have a few flaws, the most significant of which is their contact-driven nature, which necessitates physical presence.
3. Existing behavioural biometrics-based authentication techniques have a significant flaw since user behavioural variability is inconsistent and difficult to manage. It causes the system's performance to deteriorate, and the resultant recognition scores are unconvincing[28.]
4. Few research has been undertaken on keystroke biometric systems, compared to other fields. Despite having lesser accuracies than other biometric modalities, KB has some benefits, such being low cost, transparent, non-invasive to the user, and capable of continually monitoring a system[29].
5. Keystroke Dynamics Biometrics perform poorly in terms of authentication accuracy due to variations in typing rhythm caused by factors such as injury, exhaustion, or distraction. However, these the same factors also impact other biometric systems.

Methodology

The purpose of this research is to propose a better authentication method for online banking. Therefore, it will focus on the actual authentication flow and methods to detect fraud. This research differs from previous studies as it explores multiple layers of fuzzy logic. In the first stage, we will study a fuzzy rule-based approach on keystroke dynamics to identify genuine users. The outcome of the first test will be Boolean, either YES or NO. Then, in the next stage, we will utilize the first output together with three additional input data to develop a second fuzzy rule-based system to detect fraud during transaction signing in online banking. The first step of the research methodology is data collection. For this, the keystroke dynamics dataset created for "Comparing Anomaly-Detection Algorithms for Keystroke Dynamics" by Kevin Killourhy and Roy Maxion was used[30]. The second dataset is a synthetic dataset generated using the open-source tool, generatedata.com. The second step is to preprocess the data collected from these secondary sources to fit the design of the authentication fuzzy system. The third step involves defining linguistic terms for each interval. The fourth step is establishing the fuzzy membership functions and fuzzy sets. The fifth step is to fuzzify the dataset and establish fuzzy relations. The sixth step is to design the keystroke dynamics authentication fuzzy system using the Mamdani Fuzzy Inference System and the Transaction Signing Fraud Detection Fuzzy System based on the fuzzified datasets, then defuzzify the output values and evaluate the accuracy of the proposed transaction authentication method against existing authentication methods in online banking. Figure 1 illustrates the basic concept of multimodal biometric authentication using a multilevel fuzzy rules-based approach.

Operational procedure

The main drive of this chapter is to explain the research methodology, to accomplish the main objectives of this study. The major objective of this research is to propose Multi-Factor Authentication by construct the membership functions for Multiple Biometric outputs in Multilevel Fuzzy Rule-Based for fraud detection during transaction signing in Online Banking, equivalent to Objectives 1 and 2 in this research. Continually from Objective 2, to enhance the existing authentication method with multimodal biometrics using Fuzzy Rule-Based Artificial Intelligence, corresponding to Objective 3. The existing banking environment has already implemented biometric authentication and proven its effectiveness. What distinguishes the use of multimodal biometrics is the proposal to incorporate multiple biometric methods, enhancing security and reliability such as data collection involves gathering information from multiple biometric traits, such voice recordings, and keystroke. The data from different modalities is collected simultaneously or sequentially, ensuring consistency and alignment for accurate analysis. The collected data is stored in a structured format within a dataset. Hence, the research framework of this research will include 5 phases data acquisition, data processing, performing a Fuzzy approach, value predicting, and results from the validation phase.

Stage 1

Data collection

The first step of the research methodology is data collection, therefore keystroke dynamic dataset was created for "Comparing Anomaly-Detection Algorithms for Keystroke Dynamics" by Kevin Killourhy and Roy Maxion[30]. In this study, this publisher of the DSN 2009 conference is consulted. The information consists of keystroke

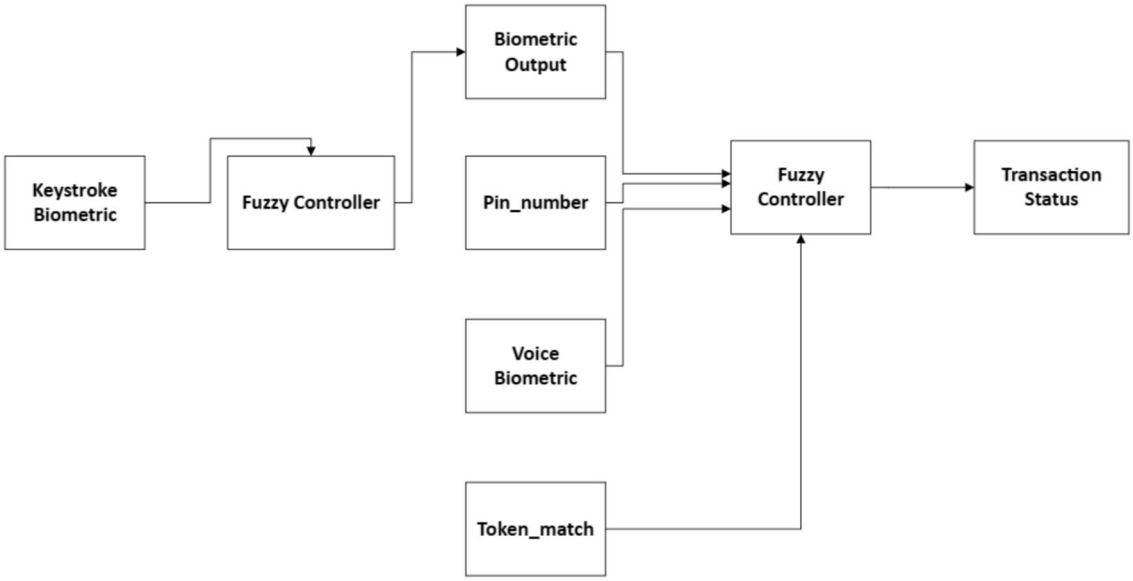

Fig. 1. Multimodal biometric authentication using multilayer fuzzy rules-based.

timings from 51 people, or typists, who each entered 400 passwords (.tie5Roanl). There are 34 columns in the table that contains the data. Every row of data contains the timing details for a single password repetition by an individual. Everybody has a unique identity in the subject column (such as s002 or s057). Although 51 people were involved in the data collection, the identities do not range from s001 to s051 since each person received a unique ID for a variety of keystroke experiments, and not every participant took part in every trial. Due to Participant 1's failure to finish the password typing assignment, s001 is not present in the dataset. The password typing session is represented by the second column, session Index, which has values between 1 and 8. The number of times the password was repeated during the session is indicated in the third column, rep, and can range from 1 to 50.

The remaining 31 columns provide the password's timing information. The column name encodes the type of timing information. The H.key column names describe the hold time for the designated key (i.e., the duration between pressing and releasing the key). The DD.key1.key2 column names give the key-down-key-down time for the named digraph. For the specified digraph, column names of the type UD.key1.key2 specify a keyup-keydown time (that is, the time between when key1 was released and when key2 was pushed).

Consider the following one-line illustration of what you'll find in the data.

subject sessionIndex rep H.period DD.period.t UD.period.t …

s002 1 1 0.1491 0.3979 0.2488 …

The sample shows the data from subject 2, session 1, repeat 1. The period key was held down for 0.1491 s (149.1 ms); the time between pressing the period key and pressing the t key (key-down-key-down time) was 0.3979 s; the time between releasing the period key and pushing the t key was 0.2488 s and so on.

The second dataset is the synthetic dataset which has been generated using the open sources tool, generatedata.com (generatedata, n.d). This is an output dataset to be implemented in fuzzy controller. The script functions as a generator for any type of random data in any format. It now has around 30 Types (data types it creates) and 8 Export Types, formats for the data (generatedata, n.d). This data contains four inputs, inputs in the format of Percentage (%), for keystroke_output, voice_detection, strength of pinnumber_input, and attempt of token_match.

Data pre-processing

As the data have been taken from research, data are processed in a good way, however, to make it work in this research some basic pre-processing method has been used. Data Cleaning is the first step as it involves handling missing data and noisy data. Next, Data Transformation by Attribute Selection new attributes are constructed from the dataset of the attributes to help the mining process such as calculating the total and average for the keystroke data for the new attribute and calculating the deviation average value from the data.

Stage 2

There are two phases involved in stage 2. As this research is purposing multiple biometric authentications using a multilevel fuzzy approach for online banking during the transaction signing, the first phase will be the Keystroke Dynamic Authentication method using Fuzzy Ruled based, refer to (Fig. 2).

There are four steps evolved in this stage, Identification of the Input parameter, Fuzzification, Construct Fuzzy Rule-Based, Generate Fuzzy Inference System.

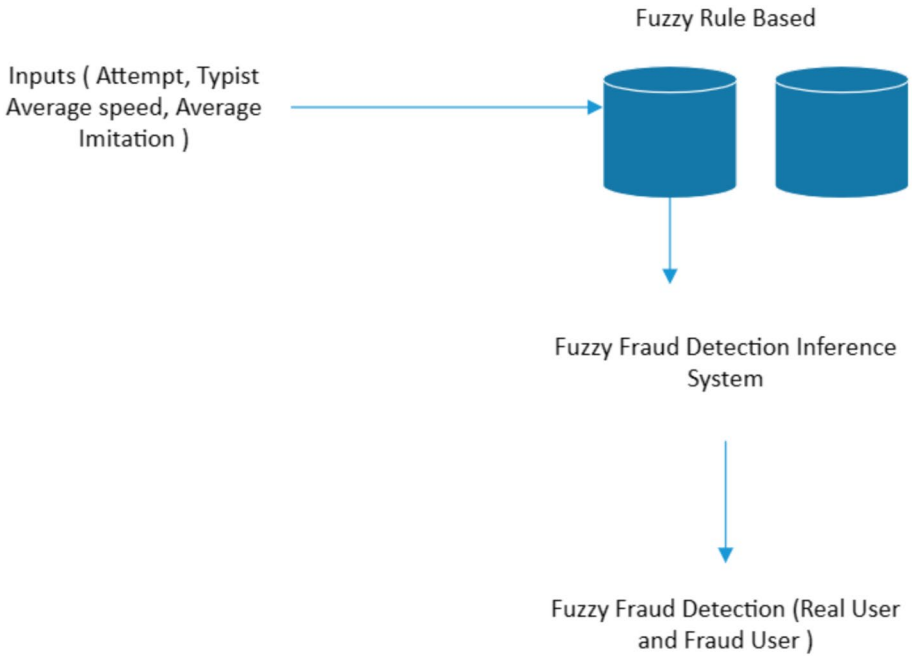

Fig. 2. Keystroke biometric authentication method using fuzzy rules-based.

