INTELLIGENT AUTHENTICATION FOR IDENTITY AND ACCESS MANAGEMENT: A REVIEW PAPER

Ass. Prof. Dr. Alia Karim Abdul-Hassan [1]
[1]University of Technology /Computer Sciences Department
110018@uotechnology.edu.iq

MSc. Iman Hasson Hadi [2]
[2]University of Technology /Computer Sciences Department
iman.h.1439@gmail.com

Abstract: ***Identity and access management (IAM) system usually consist of predefined tasks as an information security system. The main task is the authentication, since it is responsible for user identity proving for service providers that corporate with (IAM). This paper provides a review on intelligent authentication research applicable to IAM systems. These researches are evaluated according to the proposal of intelligent authentication key factors. Depending on this evaluation it could not be found research implement an authentication that satisfies all these key factors.***

Keywords: Advanced encryption standard, AES, Chebyshev, modified AES.

I. INTRODUCTION

One of the most important tasks of information security is developing an authentication method based on the digitization of identity that is required to access these systems with an acceptable level of trust. The identity refers to a group of well-defined properties that make an entity recognized compared to other entities [1]. While digital identity is a set of features owned by an entity and used by information systems to represent an identity (individual, organization, application, or device). Its management is typically delegated to Identity and Access Management (IAM) which enables the right individuals to access the right resources at the right times and for the right reasons [2]. Authentication process consists of three sub-tasks (identification, enrolment, and verification). The first and second sub-tasks related to the definition and registration of user digital attributes that will be used in verification. These definitions and configuration usually established as an agreement between IAM and service providers. The last task implemented when any user attempts to access a service provider system through IAM. So, the verification process is the essential step of any type of authentication system because it provides the identity of that user and decides whether he is authenticated or not. Traditional authentication depends on many factors, knowing-based and possession-based methods suffer from many issues as shown in figure1. For example, a password authentication method depends on simple matching between what the claimed users know as a secret phrase (password) and the stored secret phrase in the systems. The result of this matching used to prove the identity of the claimed user. This process suffers from many problems like stolen or forging the secret phrase.

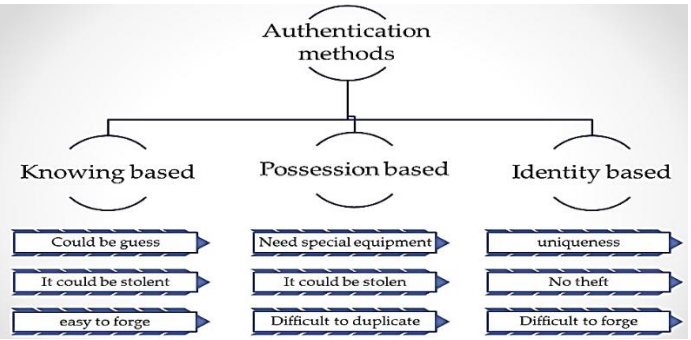

Fig 1 Authentication methods

While the identity-based method has many advantages as uniqueness and it could not guess or stolen.

II. RELATED WORK

There are many reviews and surveys had been done to study the existing authentication methods. Most of these paper focus on authentication methods on specific platform except [3] that provides an overview of existing authentication methods in general and its pros and cons when designing an online service. While [4] provide a survey of the researches on biometric authentication that utilize keystroke dynamic attributes and have used neural networks for classification. Referring to the platform [5] provides a review of several research suited for the IOT environment in the scope of identity management and authentication. As a result, this work was held to minimize the gap in analyses of intelligent authentication for identity and access management system.

III. DIGITAL IDENTITY

Individual identifications in the real world take several forms, for example, national ID card, driver licenses, passports, employee ID card. These forms of identifications share a specific characteristic that contains information which is unique to the individual, like, name, gender, and date of birth, as well as information about the authorities that issued the cards [2]. While identities in the real world are well recognized, the definition of digital identities is different. The components of digital identity as shown in figure 1, could be summarized as follows:

- Identifier specific information that uniquely identifies the subject of the identity for example (e-mail address).
- Credentials Private or public information usually used to verify an identity of the user. For example, a password, a private key.
- Core Attributes Data that give a clear description of the identity. Core attributes usually used by a different application.
- Context-specific Attributes Data that give more detail description to the identity, with a specific context where the identity is used. For example, within a document management system, the user's must follow a specific context of the document routing process with specific attributes related to (workflow, system calls, network information, time constraints, location, device type).

