Volume: 16 Issue: 04 Pages: 6515-6522 (2025) ISSN: 0975-0290

The Techniques of authentication in the Context of Cloud Computing

Amira Hassan Abed 0000-0001-6617-0596
Business Information Systems Department, Faculty of Business Administration,
Al Ryada University for science and technology, Egypt;
Email : Amira.Abed@rst.edu.eg;

----------**ABSTRACT**----------
One solution that helps with straightforward, on-demand access to a pool of reconfigurable computing resources is cloud computing. Cloud Computing is an emerging and ubiquitous trend. It allows users to enjoy the on-demand services, without the burden of data storage and maintenance costs. Users of this type of computing platform are very concerned about security, and they need to find reliable providers of cloud services. Authentication is believed to be a main necessity for assuring secure access to cloud. In this paper we discussed the comprehensive and detailed frameworks constructed to assure successful authentication in cloud computing. Also, this survey paper provides a discussion of differences between considered techniques used in different frameworks.

Keywords - **Cloud computing, authentication, cloud services, security in Cloud.**

Date of Submission: 27 Sept, 2024 Date of Acceptance: 20 Dec, 2024

I. INTRODUCTION

The revolutionary state of the art cloud computing technology offers a huge list of assistance for almost all business and organizations. It really helps the organization adopting cloud computing by reducing the cost and the complexity of the infrastructure of the provided platforms [1]. Cloud computing had became hugely adopted for the provision of services over the internet, such as Iaas, Paas, or Saas with a practical and reasonable cost for the users [2]. Where users rent these services and access them remotely over the Internet. Consequently, companies often select clouds based on the standard of services offered; yet, evaluating the quality of security measures taken by cloud providers can be challenging, since many of them won't reveal their infrastructure to clients. For that reason, Security has a huge effect on the success or failure of cloud service providers [3]. Since data is kept and transferred over the cloud, security and privacy issues are a big concern as well as information leakage [1]. Strong user authentication for the prevention of illegitimate access to the resources and services of the cloud is considered to be one of the core necessities for ensuring secure access to the cloud [4]. This is due to the fact that authentication is considered the main aspect for security. This paper will include overview for cloud computing, security overview including different authentication methods, followed by that will be a literature review for some of the proposed models and frameworks to handle authentication and a comparison between them.

II. CLOUD COMPUTING

In order to understand the security threats in cloud computing we have to first understand the characteristics of cloud, its basic types, and service architectures. The primary attributes of cloud computing include [5]:

- Self-service on demand: The user is granted access and jurisdiction over their services without the involvement of the service provider.
- Wide-ranging network connectivity: Where services can be accessed from anywhere not considering the device used, and they are available over the internet
- Resource pooling: With the help of diverse virtual and physical resource, multiple customers can access a pool of computing resources
- Rapid elasticity: Users can adapt the functionalities according to their needs. The computer resources are highly dynamic and its capacity seems to be boundless.

Cloud computing comes in three kinds: hybrid, private, and public [6]. A public cloud is a kind of cloud computing in which the physical setup is owned and managed by the service provider, but a third party offers the service online [7]. On the other hand, a private cloud can be displayed externally or on-site and is maintained either internally or by a third party. The hybrid infrastructure combines the two categories and is required to adhere to established technologies for data portability and application compatibility [6]. As for the cloud services, there are mainly three available types

Volume: 16 Issue: 04 Pages: 6515-6522 (2025) ISSN: 0975-0290

from providers of cloud services, Iaas, Paas, and Saas. In Iaas the service provider carries all the cost and to take advantage of the service and create their own software apps, customers must pay. While for Paas only the platform or stack of solutions is available, and user can save investment on hardware and software. Finally, is the Saas where the provider gives uses the service of using software [5].