Identification of the Input parameter
The above-mentioned factors are utilized to get the needed information on users' typing habits. The following are important factors that are utilized to contribute information to the fuzzy knowledge base.

$$Attempt : Numberofattemptstoenterthecorrectpassword$$

Typist Average speed: In milliseconds, the total and average time to input the password are recorded. The user's average time will be used to determine the speed category, which will be very slow, slow, fast, and very quick.

Average imitation: When a user registers for an account, the entire time is saved in the database during the enrolment process. The average time will be calculated as shown below.

$$\text{Average Time (first step)} = (\text{Total Time/Password Length})$$

These are the actual values, or the total and average time values, as calculated originally. Now, when you log in, another Total time and Average time, i.e. the attempting total time and attempting average time, will be recorded in the database. As a result, the average imitation time may be determined as shown below.

$$AverageImitation = (Attemptaveragetime - Actualaveragetime)/(secondstep)$$

The user's typing rhythm difference may be determined using these criteria, which will aid in determining the average deviation between the typing rhythms.

Fuzzification
The fuzzy expert system for Keystroke Dynamics is designed in this phase. The parameter has been constructed by input data study and calculating the total average of the keystroke inputs and divided by parameter's range. The input and output variables are specified in this step. The input is fuzzified with the assistance of a defined membership function, and fuzzy sets are defined.

In the Table 1 above, the fuzzy input variables have been given a range, and for these values, there will be some corresponding output values for which ranges have been specified. The millisecond is the unit of measurement (ms).

Construct fuzzy rule-based
The fuzzy rule-based system's knowledge base stores knowledge in the form of rules and draws inferences from these rules. As a result, rules are formed to design the knowledge base. The fuzzy system's rule is made up of simple if–then phrases.

Generate fuzzy inference system
The conditional statements in fuzzy logic are expressed using these if–then rule statements.

IF Condition-1, Condition-2, and Condition-3 are all true.
THEN Take Action #4.

Input	Parameter	Output variable
	Low | Medium | High	Real | Fraud
No of attempt	1–3 | 2–6 | 5–10	10–50 |45–100
Typist average speed	1- 300 | 200–600 | 500–100	
Average imitation	Might be negative based on the average calculation	

Table 1. Keystroke input and output.

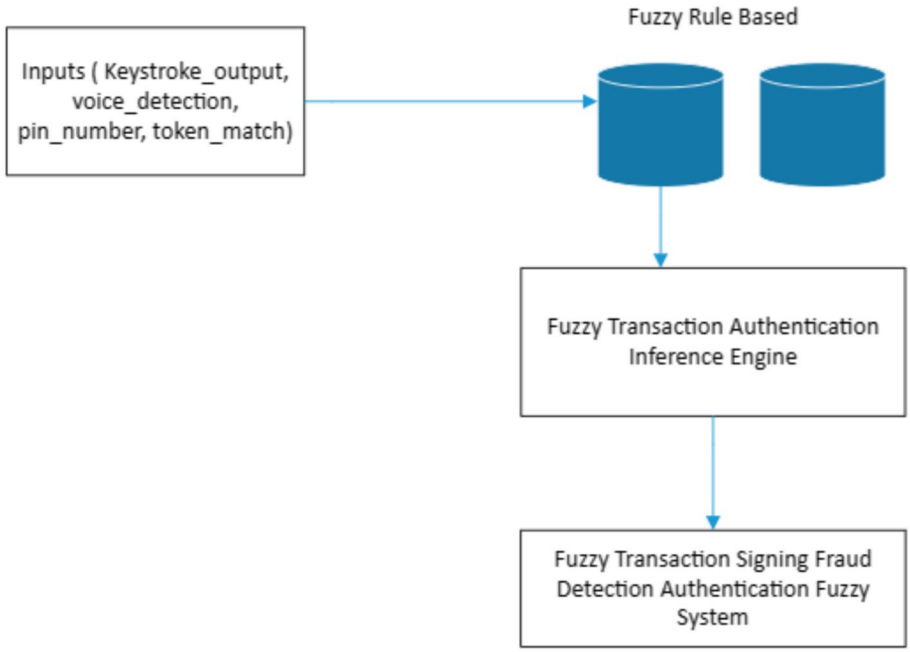

Fig. 3. Transaction signing fraud detection fuzzy system.

The system's knowledge base is a rule-based framework for keystroke dynamics.

As for phase 2, Transaction Signing Authentication using Fuzzy Approach will be constructed. The above Fig. 3 shows the purposed method for Transaction Signing Authentication in Fraud Detection using Fuzzy Approach. As with the previous Keystroke Dynamic Biometric Fuzzy System, this method has few implementation stages.

Figure 3 illustrates the initial stage of the Transaction Signing Authentication Method, which employs a Fuzzy Approach. This approach generates inputs from three sources: biometric methods, passwords, and tokens, ensuring a robust foundation. While this method shares similarities with the previously discussed research on Keystroke Dynamic Biometric, it utilizes a fuzzy rule-based system to analyse and adjust the inputs accordingly. However, what sets this method apart from the final proposed approach is its reliance on a single-layer Fuzzy Inference System. Although single-layer fuzzy systems, as implemented in numerous prior studies, can produce useful outcomes, they can result in the creation of an overwhelming number of rules. This, in turn, may lead to duplication and inaccuracies in output generation.

Fuzzy Logic Soft computing, such as fuzzy logic, replicates human decision-making. The research investigation uses fuzzy logic decision fusion, and the results are reasonable. The process of transforming each input into a linguistic variable is known as fuzzification. From linguistic variables, one or more membership functions with a degree of membership function are created.

The result is obtained by combining the degrees of membership function with established rules and rule weights. Each rule can be assigned a weight to show its impact on the output. The main block diagram for the fuzzy logic flow is shown in Fig. 4 below.

Implementing fuzzy logic

In this research, fuzzy logic is utilized for decision-making in authenticating genuine users and identifying fraudulent access during transaction signing in online banking. Multiple biometric outputs, along with two additional input variables, are used in the fuzzy logic approach for user identification. Figure 5 below illustrates the fuzzy membership function.

In this paper, each biometric modality is assigned equal weight, as both are considered equally important and should have the same opportunity to contribute to the authentication process.

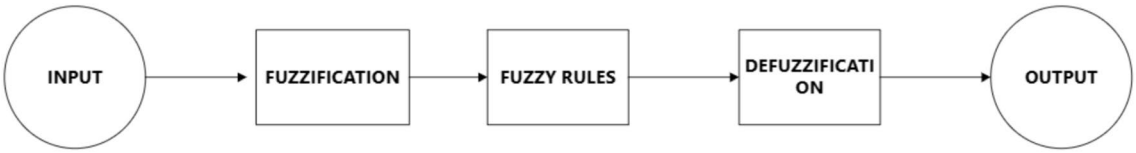

Fig. 4. Fuzzy logic flow.

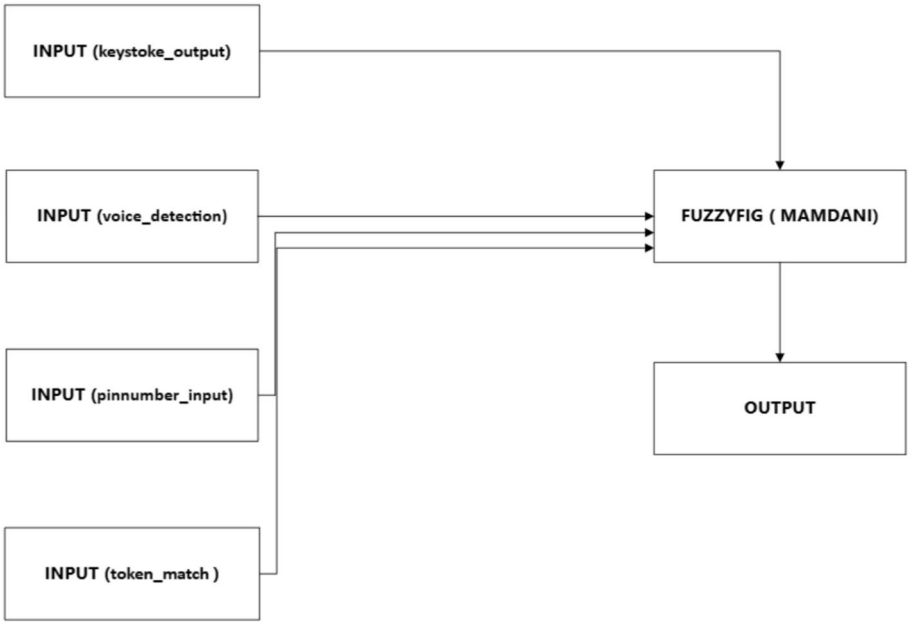

Fig. 5. Fuzzy membership function.

