Computers & Industrial Engineering 168 (2022) 108119

Contents lists available at ScienceDirect

Computers & Industrial Engineering

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

GTM approach towards engineering a features-oriented evaluation framework for secure authentication in IIoT environment

Yasir Ali [a,c], Habib Ullah Khan [b,*]

[a] Department of Computer Science, University of Swabi, KP, Pakistan
[b] Accounting and Information, College of Business and Economics, Qatar University, Doha, Qatar
[c] Government Degree College Yar Hussain Swabi, KP, Pakistan

ARTICLE INFO

Keywords:
Authentication
IIoT assessment framework
Authentication features
Graph Theory Matrix Approach

ABSTRACT

Industry Internet of Things (IIoT) has become the most evolving area over the last few years. The number of IoT devices connected in industry has sharply elevated but this surge has led to the vulnerability and data breach such as if a malicious entry is made to the secure network, it will forfeit all the network resources. For this purpose a full pledged secure authentication method is essential to safeguard IIoT network. There is a bulky list of number of authentications protocols available to keep network safe with a variety of features so but it becomes herculean task for network administrator to pick the strong and secure authentication method due to huge number of criteria, conflicting objectives and availability of authentication protocols in industry environment. It has become imperative to get the most rational authentication method in devices operating in IIoT. To address this issue, a feature-oriented assessment framework is put forward to provide a ground for ranking and selection of best authentication mechanism. This framework uses a mathematic approach known as Graph Theory Matrix Approach (GTMA) and selects the best authentication method based on the number of features. These features are related to authentication and covers almost every aspect of authentication method and are used as benchmark for selection purposes. This framework takes into account the most important features and helps in selecting the best and most ideal features-oriented authentication method that can be employed in IIoT to keep the integrity and security of connected devices and overall network infrastructure.

1. Introduction

IoT devices are covering almost every sphere of human's life such as healthcare, transportation, supply chain management, quality assurance, energy management, retailing and agriculture (Boyes, Hallaq, Cunningham, & Watson, 2018; Chaudhary, Aujla, Garg, Kumar, & Rodrigues, 2018; Suresh, Nandagopal, Raj, Neeba, & Lin, 2020). But, still are some security challenges in the deployment of IoT devices. For example the existing communication methods are not equipped with security due to the conventional architecture of TCP/IP network (Chaudhary et al., 2018). Similarly, the introduction of IoT devices made significant revolution in the operating procedure, manufacturing, quality enhancement and productivity of IIoT domain but still some security issues must be taken into account before the deployment of IoT devices. The effects of threats in IIoT can be more severe and jeopardized due the sensitive nature of data and network. There are several other security issues such as inadequate authentication practices, port exposures and obsolete application invite many risks (T. Micro). Similarly, physical access to controlling system known as industrial control system (ICS) or manufacturing bolt will not lead to products failure and physical damage but can also risk human's life. IoT device authentication, device identity validation and integrity of data have become serious concern in the industries. Its impact becomes more lethal in case of manufacturing industries like steel, petrol and chemical due to high temperature and unstable chemicals where any leakage of data through sending false commands to endpoints and cyber-attack can lead to the disastrous situations. This disastrous situations include the loss of life, causing injuries and even halting of the system. Improper and poor authentication mechanism employed in the industrial environment will create these problems (Thales).

There are multiple reasons for the unavailability of strong authentication mechanism in manufacturing industries such as the communication protocols do not go under authentication process. For example Modbus is one of the most commonly communication protocols used for

* Corresponding author.
E-mail addresses: yasiuop007@gmail.com (Y. Ali), Habib.khan@qu.edu.qa (H. Ullah Khan).

https://doi.org/10.1016/j.cie.2022.108119
Received 16 June 2021; Received in revised form 15 March 2022; Accepted 20 March 2022
Available online 24 March 2022

as industrial automation solution lacks any kind of authentication. This lack of authenticity leads to integrity issues in communication. Similarly, the current equipments in manufacturing industries have been installed ten to twenty (10 to 20) years back and they are not designed with enough computation and security abilities like cryptographic authentication in mind. The industries especially manufacturing require low latency to complete all the operations of critical processes in real time fashion. Sometimes, the manufacturing team and engineers feel intimidating and becomes reluctant to implement such a security methods of authentication that suffer from latency. Other security concerns are related to number and nature of IoT devices deployed in IIoT domain. As, a huge amount of data is sent to the cloud for decision making from IoT or edge devices in IIoT environment. This data is used by various applications and operating systems residing in these devices. Attackers can compromise the security of network as the IoT devices are not equipped with major security in mind and physical access to these devices is more easily possible. Therefore, every device must be authenticated before joining an IIoT network.

Aauthentication is a procedure through which a user or computer will have to prove its identity to server or client (Donegan, 2019). Hence, IoT devices or equipments are required to be authenticated prior to connecting them to the network (Gatto; Sadeghi, Wachsmann, & Waidner, 2015). This can be only achieved by selecting efficient and robust authentication method or scheme. Over the last few years, many authentication schemes have been introduced to provide a full-pledged access control mechanisms to the IIoT network and preventing the illegal to protect the network resources and infrastructure. The design of the authentication scheme must be efficient and secure and error-prone (Gollmann, 1996). The efficiency and security of authentication schemes employed for IIoT devices can be characterized or measured by the authentication features. In this context, the proposed features-oriented evaluation framework is presented to check the design and functionalities of different authentication schemes with respect to the features. These features are used as benchmark in proposed evaluation framework for selecting the best authentication approach that can be employed for IoT devices in the industrial environment. These features include session key agreement, password change, access control, confidentiality, integrity, availability, scalability, known key secrecy, privacy, efficient wrong password, data freshness, secure functions etc. The security features are not only important for any connectivity based system but they are also known as building blocks of connected systems. Similarly, the importance of these features can be judged by the fact that the internet data security is defined by three major features known as availability, privacy and integrity (Hamidi, 2019; Kanjee, Divi, & Liu, 2010).

The authentication features have significant role in evaluating the authentication mechanisms employed in any IoT-based system. Due to huge number of authentication protocols, conflicting criteria and huge list of features supported by the schemes, it becomes a challenging task for network administrator and developers to select the best choice of security or authentication scheme for manufacturing industry. This is due to the reason that the people working in industry environment have less technical skills and knowledge about security deployment. Thus, there is a strong need of designing an evaluation framework that can be applied to evaluate the existing authentication solutions to provide timely solutions to the authentication challenges. Therefore, we present a proposed evaluation framework will enable them to get the best authentication method based on their features for the security demands. This proposed features-oriented evaluation framework is preliminarily designed to assess and assign quantification score for ranking of the authentication mechanisms by using Graph Theory Matrix (GTM) approach that can be applied for authentication purposes in IIoT based system. GTM approach is decision making and qualitative procedure that makes decision based on decision variables. It can be applied for analysis and evaluation due to its logical and systematic nature (Geetha & Sekar, 2017). This model involves three major components such as graph representation, matrix building and permanent index representation. Digraph representation has advantage of visual analysis and modelling. Matrix representation is also helpful in analysis and mathematical modelling and computer processing (Attri, Dev, & Sharma, 2013). The proposed evaluation model produces the most promising results and is applicable in IIoT environment to fulfil the security gaps.

1.1. Motivation

The major motivations behind the proposed research work are given below as.

- We did not find any significant evaluation framework that is intended to provide solution towards the authentication issues in the industrial environment. A benchmark for assessment and ranking of authentication schemes in industrial environment is imperative to be introduced to strengthen the security of industrial applications.
- The existing works in literature are more focusing on methods such as AHP and TOPSIS techniques for the security assessment. There is need of application of a new technique to provide a decision support system or evaluation framework for assessment of authentication schemes in IIoT.
- The IoT devices operating in industrial environment require a serious security attention due to the existence of legacy technologies and nature of data. The list of authentication schemes available need to be thoroughly investigated before implementing them as authentication security solution. A resilient and ubiquitous authentication method is imperative. The proposed framework provides an ideal platform for implementing the most rational procedure/scheme for authentication of IoT-based industrial system.
- The IoT network managers find it hard to get the most secure and absolute authentication scheme due to the array of authentication schemes available. Picking the right security solution without proper knowledge and understanding become complex and daunting task. There is need of assessment model in this domain to provide a guideline to the network managers to tackle this situation.
- The features and functionalities of authentication schemes are rapidly evolving so the need of feature based evaluation framework will help the decision makers to select the right security option based on the most essential security features in industrial field.

This draft is divided into four remaining sections such as the contribution of proposed work in comparison to literature work is given in in section (2). Section (3) is related to discussing the designing benchmark and proposed evaluation framework procedure. Section (4) describes the results and discussion of the proposed model. Section (5) discusses the managerial implication of proposed work and finally section (6) concludes this research by giving the final thoughts.

