





Paper Type: Original Article

## Authentication in Cloud Computing Environments

Amira Hassan Abed <sup>1</sup> , Ahmed Abdelhafeez <sup>2,3,\*</sup>  and Mohamed M. Fouad <sup>4</sup> 

<sup>1</sup> Business information systems, Faculty of Business Administration, AL RYADA University for Sciences and Technology, Cairo, Egypt; [Amira.hassan@rst.edu.eg](mailto:Amira.hassan@rst.edu.eg).

<sup>2</sup> Department of Computer Science, Faculty of Information System and Computer Science, October 6 University, Giza, 12585, Egypt; [aahafeez.scis@o6u.edu.eg](mailto:aahafeez.scis@o6u.edu.eg).

<sup>3</sup> Applied Science Research Center. Applied Science Private University, Amman, Jordan, [a\\_abdelhafeez@asrc.asu.edu.jo](mailto:a_abdelhafeez@asrc.asu.edu.jo).

<sup>4</sup> Carleton University, Canada; [mmafoad@sce.carleton.ca](mailto:mmafoad@sce.carleton.ca).

Received: 02 Sep 2024

Revised: 21 Oct 2024

Accepted: 17 Nov 2024

Published: 19 Nov 2024

### Abstract

One solution that helps with straightforward, anytime, anywhere accessibility to reconfigurable computational capabilities is cloud computing. Users of this computing platform are genuinely concerned about security and need to find dependable providers of cloud services. Authentication is believed to be a main necessity for assuring secure cloud access. In this paper, we discussed the comprehensive and detailed frameworks constructed to assure successful authentication in cloud computing. Also, this survey paper discusses differences between considered techniques used in different frameworks.

**Keywords:** Cloud Computing; Authentication; Cloud Services; Security in Cloud.

## 1 | Introduction

The revolutionary state-of-the-art cloud computing technology offers a huge list of assistance for all businesses and organizations. It helps the organization adopt cloud computing by reducing the cost and the complexity of the infrastructure of the provided platforms [1]. Cloud computing has become 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 with standard service offered; yet, evaluating the 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 one of the core necessities for ensuring secure access to the cloud [4]. This is because authentication is considered the main aspect of security. This paper will include an overview of cloud computing and, a security overview including different authentication methods, followed by that will be a literature review of some of the proposed models and frameworks to oversee authentication and a comparison between them.



Corresponding Author: [aahafeez.scis@o6u.edu.eg](mailto:aahafeez.scis@o6u.edu.eg)



<https://doi.org/10.61356/j.mawa.2024.5429>



Licensee **Multicriteria Algorithms with Applications**. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

## 2 | Cloud Computing

To understand the risks to cloud technology security we must understand the characteristics of the 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 authority over the services without the involvement of the service suppliers.
- 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 resources, 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 their capacity seems to be boundless.

Cloud computing comes in three kinds: hybrid, private, and public [6]. A cloud that is publicly accessible is a type of computing environment where the services supplier owns and maintains the physical infrastructure, 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 cloud services, there are available types 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 software apps, customers must pay. While for PaaS only the platform or stack of solutions is available, and users can save investment on hardware and software. Finally, is the SaaS where the provider gives uses the service of using software [5].

## 3 | Security of Cloud Environment

Security threats are a huge factor to take into consideration before transferring to a cloud environment and assessing the advantages versus the disadvantages to measure the amount of risk that might be faced by the organization. Some of the major risks in cloud computing are 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 the user's identity is plotted against access privileges roles for resources [8].

### 3.1 | Authentication

Recently authentication process has followed new techniques to provide a more rigorous and stricter environment including PIN/password authentication, one-time password-based authentication, Encryption, and biometrics-based authentication [8].

- PIN/Password-based authentication: This is considered the most straightforward authentication technique, where the 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 Authentication: 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 must use a smart card that is familiar to the system then after that he uses his User ID and Password for authentication [9].
- Encryption which includes Public Key authentication and Symmetric authentication.
- Biometrics-based authentication: users can use physiological characteristics to authenticate themselves, like figure prints, face recognition, or voice recognition [9].

## 4 | Literature Review

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

K. Ambekar et al. [8] in their paper 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, and private sides with a VPN firewall between the user and the cloud host.