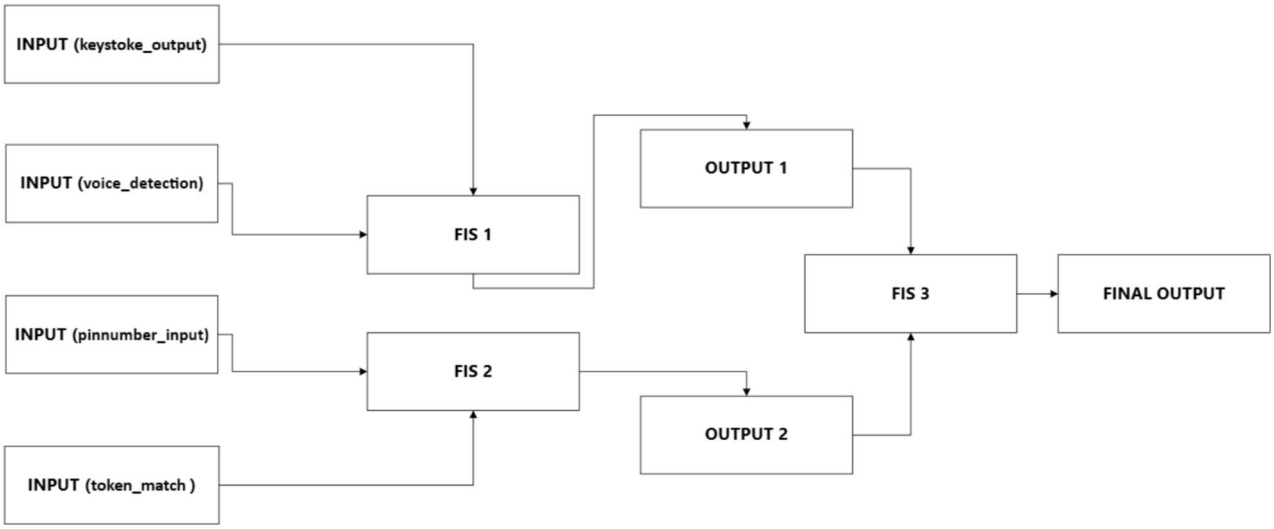

Fig. 6. Fuzzy inference system.

Fuzzy inference system

The fuzzy inference algorithm adjusts the weighting of each biometric and authentication method based on Hamming code differences. To strengthen the research and improve output accuracy, the input data is divided into several membership functions across multiple levels of the Fuzzy Inference System. Figure 6 illustrates the Fuzzy Inference System by level.

As mentioned above, three types of fuzzy sets have been combined to produce the final output for user authentication. This method was chosen over others to strengthen the evaluation process.

- FIS 1: This membership function (MF) includes two inputs—keystroke_output and voice_detection—and produces Output 1.
- FIS 2: This MF also has two inputs—pinnumber_input and token_match—and generates Output 2.
- FIS 3: This is the final MF, which combines Output 1 and Output 2 as inputs to produce the final authentication output based on assigned weightings.

Triangular and trapezoidal membership functions are used to convert the crisp values of the authentication methods into fuzzy sets.

Construct fuzzy rules
A fuzzy rule is defined as a conditional statement with the following structure IF x is A. y is B at that time, where x and y are linguistic variables. A and B are linguistic values regulated by fuzzy sets on the X and Y universes of conversation, respectively. The Mamdani approach was utilized in this study, and it is based on an inference process given by an equation.

$$\mu c\,(\ y) = \max K\left[\min[\,\mu A\ (\text{input}\,(i)\,, \mu B\,(\text{input}\,(j))\,]\right], k\ = 1, 2, 3, 4 \ldots r \tag{1}$$

In dynamic mode, it determines the yield enrolment capacity esteem for each rule. When one of the standards is dynamic, an AND operation is coupled between the inputs. The smaller data value is chosen, and its enrolment value is determined as a participation assessment of the yield for that run of the program. This procedure is repeated so that the yield participation capacities for each rule are determined. All the rules are used AND operation between the input and output. Lastly, the evaluation performance of the final output can be viewed by using the surface viewer. Surface Viewer is the place where the result of the performance can be viewed in graphical form.

Stage 3

System validation is conducted in Stage 3. This strategy involves integrating fuzzy logic into an existing banking dataset, which contains substantial biometric data from real-world banking environments. The research also proposes incorporating keystroke biometrics due to its cost-effectiveness, and applying fuzzy logic through a rule-based system to develop rules aligned with expert expectations from the current system.

As part of the study, the proposed method is applied to selected data for the assessment phase. This research will be evaluated by comparing the existing authentication method used during transaction signing in online banking with the proposed multiple authentication method using a multilevel fuzzy logic approach. Again, fuzzy logic will be employed at this stage to identify the most effective method for authenticating user login, ensuring secure money transactions and accurate user identification before accessing the application.

This approach outlines the multiple layers of authentication that occur in the backend prior to conducting the risk evaluation required for system login. The fuzzy rule-based system will be developed using expert knowledge from staff in the Risk and Technology Department of a trusted local bank in Malaysia. To enhance the value of this method, expert insights are integrated into the fuzzy rule creation process to ensure alignment with current industry standards and regulatory requirements for online banking in Malaysia.

Table 2 below presents an overview comparing the existing authentication method with the proposed method during transaction signing.

System validation was conducted in Stage 3 to assess the effectiveness of the proposed authentication method. This stage involved integrating fuzzy logic into an existing banking dataset, which contains substantial biometric data collected from real-world banking environments. The research also incorporated keystroke biometrics due to its cost-effectiveness and applied a fuzzy rule-based system to develop decision rules aligned with expert expectations from the current system. To validate the differences between the existing and proposed methods, a test was conducted using MATLAB to analyse the application risk associated with both approaches. The results revealed that the proposed system demonstrated lower risk levels, attributed to the inclusion of more input variables and multiple layers of Fuzzy Inference Systems (FIS). These enhanced rules and layered structures significantly reduced risk, confirming the effectiveness of the proposed approach for secure authentication during transaction signing. All steps from Stage 2, Phase 2 were reused in Stage 3, utilizing the same input variables. However, the membership function parameters were adjusted, and the evaluation objective shifted. At this stage, the focus was no longer on fraud detection or user verification, but rather on evaluating the robustness and safety of the authentication method for the system or application. All input data were converted into Boolean values, and fuzzy logic theory was applied to express soft linguistic variables across a continuous spectrum of truth values. Unlike traditional binary logic (0 or 1), fuzzy logic allows values within the range of 0 to 1. These values were used to enhance the four-input multi-criteria decision analysis, computing the "distance" of each input from 1 (yes) or 0 (no). If the result was closer to 1, it was rounded up; if closer to 0, it was rounded down. The final step involved experimenting with the system output, which was presented as a percentage representing the level of risk. This output provided a quantifiable measure of the system's security strength and validated the proposed method's effectiveness in reducing authentication risk. Additionally, the fuzzy rule base was developed with expert input from the Risk and Technology Department of a trusted local bank in Malaysia. This integration of domain expertise ensured that the fuzzy rules aligned with current industry standards and regulatory requirements for online banking in Malaysia.

