Information Processing and Management 62 (2025) 104233

Contents lists available at ScienceDirect

Information Processing and Management

journal homepage: www.elsevier.com/locate/infoproman

Management of evaluation processes and creation of authentication metrics: Artificial intelligence-based fusion framework

Dragan Korać [a,*], Boris Damjanović [b], Dejan Simić [c], Cong Pu [d]

[a] University of Banja Luka, Bosnia and Herzegovina
[b] University of Union Nikola Tesla, Serbia
[c] FON, University of Belgrade, Serbia
[d] Oklahoma State University, Stillwater, OK, USA

ARTICLE INFO

Keywords:
Fusion framework
Artificial intelligence
Security
Privacy
Trust

ABSTRACT

While the literature extensively covers various authentication systems, management of evaluation processes and creation of authentication metrics remain significant information challenges for researchers. To overcome this complex challenge, we present a taxonomy of research processes based on fusion and fuzzy strategies and give an overview and comparison of related studies. Specifically, we develop an artificial intelligence-based fusion framework (f_f) incorporating Mamdani-type fuzzy rules and key user factors: security, privacy, and trust. Its uniqueness and innovation lie in the application of trapezoidal functions to describe these factors as key input metric values. Moreover, we are the first to incorporate trust as an independent comparative factor and provide a comparison of traditional and modern authentication methods, including artificial intelligence (AI), electroencephalogram (EEG), electrocardiographic (ECG), and photoplethysmogram (PPG) methods. Also, we use a workflow diagram to define the topological relationships among user factors and authentication factors, clarifying the role of fusion in multifactor authentication (MFA) approaches. In comparison to other similar frameworks implemented solely for traditional methods, the proposed f_f yields better and more realistic quantification metric results. In addition, we present and discuss the key mathematical differences between one-factor authentication (1FA) and MFA, aiming to shed light on issues such as complexity and bias. Lastly, the developed f_f not only advances MFA metrics by introducing modern authentication methods such as AI, EEG, ECG, and PPG but also paves the way for future research on how and why AI algorithms need to be incorporated into information processing and the creation of strong MFA solutions.

1. Introduction

The rapid advancement of information technologies and artificial intelligence (AI) has led to inevitable changes (Chen, 2023; Korać et al., 2022a), resulting in the processing and management of vast amounts of information across nearly all information systems. AI has become a key driver of evolution and transformation in every aspect of human life (Li et al., 2025; Charef et al., 2023; Chahoud et al.,

* Corresponding author.
E-mail address: dragan.korac@pmf.unibl.org (D. Korać).

https://doi.org/10.1016/j.ipm.2025.104233
Received 17 January 2025; Received in revised form 24 May 2025; Accepted 24 May 2025
Available online 3 June 2025

2025). Each system shares the common aim of continuously seeking innovative solutions and employing a wide range of AI technologies, architectures, and approaches to optimize their benefits and improve efficiency (Pawlak & Poniszewska-Marańda, 2021). These changes create increasingly favorable conditions for attackers who are constantly evolving new cyber tactics and threats. Undoubtedly, authentication systems, as the first line of defense against these threats (Ghaemi et al., 2024; Ghafourian et al., 2023; Teh et al., 2020), play a crucial role in securing any application (Awadallah et al., 2024; Esposito et al., 2021; Jiang et al., 2020; Alizadeh et al., 2021; Zhou et al., 2020; Wang et al., 2022). Authentication also represents a key security element in mobile networks, which must be carefully addressed by developers (Mundhe et al., 2021). Numerous frameworks and protocols for various purposes have been successfully developed (e.g., Aghili et al., 2021; Pu & Li, 2020; Chang et al., 2021; Pu et al., 2022) and offered as the best authentication solutions in practice. Still, the paradox is that many developed multifactor authentication (MFA) solutions were subsequently found to be insecure and unable to achieve the required security aims (Wang & Wang, 2023), and often use numerous user criteria with different ways to quantify their values; thus, complicating efforts for users and system administrators in identifying strong and secure MFA solutions. Such MFA solutions raise issues of complexity and bias. Since MFA solutions are built on individual methods defined by deterministic features, they are often too complex to fully understand at the outset. This complexity becomes even more pronounced when modeling MFA systems in a mobile environment, as mobile technologies involve multiple, interconnected information technologies. Multi-view clustering has become increasingly prominent because different sources often provide diverse representations of information (Liu et al., 2025). Today, nearly all practical systems are affected by uncertainties (Yang et al., 2023), due to nonlinearity and stochasticity, which are two of the most important universal characteristics of such systems (Tian et al., 2019). The problem of uncertainty is inevitable in modeling processes (Yi et al., 2023). Furthermore, the challenge of information processing, evaluating, and creating strong MFA solutions becomes even more significant when applying the *"No Panacea Theorem"* for classifier combinations. This theorem, being stochastic, demonstrates that under certain input conditions, a combination algorithm can produce very poor output values (Hu & Damper, 2008). Managing these processes implies that there is no universal combination strategy or any strategy that can be applied to every situation. Therefore, the information processing and evaluation of MFA systems is a highly complex and stochastic problem that must be approached holistically through the lens of fuzzy methodology.

The task of implementing fuzzy methodology in MFA approaches is not trivial. Consequently, a deep understanding of user factors is crucial for the processing, evaluation, and information fusion of any MFA solution. Every authentication solution is based on one or more user factors, such as security, usability, accessibility, pricing, complexity, privacy, convenience, etc. (Furnell & Helkala, 2022; Stylios et al., 2021; Korać et al., 2022b). MFA is inherently tied to security as a primary user factor. In addition, security and privacy are critical issues in mobile authentication environments (Alzubaidi & Kalita, 2016; Patel et al., 2016; Soleymani et al., 2021), representing two ceaseless research issues (Tawalbeh & Saldamli, 2021). The reason for this is that the use of credentials often involves sensitive private information (Mishra et al., 2021), which may be stored on mobile devices. Undoubtedly, using sensitive information to access application domains raises security and privacy concerns (Bhattarai et al., 2024). Privacy issues are particularly significant in traditional biometric methods (Wazzeh et al., 2024; Hsieh et al., 2024). The application domain is a substantial factor that directly influences the determination of the user's priority level. For example, security and privacy are top priorities in metaverse applications, whereas they are less critical in library membership applications. However, the key reason for using trust as an independent comparison factor in this research is the development of numerous new technologies in typical e-environments, which can easily undermine a user's sense of confidence. Trust is a key standalone user factor in typical e-applications, e-vehicles, Internet of Things (IoT) devices, and cloud environments (Khan et al., 2024; Shao et al., 2022). On the other hand, trust is built on a foundation of security and privacy (Sharma et al., 2020) and represents a growing information phenomenon that requires special attention in MFA approaches. Given the fuzzy output values related to user and authentication factors, the information approach requires defining an optimal combination algorithm that selects and integrates these factors. Studying the fuzzy values of MFA solutions involves considering several different information processes and sources, making it, in itself, a problem of evaluation. In light of all the above, there is a strong need to create a framework or model (based on the three user factors discussed) for evaluating, creating, and selecting the best authentication solutions (Ali & Khan, 2022). Table 1 summarizes the acronyms used in this research.

Table 1
Acronyms explanation.

Acronyms	Explanation
1FA, 2FA, 3FA	*One, Two, Three Factor Authentication, respectively*
AI	*Artificial Intelligence*
ECG	*Electrocardiographic*
EMG	*Electromyographic*
f_f	*Fusion Framework*
FIS	*Fuzzy Inference System*
FS	*Fuzzy System*
MF	*Membership Function*
MFA	*Multifactor Authentication*
NFC	*Near Field Communication*
OTP	*One Time Password*
PIN	*Personal Identification Number*
PPG	*Photoplethysmogram*

1.1. Research challenges and motivation

Although the development of new information technologies offers many advantages related to authentication and user factors, it also presents numerous challenges. First, countless MFA processes and scenarios can arise at the intersection of these factors. To select a strong MFA solution, it is essential to evaluate each option realistically. The complexity and bias issues in these processes are not new, yet addressing them remains a challenge to this day. This information challenge continues to be a major global security aim that cannot be solved without FSs. These systems provide numerical output results in percentages, enabling clarity, precision, and ease of comparison between different MFA performance metrics. Additionally, there are numerous other challenges associated with user and authentication factors. Specifically, issues related to user security and privacy are critical areas of research when developing defense strategies. However, including the trust factor in authentication approaches introduces new fuzzy challenges related to weighted criteria, which cause changes in output fuzzy values. On the other hand, the use of emerging information technologies like artificial intelligence (AI) brings one of the biggest challenges concerning trust in utilizing AI for human decision-making (Wang & Ding, 2024). Moreover, innovative technologies enable the development of numerous new modern methods (e.g., AI, electroencephalogram (EEG), electrocardiogram (ECG), and photoplethysmogram (PPG), etc.), creating different sets of authentication scenarios, making it nearly impossible for users and system administrators (developers) to process and create a strong and secure MFA solution within a reasonable timeframe. The relevance of introducing modern methods to the trust factor lies in how these advanced technologies can enhance security and privacy, which, in turn, enhances users overall trust in MFA systems. AI technologies also bring specific challenges in the automation of tasks, the analysis and extraction of valuable information from large datasets, and the enhancement of sophisticated decision-making processes (Krichen & Abdalzaher, 2024). Therefore, this study brings together both theoretical and practical issues to identify open information challenges and future research directions related to AI technologies in authentication approaches.

1.2. Contributions of this paper

Motivated by the above discussion, we face an overwhelming number of authentication solutions driven by the development of emerging technologies. We observe that, compared to security and privacy priorities, trust is an understudied and conspicuously neglected user factor in MFA approaches. Additionally, we identify the management of evaluation processes in authentication approaches as extremely difficult, which clearly cannot be addressed without adequate authentication metrics and a suitable combination algorithm. As information technologies enable the development of numerous authentication methods that contain specific credentials (i.e., user private information), their information processing and management become increasingly laborious for system administrators. In this paper, management of evaluation processes and creation of authentication metrics represent our main research focus. In summary, we provide the following primary contributions:

- Provide an overview and comparison of related studies, highlighting that the integration of trust within the authentication environment remains an understudied area.
- Illustrate the taxonomy of processes of our research study based on fusion and fuzzy strategies.
- Give the comparison of traditional and modern methods (including modern methods such as AI, EEG, ECG, and PPG) based on independent user factors: security, privacy and trust.
- Develop an AI-based fusion framework (f_f) for numerical evaluation of authentication methods, including Mamdani-type fuzzy rules, with practical implementation for both one factor authentication (1FA) and MFA solutions.
- Present a comparison with similar research, offering more realistic quantification metric results and a more comprehensive view of the processes of evaluation, creation, and ranking of MFA solutions.
- Provide an overview of the key mathematical differences between 1FA and MFA, and define all possible information combinations marked as sets of authentication scenarios.

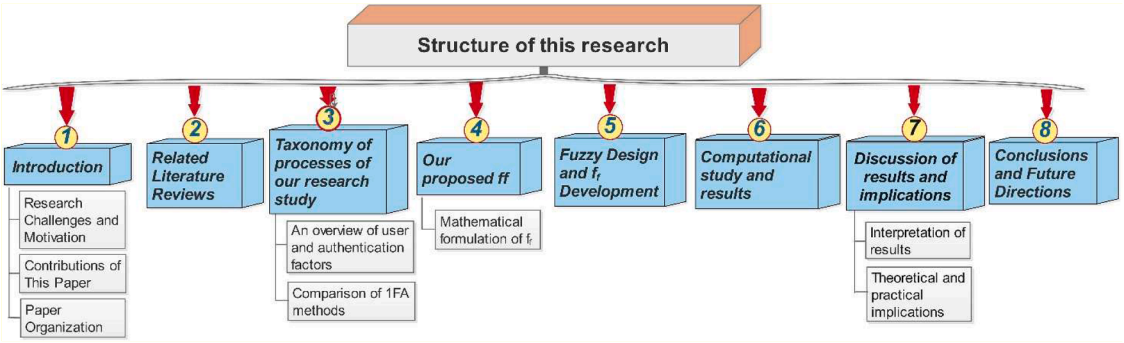

Fig. 1. Organization of this paper.

- Present information challenges and future directions, aiming to better understand and enhance the development of intelligent authentication solutions and automated combination algorithms based on AI technologies.

1.3. Paper organization

This research is organized into seven sections, as shown in Fig. 1. Section 2 describes the related literature review / survey works, Section 3 presents a taxonomy of processes of our research study, while Section 4 provides a proposal for the development of the f_f. Section 5 gives the fuzzy design and development of f_f, while Section 6 presents a computational study and results. Section 7 provides discussion of results and implications, while the last section provides conclusions and future directions.