2. Contribution based on literature study

According to our literature study, we failed to identify any evaluation framework that is intended for the evaluation and selection of right secure authentication in industrial environment. Although, there exist many works in other domains focusing on addressing the selection issues related to authentication schemes. This is first attempt to present such an evaluation framework for secure authentication in IIoT. We also failed to find any evaluation framework based on same selected criteria features, application methods and scenario in industrial environment. But, still we are going to discuss and compare our proposed evaluation framework with the similar works in other application areas. According to our literature study, many evaluation models are using Analytic Hierarchy Process (AHP), Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS), Analytic Network Process (ANP) method or DEMATEL method for the purpose of evaluating the authentication schemes in different areas. First, we are highlighting these studies then we will

discuss the existing limitations in the proposed approaches. Finally, we will compare the existing studies with our proposed features-oriented evaluation model to provide reasonable solutions towards the existing shortcomings in the literature work.

The work presented by Kumar (Kumar et al., 2020) is focused on building evaluation framework based on using Fuzzy logic, AHP and TOPSIS methods to address the usable security for web applications. They focused on the usable security features for web based applications evaluation. Similarly, the work presented by Kaur et al (Kaur, Singh, & Kumar, 2018) work is similar to our study but it is targeted towards detecting security breaches in social networks. They also used AHP-TOPSIS selection techniques for assigning weights to the features. Johnson et al (Johnson, Isaksson, Fiedler, & Wu, 2006) only applied AHP method to build a decision making model to determine the authentication level based on six (6) features such as threat level, resources, position, content, throughput and user's assessment based on two (2) authentication alternatives. The study conducted by Zhang et al (Zhang, Deng, Wei, & Deng, 2012) is also presenting a decision making model to assess the security of E-commerce. They also applied the AHP technique for evaluation and decision making. Mayer et al (Mayer, Neumann, Storck, & Volkamer, 2016; Mayer, Neumann, & Volkamer, 2016) also put forward their decision making model based on using AHP method for feasibility analysis. They adopted AHP method to the ACCESS (Authentication ChoiCE Support System) framework already suggested by Renaud et al (Renaud, Volkamer, & Maguire, 2014). AHP method along with the support of fuzzy set approach is also applied by Liu et al (Liu, Wang, Peng, & Shyu, 2015) for the evaluation of biometric technologies. They classified features into three main different categories such as technology assessment, biometric competence and biometric key elements. Han et al (Han, Li, Huang, & Feng, 2018) also developed an end-to-end security assessment framework based on Software Defined Network (SDN) for the evaluating the security levels for the CloudIoT offerings. AHP method is applied in the context of decision making and ranking purposes. They used twenty three (23) security feature as evaluation criteria in their proposed assessment model. Sari et al (Sari, Ratnasari, & Prasetio, 2016) conducted a survey based on a questionnaire to evaluate the authentication of smartphone by focusing on the user preferences. They only performed descriptive analysis. The major limitation of this work is that the quantitative assessment is missing and they did not apply any decision making method in their evaluation. Another similar study is also conducted by Eliasson et al (Eliasson, Fiedler, & Jørstad, 2009) to evaluate the authentication schemes theoretically by conducting survey based on questioning and answering technique. Park et al (Park & Shin, 2017) conducted study that is using DEMATEL and Analytic Network Process (ANP) methods for the evaluation. They have designed good criteria by selecting the most pertinent security features but the proposed model is built to take into account the generic security capabilities.

According to the literature, it has been observed that all the decision support systems or evaluation models are based on applying the AHP or TOPSIS approaches. But, these multi criteria decision making methods as AHP and ANP are applicable only when the features are independent of each other. Furthermore, according to the recent study conducted by Munier et al (Munier & Hontoria, 2021), AHP method is not ideal for complex projects, where the large number of criteria and sub-criteria are involved. These methods are also failing to provide visualization among the interrelationship of the features. It is also noticed that previously similar proposed frameworks require a sensitivity analysis and validation.

To address the limitations in the previously presented approaches or models, we present an evaluation framework for secure authentication in industrial environment. The proposed evaluation model is based on multi-methods such as the feature extraction, analysis and categorization is achieved by the Delphi method. This is first attempt to perform the feature analysis based on a systematic approach. Our evaluation criteria of features is focusing on sheer security aspects of IoT devices in industrial environment. It is covering the most essential and core features related to the authentication security. For evaluation and decision making GTM approach is adopted in IIoT field. Similarly, the proposed framework is also verified and tested by Simple Additive method (SAW) method and performance evaluation parameters like accuracy, precision and recall after conducting a systematic field study. The existing models are based on using traditional methods for authentication assessment but the application of GTM approach is new concept for building a decision making model and it is first attempt to apply it for the secure authentication evaluation. Our proposed model also supports both hierarchical and visualization among the attributes. It is based on mathematical and logical operation for analysing, evaluating and decision making (Geetha & Sekar, 2017). Our proposed authentication evaluation model is tested to check the effectiveness of the results and its practicality is judged by a systematic case study scenario. We hope this decision making model will be able to address all the decision making issues related to the selection of most apposite authentication solution in industrial environment for the decision makers, security designers, IIoT managers and industrial organizations. The complete detail of our proposed evaluation model in comparison to previously suggested approaches in terms of method, features and contribution is given in Table 1.

3. Features-oriented evaluation framework

A features-oriented evaluation framework is presented to provide a secure authentication solution based on the features collected from literature. Features are used as benchmark for selection the authentication solution in IIoT environment. The proposed framework completes in two phases. In first phase, the features related to authentication are identified and in second phase GTM approach is applied on features after selecting the high ranked authentication alternative. The detail of designing features based evaluation framework for secure authentication in industrial IoT based system is given below as.

3.1. Benchmarking

The proposed framework is based on building a criteria that can be used as benchmark for selecting the strong authentication solution to address the security issues in industrial environment. For this purpose, features focusing upon identification and access control problems are identified with intentions to allow only the legitimate devices in IIoT network. The main reason of choosing the security features is as they cover all aspects related to authentication. All features about authentications are collected from different sources. A comprehensive and rigours literature review is conducted to identify and collection authentication features for IoT devices. These features are the most common as they are used by many authentication mechanisms. Initially, 97 features are identified from different sources then after removing duplicates, only nine (9) features are selected for evaluation and decision making for different alternatives. The detail of all features selected from literature study is given in Fig. 1. All features are discussed below as.

- **Mutual authentication (C_1)**
  Mutual authentication is the procedure of verifying the identities of two entities to each other in communication. A well-designed and strong mutual authentication is imperative to avoid the man-in-the-middle attacks in IIoT environment. Mutual authentication also maintains data integrity and confidentiality. This feature is available in a lot of literature (Deebak & Al-Turjman, 2020; Kumar, Lee, & Lee, 2012; Le, Khalid, Sankar, & Lee, 2011; Mehmood, Natgunanathan, Xiang, Poston, & Zhang, 2018; Tahir, Sardaraz, Muhammad, & Saud Khan, 2020; Verma & Bhardwaj, 2020).
- **Non-repudiation (C_2)**

Table 1
Comparison of proposed evaluation framework with existing related models.

Ref	Method/Approach	Evaluation Features	Contribution
Kumar (Kumar et al., 2020)	Fuzzy logic AHP and TOPSIS integrated method	Confidentiality, Authentication, Durability, Accountability, Integrity, Recognisability, Operationability etc.	Authors addressed the usable-security of web applications
Kaur et al (Kaur et al., 2018)	AHP-TOPSIS approach	Textual features Content-specific Non-textual features, Content-free features	Profile based technique of features selection for each user in online social networking
Johnson et al (Johnson et al., 2006)	AHP technique	Threat level, Resources, Position, Content, Throughput and User's assessment	They evaluated the authentication by selecting two authentication alternatives
Zhang et al (Zhang et al., 2012)	AHP and Dempster–Shafer (DS) theory approach	Technical features, environmental features and managerial security features	A model is presented to calculate the degree of security of E-commerce
Mayer et al (Mayer et al., 2016; Mayer et al., 2016)	AHP model for realization of ACCESS model	Risk mitigation, Quality in use, User context and Business context	The major contribution to the realization of model suggested (by Renaud et al) feasibility analysis to understand about all the authentication alternatives based on ranking.
Liu et al (Liu et al., 2015)	Fuzzy AHP with set theory	Technology assessment, Biometric competence and Biometric key elements	This approach evaluates the biometric technologies based on multi criteria
Han et al (Han et al., 2018)	AHP method	Secure booting, Firewall and IPS, Device hardware physical security, Authentication,	Authors developed and end-to-end security assessment framework based on Software Defined Network (SDN) for the evaluating the security level for the CloudIoT offering
Sari et al (Sari et al., 2016)	Survey based descriptive analysis	Security and Convenience	This study conducted a survey to know about the authentication methods based on user's preferences.
Eliasson et al (Eliasson et al., 2009)	SWOT analysis method	Security, User-friendliness, Simplicity, Usability, Awareness and Algorithm	Evaluating authentication schemes in IP Multimedia Subsystem (IMS) by discussing their strengths, weaknesses, opportunities and threats
Park et al (Park & Shin, 2017)	Fuzzy DEMATEL and fuzzy AN	Authentication, Integrity, Availability, Confidentiality, Access control, Trust, Auditing, Privacy, Non-repudiation, Replay attack, Anonymity, Privacy, and Fault tolerance	An assessment model is presented for the security assessment of IoT services.
Mihajlov et al (Mihajlov, Jerman-Blazič, & Josimovski, 2011)	Conceptual framework	Secrecy, Abundance, Revelation, Privacy and Breakability	Authors presented a theoretical framework to assess the usable security in authentication schemes
Sharma et al (Sharma & Kaul, 2018)	Hybrid Fuzzy AHP and TOPSIS	Vehicle Velocity, Social Contact, Integrity, Vehicle Capability, Transmission Range, Direction, PDR, Past CH duration history	The proposed work is intended to select the cluster head in Vehicular Ad-hoc Network (VANET)
Khan et al (Khan, Atwater, & Hengartner, 2014)	Comparative evaluation of implicit authentication(IA) schemes	Accuracy, training time, detection delay, processing and memory complexity.	Authors evaluated six (6) IA authentication schemes based on comparing evaluation parameters.
Forget et al (Forget, Chiasson, & Biddle, 2015)	User-centred Feature authentication framework	Persuasion, memory, input and output and obfuscation	The proposed framework is applied to select the most viable features for authentication schemes for different applications.
Alaca et al (Alaca, Abdou, & Van Oorschot, 2019)	Framework for evaluating mimicry-resistant	Usability, Deployability and Security	The framework is intended to provide usability and security properties related to web authentication schemes.
Korać et al (Korać & Simić, 2019)	Fishbone model for multi factor authentication	Security, usability, complexity, accessibility, privacy, pricing and convenience.	This framework uses fuzzy methodology to evaluate the multi factor authentications
Wiefling et al (Wiefling, Patil, Dürmuth, & Iacono, 2020)	Evaluation model for risk-based authentication methods	Devices, Time, Perception (feelings), Authentication duration	This model evaluates the password based authentication methods based on monitoring the extra features.
Proposed work	Features-oriented evaluation framework using GTM approach with the support of Delphi and SAW	Mutual authentication, Non-repudiation, Key agreement, Known attacks, Password change Forward security, Scalability, Usability or user-friendliness and Authorization	The proposed framework evaluates the authentication schemes based on authentication features by using GTM approach in industrial domain. A feature analysis is conducted by using Delphi approach.