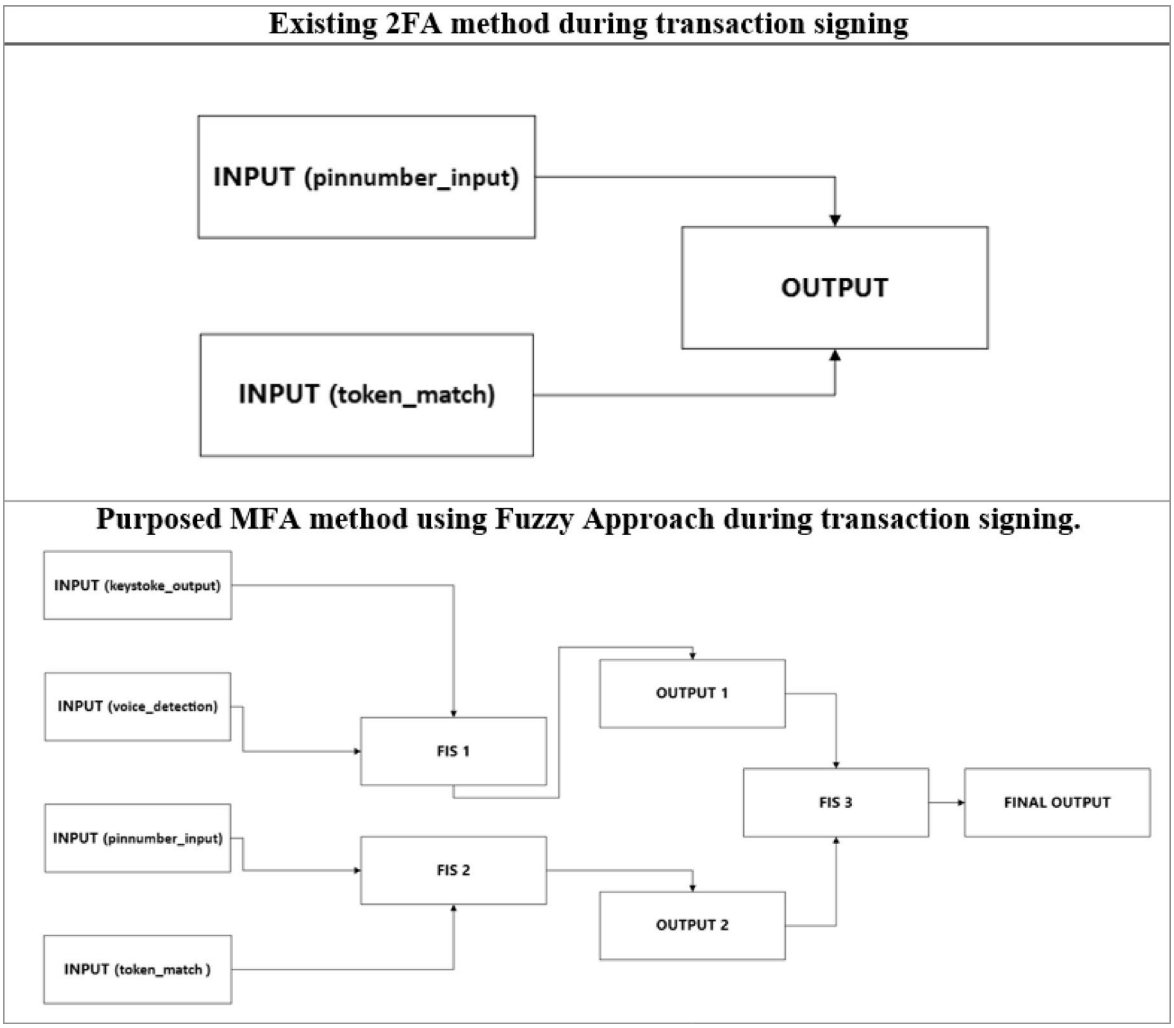

Table 2. Authentication method comparison.

Implementation method

There are numerous ways to safeguard our system against a cyberattack. For logging into an account, a password and username pairs are used as authentication methods. Passwords are required for every account in a secure system, or they will be invalidated. Passwords and usernames have always been and remain to be the most common ways of getting access to computers. Because the stand-alone computer is not connected to the Internet or a wide-area or local network, we must utilize password-based security to secure the data. Existing systems for access desire clients to validate themselves using a password and username, which means they must enter their unique passwords and usernames while logging in. This authentication mechanism relies on the private nature of the passwords and, in some cases, the authenticity of the username. If the secrecy is not broken, these tokens are able to distinguish a real user. Therefore, most Online Banking systems will authenticate the user using the 2FA method, whereby will include two-factor authentication first is user login by username and password as mentioned above and the second factor is by using the OTP generate and match before the system approved the transaction request. In this research, behavioural biometrics will be added with 2FA which will make the online system authenticate the transaction using MFA, and to research stronger Fuzzy Logic Rules-Based by using Mamdani technique has been implemented in this system. As part of a classification technique, these metrics, which are mostly dependent on keystroke timing latencies, are compared to a user profile a match or a non-match can be used to determine whether or not the user is authorized, or whether or not the user is the real author of a written sequence. The following are the several types of user authentication.

- Object-oriented user
- based on knowledge
- Based on biometrics

Voiceprint is used for "object-based" authentication. Traditional door keys can be assigned. Typically, the token-based technique is paired with the knowledge-based approach. The user is authenticated using "knowledge-

based" methods and is required to respond to at least one "secret" question Secret Questions might be static or dynamic.

FIS creation process overview

The system is designed using multi-layered FIS architecture with three main stages:

Inputs (behavioral and credential-based)
The system takes four key inputs:

- Keystroke output – behavioral biometric input based on typing patterns
- Voice detection – biometric input based on voice recognition
- PIN number input – strength score of the entered PIN
- Token match – number of attempts or match status of the token

First-level FIS modules

- Two separate fuzzy inference systems are used to process these inputs:
  - FIS 1:
- Inputs: Keystroke Output and Voice Detection
- Output: Output FIS 1 – a fuzzy risk score based on biometric authentication
  - FIS 2:
- Inputs: PIN Number Input and Token Match
- Output: Output FIS 2 – a fuzzy risk score based on traditional authentication

Each FIS uses linguistic variables (e.g., Low, Medium, High) and membership functions (e.g., triangular, trapezoidal) to fuzzify the inputs and generate intermediate outputs.

Final-level FIS (FIS 3)

- The outputs from FIS 1 and FIS 2 are then passed into a third FIS module, labeled:
  - Processing module (fuzzy inference system) – Mamdani FIS 3
- This module combines the intermediate outputs to produce a final decision:
  - Output module: Transaction Signing Risk in Application

The final output represents the overall application risk level during transaction signing, based on a comprehensive evaluation of both biometric and traditional authentication factors.

Thus, two behavioural biometric authentication methods are implemented in the system alongside the existing method. Refer to Fig. 7 for the overall fuzzy model, which represents the complete fuzzy system comprising three levels of the Fuzzy Inference System (FIS). In the first fuzzy set, three linguistic variables (fuzzy

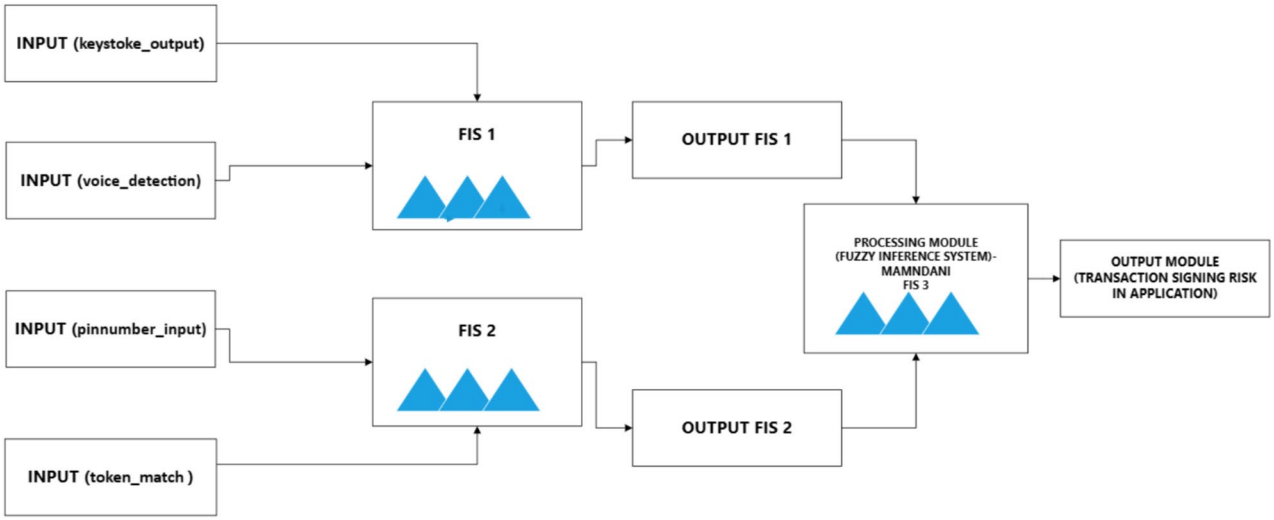

Fig. 7. User authentication approaches.

No	Input linguistic variable	Keystroke_Output
1	Low	10 to 40
2	Medium	30 to 70
3	High	60 to 100

Table 3. Keystroke_Output input value.

No	Input linguistic variable	Voice recognition
1	Low	10 to 40
2	Medium	30 to 70
3	High	60 to 100

Table 4. Voice recognition input value.

No	Output linguistic variable	Application risk 1
1	Low	10 to 40
2	Medium	30 to 70
3	High	60 to 100

Table 5. Authentication output value.

sets) are defined for the two input variables Keystroke_Output and Voice_Recognition namely: Low, Medium, and High. Similarly, three linguistic variables are defined for the output variable, Application Risk 1, also *labelled* as Low, Medium, and High. The numerical values representing the intervals for each input and output variable define the range that each linguistic term or fuzzy set covers. These are detailed in Tables 3–5, which present the input and output variables for the first FIS.

The second set of the Fuzzy Inference System (FIS) has been developed to determine the final output. In this second fuzzy set, two linguistic variables (fuzzy sets) are defined for the input variables Pin Number and Token Match namely: Low and High. Similarly, two linguistic variables are defined for the output variable, Application Risk 2, also labelled as Low and High. The numerical values representing the intervals for each input and output variable define the range that each linguistic term or fuzzy set covers. These ranges are detailed in the corresponding tables.

Results

This study presents the implementation of Multiple Biometric Authentication within a Multi-Factor Authentication (MFA) framework using Fuzzy Rule-Based Systems based on the Mamdani technique in fuzzy logic. Fuzzy logic systems offer a robust alternative to traditional mathematical modelling, especially in handling complex, nonlinear scenarios where precise models are difficult to construct. By applying fuzzy logic, this research addresses challenges that classical models cannot resolve, particularly in the context of behavioural biometrics and online banking security. To enhance the evaluation process, a multilevel Fuzzy Inference System (FIS) was developed. This system incorporates variables that influence authentication behaviour and models their relationships using linguistic terms such as very low, low, medium, high, and very high. These linguistic descriptors are mathematically represented through membership functions, and the fuzzy outputs are converted into crisp values using defuzzification techniques.