2. Related literature reviews

As discussed earlier, numerous comparative studies and frameworks have been extensively explored in the literature. This section reviews previously published papers on comparative authentication, highlighting key processes and features essential for the development of any authentication framework. Our literature search was guided by a set of keywords, including authentication, survey, review, overview, artificial intelligence, security, privacy, and trust. We sourced papers published in English from leading academic databases and publishers such as Elsevier, Springer, IEEE, ACM, ScienceDirect, and Scopus. A comparison of our paper with other related studies is provided in Table 2. This table shows that numerous numerical models/frameworks for evaluating authentication methods have been developed and studied in the literature. For example, in the works of Campbell et al. (2004), Renaud (2004), Helkala and Snekkenes (2008), Mihajlov et al. (2011, 2011a), Bonneau et al. (2012), Crawford et al. (2013), Rathgeb et al. (2015), and Kiljan et al. (2018), different numerical frameworks were developed with complex and confusing values. In the framework of Renaud (2004), output values of authentication methods are placed in the range from "0" to "1.732," where a minimum value is marked with "1.732", while a maximum value is marked with "0". In the work of Ali and Khan (2022), the authors developed a framework for authentication evaluation in the IIoT environment based on a mathematical approach for ranking and selection of the best MFA solutions. In addition, authors in studies of Korać and Simić (2017, 2019) and Kumar et al. (2020) developed frameworks based on fuzzy logic, including many different user factors. In the frameworks of Korać and Simić (2017, 2019), the authors placed the output values of authentication methods in the range from "0" to "1," whereby "0" is assigned as a minimum value and "1" as a maximum value. Qin et al., (2021) designed a fuzzy authentication system based on neural network learning and extreme value statistics, while Kumar et al., (2020) proposed a fuzzy framework based on the AHP-TOPSIS method for evaluating usable security. In addition, Parcham et al. (2016) and Shabbir et al. (2022) focused on the MFA issue for security using fuzzy logic, while Muthusamy and Rakkimuthu (2022) addressed authentication issues based on using a fuzzy neural network related to finger vein verification. Additionally, there have been attempts to compare different authentication methods. For example, Maltoni et al. (2009), Zhou et al. (2023), Awadalla et al. (2024), Alsadie et al. (2024), and Alrawili et al. (2024) used output comparisons of authentication methods by employing linguistic values.

All the above-mentioned frameworks, besides certain complexity and confusion, have unique weaknesses because they don't consider trust as a comparative user factor in authentication approaches. Still, there have been attempts to compare user factors like security, privacy, and trust in other contexts. For example, authors in the research studies of Feng et al. (2018), Miorandi et al. (2012), Shin (2010), Tewari and Gupta (2020), Sharma et al. (2019), and Merhi et al. (2019) considered and compared these factors as a whole, while in the works of Zhang et al. (2022), Evans et al. (2021), Rathore et al. (2017), Yamada & Ikeda (2017), Wu et al. (2018), and Liu and Tao (2022), the topic of trust as an individual key user factor was covered in different e-services. Also, in the works of Jain et al. (2021), Parashar et al. (2024), and Ogbanufe and Kim, 2018, covered trust, security, and privacy in the biometric authentication methods, while Zhang et al. (2023), Hamdani et al. (2022), Sun et al. (2024), Ambika (2019) considered and compared these factors, whereby the trust is only briefly described as a substantial sub-problem rather than the main research issue. There have also been attempts to address authentication issues, focusing on new innovative technologies. For example, Rahman et al., 2021 presented a model for IoT data authenticity in edge-AI, while Fortuna et al. (2023) addressed authentication metrics in the context of IoT environments. Jan et al. (2024) dealt with AI-supported hybrid mutual authentication approaches in medical things environments, while Wang et al. (2024) proposed the CL-BPA authentication scheme to secure the mobility of producers in named data networks. Ahanger et al. (2022) surveyed the state-of-the-art AI techniques for IoT security, focusing on organizational authentication technologies, while Zhang et al. (2024) surveyed the application of AI technologies-related physiological biometric features in user authentication approaches.

While existing literature surveys have provided (extensive) coverage of user factors and authentication metrics from various perspectives, there is a need to develop the f_f, including trust as a standalone comparative factor, which becomes the main comparative objective of this research.

3. Taxonomy of processes of our research study

The taxonomy of key research processes in MFA approaches, as presented in Fig. 2, is considered through three individual processes: evaluation, creation, and selection. These processes are built on the application of fuzzy and fusion strategies within a hierarchical structure. It is worth noting that the hierarchical approach facilitates the mutual interconnectedness of all blocks, along with highlighting their key features. The fuzzy strategies offer several advantages, such as handling uncertainty and imprecision in multidimensional information, enabling multi-block hierarchical connections, and ensuring flexibility, scalability, and optimization. Given the complex, multi-dimensional nature of MFA systems, which involve multiple processes, factors, and levels, fuzzy logic

Table 2
Overview and comparison of related studies (✓: Yes, ×: No).

Refs.	Year	Contributions	Comparative Study	Evaluating Framework	Auth. Factors		User Factors			AI	Output values	
					Traditional	Modern	Security	Privacy	Trust		Numerical	linguistic
Renaud, 2004	2004	The comparisons of authentication methods based on weighted values for password methods supporting three levels.	✓	✓	✓	×	✓	×	×	×	✓	×
Maltoni et al., 2009	2009	Comparison of 7 common biometric authentication methods including 7 criteria.	✓	×	✓	×	✓	✓	×	×	×	✓
Bonneau et al., 2012	2012	Comparison of the web authentication metods based on password, token, biometric (e.g., fingerprint, iris, voice) including 25 criteria.	✓	✓	✓	×	✓	×	×	×	✓	×
Crawford et al., 2013	2013	The presentation of a framework for transparent, continuous mobile device authentication based on behavioral modalities.	×	✓	✓	×	✓	×	×	×	✓	×
Korać & Simić, 2017	2017	Comparison of the traditional 12 authentication methods intended for mobile devices including all three basic authentication factors.	✓	✓	✓	×	✓	✓	×	×	✓	✓
Kiljan et al., 2018	2018	Comparisons of authentication methods for online banking environment including 3 criteria.	✓	✓	✓	×	✓	✓	×	×	✓	×
Korać & Simić, 2019	2019	Comparison of the classical 12 mobile authentication methods including all three basic authentication factors.	✓	✓	✓	×	✓	✓	×	×	✓	✓
Ali & Khan, 2022	2022	Comparison of frameworks for evaluation of authentication methods.	✓	✓	✓	×	✓	×	×	×	✓	×
Zhou et al., 2023	2023	Comparison of two hybrid password methods touch-gesture and keystroke-based passwords including interaction mode, observation angle, entry error, and observation effort.	✓	×	✓	×	✓	×	×	×	✓	×
Awadallah et al., 2024	2024	Comparative analysis of biometric modalities used for user authentication in metaverse.	✓	×	✓	✓	✓	✓	×	×	×	✓
Alsadie et al., 2024	2024	Comparison of security challenges and comparative analysis of AI techniques for classical biometric authentication in fog computing (FC) environments.	✓	×	✓	×	✓	✓	×	✓	×	✓
Alrawili et al., 2024	2024	Comparison of 12 biometric modalities based on 8 criteria.	✓	×	✓	×	✓	✓	×	×	×	✓
Our Study	**2025**	Comparison of the modern and traditional authentication methods based on 13 different methods including all three basic authentication factors.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

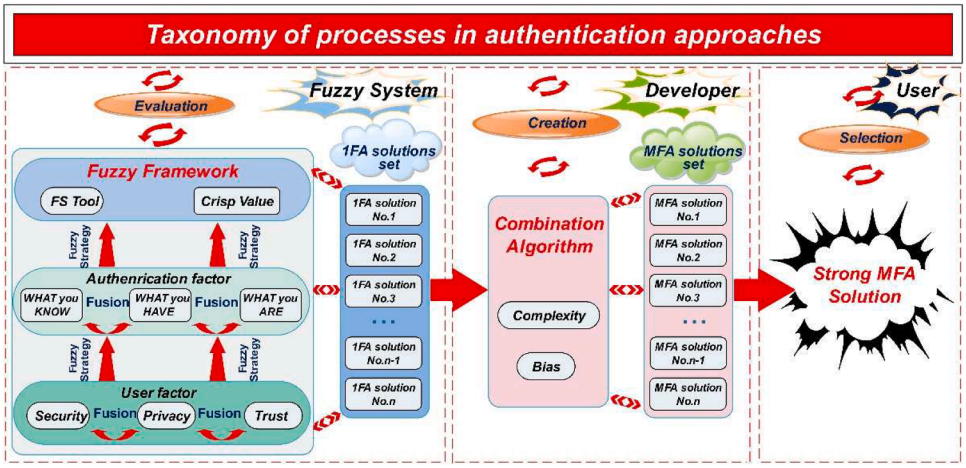

Fig. 2. The taxonomy of key research processes in authentication approaches.

enhances the comprehensive processing and evaluation of MFA, providing decision-makers with a clearer understanding of information fusion. On the other hand, the fusion strategies provide several advantages, such as the fusion of different multi-sources, enhanced security and trust, and more control over user personal information. Thus, fuzzy logic and information fusion as power tools bridge the gap present in traditional binary and rigid decision-making, providing a nuanced evaluation, creation, and selection of MFA solutions. As observed from Fig. 1, the first process unit, named the evaluation process, is responsible for the development and formation of f_f. This framework is orthogonal to the other research areas and spans user and authentication factors. Its key component is the FS tool, which enables practical implementation by integrating information from multiple sources and presenting it as a comprehensive set of possible 1FA solutions. Therefore, the fuzzy system is responsible for processes in this unit. In the next process unit, named the creation process, the developer, using the combination algorithm, processes all information from the previous level and creates the set of all potential MFA solutions. This process addresses two key research issues: complexity and bias. The responsibility for the processes in this unit lies with the developer. In the final process unit, named the selection process, the user has the opportunity to choose the final solution from the set of all previously selected authentication solutions. The responsibility for the final selection of the MFA solution lies with the user.

The taxonomy of key research processes in authentication approaches underscores the significance of user and authentication factors as multi-dimensional features, which have a direct influence on information processing and the design of strong, robust MFA solutions. Hence, before delving into the f_f development and its mathematical formulation, it is essential to first provide a brief overview of user and authentication factors, as well as a comparison of 1FA methods.

3.1. An overview of user and authentication factors

Despite the limited literature in this area, the related literature reviews singled out three user priorities (security, privacy, and trust) as very important comparative factors in authentication processes. All user factors are intrinsically connected to the user's distinct characteristics, reflecting their individual priorities and preferences. Since each user may prioritize different aspects based on their specific needs, aims, or context, these factors enable the quantification of user priorities. By incorporating user factors into authentication processes, the system ensures that the resulting MFA solution aligns with user priorities, thus providing a more relevant and secure experience. The security and privacy are well-studied user factors in comparison to trust. The contributions of the trust concept as the user factor to the literature is much less in authentication approaches than in comparison to other science fields. Achieving good trust in mobile devices can be challenging, particularly due to a large number of different mobile devices and their unique software, hardware, and network capabilities. The importance of trust in authentication approaches is to enable the establishment of user/service relationships. The trust strives for the same aim as security and privacy, to reach the highest level. Also, the credentials used for authentication processes can be classified as:

- *What you know* (G_i), (e.g., passwords, PIN, etc.)
- *What you have* (G_j), (e.g., tokens, devices, keys, AI, NFC, etc.).
- *What you are* (G_k) can be also classified as:
  1) *Physiological* based on the unique physiological user characteristics such as fingerprint, face, iris, retina, hand-geometry, vein, ear, palmprint, electroencephalogram (EEG), electrocardiographic (ECG), photoplethysmogram (PPG), etc.
  2) *Behavioral* based on the behavioral user characteristics such as voice, gait recognition, handwriting, signature, keystroke dynamics, eye movement, touch and multi-touch gesture, and many other (Zhang et al., 2024, Awadallah et al., 2024, and Alrawili et al., 2024).

In order to cope with the disadvantages of traditional methods (e.g., weak passwords, theft of mobile devices, hacking biometric credentials, etc.) (Zhou et al., 2025), new evolving modern authentication methods (e.g., AI methods and biological methods) are gaining immense traction in authentication approaches. It is necessary that the G_j factor by itself provide one protection layer, whose practical usage requires its combination with other authentication factors. Thus, the G_j factor is exclusively used as a part of MFA solutions (either 2FA or 3FA solutions) to verify a user's during authentication processes. Specifically, AI technologies coexist with other authentication methods (including biological methods such as EEG, ECG, and PPG) through fusion processes, building robust and strong MFA solutions. Also, besides complexity, accessibility, and pricing, the biological of liveliness detection methods has disadvantages associated with issues of privacy (e.g., including highly sensitive physiological signals) and trust factors (e.g., EEG electrodes, ECG, and PPG sensors are variable over time due to stress, fatigue, or other changes in user health, and they require direct connection to users, etc.).

3.2. Comparison of 1FA methods

Based on a literature analysis and the collected quantitative and qualitative information related to authentication and user factors, we have compared 1FA methods based on user factors such as security, privacy, and trust. The aim of comparative analysis in this research is to acquire linguistic results necessary for the further development of f_f architecture. Besides traditional methods, this comparison includes emerging modern methods such as physiological biometric methods based on the G_k factor (e.g., EEG, ECG, and PPG) and AI method-based G_j factor. The acquired descriptive results, as shown in Table 3, are categorized into seven levels. Entries are formed at the intersection of the literature reviews and the perception of authors. Thus, the significance and importance of comparative results derived from the differences in user and authentication factors represent a quantification input as a starting point for creating the f_f.