It is process through which the sender confirms his/her identity without denying its validity and authenticity. Non-repudiation is related to authenticity that authenticity can be achieved without non-repudiation but reverse is not true. It is the important property as SSL and TCL protocols guarantee that client is talking to the server but there is lack of session recording mechanism and authentication has be the part of the mix but not overall of it (FInjan, 2017). It also important feature based on our literature study (Deebak & Al-Turjman, 2020; Kumar & Gandhi, 2020; Park & Shin, 2017; Shakil, Zareen, Alam, & Jabin, 2020).

- **Key agreement (C_3)**
  Key agreement is procedure in which two or more parties agree on using same key for secure communication. It is used for achieving implicit authentication. It allows parties to securely communicate with each other. Key agreement is related with authentication in a sense that modern authentication protocols such as authenticated key agreement protocol (AKAP) (Kilciauskas, Butkus, & Sakalauskas, 2020) uses it for stronger security and sensitive data transmission. Keywords, key size and number of rounds and session key are also important considerations in key agreement (Kumar, Jangirala, & Ahmad, 2018; Sree).
- **Known attacks (C_4)**
  For any authentication scheme, it is necessary to know about the attack and to avoid that authentication method or to make useless the attack. If an authentication has known attack and not providing any solution then the security will be compromised (Eliasson et al., 2009). This feature is also used by different authors (Kumar et al., 2012; Kumari et al., 2020).
- **Password change (C_5)**
  Password change becomes more important especially in password-based authentication methods (Siddiqui, Abdullah, Khan, & Alghamdi, 2014). The client should be able to change the old credential in case of security breaches occur.

- **Forward security (C_6)**
  This feature is also known as forward secrecy and has become important feature of specific key exchange and authentication protocols. The forward security in context of authentication that any adversary or opponent who compromises the communication party now should not be allowed to write a message that was at earlier time (Boyd & Gellert, 2021). The latest authentication protocols and approaches are based on forward security (Saleem, Shamshad, Ahmed, Ghaffar, & Mahmood, 2021; Yao, Wang, Gan, Lin, & Huang, 2021).
- **Scalability (C_7)**
  It is the ability of to produce the maximum number of key-block parallel to the maximum amount of supported IoT devices (El Mouaatamid, Lahmer, & Belkasmi, 2020). The modern approaches or protocols related to authentication are emphasizing on scalability and efficiency (Wu, Dai, & Wang, 2020; Xu, Zeng, Yang, & Shao, 2020).
- **Usability or user-friendliness (C_8)**
  Usability is defined as the ability of authentication scheme and how it is acting. It is also important parameter in our selected list of features. The usability of authentication scheme is measured by user-friendliness, efficiency and effectiveness (Eliasson et al., 2009).
- **Authorization (C_9)**
  Authorization is related to determine the access of client access the network resources or files. It is normally coupled with authentication so server understands the identity of clients who are going to request the access for particular data or network resources (Haghparast, Berehlia, Akbari, & Sayadi, 2020; Park & Shin, 2017; Tahir et al., 2020).

3.2. Evaluation method

The proposed evaluation framework applies GTM approach for evaluation, ranking and decision making based on the features. This framework identifies the best authentication solution after the application of mathematical procedure to produce the empirical proof. The main idea is to remove the biasness and subjectivity. After finalizing the list of features, we selected four Information Technology (IT) security experts in the field of cyber security. They provided answers to the questions related to the importance of features in authentication procedure. Delphi method is used to obtain the data related to the features in designing criteria for selection of proper target authentication solution. It is the most appropriate method in selecting experts and collection of data related to particular study (Okoli & Pawlowski, 2004). The stepwise detail of the application of Delphi method in context of our research is given in Fig. 2. GTM method is applied after collection of data related to features from cyber security experts.

There are three important steps involved in this method such as digraph building, matrix creation and calculating permanent function and index. This approach consists of the following phases after identifying the criteria and alternatives (Geetha & Sekar, 2017; Geetha, 2016).

i. Diagraph representation

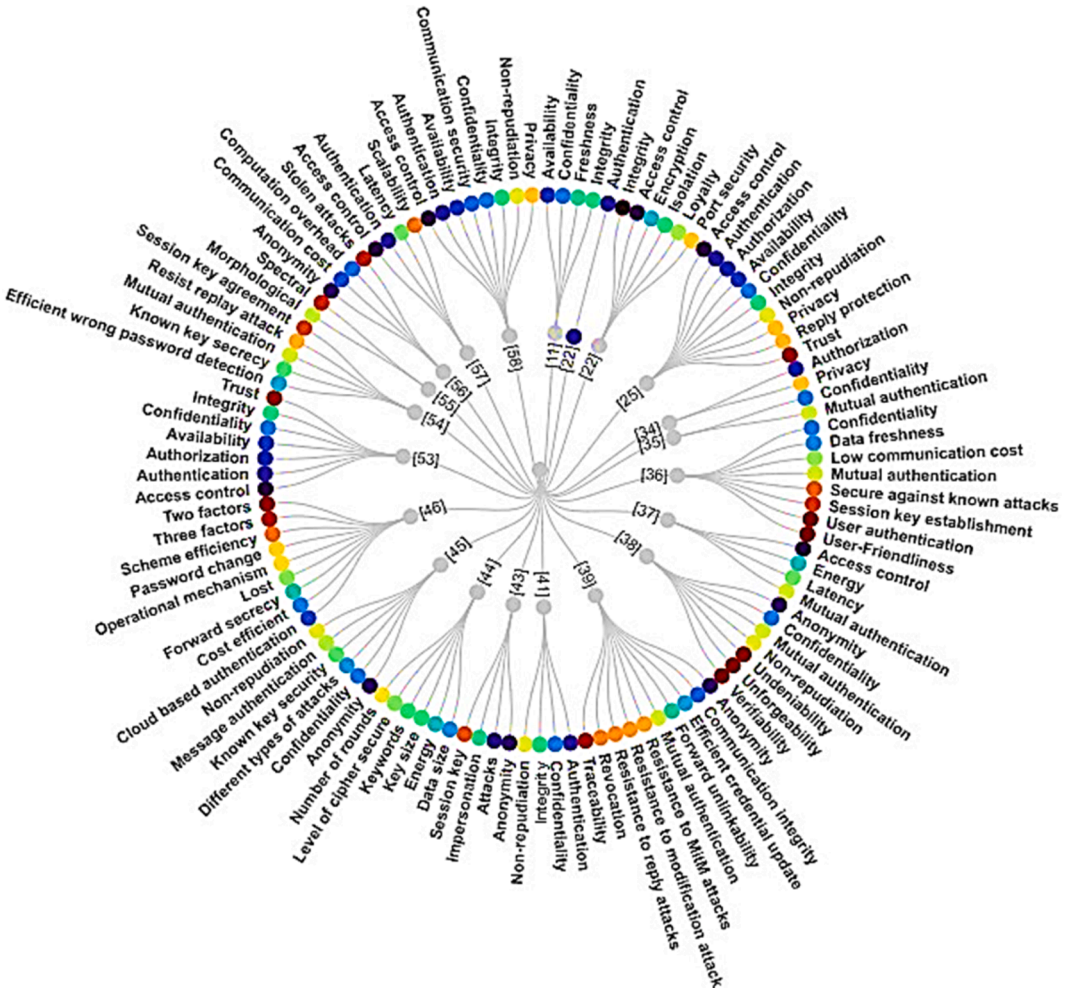

Fig. 1. List of all features.