This approach allows the system to make decisions based on imprecise or uncertain input mirroring human reasoning more closely than binary logic. The study demonstrates that fuzzy logic-based systems can yield effective results even when relying on indefinite verbal knowledge provided by human experts. One key finding is the impact of interval length during the partitioning of datasets into overlapping fuzzy sets, which significantly affects the accuracy of the online banking risk prediction model. The proposed system enhances traditional MFA by introducing behavioural biometrics specifically keystroke dynamics and voice recognition as additional authentication layers. These are integrated with existing methods such as PIN numbers, passwords, and physical tokens (e.g., smart cards or debit cards). This layered approach provides a multi-level security mechanism for authenticating users during sensitive online transactions, such as payments, fund transfers, and system logins. As an enhancement to conventional two-factor authentication (2FA), the proposed framework introduces a third layer of verification using biometric data. This not only strengthens the authentication process but also improves resistance to fraud and unauthorized access. The fuzzy logic system evaluates multiple inputs simultaneously, allowing for a more nuanced and accurate risk assessment. Overall, the results confirm that the developed fuzzy logic-based MFA framework offers a more secure and reliable authentication method compared to existing models with similar objectives. The system's ability to process uncertain and variable input data makes it particularly well-suited for real-world online banking environments, where user behaviour and risk factors are dynamic and complex.

Input data of evaluation system

As mentioned, the proposed method consists of Multiple Biometrics of Multifactor Authenticate, therefore below shows the visualization of each fuzzy set/linguistic word for the Evaluation System with 4 inputs and 1 output in the form of a Trapezoid for each fuzzy set represented by their linguistic phrases. The first and last linguistic phrases, as indicated in the diagram, are Low and High, respectively, and represented by the Trapezoidal form. Besides, the medium is represented by Triangular form. Refer (Fig. 8).

The above Fig. 9 shows the list of rules created for the risk assessment, however, by using single FIS for many inputs will cause many rules creation but increasing the number of rules may sometimes worsen performance rather than improve it. Complex rule sets have the potential to cause conflicts or unexpected side effects that impair system performance. Also, redundancy is a possibility when there are a lot of rules, this occurs when multiple rules address the same or similar scenarios. Redundant rules can cause confusion in decision-making processes and add calculating complexity. The evaluation performance of the final output can be viewed by using the surface. Surf (X, Y, Z) generates a three-dimensional surface plot, which is a three-dimensional surface with solid edge and face colours. The function displays the matrix Z values as heights above a grid in the x–y plane specified by X and Y. The colour of the surface changes as the heights given by Z change. Figures 10–12 are the outputs of the application risk by the evaluation system.

Figure 10 explained the 3D surface illustrates how different combinations of keystroke and voice recognition scores affect the resulting application risk.

The surface rises from a blue base (low risk) to a yellow peak (higher risk), showing the gradient of risk based on input values.

The mesh grid (15×15) provides a detailed view of how the system interpolates between input values.

Rule-based evaluation (rule 14)

On the right side, the *PROPERTY EDITOR* shows the configuration for Rule 14 in the fuzzy system:

Conditions

- Keystroke is medium
- Voice_recognition is high
- Pin_number is strong
- Token_match is medium

Consequence:

The resulting *application_risk* is classified as low

This rule contributes to the overall decision-making in the fuzzy system, showing how specific combinations of biometric and credential-based inputs lead to a low-risk classification.

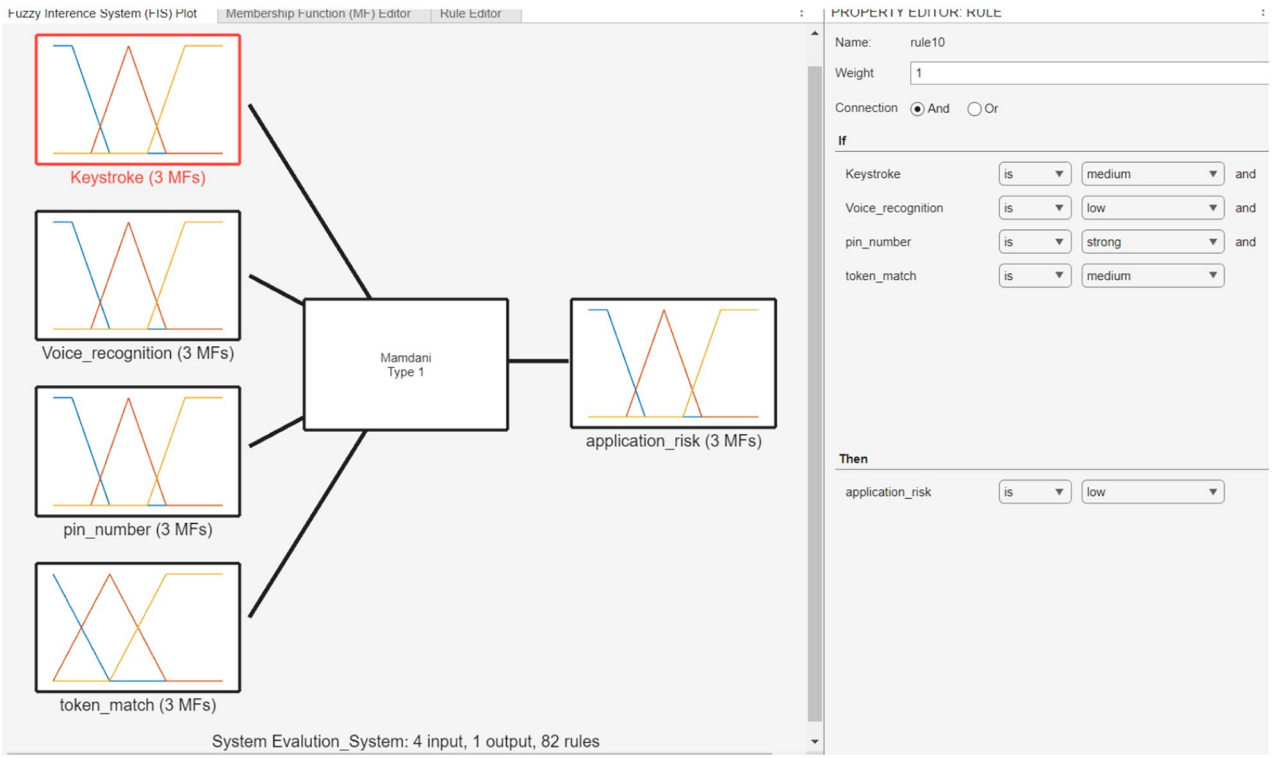

Fig. 8. Inputs of evaluation system.

System: Evalution_System

Add All Possible Rules | Clear All Rules

	Rule	Weight	Name
1	If Keystroke is low and Voice_recognition is low and pin_number is weak and token_match is low then app...	1	rule1
2	If Keystroke is low and Voice_recognition is medium and pin_number is weak and token_match is low then...	1	rule2
3	If Keystroke is low and Voice_recognition is high and pin_number is weak and token_match is low then ap...	1	rule3
4	If Keystroke is low and Voice_recognition is low and pin_number is strong and token_match is low then ap...	1	rule4
5	If Keystroke is low and Voice_recognition is low and pin_number is strong and token_match is medium the...	1	rule5
6	If Keystroke is medium and Voice_recognition is low and pin_number is weak and token_match is low then...	1	rule6
7	If Keystroke is medium and Voice_recognition is medium and pin_number is weak and token_match is low...	1	rule7
8	If Keystroke is medium and Voice_recognition is high and pin_number is weak and token_match is low the...	1	rule8
9	If Keystroke is medium and Voice_recognition is low and pin_number is strong and token_match is low the...	1	rule9
10	If Keystroke is medium and Voice_recognition is low and pin_number is strong and token_match is mediu...	1	rule10
11	If Keystroke is medium and Voice_recognition is low and pin_number is weak and token_match is medium...	1	rule11
12	If Keystroke is medium and Voice_recognition is high and pin_number is weak and token_match is low the...	1	rule12
13	If Keystroke is medium and Voice_recognition is high and pin_number is strong and token_match is low th...	1	rule13
14	If Keystroke is medium and Voice_recognition is high and pin_number is strong and token_match is mediu...	1	rule14
15	If Keystroke is medium and Voice_recognition is high and pin_number is weak and token_match is mediu...	1	rule15
16	If Keystroke is high and Voice_recognition is low and pin_number is weak and token_match is low then ap...	1	rule16
17	If Keystroke is high and Voice_recognition is medium and pin_number is weak and token_match is low the...	1	rule17
18	If Keystroke is high and Voice_recognition is high and pin_number is weak and token_match is low then a...	1	rule18
19	If Keystroke is high and Voice_recognition is low and pin_number is strong and token_match is low then a...	1	rule19
20	If Keystroke is high and Voice_recognition is low and pin_number is strong and token_match is medium th...	1	rule20
21	If Keystroke is high and Voice_recognition is low and pin_number is weak and token_match is medium the...	1	rule21
22	If Keystroke is low and Voice_recognition is low and pin_number is weak and token_match is medium then...	1	rule22
23	If Keystroke is low and Voice_recognition is low and pin_number is weak and token_match is high then ap...	1	rule23
24	If Keystroke is low and Voice_recognition is low and pin_number is strong and token_match is high then a...	1	rule24
25	If Keystroke is low and Voice_recognition is low and pin_number is very strong and token_match is low the...	1	rule25
26	If Keystroke is low and Voice_recognition is low and pin_number is very strong and token_match is mediu...	1	rule26

Fig. 9. List of rules for the evaluation system.

Discussion

Interpretation of the result using table

The proposed approach demonstrates a significantly higher level of security, as the Application Risk output consistently remains below 30%. In contrast, the results show that systems lacking Multiple Biometric Authentication, and a Fuzzy Logic-based approach exhibit substantially higher risk levels. The study reveals that online banking transaction authentication is not fully secure when relying solely on traditional methods. Even when the PIN and token match 100%, the system still reflects an application risk ranging from 50 to 70%, indicating a considerable vulnerability to fraudulent activities and potential financial theft. This stark difference highlights the effectiveness of the proposed multi-factor, fuzzy logic-enhanced authentication framework, which integrates behavioural biometrics such as keystroke dynamics and voice recognition. By incorporating multiple inputs and layered fuzzy inference systems, the model significantly reduces the risk associated with user authentication during sensitive online transactions.