Additionally, the results, as presented in Table 3, show that compared to traditional authentication methods, modern methods provide significantly stronger security, but they also raise concerns related to privacy and trust. A general comparative review of traditional and modern authentication methods based on user factors is given in Table 4. Based on all the acquired results, it is possible to access the realization of f_f as the main research interest of this study.

4. Our proposed fusion framework

On the basis of the acquired comparative descriptive results given in Table 3, the proposal for f_f development is outlined in this section. Although individual authentication factors may seem simple, their complexity arises when combining MFA solutions. Therefore, the generic architecture of the f_f is presented in Fig. 3. This architecture includes different multi-processes and four blocks: fusion, forming framework, FS tool, and numeric value. For a more complete understanding of these processes, a workflow diagram is given in Fig. 4. The diagram begins with the process of selecting an MFA solution, which defines the problem. Next, the MFA process proceeds by choosing user priorities as the first and most important step. If these priorities involve multiple user factors, their selection and integration are carried out through fusion processes. U_f fusion relies on weighted metrics, presenting the coefficient share of the user priorities in a specific MFA solution. It is worth noting that it is the user who defines thresholds of these weighted metrics at the outset of the fusion process. These metrics assess the relevance, compatibility, and contribution of each user priority, shaping the MFA solution to achieve an optimal output value. However, it is clear that individual user sources by themselves cannot fully address the variability of multiple concepts when developing the MFA solution. Thus, the choice of authentication methods is directly influenced by U_f fusion that presents a basis for their selection. Subsequently, one or more authentication methods are chosen within the same authentication factor (e.g., G_i, G_j, and G_k). The need for additional authentication method selection depends on the type of MFA solution being developed, which is intended to protect a specific application domain. It implies that if the developed authentication system is based on a 2FA or 3FA solution, the iteration process must be performed in 2 or 3 steps accordingly.

In the next step, all chosen authentication factors are fused. Finally, the fusion of all selected authentication factors and user factors

Table 3
Comparison of 1FA methods based on analysis of literature reviews (including Table 2) and perception authors.

S.No.	*Factors*	*Security*	*Privacy*	*Trust*
1	*PIN*	VVL	VVH	VVH
2	*Password*	VVL	VVH	VVH
3	*OTP*	VL	H	H
4	*NFC*	M	M	M
5	*Fingerprint*	H	VL	H
6	*Face*	VH	VL	VL
7	*Iris*	VH	VL	VL
8	*Voice/Speech*	H	VL	L
9	*Keystroke Dynamics*	H	L	L
10	*AI*	VH	VL	L
11	*EEG*	VVH	VVL	VVL
12	*ECG*	VVH	VVL	VVL
13	*PPG*	VVH	VVL	VVL

Parameters - Low (L), Very Low (VL), Very Very Low (VVL), Medium (M), High (H), Very High (VH), Very Very High (VVH).

Table 4
The general comparative review of traditional and modern authentication methods.

S.No.	Factors	Traditional authentication methods	Modern authentication methods
1	Security	H	VVH
2	Privacy	VL	VVH
3	Trust	VL	VVH

leads to a "*Decision Fusion*". Lower fusion levels are responsible for these two key factors being compliant in block decision fusion. This fusion constitutes the final decision-making, determining whether access is granted or denied. In addition, the corresponding conditions for block decision fusion imply a prior fusion application at lower levels in which user factors are fused and then authentication factors are fused. The process of fusing at lower levels is crucial because it ensures that compliance is checked separately for each set of factors before being integrated into the final decision. This approach allows the MFA system to make a more nuanced decision based on multiple conditions (e.g., multiple factors, multiple processes, and multiple levels), ensuring robust and strong MFA processes.

Thus, the fusion process is completed, and the f_f is ready to be formed. After defining f_f, the next step involves its process of fuzzification and the generation of numeric values. It is important to note that this f_f can support any authentication method based on any user priority. This f_f enables the development of numerous scenarios, with each scenario representing one outcome from the set of all possible MFA solutions. To simplify and better understand the visual representation of the generic f_f architecture and the interconnections among its basic blocks, the f_f block diagram in a chain-like structure is provided in Fig. 5. The fusion block includes several processes derived at various levels, with the aim of integration. However, due to their nature, all fusion processes can lead to an increase in nonlinearity and stochasticity. Once the fusion process is complete, f_f is ready for formation. This block is linked to the FS tool block, followed by a fuzzification process. The FS block is closely connected to the numeric value block, where a defuzzification process takes place. In fact, the FS block as a tool produces an output numeric value. Each block represents a subsystem containing a group of submodules, each defined by its specific function. The influence of these basic blocks is not based on specific features but rather on their simultaneous operation. This means that all blocks should be considered holistically, as part of an integrated chain sequence. In the context of the given f_f block diagram, a deeper level of the topological relationships reveals that the fuzzy strategy plays a crucial role in defining the numeric output value.

Additionally, this f_f enables the development of numerous scenarios, with each scenario representing one outcome from the set of possible MFA solutions. To address this complex issue, a mathematical approach is employed in this research.

4.1. Mathematical formulation of f_f

The use of mathematical approaches further emphasizes the fact that all fusion processes in authentication approaches can be defined in the form of sets. The notations used in the mathematical formulation of f_f are given in Table 5.

The set is defined by the number of potential authentication scenarios that are highly dependent on each factor type. The combination algorithm can mathematically define different sets of authentication solutions**.** The examples are given for the following sets:

- *Example 1:* N_{allFA} as a set of all possible authentication solutions includes at least one user factor and one authentication factor from any source, and it can be mathematically represented with a general formula (Eq. (1)):

$$N_{allFA} = \left(2^{U_f} - 1\right)\left(2^{g_i + g_j + g_k} - 1\right)\left(g_i, g_j, g_k \geq 0,\ i,j,k = 1,2,\ \ldots, \mathrm{m}\right)\ (\forall\, m \in N) \tag{1}$$

- *Example 2:* N_{2FA} as a set of all possible two authentication solutions includes at least one user factor and at least two-factor authentication solutions from any source, and it can be mathematically represented with a general formula (Eq. (2)):

$$N_{2FA} = \left(2^{U_f} - 1\right)\left(2^{g_i + g_j + g_k} - 1 - g_i - g_j - g_k - \binom{g_i}{2} - \binom{g_j}{2} - \binom{g_k}{2}\right)\left(g_i, g_j, g_k \geq 0,\ i,j,k = 1,2,\ \ldots,\ m\right)\ (\forall\, m \in N) \tag{2}$$

- *Example 3:* N_{3FA} as a set of all possible three-factor authentication solutions (N_{3FA}) includes at least one user factor and at least one authentication factor from each source, and it can be mathematically represented with a general formula (Eq. (3)):

$$N_{3FA} = \left(2^{U_f} - 1\right)\left(2^{g_i} - 1\right)\left(2^{g_j} - 1\right)\left(2^{g_k} - 1\right)\left(g_i, g_j, g_k \geq 0,\ i,j,k = 1,2,\ \ldots,\ m\right)\ (\forall\, m \in N) \tag{3}$$

- *Example 4:* N_{anyFA} as a set of specific authentication solutions, either strong or weak (N_{anyFA}), is based on predefined parameters for any required authentication solution. Such a set can be mathematically represented with a general formula (Eq. (4)):

$$N_{anyFA} = \binom{U_f}{u}\binom{g_i}{k_i}\binom{g_j}{k_j}\binom{g_k}{k_k} \tag{4}$$

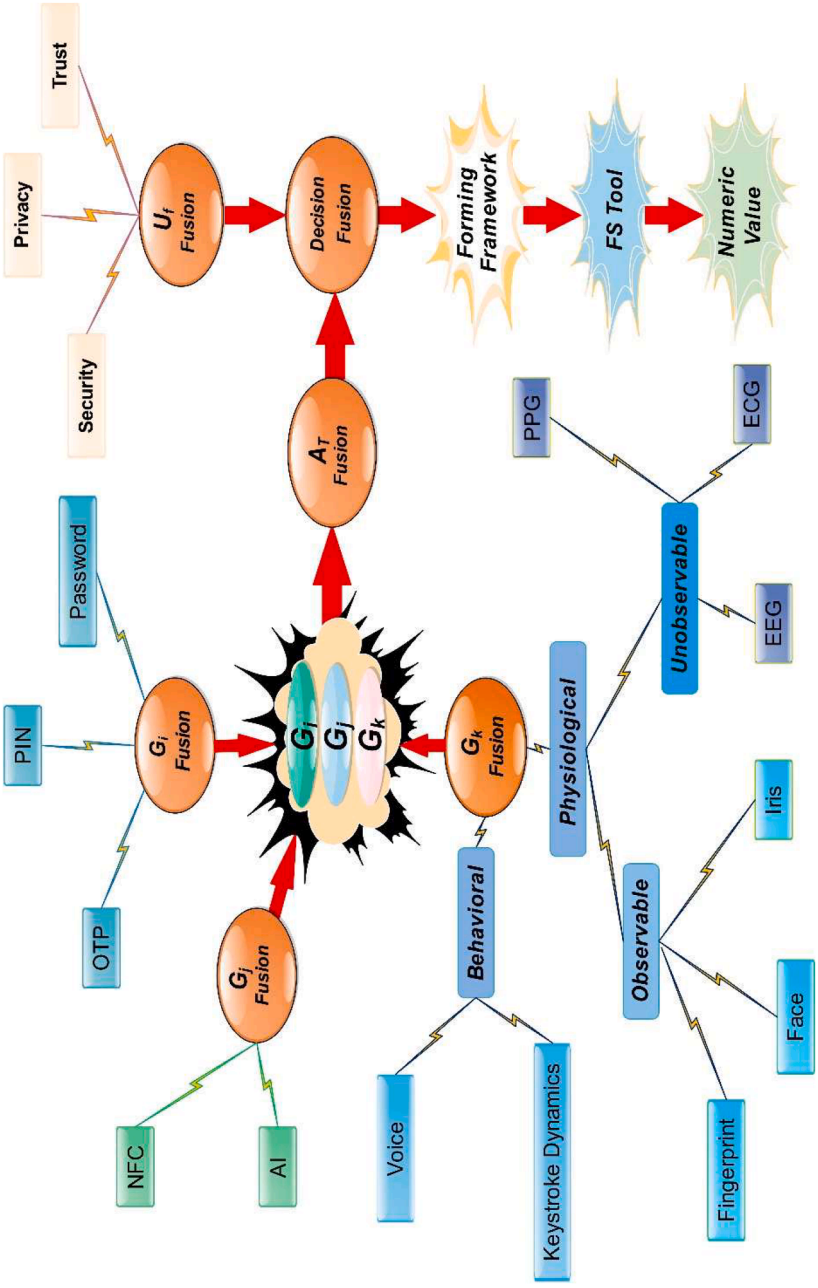

Fig. 3. The generic $_{ff}$ architecture.