When a client links to the internet, a Dynamic IP address is assigned to the device, and the User enters identity and login. 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 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 technique 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 the cloud. The main purpose is to assure an optimal security level for all concerned parties or actors. The overview idea of it divided into the 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. To execute extra security and make it nearly impossible for attackers to discover further split of the secured key, even if the initial key split is compromised, this proposed approach leverages two-factor authentication. Furthermore, a connection is made between the client's device and the anonymous key to prevent the client from using the device of another client for verification. It uses hashing of exponential calculations, and all the computations are done on the PC. When they were assessing the proposed framework, it was found that the used protocol is plausible for a highly straightforward arrangement and is not functional for a medium-sized strategy [11].

To assist fend off potential assaults, S. Ji et al. [12] suggested a schema to facilitate cloud login authentication that utilizes group signatures. 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 enrolment and verification of identification, the structure is based on group signatures. The scheme has only one Group Manager (GM) in charge of overseeing the participants and making sure the system is secure. It also has a remote cloud server that a cloud supplier manages and Group members who are users desiring to bond with the system. The proposed model included verification of identity, which has been relocated via the signing schema and group data sharing based on the bilinear map where the manager requires 2 keys for re-encrypting the keywords. At first, a member joins by sending a Join Request to the GM and when received it generates a value and sends it to the member. Followed by the generation of a private and public key. The GM then performs a calculation, checks the result, and sees if it's available in the predefined list. This makes sure that the identity authentication scheme can resist any impersonating attack [12].

M. Leila et al. [3] proposed a framework for authentication in the cloud in their study which includes the creation of a virtual private network and the help of symmetric cryptography of data. The 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 for the login and password. The algorithm used is displayed below. 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 below.

#### 4.1 | The Encryption Algorithm

INPUT (Table t and Key ky)

RESULT (Table t edited)

method AES (t, ky)

start

key\_Expansion (ky, ky).

ADD\_Round\_Key (t, tky [0]).

for (x=1; x < nr; x++)

Round (t, tky [nr]).

last\_Round (t, tky [nr]).

end

#### 4.2 | The AES Decryption Algorithm

AESDecrypt (t, ky) {

key\_Expansion (ky, Round\_keys).

ADD\_Round\_Key (state, Round\_Key [Nr]).

for (r=Nr-1; r > 0; r - -) {

Inv\_shift\_Rows (I).

Inv\_Sub\_Bytes (I).

ADD\_Round\_Key (I, Round\_Keys [r]).

Inv\_Mix\_Columns (I);} }

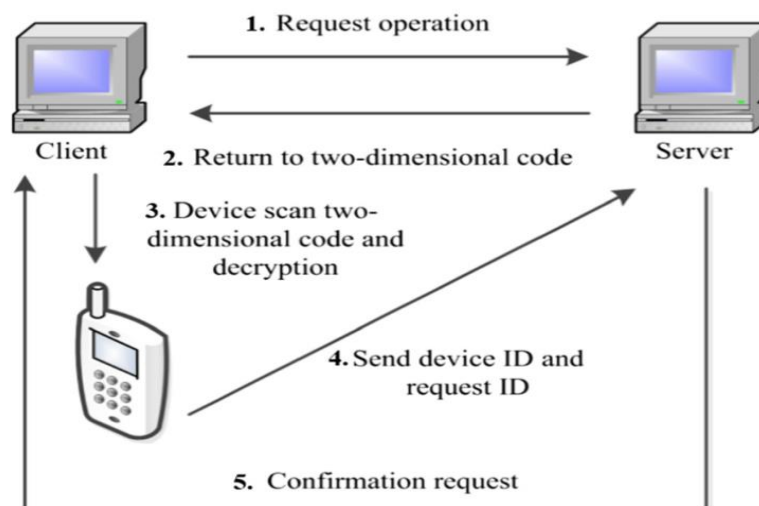
Inv\_shift\_Rows (out).

Inv\_Sub\_Bytes (out).

ADD\_Round\_Key (out, Round\_Key [0]);}

This method only allows a single individual to log into the service at a time, but it's quite time-consuming, as it encrypts all the data that will be transferred to the cloud [3].