Digraph model representation has proved to be useful in modelling and analysing various kinds of systems in fields of science and technology. A digraph is also a graph but with directed edges. The nodes are connected with each other through edges. A digraph is consisted of set of nodes and edges.

Definition: A digraph is an ordered pairs of set "G" and it can be given mathematically as:

$$G = (V, E) \tag{1}$$

"V" is set of vertices or nodes and "E" is set of edges or arcs. The set of nodes and edges are given below mathematically as in equation (2).

$$V = \{v_i\} \text{where} i = 1, 2, 3 \cdots . \text{and} E = \{E_{ij}\} \tag{2}$$

ii. Matrix representation

The matrix representation of performance attributes digraph gives a detailed picture of one-to-one representation. The matrix approach is useful in analysing the digraph expeditiously to derive the system function. A matrix called as performance attributes matrix (B) is defined, which is M × M matrix and considers all of the attributes (Bi) and their relative importance. Performance attributes matrix (B) is shown in Eq. (3).

$$B = \begin{bmatrix} B_1 & b_{12} & b_{13} & b_{14} & b_{15} & b_{16} & b_{17} & b_{17} & b_{18} \\ b_{21} & B_2 & b_{23} & b_{24} & b_{25} & b_{26} & b_{27} & b_{28} & b_{29} \\ b_{31} & b_{32} & B_3 & b_{34} & b_{35} & b_{36} & b_{37} & b_{38} & b_{39} \\ b_{41} & b_{42} & b_{43} & B_4 & b_{45} & b_{46} & b_{47} & b_{48} & b_{49} \\ b_{51} & b_{52} & b_{53} & b_{54} & B_5 & b_{56} & b_{57} & b_{58} & b_{59} \\ b_{61} & b_{62} & b_{63} & b_{64} & b_{65} & B_6 & b_{67} & b_{68} & b_{69} \\ b_{71} & b_{72} & b_{73} & b_{74} & b_{75} & b_{76} & B_7 & b_{78} & b_{79} \\ b_{81} & b_{82} & b_{83} & b_{84} & b_{85} & b_{86} & b_{87} & B_8 & b_{89} \\ b_{91} & b_{92} & b_{93} & b_{94} & b_{95} & b_{96} & b_{97} & b_{98} & B_9 \end{bmatrix} \cdots \tag{3}$$

iii. Permanent function and permanent index

The permanent function is a standard matrix function and has applications in combinatorial mathematics. The procedure for calculating permanent function is similar as finding its determinant but with positive signs. The positive signature of permutation will lead to no loss of information and better appreciation. The mathematical form for calculating permanent of the matrix A is obtained by Eq. (4).

The relative importance of attributes is helpful in finding the performance index of attributes. For instance the relative importance (a_{ij}) can be assigned by using a scale ranging from 0 and 1. The value of a_{ji} is calculated by using Eq. (5). The detail of finding relative importance of attributes is given in Table 2 (Geetha & Sekar, 2017).

$$a_{ji} = \frac{1}{aij} or 1 - a_{ij} \tag{5}$$

GTM approach starts from identifying attributes and alternatives, followed by graph representation of attributes and then attributes are represented in matrix form. Permanent index is calculated for ranking of alternatives based on the attributes. The stepwise detail of GTM approach for decision making and assessment in hierarchical fashion is given visually in Fig. 3.

3.3. GTM approach application

GTM approach is applied as evaluation tool and decision making option regarding the selection of best target solution for authentication in IIoT based system. After the collecting data from the cyber security experts and categorization of authentication features by using Delphi method as previously discussed. The proposed evaluation framework is composed of three major phases: In first phase, the features are provided as input to the evaluation model. In second phase, the processing is done by using mathematical calculations to find out permanent index of features for the alternatives. In last phase, ranking is done after empirical proofs and best alternative as target authentication solution selected based on the values assigned to the features. The visual representation of proposed evaluation framework based on the application of GTM approach for assessment and ranking of target solution for authentication is given in Fig. 4. The complete detail of GTM is given below as.

i. **Identifying features and alternatives**

In first step of the proposed evaluation framework, the main focus is to select attributes and alternatives. Data collected from security expert panel is written against ten alternatives such as from $A_1 \ldots A_{10}$. The alternatives will be evaluated with respect to features related to authentication in industrial IoT environment. Among the supposed alternatives, only that alternative will be selected as suitable alternative

$$\begin{aligned} Per(A) = & \prod_{i=1}^{M} D_i + \sum_{i=1}^{M-1} \sum_{j=i+1}^{M} .. \cdots \sum_{M=T+1}^{M} \left(d_{ij} d_{ji}\right) D_k D_l D_m D_n D_o \cdots D_t D_m + \sum_{i=1}^{M-2} \sum_{j=i+1}^{M-1} \\ & \times \sum_{k=j+1}^{M-1} \cdots . + \sum_{M=t+1}^{m} \left(d_{ij} d_{jk} d_{ki} + d_{ik} d_{kj} d_{ji}\right) D_k D_l D_m D_n D_o \cdots D_t D_m + \left[\begin{array}{l} \sum_{i=1}^{M-3} \sum_{j=i+1}^{M} \sum_{k=I+1}^{M-1} \sum_{l=i+2}^{M-1} \cdots . + \sum_{M=t+1}^{m} \left(d_{ij} d_{ji}\right)\left(d_{kl} d_{lk}\right) D_m D_n D_O \cdots \cdots . D_t D_m + \\ \sum_{i=1}^{M-3} \sum_{j=i+1}^{M-1} \sum_{k=i+1}^{M} \sum_{l=j+1}^{M} \cdots . + \sum_{M=t+1}^{m} \left(d_{ij} d_{jk} d_{kl} d_{li} + d_{il} d_{lk} d_{kj} d_{ji}\right) D_m D_n D_O \cdots \cdots . D_t D_m \end{array} \right] \\ & + \left[\sum_{i=1}^{M-2} \sum_{j=i+1}^{M-1} \sum_{k=j+1}^{M} \sum_{l=1}^{M-1} \sum_{m=l+1}^{M} .. + \sum_{M=t+1}^{m} \left(d_{ij} d_{jk} d_{kl} d_{li} + d_{il} d_{lk} d_{kj} d_{ji}\right)\left(d_{lm} d_{ml}\right) D_m D_n D_O \cdots D_t D_m \right] + \left[\sum_{i=1}^{M-4} \sum_{j=i+1}^{M-1} \sum_{k=i+1}^{M} \sum_{l=i+1}^{M} \sum_{m=j+1}^{M} \cdots + \sum_{M=t+1}^{M} \left(d_{ij} d_{jk} d_{kl} d_{lm} d_{mi} \right.\right. \\ & \left.\left. + d_{im} d_{ml} d_{lk} d_{kj} d_{ji}\right) D_n D_O \cdots D_t D_m \right] + \left[\sum_{i=1}^{M-3} \sum_{j=i+1}^{M-1} \sum_{k=i+1}^{M} \sum_{l=j+1}^{M} \sum_{m=1}^{M-1} \sum_{n=m+1}^{M} .. \sum_{M=t+1}^{M} \left(d_{ij} d_{jk} d_{kl} d_{li} + d_{il} d_{lk} d_{kj} d_{ji}\right)\left(d_{mn} d_{nm}\right) D_O \cdots \cdots D_t D_m \right] + \left[\sum_{i=1}^{M-5} \sum_{j=i+1}^{M-1} \sum_{k=j+1}^{M} \sum_{l=1}^{M} \cdots \sum_{M=t+1}^{M} \left(d_{ij} d_{jk} d_{ki} \right.\right. \\ & \left.\left. + d_{ik} d_{kj} d_{kj} d_{ji}\right)\left(d_{lm} d_{mn} d_{nl} + d_{ln} d_{nm} d_{ml}\right) D_O \ldots D_t D_m + \sum_{i=1}^{M-5} \sum_{j=i+1}^{M} \sum_{k=i+1}^{M-3} \sum_{l=i+2}^{M} \sum_{m=k+1}^{M-1} \sum_{n=k+2}^{M} \ldots \sum_{M=t+1}^{M} \left(d_{ij} d_{ji}\right)\left(d_{kl} d_{lk}\right)\left(d_m d_n\right) D_O \cdots \cdots . D_t D_m + \sum_{i=1}^{M-5} \sum_{j=i+1}^{M-1} \sum_{k=i+1}^{M} \sum_{l=i+1}^{M} \sum_{m=i+1}^{M} \\ & \times \sum_{n=j+1}^{M} .. \sum_{M=t+1}^{M} \left(d_{ij} d_{jk} d_{kl} d_{lm} d_{mn} d_{ni} + d_{in} d_{nm} d_{ml} d_{lk} d_{kj} d_{ji}\right) D_O D_t D_m \Bigg] \end{aligned} \tag{4}$$