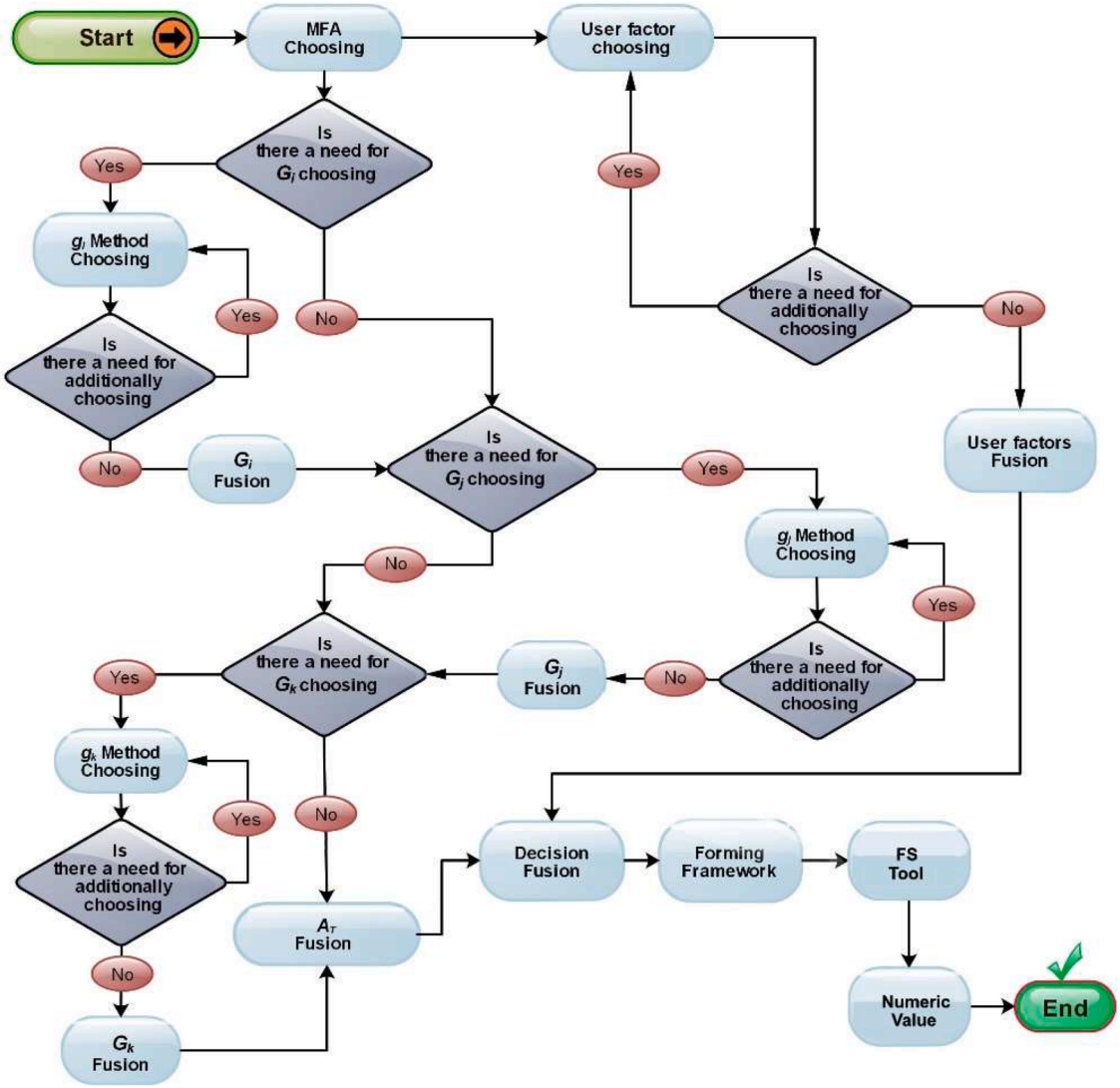

Fig. 4. Workflow of the proposed f_f.

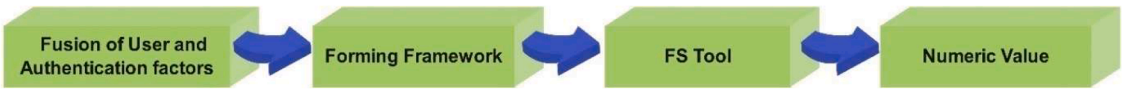

Fig. 5. The f_f block diagram.

Unlike the first three examples, which have theoretical significance in obtaining the role of the combination algorithm in authentication approaches, the given Eq. (4) has a practical significance because it reduces the number of potential solutions. Moreover, the f_f corresponding to Table 5 can be represented (Eq. (5)) as:

$$f_f = \{w_1 S + w_2 P + w_3 T\} \tag{5}$$

where weighted criteria represent w_1, w_2, and w_3. The weighted sum gives different weights for each of those user factors. We determined the weight of each user factor in building an MFA solution. The weight of criteria can be varied to conduct a sensitivity analysis of priorities regarding user requests. In this research, each user factor is observed with equal weight or the same level of importance. It is important to note that the values of all three weighted criteria are defined on the unit interval [0, 1] (Eq. (6)).

Table 5
Notations Description.

Notations	Description
A_T	*The total sum of all authentication methods*
G_i, G_j, G_k	*Authentication factor based on "What you know", "What you have", "What you are", respectively*
g_i, g_j, g_k	*"What you know", "What you have", "What you are" methods, respectively*
U_f	*The number of user factors*
S, P, T	*Security, Privacy, Trust, respectively*
M	*Number of used authentication factors*
u	*The number of used user factors*
n	*The number of used authentication factors*
k_i, k_j, k_k	*The number of used methods within each g_i, g_j, g_k factor, respectively*
w_1, w_2, w_3	*The weighted criteria of Security, Privacy, Trust, respectively*
N_{allFA}	*The set of all possible authentication solutions*
N_{2FA}	*The set of all possible two authentication solutions*
N_{3FA}	*The set of all possible three authentication solutions*
N_{anyFA}	*The set of any FA solution*
$N_{strongMFA}$	*The set of strong MFA solutions*

$$\sum_{i=1}^{3} w_i = 1 \; i = 1,2,\; 3 \; a_i \in [0,1] \tag{6}$$

Besides defining weighted criteria, the individual values of authentication methods need to be defined within each of the three authentication factors (G_i, G_i, G_k) in order to get the value of the f_f. The value sum for each authentication factor can be obtained by means of Eqs. (7)–(9):

Algorithm 1
The mathematical formulation of f_f .

Input: Defining user factors (*S, P, T*) and g_i g_j g_k methods based on factors (G_i, G_j, G_k).
Output: # Numeric value of MFA solution.
1 ***function*** numeric value Build f_f for input parameters
2:$\boldsymbol{f_f} = \{\boldsymbol{w_1 S} + \boldsymbol{w_2 P} + \boldsymbol{w_3 T}\}$
3:where $\boldsymbol{w_1} + \boldsymbol{w_2} + \boldsymbol{w_3} = 1 \; \boldsymbol{i} = 1,2,\; 3 \; \boldsymbol{a_i} \in [0,1]$
4:if *there is a need for additionally choosing* == true then *user factors choosing (S,P,T)*
5:end if
6:for user factors do fusion level
7:end for
8:if *there is a need for* G_i *choosing* == true then *choosing one of the offered* g_i *methods*
9:if *there is a need for additionally choosing* == true then return 1
10:else *(*G_i*)* fusion
11:end if
12:end if
13:if *there is a need for* G_j *choosing* == true then *choosing one of the offered* g_j *methods*
14:if *there is a need for additionally choosing* == true then return 2
15:else *(*G_j*)* fusion
16:end if
17:end if
18:if *there is a need for* G_k *choosing* == true then *choosing one of the offered* g_k *methods*
19:if *there is a need for additionally choosing* == true then return 3
20:else *(*G_k*)* fusion
21:end if
22:end if
23:for all *authentication factors* do *fusion*
24:end for
25:for *forming* $\boldsymbol{f_f}$ do *decision fusion*
26:end for
27:for $\boldsymbol{f_f}$ *numeric value* do *fuzzification*
28:end for
28:$\boldsymbol{G_i} = \boldsymbol{g_1} + \boldsymbol{g_2} + , \ldots, + \boldsymbol{g_i} \quad \boldsymbol{i} = 1,2, \ldots, \mathbf{m} \quad (\forall \, \boldsymbol{m} \in \boldsymbol{N})$
29:$\boldsymbol{G_j} = \boldsymbol{g_1} + \boldsymbol{g_2} + , \ldots, + \boldsymbol{g_j} \quad \boldsymbol{j} = 1,2, \ldots, \mathbf{m} \quad (\forall \, \boldsymbol{m} \in \boldsymbol{N})$
30:$\boldsymbol{G_k} = \boldsymbol{g_1} + \boldsymbol{g_2} + , \ldots, + \boldsymbol{g_k} \quad \boldsymbol{k} = 1,2, \ldots, \mathbf{m} \quad (\forall \, \boldsymbol{m} \in \boldsymbol{N})$
31:$\boldsymbol{A_T} = \boldsymbol{G_i} + \boldsymbol{G_j} + \boldsymbol{G_k} \quad \boldsymbol{G_i}, \boldsymbol{G_j}, \boldsymbol{G_k} \geq 0 \quad \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k} = 1,2, \ldots, \boldsymbol{m} \quad (\forall \, \boldsymbol{m} \in \boldsymbol{N})$
32: $\boldsymbol{f_f}(\boldsymbol{MFA}) = \dfrac{\boldsymbol{A_T}}{\boldsymbol{M}} \quad \boldsymbol{M} > 0 \quad \boldsymbol{M} = 1 \; (\mathbf{1FA}),\; 2 \; (\mathbf{2FA}),\; 3 \; (\mathbf{3FA}),\; \ldots,\; \boldsymbol{n}(\boldsymbol{nFA}) \; (\forall \mathbf{n} \in \mathbf{N})$
33:***return*** $\boldsymbol{f_f}$
34: **end function**

$$\sum_{i=1}^{m} g_i i = 1, 2, \ \ldots, \ \mathrm{m}(\forall\ m \in N) \tag{7}$$

$$\sum_{j=1}^{m} g_j\ j = 1, 2, \ \ldots, \ \mathrm{m}(\forall\ m \in N) \tag{8}$$

$$\sum_{k=1}^{m} g_k\ k = 1, 2, \ \ldots, \ \mathrm{m}(\forall\ m \in N) \tag{9}$$

On the basis of an obtained individual value of authentication methods within each of the three abovementioned authentication factors, it is possible to acquire their total sum (A_T) (Eq. (10)).

$$A_T = G_i + G_j + G_k\ G_i G_j,\ G_k\ \geq 0\ i, j, k = 1, 2, \ \ldots, \ m(\forall\ m \in N) \tag{10}$$

Finally, on the basis of all above-defined equations, a general mathematical formula of the f_f for the evaluation of the output value of MFA solutions is given in Eq. (11). The output value of f_f is defined by the quotient between the sum of all authentication methods (A_T) and the number of used authentication factors (M).

$$f_f(MFA) = \frac{A_T}{M} \mathrm{M} > 0\ M = 1\ (1FA),\ 2\ (2FA),\ 3\ (3FA),\ \ldots,\ n(nFA)\ (\forall\ n \in N) \tag{11}$$

In order to better understand the above-presented mathematical approach, the mathematical formulation of f_f, is given in Algorithm 1.

5. Fuzzy design and f_f development

To design and develop the f_f by a fuzzy classifier, an FS block, and numeric value block are used for the systematic study, the fuzzification, the formalization of the expertise, the inference method choice, the defuzzification, and finally the testing, adjustment, and validation of the output value. These submodules are designed based on fuzzy logic principles with the aim of acquiring numerical (crisp) output values. The workflow of the design and development methodology of the FS block is given in Fig. 6.

This figure illustrates five functional submodules within the FS block:

- *A rule base* contains the fuzzy *if – then* rules for defining the relationships between the fuzzy inputs and the desired fuzzy outputs.
- *A database* is responsible for defining the membership functions (MFs) of the fuzzy sets used in the fuzzy rules.
- *A fuzzy inference system (FIS)* as a generator of fuzzy output values is responsible for combining fuzzy inputs, MFs, and fuzzy rules. The fuzzy values of variables represent the degree of membership of a value in a specific fuzzy set that is typically defined in the range from "0" to "1". The FIS is one of the primary components of the FS block. The Mamdani-type fuzzy rules (see Mamdani & Assilian, 1975), as traditional methods and commonly used in various domains, are applied in this research. The reason is that the fuzzy rule base submodule follows a simple structure consisting of a set of fuzzy IF-THEN rules. Each rule is composed of an antecedent (input conditions) and a consequent (output action) that are connected using fuzzy logical operations. The general form of the fuzzy rule base submodule of any FS with multiple inputs and one output can be formulated as follows:

Rule 1: IF U_{f1} is p_1 AND U_{f2} is r_1 AND … AND U_{fz} is s_1, THEN Q is q_1:
Rule 2: IF U_{f1} is p_2 AND U_{f2} is r_2 AND … AND U_{fz} is s_2, THEN Q is q_2:
Rule z: IF U_{f1} is p_z AND U_{f2} is r_z AND … AND U_{fz} is s_z, THEN Q is q_z,

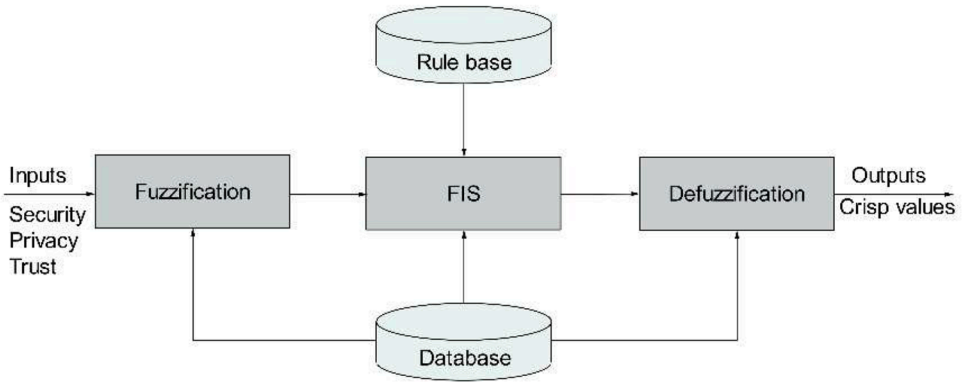

Fig. 6. Workflow of the FS block.

where

U_{fi} *(i=1, 2, ..., z), (∀ z∈N)* represents three input values: security, privacy, and trust.

Q represents one of the output values marked in the range from K to A, and

p_i, r_i, s_i, …, q_i *(i=1, 2,..., z), (∀ z∈N)* represent seven linguistic terms (VVL, VL, L, M, H, VH, and VVH) used to describe the output variables.