III. SECURITY OF CLOUD ENVIRONMENT

Security threats are a huge factor to take into consideration before transferring to cloud environment and assessing the advantages verse the disadvantages to measure the amount of risk that might be faced by the organization. Some of the major risks in cloud computing is ease of use, secure data transmission, malicious insiders, insecure API, and shared technology issues [4]. Cloud computing environment offers some security benefits to the user including Authentication, authorization, auditing, confidentiality, non-repudiation, availability, and integrity [6].

Authentication is the process of validating the identity of the users accessing a service, in cloud computing this is the preliminary prerequisite to public cloud computing environments before the users can access a secure resource and service. It is a vital step for any service provider to make sure that only users who are authorized are granted access and is considered the first step towards a secure environment [4]. This process trims down any unauthorized and improper admittance of services along with identity management in which user's identity is plotted against access privileges roles for resources [8].

- Authentication

Recently authentication process is following new techniques to provide a more rigorous and strict environment including PIN/password authentication, one-time password based authentication, Encryption, and Biometrics based authentication [8].

- PIN/Password based authentication: Is considered the most straightforward authentication technique, where user is required to enter a PIN or a password and according to its correctness the user is granted access [9].
- Authentication based on a one-time password:
  - Two Factor Authentications: Where a user receives a message including a special password after entering his User ID and password, after using the received On-Time-Password (OTP) he will be granted access [10].
  - Three or Multifactor Authentication: where the user has to use a smart cart that is familiar to the system then after that he uses his User ID and Password for authentication [9].
- Encryption which includes Public Key and Symmetric authentication.
- Biometrics based authentication: users can use physiological characteristics to authenticate themselves, like figure prints, face recognition or voice recognition [9].

IV. AUTHENTICATION MODELS

In this section, we will first make a classification of authentication models and mechanisms by specifying those that are general and those that are specific to the Cloud, and then we will make a classification by category.

1. General mechanisms

1.1. Authentication by password:

The login and the password are confidential information that the user employs in order to access a specific service (mailbox, shopping sites, etc.). [9] This is the weakest authentication and identification mechanism, because it is possible to intercept the password in transit or when it is typed on the keyboard.

- **Typology of passwords**

•**Simple and easy to remember password:** The choice of the password is often left free to the user. Most users simply use an easy-to-remember password. However, it is easy to be guessed.

•**Complex passwords:** A complex password is hard to be guessed. It combines numbers and letters, with uppercase and special characters.

•**Identifiers and passwords with a lifetime:** Although complex passwords are more secure than simple ones, several mechanisms can be used to break them. To reinforce the security policy, a password expiration period must be imposed [12]. Thanks to the lifetime technique, a hacked password cannot be used indefinitely.

•**One time password (OTP):** By adopting the OTP mechanism, the password will be unique, automatically generated, random and can only be used once [12]. For each access request, a new password will be sent to the user, via SMS or email.

•**Encrypted password:** During communication between user and server, the password is encrypted so as not to be revealed to a third party during transit or recording.

1.2. Authentication by Captcha or image scans:

•**Captcha:** This is a sequence of characters that the user must type to prove that he is not a robot.

•**Image scan:** When users is connected to a service from the laptop and want to be connected from the Smartphone, the system provides to him an image that must be scanned by this Smartphone to access the service without having to remake the whole authentication procedure.

1.3. Authentication by address, MAC or IP:

•**Authentication by MAC address:** The authentication by MAC address allows authenticating the machine, not the person. It is a particularly effective method of authenticating users who usually have access to their accounts from a regular set of machines.

Volume: 16 Issue: 04 Pages: 6515-6522 (2025) ISSN: 0975-0290

•**Authentication by IP address:** The authentication is successful or not depending on the network from which the access requestor is connected.

1.4. Biometrics:

Biometrics illustrated in Fig. 1 can be used to identify a user through his physiological characteristics such as face, iris and fingerprint, or behavioral characteristics such as gestures and signature [14]. Everyone has his own unique biometric feature. However, it can change over time (age, accident, injury, etc.).