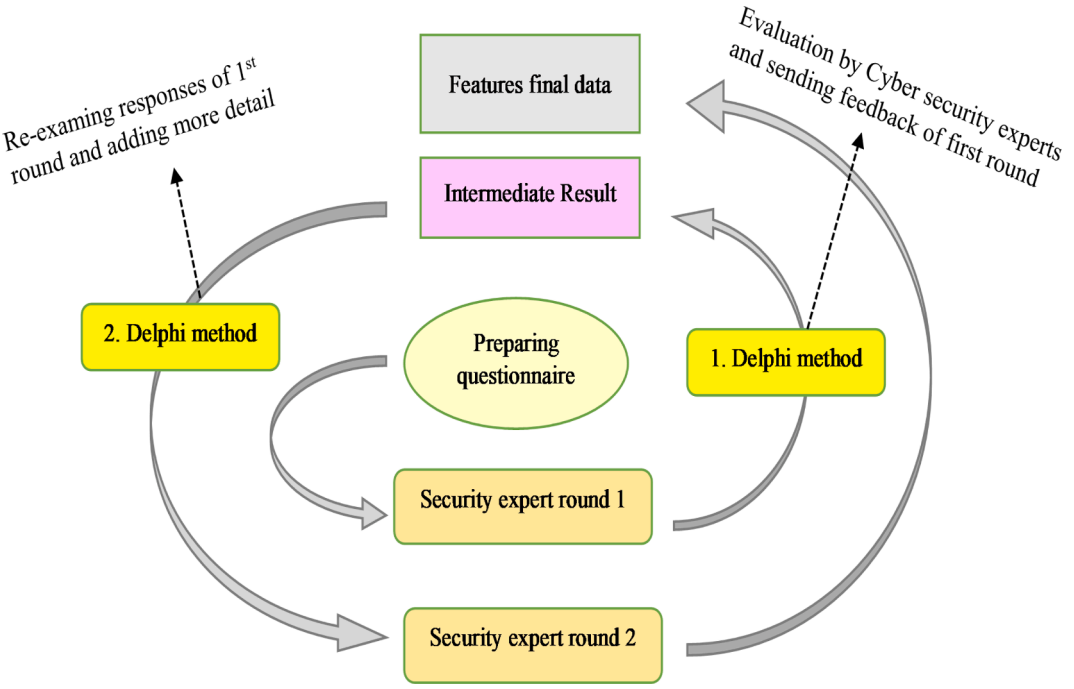

Fig. 2. Delphi method for feature and data collection.

of authentication, if it has the highest value among all the scoring values of alternatives in light of designed criteria.

ii. **Graph representation of authentication features**

In this proposed framework, we have nine (9) features based criteria and every parameter of criteria affects the authentication. The criteria elements are also inter-dependent on each other and affect the performance of each other as well. All the relationships of criteria elements are represented in the shape of graph. The criteria is represented with the nodes and their relationship is denoted by arcs or edges as shown in Fig. 5.

iii. **Matrix representation of features**

The representation of digraph is very suitable for visual analysis but is not for computer processing. Similarly, for large system then corresponding graph also becomes complicated along with its visual understandability. Therefore, it is imperative to construct a representation that is easily understandable, storing, retrieving and processing is done in efficient manner by computer. The features and data collected from cyber security experts related to authentication are given in decision matrix of size 9 × 10. In this matrix the criteria consisted of nine (9) authentication parameters are given in columns and 10 alternatives are selected for decision making based on the designed criteria. The results obtained from cyber security experts based on assigning importance to each criteria are divided among ten (10) alternatives as given below in decision matrix.

	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9
A_1	6	8	7	7	3	7	5	6	8
A_2	7	6	8	6	4	5	4	4	8
A_3	6	6	7	5	5	6	7	6	7
A_4	8	7	5	6	8	6	5	4	9
A_5	6	7	7	6	6	5	6	5	7
A_6	5	5	6	7	5	7	4	8	6
A_7	8	8	7	7	6	8	5	6	8
A_8	6	8	6	4	4	5	6	7	5
A_9	7	6	6	8	7	8	5	4	7
A_{10}	8	3	5	6	3	5	6	5	8

iv. Normalizing decision matrix

The decision matrix is normalized for both beneficial and non-beneficial criteria. All the values of decision matrix are beneficial criteria it means higher values for the elements of this matrix is desired. For beneficial and non-beneficial criteria the following equations are used.

For beneficial criteria.

$$X_{ij} = \frac{X_{ij}}{X_j^m ax} \tag{6}$$

For non-beneficial criteria.

$$X_{ij} = \frac{X_{ij}}{X_j^m in} \tag{7}$$

The decision matrix is normalized to avoid the element of subjectivity and the detail of normalized decision matrix is given below as.

Table 2
Attributes relative importance.

Description of class	Relative importance	
	a_{ij}	$a_{ji=1-}$ a_{ij}
Two equally important attributes	0.5	0.5
One attribute (i) is slight important than other attribute(j)	0.6	0.4
Attribute (i) is strongly more important over the other(j)	0.7	0.3
Attribute (i) is very strongly more important over the other(j)	0.8	0.2
Attribute(i) is extremely important over the other(j)	0.9	0.1
Attribute(i) is exceptionally more important over the other(j)	1.0	0.0

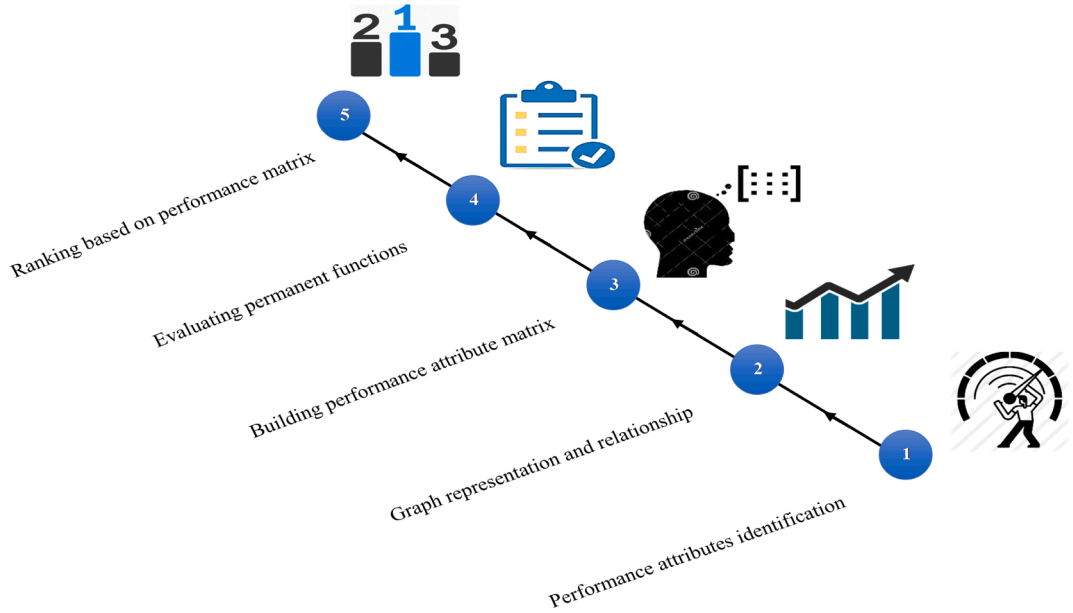

Fig. 3. GTM approach step-wise procedure.

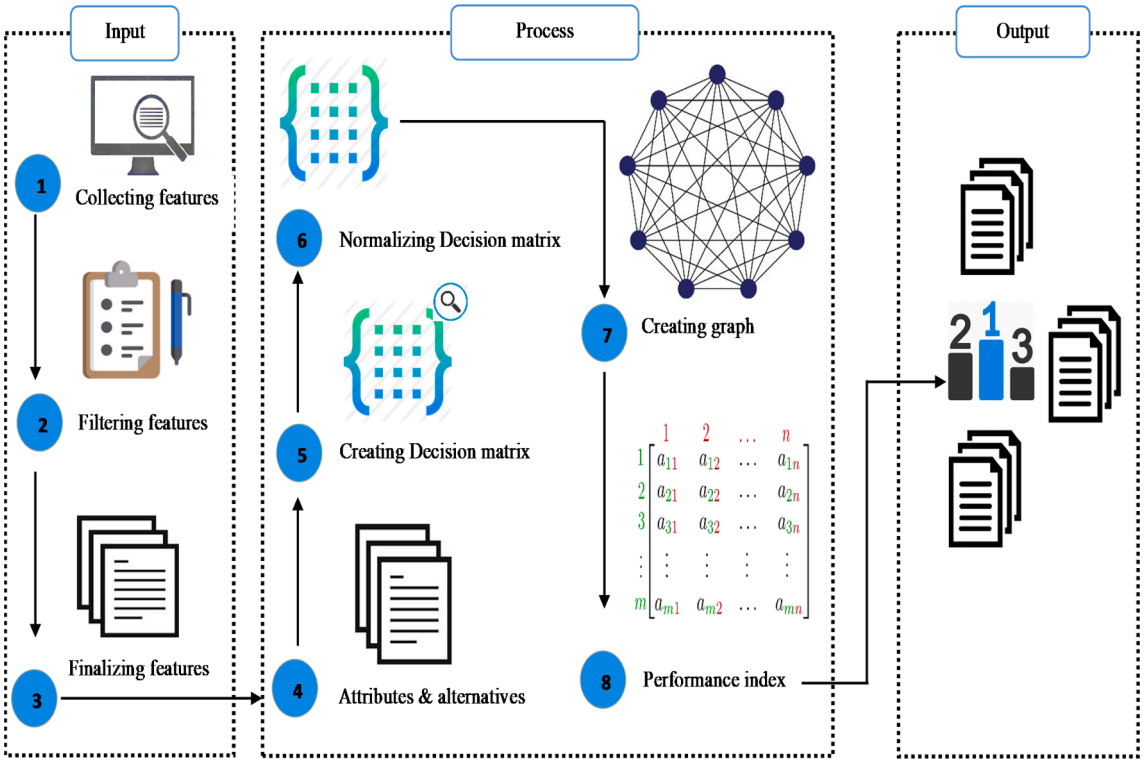

Fig. 4. Evaluation framework structure.