- *A fuzzification* maps numerical input values into fuzzy linguistic values.
- *A defuzzification* produces a numeric output value from the fuzzy output results as the overall FIS result.

In this research, the MF is uniquely represented with user factors because all three user priorities share the same MF. The MFs for user factors with linguistic values are presented in Fig. 7. For input values, a trapezoidal curve shape is used to define the fuzzy sets. The reason is that, compared to triangular, Gaussian, and bell-shaped functions, the trapezoidal function yields the best output, resulting in the smallest error. A generic mathematical representation of the trapezoidal MF μ(x) is:

$$\mu(x) = \begin{cases} 0, & x < a_1 \\ \dfrac{x - a_1}{a_2 - a_1}, & a_1 \le x \le a_2 \\ 1, & a_2 \le x \le a_3 \\ \dfrac{x - a_4}{a_3 - a_4}, & a_3 \le x \le a_4 \\ 0, & x > a_4 \end{cases} \tag{12}$$

A fuzzy set is a set consisting of one or more trapezoidal fuzzy numbers defined with four parameters (a_1, a_2, a_3, a_4) (Xiao et al., 2012), as extreme functions determining the shape of the trapezoid as shown in Fig. 8. The MF of a trapezoidal fuzzy number is piecewise linear and trapezoidal, which can capture the vagueness of those linguistic values as in Fig. 7. To assign fuzzy numeric values, we first define the linguistic values and their boundaries. Assign a fuzzy numeric value to each descriptive term based on its degree of membership in the corresponding fuzzy set. Thus, this fuzzy approach allows for more nuanced decision-making by reflecting partial membership in linguistic values rather than rigid classifications, and as such can be used in further analysis or calculations.

The key conditions for forming a function shape are parameters that need to be ordered in an increasing order $a_1 < a_2 < a_3 < a_4$, and the selected values that need to be relevant and consistent with the fuzzy system's design. As observed in Fig. 1, the fuzzy interval includes the range defined by the end parameters a_1 and a_4, while its core is defined by the interval between defined parameters a_1 and a_4. When the intervals overlap, as shown in Fig. 7, the minimum value of the core of the fuzzy interval, defined with a_2, corresponds to the maximum value of the previous interval's support, while the maximum value of the core of the fuzzy interval, defined with a_3, corresponds to the minimum value of the next interval's support. Given that parameters help to define the boundaries and the slope of the trapezoid, which in turn determines how input values are mapped to membership degrees between 0 and 1; hence we define four extremes this trapezoidal function:

- a_1 - left boundary of the lower base/the rising edge of the trapezoid,
- a_2 - beginning of the upper base - the point where the membership value starts being 1,

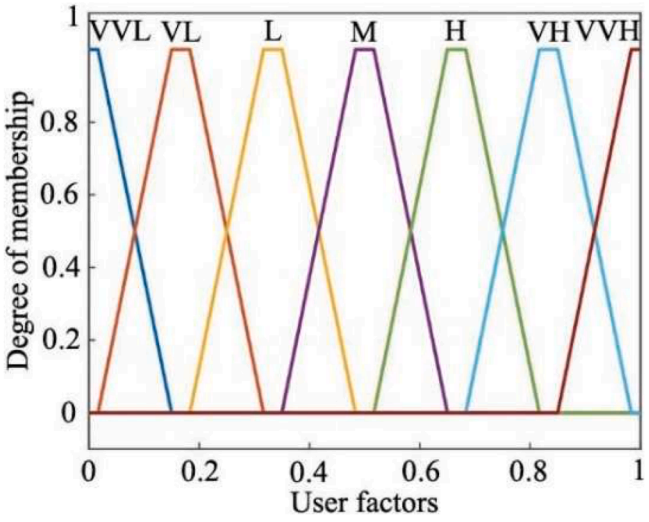

Fig. 7. MFs for user factors.

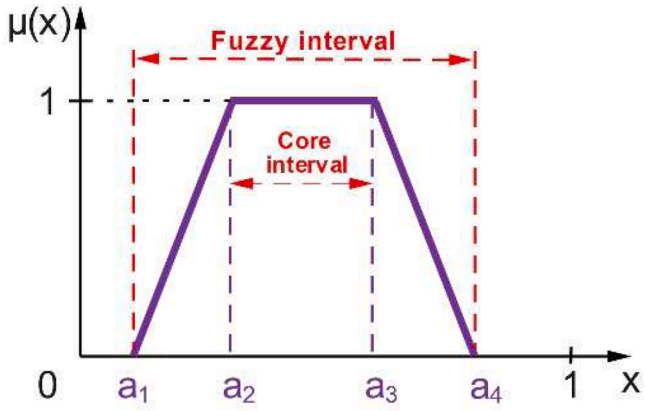

Fig. 8. A generic illustration of the trapezoidal fuzzy number x.

- a_3 - right boundary of the upper base - the falling edge of the trapezoid,
- a_4 - right boundary of the lower base - the falling edge of the trapezoid.

In this research, for instance, the linguistic variable "*medium*" is represented by developers with fuzzy numbers such as a_1 (0.35), a_2 (0.4833), a_3 (0.5167), and a_4 (0.65), the MF of which is:

$$\mu(x) = \begin{cases} 0, & x < 0.35 \\ \dfrac{x - a_1}{a_2 - a_1}, & 0.35 \le x \le 0.4833 \\ 1, & 0.4833 \le x \le 0.5167 \\ \dfrac{x - a_4}{a_3 - a_4}, & 0.5167 \le x \le 0.65 \\ 0, & x > 0.65 \end{cases} \tag{13}$$

The MFs are generated by the MATLAB fuzzy logic toolbox, which itself provides tools and functions for developers to input, visualize, and manipulate MFs. However, it does not automatically generate the parameter values for trapezoidal MF. The responsibility for defining those parameter values lies with the developers. They define the parameter values based on their specific application and domain knowledge. When developers create the FIS, they manually define the parameter values for the MFs, including the parameters of the trapezoidal MF. The table of all fuzzy input rules based on the trapezoidal function is given in Table 6. This rule plays a key role in the process of converting linguistic values into fuzzy numeric values, named the fuzzification process, as it directly affects the output results. An important feature of fuzzy intervals is their ability to assign criteria in a simpler and more intuitive way. This means that developers can use fuzzy intervals as a valuable tool, but they are not absolved of the responsibility to make appropriate choices within those intervals.

Furthermore, developers who apply the fuzzy input rule table to Table 3 with assigned linguistic values create fuzzy numeric values as shown in Table 7. In this stage, the aim is to assign fuzzy numeric values to each of these linguistic values, but their values have to lie within the defined fuzzy interval. For instance, in the context of the PIN method, the linguistic value of "VVL" for the security factors is assigned a fuzzy value of 0.02 (indicating low membership), while the linguistic value of "VVH" for privacy and trust factors is assigned a fuzzy value of 0.98 (indicating very very high membership).

Table 6
The table of rule for fuzzy input.

Input/Linguistic value	*Fuzzy interval*			
	a_1	a_2	a_3	a_4
VVL	-0.15	-0.01667	0.01667	0.15
VL	0.01667	0.15	0.1833	0.3167
L	0.1833	0.3167	0.35	0.4833
M	0.35	0.4833	0.5167	0.65
H	0.5167	0.65	0.6833	0.8167
VH	0.6833	0.8167	0.85	0.9833
VVH	0.85	0.9833	1.017	1.15

Table 7
The fuzzy numeric value of 1FA methods.

S.No.	Factors	Security	Privacy	Trust
1	*PIN*	0.02	0.98	0.98
2	*Password*	0.05	0.95	0.95
3	*OTP*	0.1	0.88	0.88
4	*NFC*	0.5	0.5	0.5
5	*Fingerprint*	0.65	0.21	0.55
6	*Face*	0.72	0.19	0.20
7	*Iris*	0.74	0.18	0.17
8	*Voice/Speech*	0.69	0.19	0.32
9	*Keystroke Dynamics*	0.58	0.25	0.34
10	*AI*	0.86	0.16	0.25
11	*EEG*	0.95	0.1	0.12
12	*ECG*	0.98	0.08	0.1
13	*PPG*	0.92	0.12	0.15

In this work, Fig. 9 is provided to facilitate a better understanding of Table 7. This figure presents a comparative statistical analysis of the fuzzy numeric values for the selected 1FA methods.

In the next step, the numeric value block, as part of the proposed functional FIS submodule, is based on a defuzzification process, whereby the output results are represented on a scale from 0 to 10 or as percentages from 0 to 100%. Additionally, a trapezoidal curve shape of the MF is used to define the output value variables. These values are classified from "A" to "K," where "A" marked with "10" represents the highest value, while "K" marked with "0" represents the lowest value. The MFs for evaluating MFA solutions are shown in Fig. 10. In the final phase, the developed fuzzy rules submodule, based on expert knowledge, is used to define the relationship between input and output mappings. As this research involves three inputs and seven linguistic variables, the maximum number of rules is 343 (i.e., 7^3) for this FS. The increase in the number of fuzzy rules presents two main challenges: computational complexity (e.g., processing time and inference engine load) and memory requirements (e.g., rule base and intermediate data storage). To address this, a reduction process was applied to the primary rules, selecting only 100 out of the 343 possible rules for constructing a complementary rule base. The complementary rule base involves selecting rule subsets for each output value, with the aim of simplifying the primary rules by removing redundant or less influential rules, while preserving the essential behavior of the FS. Since the complementary rule base implicitly includes the primary rules (i.e., the 343 possible rules), the reduction process does not affect the accuracy of the output results. With the defined fuzzy rules in the fuzzy rule base, the performance of the FS block was examined to assess how well the fuzzy system operates and whether it meets the desired objectives and requirements.

6. Computational study and results

This section provides three real-world case scenarios, highlighting empirical validation of the proposed framework. The first two scenarios relate to the practical application of f_f for 1FA and MFA solutions, while the third scenario relates to the combination algorithm. To conduct computational case scenarios, we provide a summary of the input used parameters, as listed in Table 8. Our aim is to evaluate and rank 1FA and 2FA solutions and explore the combination algorithm by identifying all potential authentication solutions. Therefore, a user request is directed to find the sets of authentication solutions based on the use of three authentication and

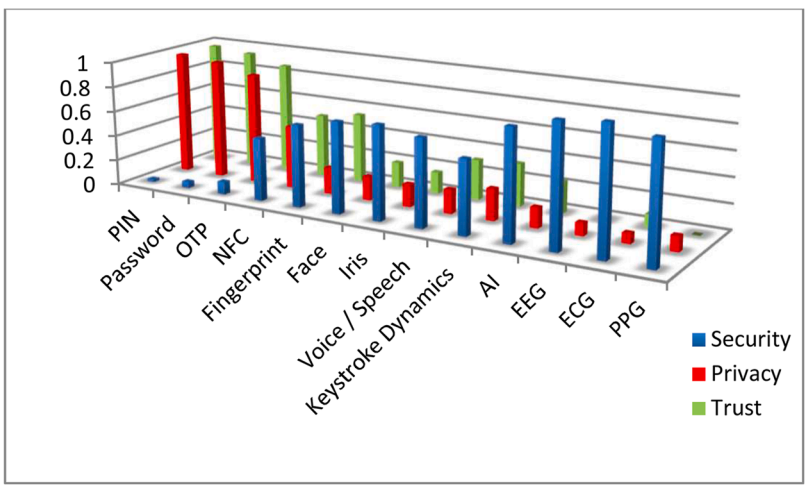

Fig. 9. A comparative statistical analysis of the fuzzy numeric value for the selected 1FA methods.

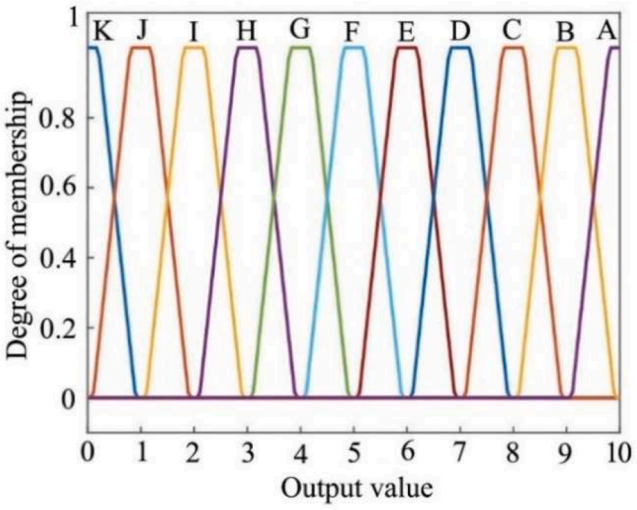

Fig. 10. MFs for evaluation of MFA solutions.

Table 8
Summary of the used input parameters.

Parameters	*Description*	*Number used parameters*
U_F	*Security, privacy, trust*	*3*
u	*The number of used user factors*	*3*
g_i	*PIN, Password, OTP*	*3*
g_j	*AI, NFC*	*2*
g_k	*Fingerprint, Face, Iris, Voice, Keystroke Dynamics, EEG. ECG, PPG*	*8*
k_i	*The number of used g_i methods*	*1*
k_j,	*The number of used g_j methods*	*1*
k_k	*The number of used g_k methods*	*2*

user factors with equal weighting.