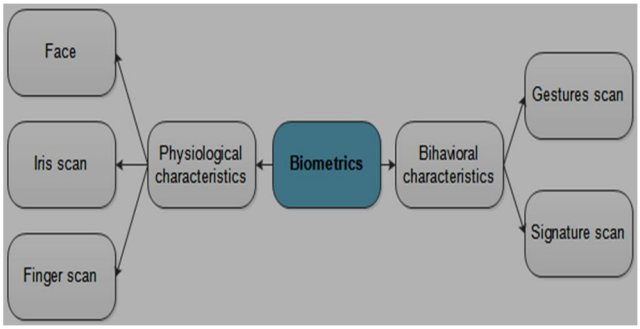

Fig. 1: Biometrics

1.5. Data encryption

This is a good authentication, avoiding the identity theft and the replay of an authentication. It implements a proof of possession of a secret element (cryptographic key), by means of an authentication protocol guaranteeing the confidentiality of the secret element [15]. Encryption is also an indispensable tool for protecting information in computer systems.

1.6. Two factor and multi-factor authentication:

Two-factor or multi-factor authentication provides strong authentication by the combination of two or more of the solutions presented above.

1.7. Multilevel authentication:

The multi-level authentication reinforces security by authenticating user at several levels. The authentication process is made, for example, at the organization level, then at the team level and finally at the user level.

1.8. Authentication duration:

Regardless of the user authentication method, when the user fails to authenticate him in the defined authentication duration, the action is recorded as fraudulent and therefore access will be refused for him thereafter.

2. Models specific to Cloud

2.1. Trust

Trust is currently used in Cloud Computing as a means of authentication [16]. Depending on the adopted security policy and the trust level of the user, which judges his behavior, the authentication is accepted or refused.

2.2. Trusted third party (TTP)

A trusted third party (TTP) is an entity used in the context of the Cloud to facilitate and secure interactions between two parties (consumer and provider) that both trust this third party [17]. It can manage authentication, control access to resources, and more.

V. LITERATURE REVIEW

Throughout this section we are going to go through some different techniques and frameworks that have been done regarding authentication for cloud computing.

K. Ambekar et al. [8] in their paper they examined the effects of their suggested VPN-based improved security paradigm on computer systems. In the traditional security cloud approach, if an attacker gains access to the network, both the server's IP address as well as the server itself may become visible. This might compromise the user ids and the hashed passwords and servers will be more susceptible to further damage. They proposed a model that is divided into three areas the user side, public cloud side and private cloud side with a VPN firewall between the user and the cloud host.

A Live IP is allocated to the machine when a user is connected to the internet, and user provides the user name and password. A domain server is placed in the private cloud for additional security in charge of creating and authenticating users. After that the credentials are passed through the VPN firewall to the server for authentication, if it is successfully authenticated a One Time Password (OTP) generator is set in motion and the user will receive his OTP and use it for authentication again. A server containing a list of other servers located in the private cloud along with backup servers in case of failure. After that user is authenticated using a two factor authenticating techniques and selects any service available based on its authentication privileges. The user is redirected after the server retrieves the local IP address of the server hosting the requested service. The two factor authentication practice used lessens various types of attacks and increases security for cloud computing also the fact that the servers are placed in the private cloud increases security [8].

In the paper by R. Shahabadkar et, al. [11] a framework they applied two variable validation (2FA) access control and used the technique of secret key management over cloud. The main purpose is to assure an optimal security level for all concerned parties or actors. The over view idea of it divided into user key generation process and access authentication process, where the system divides the secret key and keeps one part over the client’s machine and the other is kept over a secured device. In order to execute extra security and make it nearly impossible for attackers to discover further split of the secured key, even in the event that the initial key split is compromised, this proposed approach leverages two factor authentications. Furthermore, a connection is made between the client's device and the anonymous key to prevent the client from using the device of another

Volume: 16 Issue: 04 Pages: 6515-6522 (2025) ISSN: 0975-0290

client for verification. It uses hashing of exponentials calculations and all the computations are done on the PC. When they were assessing the proposed framework it was found out that the used protocol is plausible for highly straightforward arrangement and is not functional for medium size strategy [11].