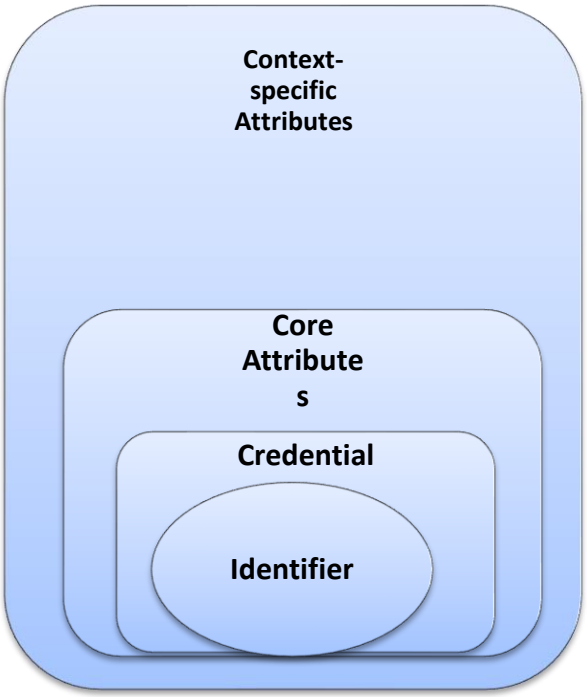

Fig.2 Digital identity Components

These four types of information can be selected for different needs, ranging from identity proof (similar to ID card information) to gain authorized rights (like the use of e-passport to establish the right to travel). Digital identity could consist of descriptive information about an individual, such as a name, an ID number, or a passport number. In addition, it could also contain biometric information, such as iris or fingerprint features, and information about user behaviour, including Web searches and data uploads and downloads. Digital identity may include identifiers, like login names used to enter to information systems [6].

IV. IAM Definition

One definition of IAM that describe its main component, "Identity and access management refers to the processes, technologies, and policies for managing digital identities and controlling how identities can be used to access resources " [7]. The essential modules of IAM are (Source of truth or Authority, Roles and their relationships, Registration, Provisioning, Integration between security apps and business apps, Authentication, Authorization/access management) [8].

Indeed, the IAM system has many functions that achieve the goals of the above modules, the First, specify the identity of the individual that has the right to access specific information. Second, information resource access correctness: by matching the access definition and the business function. In addition, it ensures that there is no specific resource conflict with access rights. Finally, information system resources, access, and activity must be registered and audited with reporting service. IAM processes should be designed in a manner that supports regulatory compliance [9].

V. Intelligent Authentication for IAM

The goal of authentication is to verify the identity of an entity with accepted threshold trust, according to the security requirements of the information system. The authentication method must be trustable when it provides a technique that will lead to an implementation without backdoor's [10]. Authentication in IAM will prove the identity of the user once, at log in session [11].

Intelligent Authentication could be a hyper method to authenticate user identity based on his attributes in a contextual manner with specific business processes, other system environments attributes and user biometric information. Usually, the user attributes matching and verification decision processes are implemented using intelligent methods and tools like soft computing.

In case of identity and access system, authentication method can take place once user population and information system resources are defined, and executed the policies that match up the two, which represent the basis of the IAM system.

VI. Intelligent Secure IAM Key Factors

Authentication in identity and access management system has many key factors which are related to many issues (like application type, system platform, etc.). The following are the main key factors:

1- The appropriate number and type of attributes: this refers to the attributes of the pretender, they must be chosen carefully to describe the authenticated user in an unambiguous manner. These attributes could be biometric, demographic, IAM context-specific, user behaviour attributes.

2- Adaptive authentication: is authentication that makes use of past sessions data (like user behaviour history) to refine the policies and rules of IAM.
3- Special purpose training data set: which describes the interactions among user attributes applications, processes which are related to IAM policies.
4- Proper user recognition method: the proper recognition that uses a powerful method that discriminates between the authenticated users and unauthenticated users with a high degree of accuracy.