	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9
A_1	0.75	1	0.88	0.88	0.38	0.88	0.71	0.75	0.89
A_2	0.88	0.75	1	0.75	0.50	0.63	0.57	0.50	0.89
A_3	0.75	0.75	0.88	0.63	0.63	0.75	1	0.75	0.78
A_4	1	0.88	0.63	0.75	1	0.75	0.71	0.50	1
A_5	0.75	0.88	0.88	0.75	0.75	0.63	0.86	0.63	0.78
A_6	0.63	0.63	0.75	0.88	0.63	0.88	0.57	1	0.67
A_7	1	1	0.88	0.88	0.75	1	0.71	0.75	0.89
A_8	0.75	1	0.75	0.50	0.50	0.63	0.86	0.88	0.56
A_9	0.88	0.75	0.75	1	0.88	1	0.71	0.50	0.78
A_{10}	1	0.38	0.63	0.75	0.38	0.63	0.86	0.63	0.89

v. Determining permanent function for each alternative

The permanent function of each alternative is calculated by using equation (2) and the relative importance among the criteria is obtained by using equation (3). The detail of relative importance among the criteria elements is given below as.

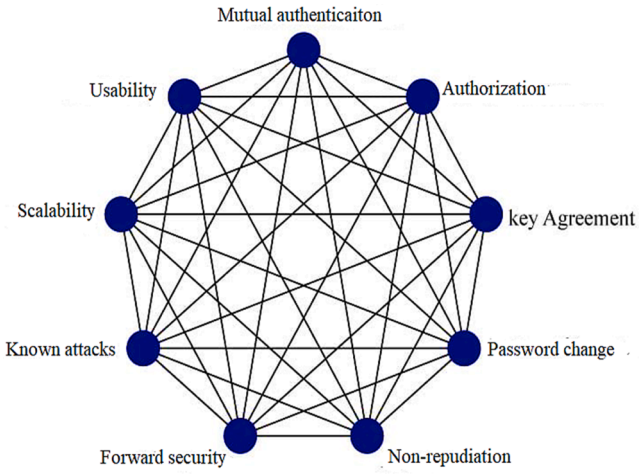

Fig. 5. Features diagraph.

	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9
C_1	1	0.6	0.5	0.4	0.6	0.5	0.6	0.7	0.5
C_2	0.4	1	0.5	0.7	0.5	0.5	0.4	0.8	0.4
C_3	0.5	0.5	1	0.5	0.7	0.4	0.7	0.6	0.5
C_4	0.6	0.3	0.5	1	0.7	0.5	0.6	0.5	0.5
C_5	0.4	0.5	0.3	0.3	1	0.6	0.8	0.6	0.4
C_6	0.5	0.5	0.6	0.5	0.4	1	0.9	0.7	0.5
C_7	0.4	0.6	0.3	0.4	0.2	0.1	1	0.6	0.2
C_8	0.3	0.2	0.4	0.5	0.4	0.3	0.4	1	0.2
C_9	0.5	0.6	0.5	0.5	0.6	0.5	0.8	0.8	1

vi. **Ranking alternatives and decision making**

After determining the permanent matrix for all alternatives based on the relative importance of features, the ranking is performed. The higher values of permanent matrix will give the best solution and lower value will be considered as worst solution. The permanent functions calculated for each alternative are given in Table 3.

A_7 has higher values among the alternatives according to the scoring values of Table 3. So, it is considered to be the most rational choice as a target authenticaion solution based on identified authenticaon attributes in IIoT enviroment.

4. Results and discussion

IoT devices operating in industrial environment require serious security attention due to the nature of data transmitted in the network. Any illegal access to the network will jeopardize the entire network resources. Therefore, a robust security mechanism for authentication and identity management will be the key to keep the network safe. The proposed evaluation framework helps in building a decision support system related to security in IIoT environment. The quantitative results obtained through this framework are quite helpful for decision makers and industrial manager to employ the most ideal security option based on their security needs. This framework evaluates the authentication schemes based on the number of features pertinent to security. We have selected nine (9) criteria for the evaluation of ten (10) authentication alternatives by applying the GTM approach supported by Delphi method for the taxonomy of features. This mathematical model selects the best alternative of authentication after empirical assessment of quantitative data. The weights assigned to the features in the criteria for highly ranked authentication alternative are depicted in Fig. 6.

Obviously, the proposed evaluation framework selects the best choice of authentication as the input values of the features of the selected authentication alternative are highly desirable for any secure authentication procedure. Simple Additive Weighting (SAW) method is applied to check the accuracy and consistency of the results that are obtained through the proposed evaluation framework. This method validates the results of our proposed evaluation by selecting the same authentication alternatives and features based on applying a simple procedure. As, there does not exist evaluation model in this domain, therefore, it is important to know about that how our proposed approach has accurately produced the required results. This method just verifies that proposed mathematical model has produced the desirable results by following a more sophisticated and advanced procedure for assessment and ranking purpose. The detail of output obtained through SAW approach in comparison to our proposed evaluation framework is given in Table 4.

Comparison of both methods is depicted in Fig. 7. Similarly, same input is given to the SAW method and it uses different mathematical procedure steps to yield the same result as produced by the proposed evaluation framework for the same number of features and alternatives.

This evaluation model is based on authentication features, so it is also important to investigate the features selected in this study. We conducted a field study to remove the biasness in the selection of features. As the proposed evaluation framework takes into account the authentication features. Therefore, the features selection process is also evaluated by conducting a field study with expert's panel. They evaluated the framework for features and shared feedback about the features evaluation framework. The relevancy, irrelevancy, recommended and not-recommended features need to be identified. The performance and effectiveness of proposed framework is evaluated for features based on three metrics such as accuracy, precision and recall. This method is the most effective for evaluation of features-based systems contextual systems and has been applied for assessment of features (Adomavicius & Tuzhilin, 2011; Alsubaei, Abuhussein, Shandilya, & Shiva, 2019). Following equations are used to calculate the evaluation parameters.

$$\text{Accuracy} = (a+d)/(a+b+c+d) \tag{8}$$

$$\text{Precision} = (a)/(a+b) \tag{9}$$

$$\text{Recall} = (a)/(a+c) \tag{10}$$

In above equations, we used four (4) kind of variables for the classification that are given below as.

a: Shows the number of features used by proposed framework and suggested by expert group
b: Number of features suggested only by proposed evaluation framework
c: Number of features suggested by the expert's group
d: Number of features not suggested by expert's group nor by our proposed framework

The feature classification in terms of recommended, not-recommended, relevant and irrelevant is given in Table 5.

The results obtained after using the equations for accuracy, precision and recall are given in Table 6. The proposed framework produces some

Table 3
Ranking alternatives.

S/No.	Alternatives	Values of Permanent matrix (Per())	Ranking
1	A_1	1028.04	4
2	A_2	856.1	9
3	A_3	1021.16	5
4	A_4	1050.21	3
5	A_5	986.378	6
6	A_6	927.199	7
7	**A_7**	**1219.52**	**1**
8	A_8	884.356	8
9	A_9	1055.59	2
10	A_{10}	829.295	10

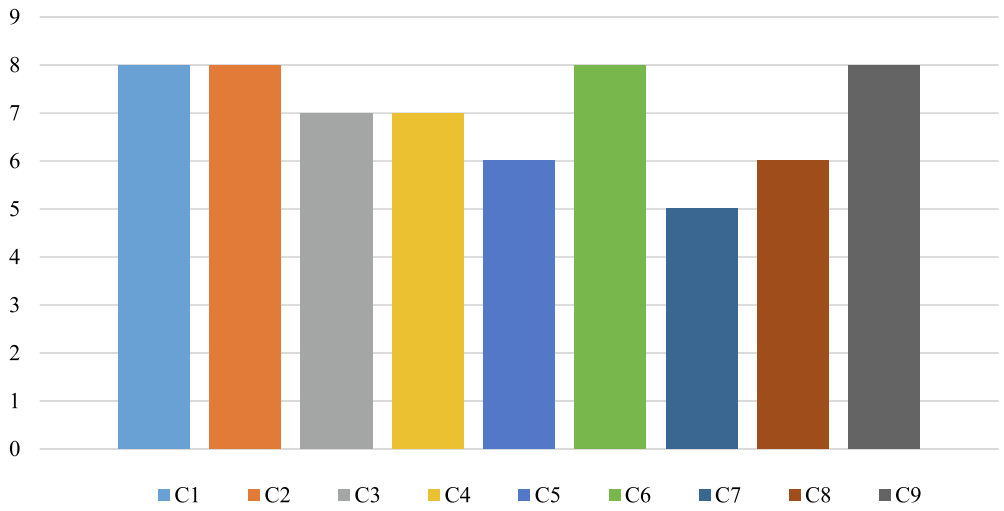

Fig. 6. Feature score of selected authentication alternative.

promising quantitative outcomes. Hence, this framework can be used as evaluation approach for secure authentication in industrial environment.