In order to assist fend off potential assaults; S. Ji et al. [12] suggested a schema to facilitate cloud login authentication that utilizes group signature. The main contributions of the proposed framework include:

- Supporting multi-user online identity authentication.
- Encouraging dynamic operations to satisfy the demands of the actual cloud platform.
- Ability to resist the impersonating attacks.

To perform the authentication function in the authentication scheme, which includes member registration and identity authentication, the structure is based on group signatures. The scheme has only one Group Manager (GM) in charge of managing the members and making sure the scheme is secure. It also includes a cloud server which is managed by a cloud server provider and Group members who are users desiring to bond with the system. The proposed model included identity authentication which is relocated from the group signature schema and group data sharing based on the bilinear map where the group manager requires two private keys for re-encrypting the key words. At first a member joins by sending a Join Request to the GM and when received it generates a value and send it to the member, followed by the generation of the private and public key. The GM then performs a calculation and check the result and see if its available in the predefined list. This makes sure that the identity authentication scheme can resist any impersonating attack [12].

M. Leila et al. [10] proposed a framework for authentication in cloud in their study which includes the creation of a virtual private network and the help of symmetric cryptographic of data. In the An algorithm was employed in the creation of the virtual private network phase, and when users attempted to connect to the VPN client, it asked for their user ID and password. Following this phase, the client will attempt to establish a connection to the security gateway. This process takes around 30 seconds, and occasionally the attempts are unsuccessful even after asking the login and password. The algorithm used is displayed bellow. The other part of the framework “Access with authentication” includes the user going to the internet and opening his URL and when this page opens another user Id and password are requested. In this procedure, the first client encrypts the password using Advanced Encryption Standard (AES) symmetric cryptography. It included two algorithms one to encrypt and one to decrypt displayed bellow.

The encryption algorithm:

```
INPUT (Table t and Key ky )
RESULT ( Table t edited)
method AES ( t,  ky )
start
key_Expansion (ky, tky );
ADD_Round_Key (t, tky [0];
for ( x=1; x < nr; x++)
Round (t, tky [nr] ) ;
last_Round (t, tky [nr] ) ;
end
```

The AES decryption algorithm is as follows:

```
AESDecrypt ( t , ky) {
key_Expansion (ky, Round_keys );
ADD_Round_Key (state, Round_Key [Nr] );
for ( r=Nr-1; x > 0; r - -)  {
Inv_shift_Rows ( T ) ;
Inv_Sub_Bytes ( T ) ;
ADD_Round_Key ( T , Round_Keys  [r] );
Inv_Mix_Columns ( T ) ;  }
Inv_shift_Rows ( out ) ;
Inv_Sub_Bytes (out) ;
ADD_Round_Key (out, Round_Key [0] );   }
```

By this solution only one user can be granted access to service but it takes a lot of time as it encrypts all the data which will be transferred in the cloud [3].

In paper [13] by M. Zhang et, al. they encouraged the growth of the Internet of things and suggested a cloud-based, two-dimensional code identification authentication system. The two-dimensional code technology that is being employed has a regular pattern and is set up similarly to how a computer recognizes the "0" and "1" sequence, which is similar to a bar code. Security measures and following, robust anti-loss, and very easy mobile device recognition are some of this code's features. Because error correction mechanisms are used throughout the coding and decoding process to ensure the integrity of the data, this sort of code has a good security performance but a low reliability. The used methodology included three parts the two-dimensional code registration process, Identity authentication process description, and server authentication. The two-dimensional coding registrations procedure entails providing the server with the information that has been encrypted using the encryption key before the information is decrypted and sent back. Subsequently, the code is received and decoded by the customer's mobile terminal. Only after obtaining the confirmation notification will the client account is enabled [13]. The next step in the relatively easy identity authentication procedure is for the user to log in. Then, the two-dimensional coding server uses the IP to construct a GUID while encrypting it. Following that is the scanning of the two-dimensional code then the user sends the requested ID and Hardware ID to server. Finally, the server confirms the relationship between them. The steps for schematic diagram of two-dimension code identification process are displayed in the following figure 2.