Therefore, using the parameters given in Table 8 and assigning equal weighted criteria (Eq. (14)), whereby

$$w_1 = w_2 = w_3 = \frac{1}{3} \tag{14}$$

Eq. (6) can be represented as (Eq. (15)):

$$\frac{1}{3}+\frac{1}{3}+\frac{1}{3}=1 \tag{15}$$

Taking into account all the above conditions presented in expressions 14 and 15, the f_f in this case study has the following form (Eq. (16)):

Table 9
The practical results of applying the f_f for evaluating 1FA solutions with ranking.

S.No.	*Selection of authentication method*	*Output value*	*Percentage (%)*	*Ranking*
12	*ECG*	8.87	88.7%	1
11	*EEG*	8.3	83%	2
13	*PPG*	8.23	82.3%	3
10	*AI*	8.13	81.3%	4
7	*Iris*	8.0	80%	5
6	*Face*	7.34	73.4%	6
5	*Fingerprint*	7.0	70%	7
8	*Voice / Speech*	6.16	61.6%	8
9	*Keystroke Dynamics*	6.0	60%	9
4	*NFC*	5.0	50%	10
3	*OTP*	2.09	20.9%	11
2	*Password*	1.51	15.1%	12
1	*PIN*	0.47	4.7%	13

$$f_f = \left\{\frac{1}{3}S + \frac{1}{3}P + \frac{1}{3}T\right\} \tag{16}$$

6.1. Computational case scenario

After setting up the functional FS block, the f_f is applied to evaluate and rank 1FA solutions. The aim is to validate the framework for how the developed f_f can be practically applied in a real-world scenario. The practical results of 1FA solutions (including modern methods), along with their rankings, are shown in Table 9. This table highlights g_k methods as the highest-ranking, with emerging authentication methods such as the ECG method predominating with 8.92, while g_i methods have the lowest ranking, with the PIN method scoring 0.86. The calculation of the 1FA method is a prerequisite for accessing the MFA solution evaluation, as individual methods and their values represent the foundational elements of each MFA solution.

6.2. Computational case scenario

Based on the used input parameters presented in Table 8 and the acquired results given in Table 9, the additional computational work can be calculated for the selected 2FA solutions. The eight examples of calculating the values of 2FA solutions corresponding to Eq. (11), are used in this research (Eqs. (17)–(24)):

$$f_f(password\ +\ keystroke\ dynamic) = \frac{1.51 + 6}{2} = 3.755 \tag{17}$$

$$f_f(face +\ voice) = \frac{7.34 + 6.16}{2} = 6.75 \tag{18}$$

$$f_f(face +\ Password) = \frac{7.34 + 1.51}{2} = 4.42 \tag{19}$$

$$f_f(face +\ Iris) = \frac{7.34 + 8}{2} = 7.67 \tag{20}$$

$$f_f(Fingerprint\ +\ Password) = \frac{7 + 1.51}{2} = 4.22 \tag{21}$$

$$f_f(AI\ +\ ECG) = \frac{8.13 + 8.87}{2} = 8.5 \tag{22}$$

$$f_f(AI\ +\ EEG) = \frac{8.13 + 8.3}{2} = 8.21 \tag{23}$$

$$f_f(AI\ +\ PPG) = \frac{8.13 + 8.23}{2} = 8.18 \tag{24}$$

It is important to note that all values of the individual authentication methods used in Eqs. (17)–(24) are derived from Table 9, which lists the specific methods that constitute the selected 2FA solution. For this case study, we have used five examples of traditional 2FA solutions proposed by other authors, while our selection includes three examples of modern MFA solutions. The practical results of applying the f_f for evaluation and ranking of 2FA solutions are given in Table 10. By testing selected 2FA solutions from a real-world scenario, we have demonstrated the validity and effectiveness of the developed f_f in ranking and evaluating the 2FA solutions based on multiple criteria.

6.3. Computational case scenario

The aim of conducting this computational case scenario is to identify all potential combinations of authentication solutions based

Table 10
The practical results of applying the f_f for evaluating 2FA solutions with ranking.

S.No.	Selection of 2FA method	State-of-art	Output value	Percentage (%)	Ranking
1	*Password + keystroke dynamic*	Monrose et al. (2002)	3.75	37.5%	8
2	*Face + Voice*	Tresadern et al. (2013)	6.75	67.5%	5
3	*Face + Password*	Kang et al. (2014)	4.42	44.2%	6
4	*Face + Iris*	DeMarsico et al. (2014)	7.67	76.7%	4
5	*Fingerprint + Password*	Go et al. (2014)	4.22	42.2%	7
6	*AI + ECG*	Our study	8.5	85%	1
7	*AI + EEG*	Our study	8.21	82.1%	2
8	*AI + PPG*	Our study	8.18	81.8%	3

on the input parameters provided in Table 8. Taking into account all the used parameters corresponding to Table 8, it is possible to calculate all sets of potential outcomes. Specifically, the extra empirical work corresponding toEqs. (1)–(4) can be calculated (Eqs. (25)–(28)):

$$N_{allFA} = \left(2^3-1\right)\left(2^{2+3+8}-1\right) = 7*8191 = 57\ 337 \tag{25}$$

$$N_{2FA} = \left(2^3-1\right)\left(2^{2+3+8}-1-2-3-8-\binom{2}{2}-\binom{3}{2}-\binom{8}{2}\right) = 7*8\ 146 = 57\ 022 \tag{26}$$

$$N_{3FA} = \left(2^3-1\right)\left(2^2-1\right)\ \left(2^3-1\right)\left(2^8-1\right) = 7*3*7*255 = 37\ 485 \tag{27}$$

$$N_{strongMFA} = \binom{3}{3}\binom{2}{1}\binom{3}{1}\binom{8}{2} = 1*2\ *3\ *28 = 168 \tag{28}$$

The summary of all possible outcomes of the combination algorithm is given in Table 11. This table provides a clearer understanding of the possibility of developing a large number of practical solutions. Each of these solutions, depending on the given input parameters and observed user priorities, could potentially represent the optimal and most applicable solution in practice.

7. Discussion of results and implications

This section presents a discussion of the results and their implications, divided into two parts. First, we interpret the obtained results, while second, we offer the theoretical and practical implications, outlining their most important aspects.

7.1. Interpretation of results

Having presented the study's empirical findings in the previous section, this section serves to critically discuss the acquired results through comparative reviews and analyze how different user factors impact the output value of authentication solutions. The comparative reviews of the acquired results for traditional 1FA/2FA solutions with other related research are given in Fig. 11(a) and (b), respectively. The output results show that the developed f_f produces realistic output values in which the new modern methods are pushing all values of MFA metrics and decreasing the values of traditional methods. Specifically, modern authentication methods have challenged the effectiveness of traditional approaches by demonstrating that when scores between two or more MFA solutions are similar, a higher score does not necessarily indicate stronger authentication security, as presented in previous studies. On the other hand, the FIS output surface provides a visual representation that allows the analysis of how different user factors impact the output value of authentication solutions. The response surfaces of the f_f are given in Fig. 12(a–c). This figure shows examples of those relations.

As observed from these figures, the maximum of the function covers the diagram's upper surface as an extremum function with the defined maximal output values of user factors. This diagram points out that there is a similarity between these factors regarding their high impact on the output value. These facts indicate a close relation between user factors where the trust has a significant impact on the other two factors. This points out the symbiotic existence of these factors in which the privacy and security factors are in function to gain the user's trust while the trust is a trigger for their launching. It is obvious that the trust is built on a framework of security and privacy and as such represents an inevitable factor in all authentication approaches. If there are no trust relationships in the authentication environment, even the best offered MFA solutions will be completely useless. The user will not wish to access authentication processes. Therefore, all presented facts confirm that user factors are closely related, where each factor plays an important role related to the output value and ranking of authentication solutions.

When it comes to the combination algorithm, the acquired results show that the number of possible developed authentication solutions is extremely large for a very small number of input factors. The combination algorithm has a possibility to generate a wide variety of authentication solutions. However, we point out that as the number of input factors is far greater in practice, the set of possible authentication solutions strives to a set of an infinite number. Also, this research reveals that thousands of potential developed different outcomes can be offered as the best MFA solutions in practice. The reason is that each offered solution is not fixed, but their output values are directly conditioned by the user priorities. Moreover, the mathematical approach enables a detailed comparative analysis between 1FA and MFA, as presented in Table 12, providing valuable insights into their distinct mathematical differences. Key features that uniquely define each approach include factor, function, model, form, value, time, resources, bias, and solution set.

7.2. Theoretical and practical implications

The theoretical implications of this research are significant for both academic and research communities. For the academic community, the study introduces the innovative concept of trust-based user prioritization and demonstrates how AI technologies can be effectively integrated into authentication processes. For the research community, it provides a theoretical foundation for analyzing trust factors associated with authentication metrics, encouraging interdisciplinary approaches to evaluation processes and the development of authentication frameworks. Therefore, the theoretical implications lie in redefining how MFA solutions are created and evaluated. This is achieved by formally incorporating trust as an independent user factor, applying fuzzy methodologies

Table 11
The summary of the combination algorithm outcomes.

Example number	*Type of solution*	*Description*	*Number of outcomes*
1	N_{allFA}	*Set of all possible authentication solutions*	*57 337*
2	N_{2FA}	*Set of all possible two authentication solutions*	*57 022*
3	N_{3FA}	*Set of all possible three authentication solutions*	*37 485*
4	$N_{strongMFA}$	*Set of strong 3FA*	*168*

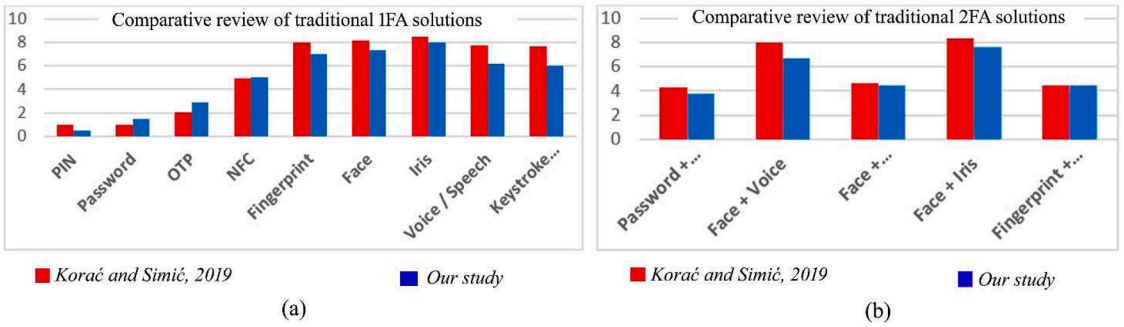

Fig. 11. Comparative reviews of the acquired results for traditional 1FA /2FA solutions with other related research.

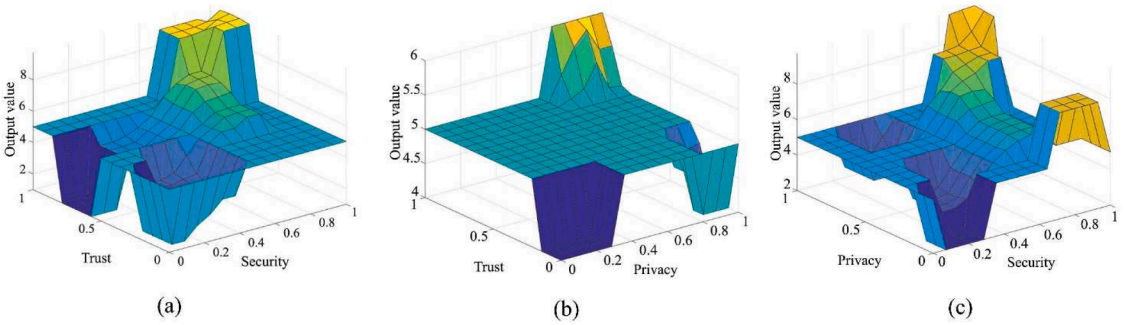

Fig. 12. Response surfaces of the f_f, illustrating the relationships between user factors.

Table 12
The comparative review between 1FA and MFA.