5. Managerial implications

The proposed evaluation model has a good applicability to certain extent and can be used effectively to determine the best security solution for the business needs related to security in the industry. In industrial environment, where the security demands are high, the proposed framework will provide a good platform for the decision makers and network engineers to select the right security choice based on their security requirements. The proposed methodology presents a mathematical procedure for evaluating the existing authentication schemes in industrial environment and can be applied without any significant overhead. It will enable the industry managers and decision makers to make better decisions regarding the deployment of right authentication scheme for IoT devices operating in industrial environment. This framework is very useful for the uncertain situations due to complex and multiple criteria for the selection of best authentication scheme in industrial environment.

This framework will also enable the managers to upgrade or enhance the features of existing security solution. The confidentiality, availability and integrity are the important security performance parameters and this framework takes into account all the important security aspects of IIoT based network. The major focus of the proposed framework is, it evaluates the existing authentication schemes based on the features and functionalities.

In Industrial environment, a strong security is indispensable as the industry managers lack knowledge and experience related to the installation of right authentication schemes in the IIoT network devices. This framework will provide an insight about selecting the right most security solution for the security demands of their network and IIoT devices.

The proposed evaluation framework is generic in nature, it will also allow the industry network managers to check or evaluate the authentication schemes and check granularity of security methods that are currently employed in ICS devices, gateway and other network entry points. There is no proper benchmark that can be used to select and rank the authentication schemes based on criteria features. It will provide a better security solution to diminish the cyber risks and IIoT attacks surfaces to more extent.

This is very flexible framework as it gives the flexibility to add more security features due to changing security challenges in the industrial domain. The proposed framework provides information feedback and knowledge about the existing authentication models by looking into the features. It will help the security professional designers to identify the right features and adopt in the authentication mechanism. Thus, the proposed evaluation framework will help the designers to incorporate the most essential features and implement the most reliable and successful authentication schemes in the IIoT.

The existing executives of industrial system pay a lot of money to address the security concerns in the third party industrial IoT platforms. The proposed evaluation framework will enable them to evaluate the available authentication methods by saving time, money and energy. It will enable them to adopt the right security solution for their organizational needs.

As, the number of authentication schemes are exponentially increasing in the market, so the right decision making and installation of the most befitted authentication scheme can be time-consuming and complex task. Hence, the proposed evaluation framework can be used to address the selection issues related to authentication schemes. This framework can be generalized for all kinds of authentication schemes due to its versatile security nature and mathematical modelling technique. The proposed evaluation model is the most efficient and applicable especially in industrial environment, where the manufacturing companies can select the desired authentication mechanism based on features and functionalities of their own choices.

6. Conclusion

Security has become a major factor for industry due to the number of threats and vulnerabilities such as legacy devices, less powerful authentication protocols and proliferation of IoT devices. Therefore, it is indispensable to bring a strong authentication mechanism that can address all the issues related to authentication. The proposed work is

Table 4
SAW method results.

Alt	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}
Ranking score (S_i)	6.369	6.018	6.164	6.847	6.147	5.883	7.14	5.458	6.617	5.819
Ranking	4	7	5	2	6	8	1	10	3	9

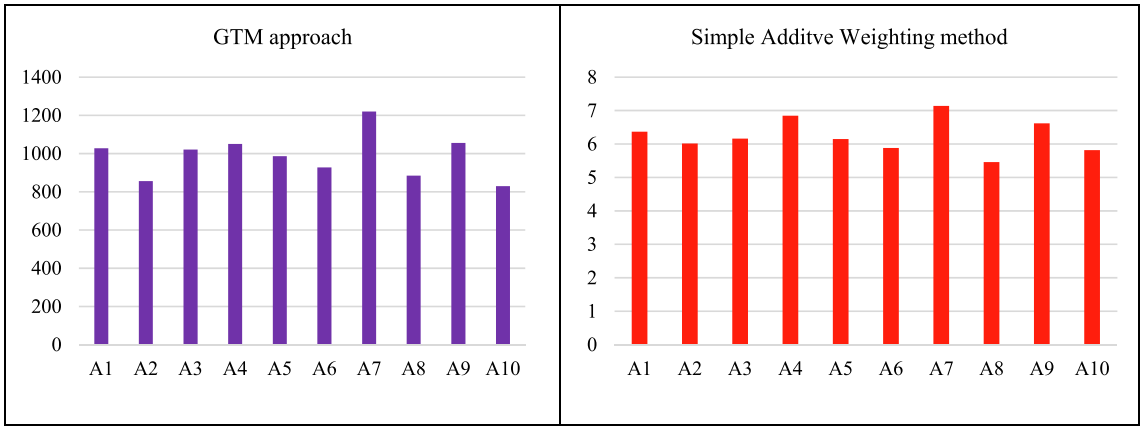

Fig. 7. Comparison of proposed work with SAW method for authentication performance.

Table 5
Recommendations classification.

	Relevant	Irrelevant
Recommended	a	c
Not recommended	b	d

Table 6
Recommendation evaluation parameters results.

Experts	a	b	c	d	Accuracy (%)	Precision (%)	Recall (%)
1	11	3	2	5	76	79	85
2	11	2	1	3	82	85	92
3	9	0	0	10	100	100	100
4	12	1	1	9	91	92	92
5	14	1	0	5	95	93	100
6	25	3	1	5	88	89	96
7	11	2	1	11	88	85	92
8	21	2	0	9	94	91	100
9	15	1	1	9	92	94	94
10	26	2	1	8	92	93	96
Average					90	90	95

presented to provide a full-pledged security system by using authentication features. This evaluation framework evaluates the IoT devices from different authentication dimensions and finally selects the most appropriate target authentication solution after mathematical procedure of evaluation. This framework picks the most rational and suitable target authentication solution to meet the existing authentication problems in IIoT environment. The proposed evaluation framework uses GTM approach for evaluation, ranking alternatives and decision making. Features collected related to authentication are selected as benchmark of assessment. Deplhi method is applied for categorization and collecting data from cyber security expert's panel. This is first type of evaluation framework of its kind to address the prevailing issues in authentication of IIoT devices.

Our future work is to include more features and to use advaced evaluation approaches to provide more secure solution towards the existing security issues in IIoT.

CRediT authorship contribution statement

Yasir Ali: Data curation, Conceptualization, Formal analysis, Investigation, Methodology, Software, Validation, Visualization, Writing – original draft, Writing – review & editing. **Habib Ullah Khan:** Conceptualization, Methodology, Writing – original draft.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This publication was supported by Qatar National Library, Doha, Qatar, and Qatar University Internal Grant No. QUHI-CBE-21/22-1.