Volume: 16 Issue: 04 Pages: 6515-6522 (2025) ISSN: 0975-0290

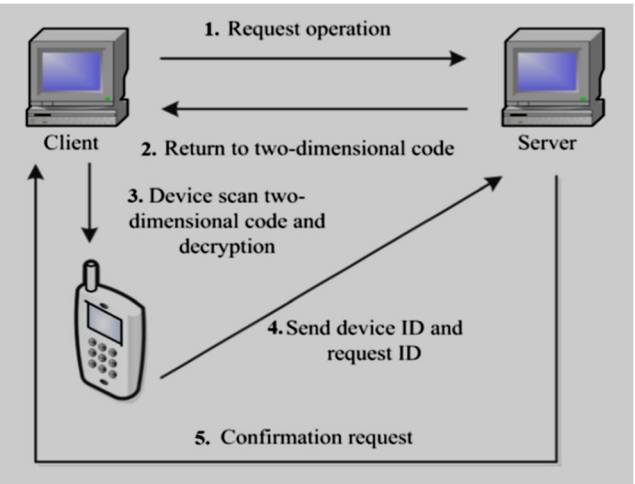

fig. 2: two-dimensional code identification

After that the Server authentication step is set in action and it includes the following [13]:

- Customer uses their mobile device to enter Id and password on the two dimensional code interface and carry out the symmetric key encryption. The information is to be verified after sent by the code in the client terminal.
- After the code decrypts the data that has been encrypted and generates the user's fixed-length briefs, an algorithm is run to produce the dynamic key.
- The user identity and databases in the two-dimensional code retrieve the comparable password. The dynamic key that is generated decrypts the password.
- The procedure's operation is performed for creating an appropriate dynamic key if the password entered in the previous stage is correct; if not, the process fails.
- The created dynamic key is used to carry on to encrypt files stored in the mobile terminal
- After that one-way hash operation is carried out to produce a new dynamic key.
- The symmetric algorithm for encryption then double-encrypts the data to produce a new two-dimensional code, which the customer's mobile terminal sends to the server along with the creation of an entirely novel secret key.
- The server continues decoding and decrypting the new code received, if the information is uniform the verification is successful otherwise the request is denied.

The use of the two times of the two dimensional code schemes increases the security and is simple and feasible with short code length [13].

M. Kumari and R. Nath [14] proposed a framework in their paper “Data Security Model in Cloud Computing Environment” to overcome some drawbacks in previous authentication models for cloud computing. They improved it through three phases categorization, storage and retrieval. [15] The categorization phase includes algorithm for data categorization and the storage phase comes after the categorization is successfully done. The data is sent to cloud storage with the public, confidential and sensitive data according to its categorization value [16] and after the integrity of data is checked using Message Authentication Code (MAC). MAC is mainly a hash code that is attached to the message in order to check on the integrity of data during the transmission [17]. If the data is manipulated during the conduction MAC will not harmonize with the message and the data is corrupted. [18, 19] The third phase is the Retrieval phase and it is divided with regards to the public, confidential and sensitive data. It is carried after the effective storage of data and each category uses a different mechanism as for the public data the password mechanism is followed and graphical password is used for the confidential data and OTP is used for the sensitive data. [20] The retrieval phase followed some guidelines for data access including [21-26]:

- Not allowing access to confidential and sensitive data to users on public data.
- Allowing access to confidential and public data if the user is granted access on sensitive data.

VI. COMPARATIVE STUDY

This section includes a comparison between the frameworks discussed in the review section.