Features	1FA	MFA
Factor	Single	*Multi*
Function	*Linearity*	*Nonlinearity*
Model	*Deterministic*	*Stochasticity*
Form	*Simple*	*Complex*
Value	*Static*	*Dynamic*
Time and resource	*Less*	*Much*
Bias	*No*	*Yes*
Solution set	*Final*	*Infinite*

(specifically, Mamdani-type fuzzy logic with a trapezoidal MF), and integrating new technologies and authentication methods within the developed AI-based fusion framework. Additionally, abstracting authentication processes through various theories and decision-making processes expands the theoretical framework underlying MFA strategies. By comparing various authentication frameworks, our proposed framework facilitates the identification and formalization of trust as a distinct, independent factor in the evaluation of MFA systems, an aspect largely overlooked in prior frameworks. This underscores the importance of trust as a user priority in enhancing both the effectiveness and acceptance of the proposed MFA solutions. Accordingly, the theoretical implications reflect a transition from a strictly technical paradigm to a sociotechnical approach that accounts for both system performance and user priorities (e.g., security, privacy, and trust), emphasizing the integrative role of trust and AI technologies in MFA strategies. Also, this

study adopts a mathematical perspective for evaluating MFA solutions, highlighting the potential to develop numerous theoretical MFA scenarios. Overall, the research advances the theoretical understanding of AI as an authentication factor, enabling its systematic evaluation and reinforcing its value in improving both defensive strategies and user experience.

From a practical standpoint, the proposed AI-based framework shares similarities with other fuzzy logic-based authentication frameworks but distinguishes itself by emphasizing trust as a novel and weighted factor in MFA evaluation. Its practical implications highlight the transformative potential of the AI-powered fusion framework in improving operational efficiency and user decision-making, as shown in Figs. 11 and 12. While the framework addresses the need to enhance the efficiency of MFA processes, it is faced with practical limitations associated with resources, the large volume of information processing, and the trade-offs of balancing user priorities and emerging technologies. The large volume of information processing highlights the need for AI-driven automated algorithms to manage the combinatorial complexity involved in developing MFA solutions, as manual combination is inefficient and impractical for timely processing. The proposed framework utilizing AI as an authentication factor creates new practical opportunities for algorithmic combinations and emphasizes it as a relatively unexplored aspect of MFA strategies. Given that new technologies have the potential to enhance security metrics, their true value lies in user acceptance or rejection of the proposed MFA method, influencing all other user factors, which, in turn, strongly influence an organization's reputation. Therefore, the practical implications of integrating user priorities point out that the framework positions trust as a central, unifying user priority that underpins all other user factors. Without user trust, other priorities lose practical relevance, making it essential to the design and acceptance of authentication systems. Overall, the framework lays a strong foundation for the practical development of stronger and more robust MFA solutions. Additionally, it paves the way for future studies on the practical application of AI in authentication systems.

8. Conclusions and future directions

Based on the above discussion and related literature review, it can be concluded that growing information challenges for continuously finding better evaluation frameworks and combination algorithms for the creation of strong and secure MFA solutions are never-ending. The real significance of evaluation processes in authentication approaches is twofold and immeasurable. First, it helps developers create more powerful and strong MFA solutions that provide a more secure user environment. Second, it ensures the right balance between key user factors (e.g., security, privacy, and trust), thereby enhancing an organization's reputation. In that context, we propose a unique f_f for evaluating authentication solutions that incorporates all the aforementioned user factors. Unlike other frameworks, this framework, which is highly adaptable, scalable, and very efficient in practice, enables developers to create MFA solutions tailored to individual user priorities and provides multiple "best" outcomes depending on those user requirements. In addition, the comparative approach between traditional and modern technologies, including AI-based methods and biological liveliness detection methods (e.g., EEG, ECG, and PPG), points out that AI technologies can be applied in various ways in authentication processes, as an individual authentication factor (e.g., "*what you have*") and as an algorithm. The advantages of AI technologies not only enhance MFA metrics, reduce complexity, and eliminate bias, but also create new combinatorial possibilities for information processing, ultimately improving overall MFA defense strategies.

This study, employing a comparative mathematical approach based on case studies, clearly validates that MFA systems are significantly more complex, dynamic, and resource-intensive than 1FA systems. Also, this approach points out two limitations associated with the evaluation process and bias issue. The large amount of information processing presents a limitation for developers, who also need to deal with the MFA bias issue, as it comes from their side. The evaluation process requires more time and resources and potentially introduces greater variability. Given the infinite number of potential authentication combinations, manually combining them is exhaustive and impractical for timely information processing and management. Therefore, future research should focus on developing automated AI-driven combination algorithms. Since these algorithms involve multiple fusion analyses, their development should be paired with a comprehensive fusion architecture, which serves as a core pillar of an agile defensive cyber strategy. Practically, these identified limitations represent an excellent way to define future research directions, with a focus on developing intelligent MFA solutions and gaining a deeper understanding of AI algorithm functionality.

CRediT authorship contribution statement

Dragan Korać: Writing – original draft, Visualization, Validation, Software, Methodology, Investigation, Conceptualization. **Boris Damjanović:** Supervision, Formal analysis. **Dejan Simić:** Supervision, Formal analysis. **Cong Pu:** Supervision, Formal analysis.

Declaration of competing interest

Authors declare that they have no conflict of interest.

Data availability

No data was used for the research described in the article.

References

Aghili, S. F., Mala, H., Schindelhauer, C., Shojafar, M., & Tafazolli, R. (2021). Closed-loop and open-loop authentication protocols for blockchain-based IoT systems. *Information Processing & Management, 58*(4), Article 102568.

Ahanger, T. A., Aljumah, A., & Atiquzzaman, M. (2022). State-of-the-art survey of artificial intelligent techniques for IoT security. *Computer Networks, 206*, Article 108771.

Ali, Y., & Khan, H. U. (2022). GTM approach towards engineering a features-oriented evaluation framework for secure authentication in IIoT environment. *Computers & Industrial Engineering, 168*, Article 108119.

Alizadeh, M., Tadayon, M. H., & Jolfaei, A. (2021). Secure ticket-based authentication method for IoT applications. *Digital Communications and Networks, 9*(3), 710–716.

Alrawili, R., AlQahtani, A. A. S., & Khan, M. K. (2024). Comprehensive survey: Biometric user authentication application, evaluation, and discussion. *Computers and Electrical Engineering, 119*(Part A), Article 109485.

Alsadie, D. (2024). Artificial intelligence techniques for securing fog computing environments: Trends, challenges, and future directions. *IEEE Access, 12*, 151598–151648. https://doi.org/10.1109/ACCESS.2024

Alzubaidi, A., & Kalita, J. (2016). Authentication of smartphone users using behavioral biometrics. *IEEE Communications Surveys & Tutorials, 18*(3), 1998–2026.

Ambika, N. (2019). Energy-perceptive authentication in virtual private networks using GPS data. In Z. Mahmood (Ed.), *Security, privacy and trust in the IoT environment*. Cham: Springer. https://doi.org/10.1007/978-3-030-18075-1_2.

Awadallah, A., et al. (2024). Artificial intelligence-based cybersecurity for the metaverse: Research challenges and opportunities. *IEEE Communications Surveys & Tutorials*. https://doi.org/10.1109/COMST.2024.3442475

Bhattarai, I., Pu, C., Choo, K. K. R., & Korać, D. (2024). A lightweight and anonymous application-aware authentication and key agreement protocol for the internet of drones. *IEEE Internet of Things Journal, 11*(11), 19790–19803.

Bonneau, J., Herley, C., Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proceedings of the 2012 IEEE symposium on security and privacy (SP)* (pp. 553–567). IEEE.

Campbell, T. R., Arabnia, H. R., & Droegehom, O. (2004). Protecting the infrastructure: evaluating a model for secured network connectivity using identity and authentication for use in a mobile computing environment. In *Proceedings of the international conference on internet computing* (pp. 376–382).

Chahoud, M., Mourad, A., Otrok, H., Bentahar, J., & Guizani, M. (2025). Trust driven on-demand scheme for client deployment in Federated learning. *Information Processing & Management, 62*(2), Article 103991.

Chang, D., Garg, S., Ghosh, M., & Hasan, M. (2021). BIOFUSE: A framework for multi-biometric fusion on biocryptosystem level. *Information Sciences, 546*, 481–511.

Charef, N., Aloqaily, M. A. B., Bouachir, O., & Guizani, M. (2023). Artificial intelligence implication on energy sustainability in Internet of Things: A survey. *Information Processing & Management, 60*(2), Article 103212.

Chen, X., Xie, H., Li, Z., Cheng, G., Leng, M., & Wang, F. L. (2023). Information fusion and artificial intelligence for smart healthcare: A bibliometric study. *Information Processing & Management, 60*(1), Article 103113.

Crawford, H., Renaud, K., & Storer, T. (2013). A framework for continuous, transparent mobile device authentication. *Computers & Security, 39*, 127–136.

DeMarsico, M., Galdi, C., Nappi, M., & Riccio, D. (2014). FIRME: Face and iris recognition for mobile engagement. *Image and Vision Computing, 32*(12), 1161–1172.

Esposito, C., Ficco, M., & Gupta, B. B. (2021). Blockchain-based authentication and authorization for smart city applications. *Information Processing & Management, 58*(2), Article 102468.

Evans, A. M., Stavrova, O., & Rosenbusch, H. (2021). Expressions of doubt and trust in online user reviews. *Computers in Human Behavior, 114*, Article 106556.

Feng, W., Yan, Z., Zhang, H., Zeng, K., Xiao, Y., & Hou, Y. T. (2018). A survey on security, privacy, and trust in mobile crowdsourcing. *IEEE Internet of Things Journal, 5*(4), 2971–2992.

Fortuna, C., Yetgin, H., Ogrizek, L., Municio, E., Marquez-Barja, J. M., & Mohorcic, M. (2023). HANNA: Human-friendly provisioning and configuration of smart devices. *Engineering Applications of Artificial Intelligence, 126*(A), Article 106745.

Furnell, S., Helkala, K., & Woods, N. (2022). Accessible authentication: Assessing the applicability for users with disabilities. *Computers & Security, 113*, Article 10256.

Ghaemi, H., Abbasinezhad-Mood, D., Ostad-Sharif, A., & Alizadehsani, Z. (2024). Novel blockchain-assisted fault-tolerant roaming authentication protocol for mobility networks without home agent entanglement. *Journal of Network and Computer Applications, 224*, Article 103843.

Ghafourian, M., Sumer, B. Vera-Rodriguez, R. Fierrez, J. Tolosana, R. Moralez, A. Kindt, E. 2023. Combining Blockchain and Biometrics: A Survey on Technical Aspects and a First Legal Analysis, arXiv:2302.10883, doi: 10.48550/arXiv.2302.10883.

Go, W., Lee, K., & Kwak, J. (2014). Construction of a secure two-factor user authentication system using fingerprint information and password. *Journal of Intelligent Manufacturing, 25*(2), 217–230.

Hamdani, S. W. A., Abbas, H., Janjua, A. R., Shahid, W. B., Amjad, M. F., Malik, J., Murtaza, M. H., Atiquzzaman, M., & Khan, A. W. (2022). Cybersecurity Standards in the Context of Operating System: Practical Aspects. *Analysis, and Comparisons, ACM Computing Surveys, 54*(3), 1–36.

Helkala, K., & Snekkenes, E. (2008). A method for ranking authentication products. In *Proceedings of the second international symposium on human aspects of information security & assurance (HAISA 2008). Plymount, UK* (pp. 80–93).

Hsieh, Y. H., Guan, X. Q., Liao, C. H., & Yuan, S. M. (2024). Physiological-chain: A privacy preserving physiological data sharing ecosystem. *Information Processing & Management, 61*(4), Article 103761.

Hu, R., & Damper, R. I. (2008). A "No Panacea Theorem" for classifier combination. *Pattern Recognition Journal, 41*(8), 2665–2673.

Jain, A.K., Deb, D. Engelsma, J.J., 2021. Biometrics: Trust, but Verify. ArXiv abs/2105.06625.

Jan, M. A., Zhang, W., Akbar, A., Song, H., Khan, R., & Chelloug, S. A. (2024). A hybrid mutual authentication approach for artificial intelligence of medical things. *IEEE Internet of Things Journal, 11*(1), 311–320. https://doi.org/10.1109/JIOT.2023.3317292

Jiang, Q., Zhang, N., Ni, J., Ma, J., Ma, X., & Choo, K. K. R. (2020). Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles. *IEEE Transactions on Vehicular Technology, 69*(9), 9390–9401.

Kang, J., Nyang, D. H., & Lee, K. H. (2014). Two-factor face authentication using matrix permutation transformation and a user password. *Information Sciences, 269*, 1–20.

Khan, I. A., Razzak, I., Pi, D., Khan, N., Hussain, Y., Li, B., & Kousar, T. (2024). Fed-inforce-fusion: A federated reinforcement-based fusion model for security and privacy protection of IoMT networks against cyber-attacks. *Information Fusion, 101*, Article 102002.

Kiljan, S., van Eekelen, M., & Vranken, H. (2018). Evaluation of transaction authentication methods for online banking. *Future Generation Computer Systems, 80*, 430–447.

Korać, D., Damjanović, B., & Simić, D. (2022a). A model of digital identity for better information security in e-learning systems. *The Journal of Supercomputing, 78*, 3325–3354. https://doi.org/10.1007/s11227-021-03981-4

Korać, D., Damjanović, B., Simić, D., & Choo, K. K. R. (2022b). A hybrid XSS attack (HYXSSA) based on fusion approach: Challenges, threats and implications in cybersecurity. *Journal of King Saud University - Computer and Information Sciences, 34*(10), 9284–9300. Part B.