Figure 13 above illustrates the Application Risk value of the proposed authentication system using a single-layer Fuzzy Inference System (FIS). In this scenario, all input values Keystroke Dynamics, Voice Recognition, PIN, and Token Match—are present and actively used to authenticate the transaction. All inputs scored high, and both the PIN and token were a 100% match. As a result, the application risk output was minimized to 22.4%. Since this configuration uses only one layer of FIS, the risk score is relatively low due to limited evaluation depth and a short processing cycle. Consequently, the findings indicate a low-risk outcome. However, incorporating additional FIS layers could significantly enhance the system's decision-making capabilities and improve the overall performance of the machine learning process.

Figure 14 above presents the Application Risk value of the proposed authentication system when using a single-layer Fuzzy Inference System (FIS) with only PIN and Token Match as input values, excluding biometric authentication. Although both the PIN and token were a 100% match, the resulting application risk remained at a moderate level of 50%. The results below represent the Application Overall Risk Assessment (Transaction Signing Risk Assessment) using the multi-layer FIS in the proposed method. These findings confirm that by integrating multiple authentication approaches including behavioural biometrics, passwords, and tokens online banking transaction signing can be significantly improved and secured compared to the existing methods. Furthermore, the proposed Multiple Biometric Authentication framework, based on a multi-level fuzzy logic approach, offers enhanced precision and robustness. This improvement not only strengthens the authentication

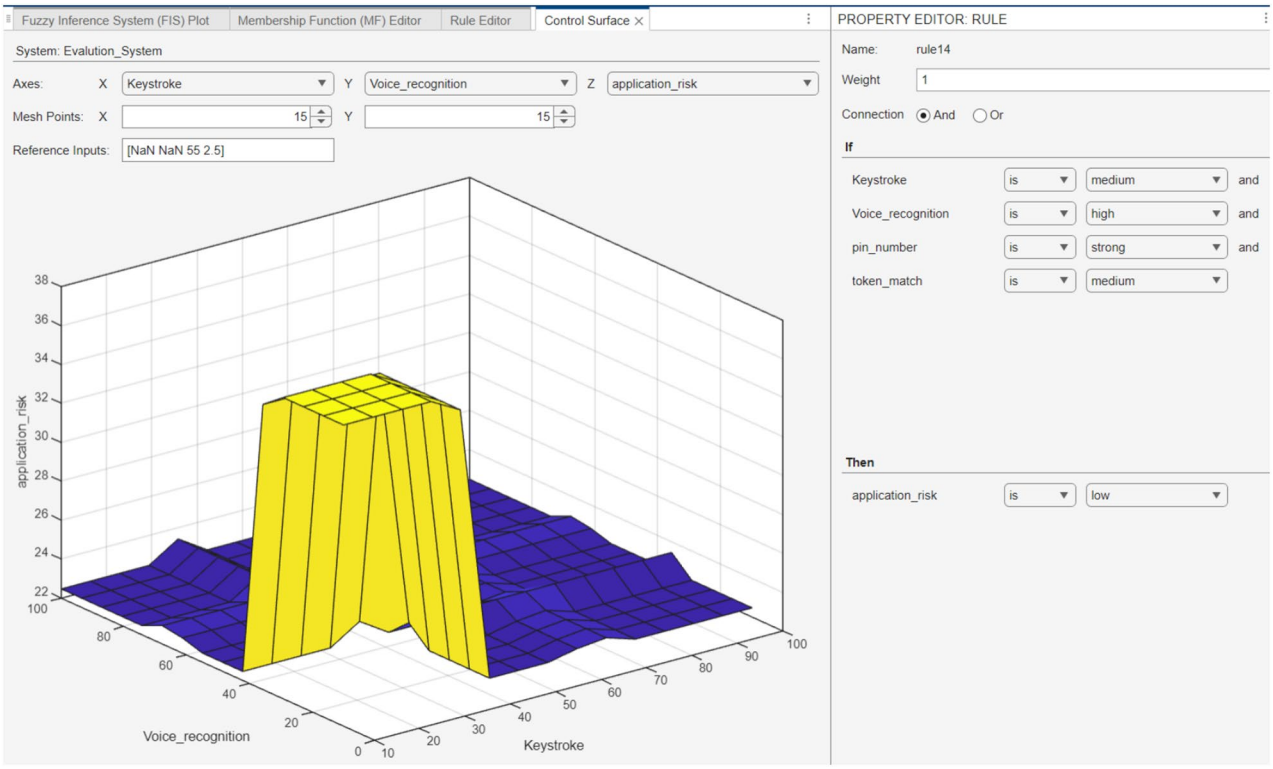

Fig. 10. Surface output of evaluation system.

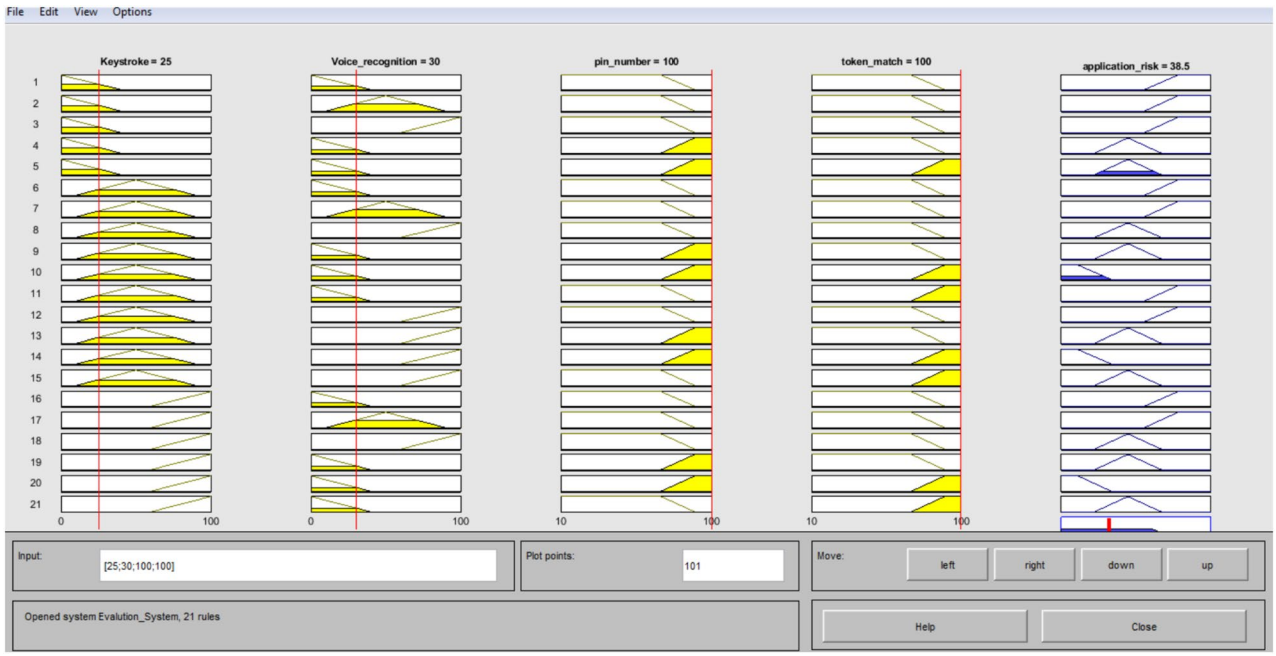

Fig. 11. Evaluation rules output 1.

process but may also raise awareness among users and stakeholders about the importance of evaluating risks associated with online banking transaction signing and user authenticity.

Table 6 presents the Application Risk values for transaction signing using the existing authentication method, which does not incorporate keystroke dynamics or voice recognition. The evaluation is based solely on two inputs: PIN strength score (%) and Token Match (measured by the number of attempts).

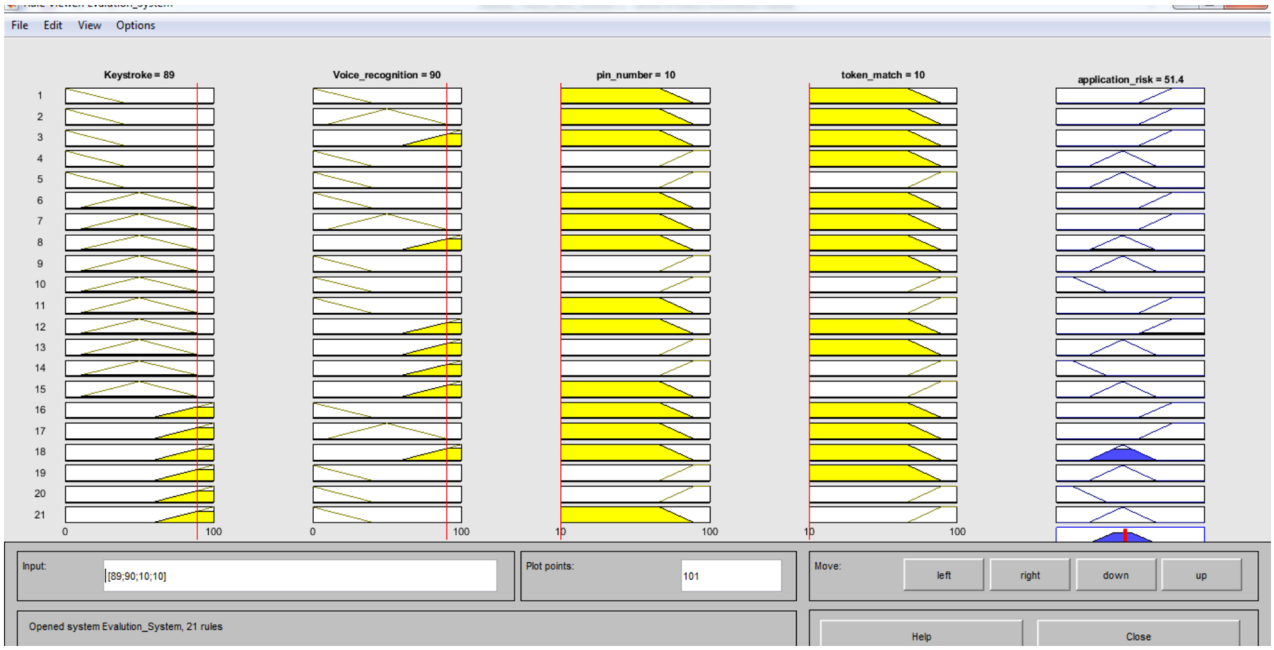

Fig. 12. Evaluation rules output 2.