Volume: 16 Issue: 04 Pages: 6515-6522 (2025) ISSN: 0975-0290

Table 1: Comparison between the frameworks

Author(s)	**Technique**	**Advantages**	**Disadvantages**
K. Ambekar et. al. [8]	• Using VPN to provide a secured authentication in addition to two factor authentication. • One Time Password (OTP) is sent to the user if ID and password are authenticated successfully after passing the VPN firewall.	• The use of VPN gives better response time than the conventional VPN. • The use of 2 key factor increase security. • The placement of servers in private cloud also increases security. • The packets on the network can be seen as a garbage value if sniffed.	• The model was only tested by three users due to limited resources
Geet Anjali Ch. & Jainul A.. [10]	• The framework creates a virtual deprived (VPN) between customer and provider and uses symmetric cryptographic. • The user accesses the cloud and the authentication algorithm used to encrypt and decrypt is of Symmetric Encryption Algorithm AES (Advanced Encryption standards).	• Increases the security of cloud environment especially authentication from a cryptographic point of view. • The use of AES algorithm allows only one user to access a service and increase the security. • All data being transferred is encrypted to increase security.	• Encryption of all data being transferred consumes a lot of time. • The framework proposed needs to incorporate the interoperability issue in cloud.
R. Shahabadkar et, al. [11]	• The framework uses two factor authentication, the technique of secret key management, and hashing calculations • The secret key is split into 2 different location.	• Enhances the mechanism of secure authentication. • Controls the communication system over cloud environment. • The framework is successful in case of straightforward arrangement.	• The is not functional for medium and large size strategies. • The framework needs to improve its effectiveness.
S. Ji et. al. [12]	• Support multi user authentication, dynamic operations, and resist impersonating attacks • Bilinear map is used to implement authentication • The used identity authentication is transplanted from the group signature scheme.	• The use of bilinear map makes it difficult to break the system due to the fact that it is mathematically hard to solve • The system can support the impersonating attack resistance • The scheme consumes less computation cost and can be easily used in different cloud applications.	• The framework efficiency needs to tested more and enhanced.
M. Zhang et. al. [13]	• The framework uses two-time two-dimensional code for authentication and is divided into 3 process including 1. Two-dimensional code registration 2. Identity authentication process 3. Server authentication • Two dimensional code is used to do the encryption via the public system. • User uses mobile to scan the code. • Unique identification IMEI (international mobile equipment identity number) is used as the authentication mode and is carried	• The two dimensional code is simple, feasible and promotes better security due to its complexity • The security is increased as each user has a different key • The increasing use of server – side in the verification process reduces the leakage of information • The design can transform the data by itself and doesn't need to bring its own encryption function. [27]	• Although the use of two dimensional code can sometimes lead to reducing the reliability • More attention needs to be given to the possibility of data modification which can create huge threats to the security of user information. [28] • A small amount of data is tampered with in the use of two time two dimensional code so the use of multiple encryption should be

Volume: 16 Issue: 04 Pages: 6515-6522 (2025) ISSN: 0975-0290

	out as secondary encryption to find the mutual authentication between mobile terminal and server • QR coding technology is also used and dynamic authentication of mobile terminal is realized by using two-dimensional code.		considered to increase security and reliability. [29]
M. Kumari et. al. [14]	• The proposed model is divided into 3 phases: categorization, storage and retrieval phase. • In the categorization phase the sensitivity of the data is calculated and accordingly the data is classified into public, confidential or sensitive. • In the storage phase each type of data uses a different level of security. MAC (message Authentication Code) hashing is used to assure data integrity before its sent to cloud for storage. • In the retrieval phase user uses different authentication techniques according to the categorization of data (including • passwords, graphical passwords & OTP).	• This model provides authentication, confidentiality, integrity, availability and security from cloud provider. • The user authentication is done by the data owner itself which reduces the issue of loss and has control over data access.	• The model is theoretical and has not been tested and nothing has been mentioned with regards to the time it takes to complete the whole process.