Korać, D., & Simić, D. (2017). Design of fuzzy expert system for evaluation of contemporary user authentication methods intended for mobile devices. *Journal of Control Engineering and Applied Informatics, 19*(4), 93–100.

Korać, D., & Simić, D. (2019). Fishbone model and universal authentication framework for evaluation of multifactor authentication in mobile environment. *Computers & Security, 85*, 313–332.

Krichen, M., & Abdalzaher, M. S. (2024). Performance enhancement of artificial intelligence: A survey. *Journal of Network and Computer Applications, 232*, Article 104034.

Kumar, R., Khan, A. I., Abushark, Y. B., Alam, M. M., Agrawal, A., & Khan, R. A. (2020). An integrated approach of fuzzy logic, AHP and TOPSIS for estimating usable security of web applications. *IEEE Access, 8*, 50944–50957.

Li, Q., Li, Y., Zhang, S., Zhou, X., & Pan, Z. (2025). A theoretical framework for human-centered intelligent information services: A systematic review. *Information Processing & Management, 62*(1), Article 103891.
Liu, K., & Tao, D. (2022). The roles of trust, personalization, loss of privacy, and anthropomorphism in public acceptance of smart healthcare services. *Computers in Human Behavior, 127*, Article 107026.
Liu, Z., Qiu, H., Deveci, M., Pedrycz, W., & Siarry, P. (2025). Multi-view neutrosophic *c*-means clustering algorithms. *Expert Systems with Applications, 260*, Article 125454.
Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). *Handbook of fingerprint recognition* (Second Edition). London Limited: Springer-Verlag.
Mamdani, E., & Assilian, S. (1975). An experiment in linguistic synthesis with a fuzzy logic controller. *International Journal of Man-Machine Studies, 7*(1), 1–13.
Merhi, M., Hone, K., & Tarhini, A. (2019). A cross-cultural study of the intention to use mobile banking between Lebanese and British consumers: Extending UTAUT2 with security. *Privacy and Trust Technology in Society, 59*, Article 101151. https://doi.org/10.1016/j.techsoc.2019.101151
Mihajlov, M., Jerman-Blazic, B., & Josimovski, S. (2011). A conceptual framework for evaluating usable security in authentication mechanisms-usability perspectives. In *Proceedings of the 2011 5th International conference on network and system security* (pp. 332–336). NSS.
Mihajlov, M., Jerman-Blazic, B., & Josimovski, S. (2011a). Quantifying usability and security in authentication. In *Proceedings of the 2011 IEEE 35th annual computer software and applications conference* (pp. 626–629). COMPSAC.
Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I. 2012. Internet of things: Vision, applications and research challenges Ad Hoc networks, 10, 1497-1516.
Mishra, R. A., Kalla, A., Braeken, A., & Liyanage, M. (2021). Privacy protected blockchain based architecture and implementation for sharing of students' credentials. *Information Processing & Management, 58*(3), Article 102512.
Monrose, F., Reiter, M. K., & Wetzel, S. (2002). Password hardening based on keystroke dynamics. *International Journal of Information Security, 1*(2), 69–83.
Mundhe, P., Verma, S., & Venkatesan, S. (2021). A comprehensive survey on authentication and privacy-preserving schemes in VANETs. *Computer Science Review, 41*, Article 100411.
Muthusamy, D., & Rakkimuthu, P. (2022). Trilateral filterative hermitian feature transformed deep perceptive fuzzy neural network for finger vein verification. *Expert Systems with Applications, 196*, Article 116678.
Ogbanufe, O., & Kim, D. J. (2018). Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment. *Decision Support systems, 106*, 1–14.
Parashar, A., Parashar, A., Shabaz, M., Gupta, D., Sahu, A. K., & Khan, M. A. (2024). Advancements in artificial intelligence for biometrics: A deep dive into model-based gait recognition techniques. *Engineering Applications of Artificial Intelligence, 130*, Article 107712.
Parcham, E., Mandami, N., Washington, A. N., & Arabnia, H. A. (2016). Facial expression recognition based on fuzzy networks. In *Proceedings of the 2016 international conference on computational science and computational intelligence (CSCI)* (pp. 829–835). https://doi.org/10.1109/CSCI.2016.0161
Patel, V. M., Chellappa, R., Chandra, D., & Barbello, B. (2016). Continuous user authentication on mobile devices: recent progress and remaining challenges. *IEEE Signal Processing Magazine, 33*(4), 49–61.
Pawlak, M., & Poniszewska-Marańda, A. (2021). Trends in blockchain-based electronic voting systems. *Information Processing and Management, 58*(4), Article 102745.
Pu, C., & Li, Y. (2020). Lightweight authentication protocol for unmanned aerial vehicles using physical unclonable function and chaotic system. In *Proceedings of the 2020 IEEE international symposium on local and metropolitan area networks* (pp. 1–6). LANMAN.
Pu, C., Wall, A., Choo, K. K. R., Ahmed, I., & Lim, S. (2022). A lightweight and privacy-preserving mutual authentication and key agreement protocol for internet of drones environment. *IEEE Internet of Things Journal, 9*(12), 9918–9933, 15 June15.
Qin, Z., Huang, G., Xiong, H., Qin, Z., & Choo, K. K. R. (2021). A fuzzy authentication system based on neural network learning and extreme value statistics. *IEEE Transactions on Fuzzy Systems, 29*(3), 549–559. https://doi.org/10.1109/TFUZZ.2019.2956896
Rahman, M. S., Khalil, I., Yi, X., Atiquzzaman, M., & Bertino, E. (2021). A lossless data-hiding based IoT data authenticity model in edge-AI for connected living. *ACM Transactions on Internet Technology, 22*(3), 1–25.
Rathgeb, C., Gomez-Barrero, M., Busch, C., Galbally, J., Fierrez, J., 2015. Towards cancelable multi-biometrics based on bloom filters: a case study on feature level fusion of face and iris, 3rd international workshop on biometrics and forensics (IWBF 2015), pp. 1-6, 10.1109/IWBF.2015.7110225.
Rathore, S., Sharma, P. K., Loia, V., Jeong, Y. S., & Park, J. H. (2017). Social network security: Issues, challenges, threats, and solutions. *Information Science, 421*, 43–69.
Renaud, K. (2004). Quantifying the quality of web authentication mechanisms: A usability perspective. *Journal of Web Engineering, 3*(2), 95–123.
Shabbir, M., Ahmad, F., Shabbir, A., & Alanazi, S. A. (2022). Cognitively managed multi-level authentication for security using fuzzy logic based quantum key distribution. *Journal of King Saud University – Computer and Information Sciences, 34*(4), 1468–1485.
Shao, Z., Zhang, L., Brown, S. A., & Zhao, T. (2022). Understanding users' trust transfer mechanism in a blockchain-enabled platform: A mixed methods study. *Decision Support Systems, 155*, Article 113716.
Sharma, V., You, I., Andersson, K., Palmieri, F., Rehmani, M. H., & Lim, J. (2020). *Security, privacy and trust for smart mobile- Internet of Things (M-IoT): A survey, 8* pp. 167123–167163). IEEE Access.
Sharma, V., You, I., Jayakody, D. N. K., & Atiquzzaman, M. (2019). Cooperative trust relaying and privacy preservation via edge-crowdsourcing in social Internet of Things. *Future Generation Computer Systems, 92*, 758–776.
Shin, D. H. (2010). The effects of trust, security and privacy in social networking: a security-based approach to understand the pattern of adoption. *Interacting with Computers, 22*(5), 428–438.
Soleymani, S. A., Goudarzi, S., Anisi, M. H., Zareei, M., Abdullah, A. H., & Kama, N. (2021). A security and privacy scheme based on node and message authentication and trust in fog-enabled VANET. *Vehicular Communications, 29*, Article 100335.
Stylios, I., Kokolakis, S., Thanou, O., & Chatzis, S. (2021). Behavioral biometrics & continuous user authentication on mobile devices: A survey. *Information Fusion, 66*, 76–99.
Sun, L., Li, H., & Muhammad, G. (2024). Randomized attention and dual-path system for electrocardiogram identity recognition. *Engineering Applications of Artificial Intelligence, 132*, Article 107883.
Tawalbeh, L. A., & Saldamli, G. (2021). Reconsidering big data security and privacy in cloud and mobile cloud systems. *Journal of King Saud University Computer and Information Sciences, 33*(7), 810–819.
Teh, P. S., Zhang, N., Tan, S. Y., et al. (2020). Strengthen user authentication on mobile devices by using user's touch dynamics pattern. *Journal of Ambient Intelligence and Humanized Computing, 11*, 4019–4039.
Tewari, A., Gupta, B., 2020. Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework future generation computer systems, 108 909-920.
Tian, E., Wang, Z., Zou, L., & Yue, D. (2019). Chance-constrained H∞ control for a class of time-varying systems with stochastic nonlinearities: The finite-horizon case. *Automatica, 107*, 296–305.
Tresadern, P., Cootes, T. F., Poh, N., Matejka, P., Hadid, A., Levy, C., … Marcel, S. (2013). Mobile biometrics: combined face and voice verification for a mobile platform. *IEEE Pervasive Computation, 12*(1), 79–87.
Wang, C., Zhou, T., Ma, M., Xiong, Y., Zhang, X., & Liu, C. (2024). An efficient certificateless blockchain-enabled authentication scheme to secure producer mobility in named data networks. *Journal of Network and Computer Applications, 232*, Article 104007. Journal of Network and Computer Applications, 232, 104007.
Wang, P., & Ding, H. (2024). Information fusion and artificial intelligence for smart healthcare: a bibliometric study. *Information Processing & Management, 61*(4), Article 103732.
Wang, Q., & Wang, D. (2023). Understanding failures in security proofs of multi-factor authentication for mobile devices. *IEEE Transactions on Information Forensics and Security, 18*, 597–612.
Wang, S., Hu, X. Z., Liu, Y. Y., Tao, N. P., Lu, Y., Wang, X. C., Lam, W., Lin, L., & Xu, C. H. (2022). Direct authentication and composition quantitation of red wines based on Tri-step infrared spectroscopy and multivariate data fusion. *Food Chemistry, 372*, Article 131259.
Wazzeh, M., Arafeh, M., Sami, H., Ould-Slimane, H., Talhi, C., Mourad, A., & Otrok, H. (2024). CRSFL: Cluster-based resource-aware split federated learning for continuous authentication. *Journal of Network and Computer Applications, 231*, Article 103987.

Wu, D., Si, S., Wu, S., & Wang, R. (2018). Dynamic trust relationships aware data privacy protection in mobile crowd-sensing. *IEEE Internet of Things Journal, 5*(4), 2958–2970.

Xiao, Z., Xia, S., Gong, K., & Li, D. (2012). The trapezoidal fuzzy soft set and its application in MCDM. *Applied Mathematical Modelling, 36*(12), 5844–5855.

Yamada, A., & Ikeda, T. (2017). Enhanced PKI authentication with trusted product at claimant. *Computers & Security, 67*, 324–334.

Yang, T., Li, Y. J., Qian, Y., & Wang, F. Y. (2023). Consistent matrix: A feature selection framework for large-scale datasets. *IEEE Transactions on Fuzzy Systems, 31*(11), 4024–4038.

Yi, J., Li, J., & Yang, C. (2023). Adaptive fuzzy prescribed-time connectivity-preserving consensus of stochastic nonstrict-feedback switched multiagent systems. *IEEE Transactions on Fuzzy Systems, 31*(10), 3346–3357. https://doi.org/10.1109/TFUZZ.2023.3252601. Oct.

Zhang, J., Luximon, Y., & Li, Q. (2022). Seeking medical advice in mobile applications: How social cue design and privacy concerns influence trust and behavioral intention in impersonal patient-physician interactions. *Computers in Human Behavior, 130*, Article 107178.

Zhang, R., Zhang, L., Choo, K. K. R., & Chen, T. (2023). Dynamic authenticated asymmetric group key agreement with sender non-repudiation and privacy for group-oriented applications. *IEEE Transactions on Dependable and Secure Computing, 20*(1), 492–505.

Zhang, Z., Ning, H., Farha, F., Ding, J., & Choo, K. K. R. (2024). Artificial intelligence in physiological characteristics recognition for internet of things authentication. *Digital Communications and Networks, 10*(3), 740–755.

Zhou, L., Wang, K., Lai, J., & Zhang, D. (2023). A comparison of a touch-gesture- and a keystroke-based password method: Toward shoulder-surfing resistant mobile user authentication. *IEEE Transactions on Human-Machine Systems, 53*(2), 303–314. https://doi.org/10.1109/THMS.2023.3236328

Zhou, L., Zhang, C., Qiu, Z., & He, Y. (2020). Information fusion of emerging non-destructive analytical techniques for food quality authentication: A survey. *TrAC Trends in Analytical Chemistry, 127*, Article 115901.

Zhou, Z., Liu, Y., Zhu, X., Zhang, S., & Liu, Z. (2025). Privacy-preserving cancelable multi-biometrics for identity information management. *Information Processing & Management, 62*(1), Article 103869.