VII. Soft Computing

An Intelligent system has the ability to recognize and capture useful information from an object that is changed, it is already familiar with the original one [12]. So, it could possibly define Soft computing as an approach to invent computationally intelligent systems that is tolerant of imprecision, uncertainty, randomness, and partial truth [13] based on artificial intelligence techniques that provide efficient and feasible solutions in comparison with hard computing. These techniques are integrated to find intelligent solutions for the problems which are complex and need hybridized methods that are similar to human thinking in solving a problem [14]. Usually, soft computing implements AI methods for data processing and decision making. Most important AI methods as follows:

- Fuzzy logic: is derived from fuzzy set theory related to the reasoning that is approximate. It is the application form of the fuzzy set [15]. the fuzzy logic uses truth degrees as a mathematical model for vague facts. The reason for choosing fuzzy logic in biometric authentication because biometric data can difficultly be analysed with hard (crisp) logic of 0 (false) or 1(true) [16].
- Neural networks: neural networks represent models that is inspired by how the human brain works, using artificial neurons connected to each other. Most of the artificial neurons feed from the output of other artificial neurons. A few numbers of the artificial neurons produce their output out of the network as the prediction [17].
- Machine learning methods: Arthur Samuel (1959), defined machine learning as a "field of study that gives computers the ability to learn without being explicitly programmed." These methods work on classification and prediction, based on known features previously learned using the training data. These algorithms need a goal (problem formulation) from the domain (e.g., dependent variable to predict) [18].

VIII. Intelligent Authentication Architecture

The intelligent authentication architecture can be constructed using soft computing technique (see figure 3) like fuzzy logic at first layer to overcome the artefacts in the acquisition of user attributes (especially if it is biometric).
When the matching and recognition is verified then the user can be authenticated with a limited access to service providers. The main steps are described in Algorithm 1.

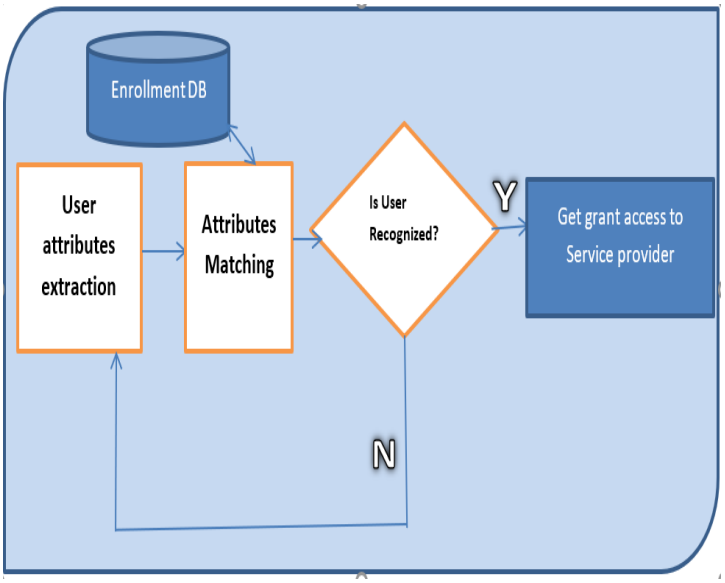

Fig. 3 The Intelligent Authentication architecture

Algorithm 1: Biometric authentication
Input: user biometric information (e.g) voice print.
Output: user recognition decision (yes or no)
---
step1: Acquisition: a specific routine is used to capture the biometric trait (voice of the user) in a digital format.
Step2: Segmentation: The digital format is then segmented in order to have only the region of interest containing the biometric information.
Step3: Preprocessing: here an enhancement process is implemented to increase the quality.
Step4: Feature extraction and matching: the discriminant features are extracted and stored in a template, the template is matched with a specific enrolled template using the fuzzy system, to decide if it belongs to the same person.
Step5: Matching result: if the decision result is **yes** user get grand access to the service provider according to IAM policies, else the system permits to repeat the recognition steps for a specific number of trials and return recognition decision (yes or no).