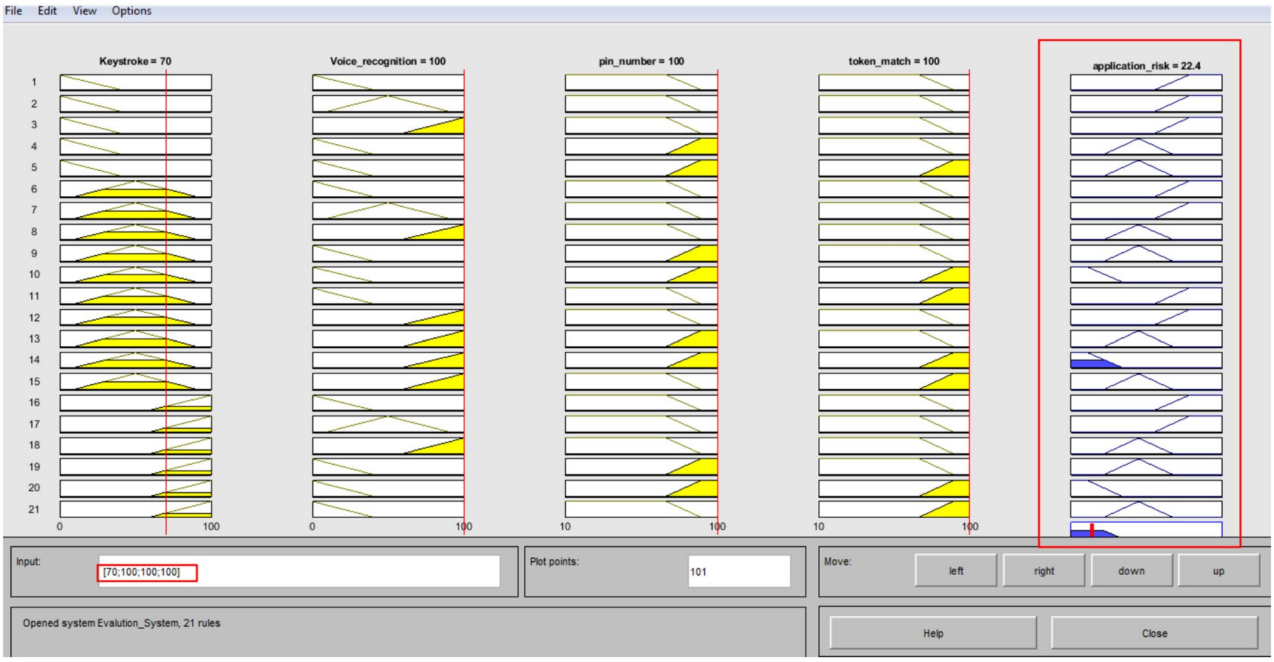

Fig. 13. Application risk score (%).

Although the current system does not inherently utilize fuzzy logic, for evaluation purposes, a Fuzzy Inference System (FIS) was implemented in MATLAB using input parameters that reflect the existing authentication process. The risk assessment was conducted using a single-layer FIS, and the results indicate that, due to the limited number of inputs and lack of biometric data, the resulting application risk levels were high, even with the application of fuzzy logic.

These findings highlight the limitations of the current method and underscore the need for a more robust, multi-factor authentication framework that includes behavioural biometrics and layered fuzzy logic for improved security.

Fig. 14. Application risk score 1 (%).

pinnumber_input	token_match	Application risk (%)
40	1	82.6
60	1	82.6
85	1	70
10	3	84.7
20	3	84.7
10	4	84.7
80	1	50
37	2	80.1
65	1	70
40	1	70
50	2	70
70	3	70
10	4	84.7
90	1	70
95	1	70
55	2	70
88	1	70
94	1	70
73	1	70
98	1	70

Table 6. Risk evaluation for existing system.

Experimental analysis and visualization

To strengthen the experimental analysis, additional visualizations that illustrate the behaviour of the fuzzy system under different input conditions were generated the Fuzzy Risk Surfaces.

- Left: Risk surface from biometric inputs (keystroke + voice)
- Middle: Risk surface from credential inputs (PIN + token)
- Right: Combined risk output from both biometric and credential layers

Figure 15 plots demonstrate how the system dynamically adjusts risk based on input combinations, validating the effectiveness of the multi-layered fuzzy inference system.

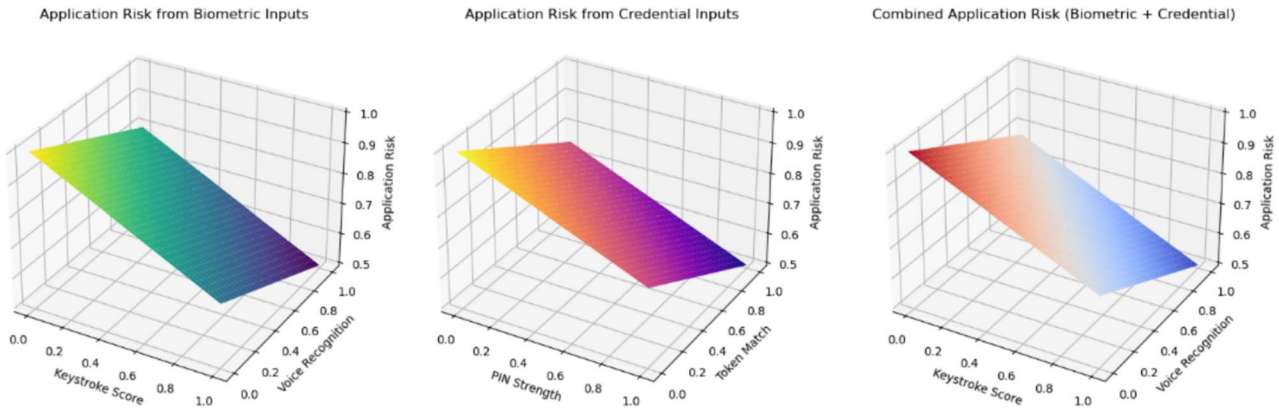

Fig. 15. Fuzzy Risk Surfaces for 3 different FIS.

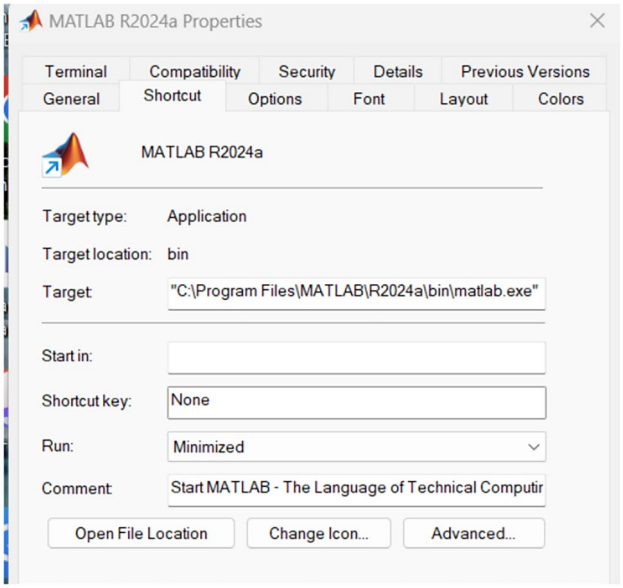

Fig. 16. MATLAB R2024a properties.

All graphs and membership function images used were generated using MATLAB R2024a, a high-level language and interactive environment for numerical computation, visualization, and programming. For further details about the software, refer to the official MATLAB website: https://www.mathworks.com/products/matlab.html. Figure 16 shows the properties and configurations as generated using MATLAB R2024a.

Table 7 presents the Application Risk values for transaction signing using the proposed authentication method, which incorporates keystroke dynamics, voice recognition, PIN strength score (%), and token match (number of attempts). The risk assessment was conducted using a three-layer Fuzzy Inference System (FIS) within the Transaction Signing Risk Assessment system. The results clearly demonstrate that the proposed method significantly reduces the risk associated with transaction signing in online banking applications. By combining multiple authentication factors including behavioural biometrics and traditional credentials the system enhances both security and privacy. While the existing method is not inherently insecure, the newly developed approach proves to be more effective, stable, and resilient against potential threats.