VII. CONCLUSION

This paper, highlighted the importance of providing high authentication in cloud computing. It also reviewed the past and the state of the art mechanisms and frameworks in the field of authentication in cloud computing environment. Various different authentication techniques have been used including password based authentication, two/three/multifactor authentication, symmetric authentication for encryption. These authentication techniques have been used differently in each framework to increase authentication. The different techniques used in each framework and advantages and disadvantages are summed up in a comparative format.

REFERENCES

[1]. Amira H., Mona N. & Walaa S. “The Future of Internet of Things for Anomalies Detection using Thermography”, International Journal of Advanced Networking and Applications (IJANA), Volume 11 Issue 03 Pages: 4294-4300 (2019) ISSN: 0975-0290

[2]. Amira H., Mona N., & Basant S. “The Principle Internet of Things (IoT) Security Techniques Framework Based on Seven Levels IoT’s Reference Model” Proceedings of Internet of Things—Applications and Future ITAF 2019. Springer publisher, Part of the Lecture Notes in Networks and Systems book series (LNNS, volume 114)

[3]. Amira H. " Internet of Things (IoT) Technologies for Empowering E-Education in Digital campuses of Smart Cities.”, International Journal of Advanced Networking and Applications (IJANA), Volume 13 Issue 2, pp. Pages: 4925-4930(2021).

[4]. Amira H. A. “Recovery and Concurrency Challenging in Big Data and NoSQL Database Systems”, International Journal of Advanced Networking and Applications (IJANA), Volume 11 Issue 04, pp. Pages: 4321-4329 (2020).

[5]. Mona N. & Amira H., “Business Intelligence (BI) Significant Role in Electronic Health Records - Cancer Surgeries Prediction: Case Study ”, International Journal of Advanced Networking and Applications (IJANA), Volume: 13 Issue: 06 Pages: 5220-5228(2022) ISSN: 0975-0290.

[6]. Amira H., Mona Nasr, Laila Abd Elhamid & Laila El-Fangary " Applications of IoT in Smart Grids using Demand Respond for Minimizing On-peak load”, International Journal of computer science and information security (IJCSIS). Vol. 19. No. 8. (2021).

[7]. Mohamed Attia & Amira H. " A comprehensive investigation for Quantifying and Assessing the Advantages of Blockchain Adoption in Banking industry". IEEE. 2024 6th International Conference on Computing and Informatics (ICCI), pp. 322-33.doi: 10.1109/ICCI61671.2024.10485028.

[8]. Kamatchi R., K. A. (2023). Enhanced User Authentication Model in Cloud Computing Security . Springer International Publishing AG. DOI 10.1007/978-3-319-47952-1_26

[9]. DeepaPanse P. Haritha, "Multi-factor Authentication in Cloud Computing for Data Storage Security", International Journal of

Volume: 16 Issue: 04 Pages: 6515-6522 (2025) ISSN: 0975-0290

Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 8, August 2023 ISSN: 2277 128X

[10]. Geet Anjali Ch. & Jainul A., "Modified Secure Two Way Authentication System in Cloud Computing Using Encrypted One Time Password", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2024, 4077-4080

[11]. shahabadkar, R., Reddy, S. S., Manjunath, C., & Channabasava, U. (2023). Secure Framework of authentication mechanism over cloud enviroment. Springer International Publishing

[12]. Ji , S., Liu, D., & Jian A. (2024). Exploting Group signature to implement user authentication in cloud computing .China : Springer Nature Singapore PTE LTD.

[13]. Zhang, M., Ma, Z., & Zhang, Y. (2023). An identity authentication scheme based on cloud computing enviroment . (CrossMark, Ed.) NEw York: Springer Science and Business Media New York.

[14]. Kurmari , M., & Nath , R. (2022). Data Security Model in Cloud Computing Enviroment . India: Springer Nature Singapore.

[15]. Amira H., Mona Nasr & Laila Abd Elhamid “A conceptual Framework for Minimizing Peak Load Electricity using Internet of Things”, International Journal of Computer Science and Mobile Computing , Vol. 10. No. 8. pp: 60-71. (2021).