IX. AUTHENTICATION RESEARCH REVIEW

Many types of research focus on improving IAM security in many approaches. Most of them focus on utilizing biometric user attributes. [19] Proposed a dynamic policy management process which structures the activities required for policy management in identity and access management environments by using k-mean clustering contextual data to produce dynamic policies. While [20] proposed the computation of an authentication score based on a user's recent activity. [21] Utilize automated face recognition to authenticate identity. In [22] a multi-modal digital identity management system was proposed as a solution for managing digital identity information in an effort to reduce the cases of identity fraud and theft, an artificial intelligence technology is used to implement a technique of information fusion to combine the user's credential attributes for optimum recognition. [23] Proposed a method for automatic correlation of identity records from various sources.

Most authentication methods depend on three concepts (a) something you know (b) something you have (c) something you are, but [24] proposed a solution depending on the fourth concept that related to something you do, relies on analytic techniques to transfer big data characteristics into relevant security user profiles. While [25] proposed the activity-related, that is related to pretension biometrics and includes the dynamic information of the movement of the head, the arm, the palm and the fingers derived when performing short everyday activities. [26] Proposed multi-modal biometric authentication. [27] Proposed a two-step authentication method based on an own-built fingertip sensor device which can capture motion data and physiological data simultaneously. [11] Proposed continuous authentication has built around the biometrics supplied by the user's physical or behavioural characteristics and continuously checks the identity of the user throughout a session. In [28] a Fuzzy Logic based implicit authentication scheme is proposed by computing an aggregate score based on selected features and a threshold in real-time based on current and historic data depicting user routine.

X. INTELLIGENT AUTHENTICATIONS KEY FACTOR EVALUATION

According to the main key factors challenges (mentioned in section 6). Table1 displays the comparison result and show the ideal authentication framework for IAM will face all challenges.

Key factor / research	1	2	3	4
[19]	Yes	Yes	Yes	No
[27]	No	No	No	Yes
[22]	Yes	No	No	Yes
[23]	Yes	Yes	Yes	No
[11]	Yes	No	No	Yes
[20]	No	No	Yes	No
[21]	Yes	Yes	No	Yes
[26]	Yes	No	No	Yes
[28]	No	Yes	No	Yes
The ideal Intelligent authentication for IAM	Yes	Yes	Yes	Yes

TABLE (1): THE IDEAL AUTHENTICATION FRAMEWORK FOR IAM WILL FACE ALL CHALLENGES.

XI. CONCLUSION

Most researchers focus on the authentication method that is specific to the hardware/software platform (e.g. mobile platform or using a special purpose device). As a conclusion, intelligent, secure IAM can be developed based on analyses of identity data that is correlated with user biometric attributes and user context-specific attributes which could be extracted from the IAM system. The ideal authentication method for IAM could be more efficient when it designed an intelligent process. In addition, when authentication obey specific key factor (like user attributes type, proper matching, and adaptability) this will enhance the recognition rate of the authenticated users.

XII. FUTURE WORK

This work proposes key factors to evaluate research that propose intelligent authentication applicable to IAM. The following research will be held in the purpose of implementing a traditional authentication method for IAM side by side with the proposed the architecture of ideal intelligent authentication in order to implement experiments that help to have a comparative study of these methods and measure the improvements to IAM security.

REFERENCES

[1] Ghazi Ben Ayed, Architecting User-Centric Privacy-as-a-Set-of-Services: Digital Identity-Related Privacy Framework, Springer, 2014.

[2] D. Hühnlein, H. Robnagel, C. Schunck, M. Talamo (Eds.): Identity Mining Vs Identity Discovering: a new approach based on data mining in the context of Big Data Open Identity Summit 2016, Lecture Notes in Informatics (LNI), Bonn 2016.

[3] S. Zulkarnain, S. Idrus, E. Cherrier, C. Rosenberger, and J.-J. Schwartzmann, "A Review on Authentication Methods," A Rev. Authentication Methods. Aust. J. Basic Appl. Sci., vol. 7, no. 5, pp. 95–107, 2013.