Future work

To further strengthen the system, future research should focus on developing a fully-fledged early warning system capable of analysing data in near real-time. This includes:

- Real-time data management for continuous monitoring and adaptive risk evaluation.
- Location mapping through a web-based platform integrated with Google Maps to track suspicious login attempts or potential hacker activity.
- Expanded data collection methodologies, beyond the current focus on age groups, to include additional demographic and behavioural factors for a more comprehensive risk model.

Authentication phase 1	Authentication phase 2	OVERALL Application risk (%)
50	50	20.6
22.2	50	20.9
20.6	50	20.7
50	84.7	50
83.7	84.7	50
82.8	84.7	50
81.4	50	50
72.8	50	50
84.7	50	50
50	50	20.6
83.9	84.7	50
50	50	20.6
20.6	84.7	50
81.7	50	50
82.8	50	50
83.9	83.7	50
82.6	50	50
84.7	84.7	50
50	50	20.6
84.3	50	50

Table 7. Evaluation system output table.

Moreover, the integration of pervasive computing and Internet of Things (IoT) devices such as sensors can serve as additional data sources for the fuzzy logic system. Sensor data could replace or complement interview-based inputs, improving system responsiveness and accuracy.

Conclusions

Fuzzy logic offers an alternative approach to expressing the linguistic and subjective elements of real-world computational challenges. The purpose of using a fuzzy logic model in this research is to ensure that the system produces meaningful and accurate outcomes based on uncertain, vague, and imprecise verbal information by mimicking human reasoning. In this study, a Mamdani-type fuzzy inference system with two inputs and one output was designed to predict risk status in the context of online banking. The results obtained from the proposed Multiple Biometric Authentication model for online banking showed strong alignment with the expected outcomes, achieving a minimum application risk value compared to existing authentication methods. The primary objective of this project was to develop an expert system capable of proposing a more secure authentication mechanism for transaction signing in internet banking. Additionally, the study aimed to enhance fuzzy risk assessment techniques tailored specifically for the banking environment. This improvement allows for more effective evaluation of risks associated with user login activities, helping to prevent unauthorized access, hacking attempts, and financial losses. By refining the fuzzy logic approach, the system can better analyse user behaviour, detect potential threats, and implement appropriate security measures to protect both users and financial institutions. It has been demonstrated that a fuzzy rule-based approach can be effectively used to analyse, model, and support decision-making processes that help prevent fraudulent activities. The case study provided a practical understanding of how expert systems can be applied in real-world scenarios. The risk assessment framework introduced in this research is notably more advanced than existing online banking authentication procedures, offering a more stable, accurate, and secure solution for transaction verification.

Data availability

The data used to support the findings of this study are included within the article.

Received: 31 May 2024; Accepted: 24 July 2025
Published online: 25 September 2025

References

1. Khalifa, W., Roushdy, M. I. & Salem, A. B. M. A rough set approach for user identification based on EEG signals. *Egypt. Comput. Sci. J. (ECS)* **38** (3), 43–50 (2014).
2. Sadekin, M. S., & Shaikh, A. Security of E-banking in Bangladesh. *J. Finance Account.* 65–93 (2016).
3. Lam, L. & Suen, C. Y. Application of majority voting to pattern recognition: An analysis of its behavior and performance. *IEEE Trans. Syst. Man Cybern. Part A Syst. Hum.* **27** (5), 553–568 (1997).
4. Jiang, H., Ji, P., Zhang, T., Cao, H. & Liu, D. Two-factor authentication for keyless entry system via finger-induced vibrations. *IEEE Trans. Mob. Comput.* **23** (10), 9708–9720 (2024).
5. Utakrit, N. *Security Awareness by Online Banking Users in Western Australian of Phishing Attacks* (Edith Cowan University, 2012).

6. Gunson, N. et al. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Comput. Secur.* **30** (4), 208–220 (2011).
7. Silva, R. D. Calls for behavioural biometrics as bank fraud soars. *Biomet. Technology Today* **2021** (9), 7–9 (2021).
8. Wang, C., Wang, Y., Chen, Y., Liu, H. & Liu, J. User authentication on mobile devices: Approaches, threats and trends. *Comput. Netw.* **170**, 107118 (2020).
9. Sinigaglia, F., Carbone, R., Costa, G. & Zannone, N. A survey on multi-factor authentication for online banking in the wild. *Comput. Secur.* **95**, 101745 (2020).
10. Freksa, C. & Mark, D. M. *Spatial Information Theory: Cognitive and Computational Foundations of Geographic Information Science (Lecture Notes in Computer Science 1661)* (Springer, 1999).
11. Zhong, Y. & Deng, Y. Recent advances in user authentication using keystroke dynamics biometrics. *GCSR* **2**, 1–22 (2015).
12. iDenfy. (n.d.). Biometrics in banking. https://www.idenfy.com/blog/biometrics-in-banking/ (2025).
13. Hublikar, S., Pattanashetty, V. B., Mane, V., Pillai, P. S. & Lakkannavar, M. Biometric-based authentication in online banking. In *Information and Communication Technology for Competitive Strategies (ICTCS 2021)* (eds Hublikar, S. et al.) (Springer, 2025).
14. S&P Global Ratings. (2023). Banking Industry Country Risk Assessment: Malaysia. https://www.spglobal.com/_assets/documents/ratings/research/101596404.pdf (2025).
15. Kitsios, F., Giatsidis, I. & Kamariotou, M. Digital transformation and strategy in the banking sector: Evaluating the acceptance rate of e-services. *J. Open Innov. Technol. Market Complex.* **7**(3), 204. https://doi.org/10.3390/joitmc7030204 (2021).
16. Hublikar, S., Pattanashetty, V. B., Mane, V., Pillai, P. S. & Lakkannavar, M. Biometric-based authentication in online banking. In *ICTCS 2021* (eds Hublikar, S. et al.) (Springer, 2025).
17. Shubhamgi, D. C., & Bali, M. Multi-biometric approaches to face and fingerprint biometrics. *Int. J. Eng. Res. Technol.* 2278–0181 (2012).
18. Panja, B., et al. Cybersecurity in banking and financial sector: Security analysis of a mobile banking application. In *2013 International Conference on Collaboration Technologies and Systems (CTS)*. (IEEE, 2013).
19. Hassan, O. A., Samhan, A., Alhajhassan, S. & Hammad, R. ARivaT: A tool for automated generation of Riva-based business process architecture diagrams. *IEEE Access* **11**, 46257–46270 (2023).
20. Harini, N. & Padmanabhan, T. 2CAuth: A new two factor authentication scheme using QR-code. *Int. J. Eng. Technol.* **5** (2), 1087–1094 (2013).
21. Adrian, T. & Ashcraft, A. B. Shadow banking: A review of the literature. In *Banking Crises* (eds Adrian, T. & Ashcraft, A. B.) (Springer, 2016).
22. Al-Otaibi, S. et al. The satisfaction of Saudi customers toward mobile banking in Saudi Arabia and the United Kingdom. *J. Glob. Informat. Manag. (JGIM)* **26** (1), 85–103 (2018).
23. Lee, A. J. Y., et al. Customers' satisfaction towards online banking in Malaysia: A primary data analysis. UTAR. (2017).
24. Wang, X., Zheng, Q., Zheng, K. & Wu, T. User authentication method based on MKL for keystroke and mouse behavioral feature fusion. *Secur. Commun. Netw.* **2020**, 1–14. https://doi.org/10.1155/2020/9282380 (2020).
25. Božić, V. Fuzzy approach to risk management: Enhancing decision-making under uncertainty. https://doi.org/10.13140/RG.2.2.13517.82405 (2023).
26. Sanchez-Roger, M., Oliver-Alfonso, M. D. & Sanchís-Pedregosa, C. Fuzzy logic and its uses in finance: A systematic review exploring its potential to deal with banking crises. *Mathematics* **12**(5), 782. https://doi.org/10.3390/math12050782 (2025).
27. Su, Y., & Xi, M. Systematic solutions to login and authentication security: A dual-password login-authentication mechanism. arXiv:2404.01803 (2024).
28. Prabha, N. & Manimekalai, S. Real time credit card fraud detection using fuzzy and deep neural network. *Int. J. Comput. Applic.* **186**(64), 47–52. https://doi.org/10.5120/ijca2025924393 (2025).
29. Khan, A. R. & Alnwihel, L. K. A brief review on cloud computing authentication frameworks. *Eng. Technol. Appl. Sci. Res.* **13** (1), 9997–10004 (2023).
30. Killourhy, K. S., & Maxion, R. A. Comparing anomaly-detection algorithms for keystroke dynamics. *Proceedings of the 2009 IEEE/IFIP International Conference on Dependable Systems & Networks*, 125–134. (IEEE, 2009).

Acknowledgements
I am grateful to the faculty and staff of the FTMK department at University Technical Malaysia Melaka, UTEM for their guidance and support throughout this project.

Author contributions
N.M.A. devised the project and developed the main conceptual ideas. S.S.S.A. and N.K. formulated the methodology. Y.U.G. developed the software used in the study. Z.S. and N.M.A. performed the validation. N.M.A., S.S.S.A., N.K., Y.U.G., and Z.S. conducted the formal analysis. N.M.A. carried out the investigation and managed resources and data curation. S.S.S.A. and N.M.A. prepared the original draft. N.M.A., N.K., and Y.U.G. reviewed and edited the manuscript. S.S.S.A. and Z.S. handled the visualization. S.S.S.A. and N.M.A. supervised the project. S.S.S.A., N.K., Y.U.G., and Z.S. managed project administration and secured funding. All authors have read and agreed to the published version of the manuscript.

Declarations

Competing interests
The authors declare no competing interests.

Additional information
Correspondence and requests for materials should be addressed to Y.U.G.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.