[16]. Amira H., Faris H. Rizk, Ahmed Mohamed Zaki, Ahmed M. Elshewey. " The Applications of Digital Transformation Towards Achieving Sustainable Development Goals: Practical Case Studies in Different Countries of the World". Journal of Artificial Intelligence and Metaheuristics (JAIM). Vol. 07, No. 01, PP. 53-66, (2024)

[17]. Marwa S., Amira H., & Mahmoud A.. “The Success Implementation CRM Model for Examining the Critical Success Factors Using Statistical Data Mining Techniques” International Journal of Computer Science and Information Security (IJCSIS), Vol. 15, No. 1, .p: 455 – 475 (2017).

[18]. Amira H., & Essam M.. "Modeling Deep Neural Networks for Breast Cancer Thermography Classification: A Review Study ." International Journal of Advanced Networking and Applications (IJANA), Volume 13 Issue 2, pp. :4939-4946(2021).

[19]. Amira H. Abed. " Deep Learning Techniques for Improving Breast Cancer Detection and Diagnosis", International Journal of Advanced Networking and Applications (IJANA), Volume 13 Issue 06, pp. : 5197-5214(2022) ISSN: 0975-0290.

[20]. Amira H., Essam M., Om Prakash j. & Ahmed A.. "A Comprehensive Survey on Breast Cancer Thermography Classification Using Deep Neural Network ", Machine Learning and Deep Learning in Medical Data Analytics and Healthcare Applications. book. routledge, CRC Press, Taylor and Francis Group Pages: 250-265 (2022).

[21]. Naglaa S. & Amira H., “Big Data with Column Oriented NOSQL Database to Overcome the Drawbacks of Relational Databases”, International Journal of Advanced Networking and Applications (IJANA), Volume 11 Issue 5, pp. Pages: 4423-4428 (2020).

[22]. Amira H., & Mona N. “Diabetes Disease Detection through Data Mining Techniques”, International Journal of Advanced Networking and Applications (IJANA), Volume 11 Issue 1, pp. Pages: 4142-4149 (2019).

[23]. Marwa S., Amira H., & Mahmoud A. “A systematic review for the determination and classification of the CRM critical success factors supporting with their metrics”. Future Computing and Informatics Journal. Vol:(3). pp:398-416. (2018)

[24]. Amira H. A. & bahloul, M. (2023) "Authenticated Diagnosing of COVID-19 using Deep Learning-based CT Image Encryption Approach," Future Computing and Informatics Journal: Vol. 8: Iss. 2, Article 4.

[25]. Ahmed M. , Sayed M. , Amel A., Marwa R. & Amira H. Abed. Optimized Deep Learning for Potato Blight Detection Using the Waterwheel Plant Algorithm and Sine Cosine Algorithm. Potato Res. (2024). https://doi.org/10.1007/s11540-024-09735-y

[26]. Amira H. Abed. "The Applications of Deep Learning Algorithms for Enhancing Big Data Processing Accuracy". International Journal of Advanced Networking and Applications (IJANA), Volume: 16 Issue: 02 Pages: 6332-6341 (2024) ISSN: 0975-0290.

[27]. Amira H., Ahmed A. &Mohamed M. "Authentication in Cloud Computing Environments", Multicriteria Algorithms with Applications, Vol. 5 (2024), pp:59–67

[28]. Amira H. & Hany F." The Evaluation of Electronic Human Resources (eHR) Management based Internet of Things using Machine Learning Techniques", International Journal of Advanced Networking and Applications, Volume 16 Issue 03, pp.: 6437-6452 (2024) ISSN: 0975-0290.

[29]. Amira H. "Enhancing Big Data Processing Performance using Cutting-Edge Deep Learning Algorithms,” Al-Ryada Journal for Computational Intelligence and Technology (ARJCIT), Vol. 1 - (1) – 2024, PP: 39: 53.