[4] M. L. Ali, K. Thakur, and C. C. Tappert, "Review Papers User Authentication and Identification Using Neural Network," i-manager's J. Pattern Recognit., vol. 2, no. 2, p. 2015, 2015.

[5] H. Kim and E. A. Lee, "Authentication and Authorization for the Internet of Things," IT Prof., vol. 19, no. 5, pp. 27–33, 2017.

[6] Elisa Bertino Kenji Takahashi, Identity Management Concepts, Technologies, and Systems, ARTECH HOUSE,2011.

[7] Frederick Chong , Identity and Access Management, Microsoft Corporation, July 2004.

[8] Jeff Scheidel, Designing an IAM Framework with Oracle Identity and Access Management Suite, The McGraw-Hill Companies, Inc.,2010.

[9] Sajay Rai, Ernst & Young LLP Authors, Digital Identity and Access Management, The Institute of Internal Auditors,2007.

[10] Zulkarnain Syed Idrus, Estelle Cherrier, Christophe Rosenberger, Jean-Jacques Schwartzmann.A Review on Authentication Methods. Australian Journal of Basic and Applied Sciences, 2013.
[11] Soumik Mondal, Continuous User Authentication and Identification, Norwegian University of Science and Technology,2016.
[12] F. O. Karray and C. De Silva, "Soft Computing and Intelligent Systems Design: Theory, Tools, and Applications," Book, p. 585, 2004.
[13] Madhuri Potey1 and Dr. Pradeep K Sinha, Review And Analysis Of Machine Learning And Soft Computing Approaches For User Modeling, International Journal of Web & Semantic Technology (IJWesT) Vol.6, No.1, January 2015.
[14] https://www.igi-global.com/dictionary/soft-methods-automatic-drug-infusion/27620.
[15] K.R.Venugopal, K.G. Srinivasa and L.M. Patnaik, Soft Computing for Data Mining Applications,Springer,2009.
[16] M. A. Jayaram, Hasan Fleyeh, Soft Computing in Biometrics: A Pragmatic Appraisal, American Journal of Intelligent Systems, 2013.
[17] Geoff Hulten, Building Intelligent Systems: A Guide to Machine Learning Engineering, 2018.
[18] A. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Commun. Surv. Tutorials, vol. PP, no. 99, p. 1, 2015.
[19] Matthias Hummer,Michael Kunz2, Michael Netter, Ludwig Fuchs ,and Günther Pernul, Adaptive identity and access management—contextual data based policies, EURASIP Journal on Information Security ,2016.
[20] Elaine Shi, Yuan Niu, Markus Jakobsson, and Richard Chow, Implicit Authentication through Learning User Behavior,2010.
[21] Timur Kartbaev , Bahitzhan Akhmetov, Aliya Doszhanova, Kaiyrkhan Mukapil,Aliya Kalizhanova, Gulnaz Nabiyeva, Lyazzat Balgabayeva, Feruza Malikova, Development Of A Computer System For Identity Authentication Using Artificial Neural Networks Timur, Image Anal Stereo,2017.
[22] Jackson Phiri, A Digital Identity Management System, 2007.
[23] Tomáš Jendek, Intelligent identity information processing, diploma thesis, Slovak University of Technology in Bratislava,2014.
[24] Anas Ibrahim, Data Science Solution for User Authentication, The University of Western Ontario,2017.
[25] Anastasios Drosou, Activity related Biometrics for Person Authentication, Imperial College London Department,2013.
[26] K.Gunasekaran, P.Mahalakshmi, Implementation of Multimodal Biometric Authentication Using Soft Computing Techniques, Pavendar Bharathidasan College of Engg & Tech,2014.
[27] Guannan Wu, Jian Wang , Yongrong Zhang and Shuai Jiang, A Continuous Identity Authentication Scheme based on Physiological and Behavioral Characteristics. National University of defense technology, China, 2018.
[28] Feng Yao, Suleiman Y. Yerima, Boojoong Kang, Sakir Sezer, Fuzzy Logic-Based Implicit Authentication For Mobile Access Control, SAI Computing Conference, London, 2016.