References

Adomavicius, G. & Tuzhilin, A. (2011). Context-aware recommender systems. In: Recommender systems handbook, ed: Springer, pp. 217-253.
Alaca, F., Abdou, A. M., & Van Oorschot, P. (2019). Comparative analysis and framework evaluating mimicry-resistant and invisible web authentication schemes. *IEEE Transactions on Dependable and Secure Computing*.
Alsubaei, F., Abuhussein, A., Shandilya, V., & Shiva, S. (2019). IoMT-SAF: Internet of medical things security assessment framework. *Internet of Things, 8*, Article 100123.
Attri, R., Dev, N., & Sharma, V. (2013). Graph theoretic approach (GTA)–a multi-attribute decision making (MADM) technique. *Research Journal of Engineering Sciences, 2*, 50–53.
Boyd, C., & Gellert, K. (2021). A modern view on forward security. *The Computer Journal, 64*, 639–652.
Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry, 101*, 1–12.
Chaudhary, R., Aujla, G. S., Garg, S., Kumar, N., & Rodrigues, J. J. (2018). SDN-enabled multi-attribute-based secure communication for smart grid in IIoT environment. *IEEE Transactions on Industrial Informatics, 14*, 2629–2640.
Deebak, B., & Al-Turjman, F. (2020). Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical things. *IEEE Journal on Selected Areas in Communications*.
Donegan, K. (2019). *5 common authentication factors to know*. Available: https://searchsecurity.techtarget.com/feature/5-common-authentication-factors-to-know.
El Mouaatamid, O., Lahmer, M., & Belkasmi, M. (2020). A scalable group authentication scheme based on combinatorial designs with fault tolerance for the internet of things. *SN Computer Science, 1*, 1–13.
Eliasson, C., Fiedler, M., & Jørstad, I. (2009). A criteria-based evaluation framework for authentication schemes in IMS. In: 2009 International Conference on Availability, Reliability and Security, pp. 865-869.
FInjan. (2017). *What is Non-Repudiation? Principles, Techniques and Best Practices*. Available: https://blog.finjan.com/what-is-non-repudiation/uns.
Forget, A., Chiasson, S., & Biddle, R. (2015). User-centred authentication feature framework. Information & Computer Security.
Gatto J. (202). *What are the Risks Associated with Industrial IoT (Industrial Internet of Things)?* Available: https://www.attilasec.com/blog/what-are-the-risks-associated-with-industrial-iot.
Geetha, N., & Sekar, P. (2017). Graph theory matrix approach with fuzzy set theory for optimization of operating parameters on a diesel engine. *Materials Today: Proceedings, 4*, 7750–7759.
Geetha, N., & Sekar, P. (2017). Graph theory matrix approach–a qualitative decision making tool. *Materials Today: Proceedings, 4*, 7741–7749.
Geetha, N. (2016). Graph Theory Matrix Approach In Selecting Optimal Combination Of Operating Parameter.
Gollmann, D. (1996). What do we mean by entity authentication?. In: Proceedings 1996 IEEE symposium on security and privacy, pp. 46-54.

Haghparast, M. B., Berehlia, S., Akbari, M., & Sayadi, A. (2020). Developing and evaluating a proposed health security framework in IoT using fuzzy analytic network process method. *Journal of Ambient Intelligence and Humanized Computing*, 1–18.

Hamidi, H. (2019). An approach to develop the smart health using Internet of Things and authentication based on biometric technology. *Future Generation Computer Systems, 91*, 434–449.

Han, Z., Li, X., Huang, K., & Feng, Z. (2018). A software defined network-based security assessment framework for cloudIoT. *IEEE Internet of Things Journal, 5*, 1424–1434.

Johnson, H., Isaksson, L., Fiedler, M., & Wu, S. F. (2006). A decision system for adequate authentication. *International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06)*.

Kanjee, M. R., Divi, K., & Liu, H. (2010). A physiological authentication scheme in secure healthcare sensor networks. In: 2010 7th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), pp. 1-3.

Kaur, R., Singh, S., & Kumar, H. (2018). AuthCom: Authorship verification and compromised account detection in online social networks using AHP-TOPSIS embedded profiling based technique. *Expert Systems with Applications, 113*, 397–414.

Khan, H., Atwater, A., & Hengartner, U. (2014). A comparative evaluation of implicit authentication schemes. In *International Workshop on Recent Advances in Intrusion Detection* (pp. 255–275).

Kilciauskas, A., Butkus, G., & Sakalauskas, E. (2020). Authenticated key agreement protocol based on provable secure cryptographic functions. *Informatica, 31*, 277–298.

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

Kumar, P. M., & Gandhi, U. D. (2020). Enhanced DTLS with CoAP-based authentication scheme for the internet of things in healthcare application. *The Journal of Supercomputing*, 1–21.

Kumar, V., Jangirala, S., & Ahmad, M. (2018). An efficient mutual authentication framework for healthcare system in cloud computing. *Journal of Medical Systems, 42*, 142.

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.

Kumar, P., Lee, S.-G., & Lee, H.-J. (2012). E-SAP: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. *Sensors, 12*, 1625–1647.

Kumari, A., Kumar, V., Abbasi, M. Y., Kumari, S., Chaudhary, P., & Chen, C.-M. (2020). Csef: Cloud-based secure and efficient framework for smart medical system using ecc. *IEEE Access, 8*, 107838–107852.

Le, X. H., Khalid, M., Sankar, R., & Lee, S. (2011). An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare. *Journal of Networks, 6*, 355–364.

Liu, C. H., Wang, J. S., Peng, C. C., & Shyu, J. Z. (2015). Evaluating and selecting the biometrics in network security. *Security and Communication Networks, 8*, 727–739.

Mayer, P., Neumann, S., Storck, D., & Volkamer, M. (2016). Supporting Decision Makers in Choosing Suitable Authentication Schemes. *HAISA*, 67–77.

Mayer, P., Neumann, S., & Volkamer, M. (2016). POSTER: Towards Collaboratively Supporting Decision Makers in Choosing Suitable Authentication Schemes. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1817–1819).

Mehmood, A., Natgunanathan, I., Xiang, Y., Poston, H., & Zhang, Y. (2018). Anonymous authentication scheme for smart cloud based healthcare applications. *IEEE Access, 6*, 33552–33567.

Mihajlov, M., Jerman-Blazič, B., & Josimovski, S. (2011). A conceptual framework for evaluating usable security in authentication mechanisms-usability perspectives. In: 2011 5th international conference on network and system security, pp. 332-336.

Munier, N., & Hontoria, E. (2021). Uses and limitations of the AHP method. Management for Professionals.

Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: An example, design considerations and applications. *Information & Management, 42*, 15–29.

Park, K. C., & Shin, D.-H. (2017). Security assessment framework for IoT service. *Telecommunication Systems, 64*, 193–209.

Renaud, K., Volkamer, M., & Maguire, J. (2014). ACCESS: describing and contrasting. In: International Conference on Human Aspects of Information Security, Privacy, and Trust, pp. 183-194.

Sadeghi, A.-R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial internet of things. In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)* (pp. 1–6).

Saleem, M. A., Shamshad, S., Ahmed, S., Ghaffar, Z., & Mahmood, K. (2021). Security analysis on "a secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems". *IEEE Systems Journal*.

Sari, P., Ratnasari, G., & Prasetio, A. (2016). An evaluation of authentication methods for smartphone based on users' preferences. In *IOP Conference Series: Materials Science and Engineering* (p. 012036).

Shakil, K. A., Zareen, F. J., Alam, M., & Jabin, S. (2020). BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud. *Journal of King Saud University-Computer and Information Sciences, 32*, 57–64.

Sharma, S., & Kaul, A. (2018). Hybrid fuzzy multi-criteria decision making based multi cluster head dolphin swarm optimized IDS for VANET. *Vehicular Communications, 12*, 23–38.

Siddiqui, Z., Abdullah, A. H., Khan, M. K., & Alghamdi, A. S. (2014). Smart environment as a service: Three factor cloud based user authentication for telecare medical information system. *Journal of Medical Systems, 38*, 9997.

Sree, S. R. Secure Data Transmission on Internet of Healthcare Things.

Suresh, A., Nandagopal, M., Raj, P., Neeba, E., & Lin, J.-W. (2020). *Industrial IoT Application Architectures and Use Cases*. CRC Press.

T. Micro. *Industrial Internet of Things (IIoT)*. Available: https://www.trendmicro.com/vinfo/us/security/definition/industrial-internet-of-things-iiot.

Tahir, M., Sardaraz, M., Muhammad, S., & Saud Khan, M. (2020). A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics. *Sustainability, 12*, 6960.

Thales. *The Role of Authentication in Manufacturing IoT*. Available: https://www.google.com/search?q=WWW.451RESEARCH.COM+The+Role+of+Authentication+in+Manufacturing+IoT&ei=NMWfYKaEKJ2EhbIPxdqYiAg&oq=WWW.451RESEARCH.COM+The+Role+of+Authentication+in+Manufacturing+IoT&gs_lcp=Cgdnd3Mtd2l6EAxQ5SdY87UBYKnDAWgBcAB4AIABvgSIAekJkgEJMi0xLjAuMS4xmAEAoAEBoAECqgEHZ3dzLXdpesABAQ&sclient=gws-wiz&ved=0ahUKEwim7vq23svwAhUdQkEAHUUtBoEQ4dUDCA4.

Verma, U., & Bhardwaj, D. (2020). Design of lightweight authentication protocol for fog enabled internet of things-a centralized authentication framework. *International Journal of Communication Networks and Information Security, 12*, 162–167.

Wiefling, S., Patil, T., Dürmuth, M., & Iacono, L. L. (2020). Evaluation of risk-based re-authentication methods. In *IFIP International Conference on ICT Systems Security and Privacy Protection* (pp. 280–294).

Wu, Y., Dai, H. -N., & Wang H. (2020). Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in Industry 4.0. IEEE Internet of Things Journal.

Xu, X., Zeng, Z., Yang, S., & Shao, H. (2020). A novel blockchain framework for industrial IoT edge computing. *Sensors, 20*, 2061.

Yao, M., Wang, X., Gan, Q., Lin, Y., & Huang, C. (2021). An improved and privacy-preserving mutual authentication scheme with forward secrecy in VANETs. Security and Communication Networks, vol. 2021.

Zhang, Y., Deng, X., Wei, D., & Deng, Y. (2012). Assessment of E-Commerce security using AHP and evidential reasoning. *Expert Systems with Applications, 39*, 3611–3623.