In a paper [13] by M. Zhang et al. they encouraged the growth of the IoT concept and suggested a cloud-based, 2D coding identification authentication system. The 2D coding method that is being employed has a consistent direction and is set up similarly to how a computer recognizes the "0" and "1" sequences, which is like 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 registration 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 be enabled [13]. The next step in the 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 client provides the server with the desired Identity and Device Identity. Finally, the server confirms a relationship between them, see Figure 1.



**Figure 1.** Two-dimensional code identification.

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

- The customer uses their mobile device to enter their ID and password on the 2D coding interface and apply symmetrical key protection.
- 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.
- The user identity and databases in the 2D coding retrieve A comparable passcode. The dynamic key that is generated decrypts the password.

- The procedure's operation is done to create 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 continue encrypting data on mobiles.
- A new variable key is then created by performing a simple hashing operation.
- The Asymmetrical security technique then double-encrypts the data to produce a new two-dimensional code, which the device sends to the server along with the creation of an entirely novel secret key.
- The server continues decoding and decrypting the new code received, the test of authenticity is successful if the data is consistent; if not, the inquiry is rejected. [13].

M. Kumari and R. Nath [14] proposed a framework to overcome some drawbacks in previous authentication models for cloud computing. They made three stages of improvements: classification, storing, and retrieving. [15] The categorization phase includes an algorithm for data categorization and the storage phase comes once the categorization is completed. 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 the data is checked using Message Authentication Code (MAC). In this case, the message's MAC hash code is used to verify the data's integrity while it is being transmitted. [17] Data corruption results from data manipulation while transmission since the MAC fails to synchronize with the message. [18] The third phase is the Retrieval phase, which is divided into public, confidential, and sensitive data. [19] It is carried out after the effective storage of data and each category uses a different mechanism for the public data the password mechanism is followed, and a 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]:

- Not allowing access to confidential and sensitive data to users on public data [22].
- Allowing access to confidential and public data if the user is granted access to sensitive data [23].

## 5 | Comparative Study

This section includes a comparison between the frameworks discussed in the review section as presented in Table 1.

**Table 1.** Comparison between the frameworks.

Author(s)	Technique	Advantages	Disadvantages
<b>K. Ambekar et. al. [8]</b>	<ul style="list-style-type: none"> <li>• Providing a secure login by employing VPN in addition to two-factor authentication.</li> <li>• An OTP (one-time password) gets transmitted to the user if the ID and password are authenticated successfully after passing the VPN security system.</li> </ul>	<ul style="list-style-type: none"> <li>• Using a VPN improves reaction time over using a traditional Network. <ul style="list-style-type: none"> <li>• If any data over the system is sniffed, it may be viewed as spam.</li> </ul> </li> <li>• The two key factors increase security.</li> <li>• The placement of servers in a private cloud also increases security.</li> </ul>	<ul style="list-style-type: none"> <li>• The model was only evaluated by three users due to limited resources.</li> </ul>
<b>R. Shahabadkar et, al. [11]</b>	<ul style="list-style-type: none"> <li>• The framework uses two-factor authentication, the technique of secret key management, and hashing calculations.</li> <li>• The secret key is split into 2 different locations.</li> </ul>	<ul style="list-style-type: none"> <li>• Enhances the mechanism of secure authentication.</li> <li>• Controls the communication system over the cloud environment.</li> <li>• The framework is successful in the case of straightforward arrangement.</li> </ul>	<ul style="list-style-type: none"> <li>• The is not functional for medium and generous-size strategies.</li> <li>• The framework needs to improve its effectiveness.</li> </ul>



<p><b>S. Ji et. al. [12]</b></p>	<ul style="list-style-type: none"> <li>• Support multiuser authentication, and dynamic operations, and resist impersonating attacks.</li> <li>• The bilinear map is used to implement authentication.</li> <li>• The used identity authentication is transplanted from the group signature scheme.</li> </ul>	<ul style="list-style-type: none"> <li>• The use of a bilinear map makes it difficult to break the system since it is mathematically hard to solve.</li> <li>• The system can support the impersonating attack resistance.</li> <li>• The scheme consumes less computation cost and can be easily used in different cloud applications.</li> </ul>	<ul style="list-style-type: none"> <li>• The framework efficiency needs to be tested more and enhanced.</li> </ul>
<p><b>M. Leila et, al. [3]</b></p>	<ul style="list-style-type: none"> <li>• The framework creates a virtual deprived (VPN) between customer and provider and uses symmetric cryptography.</li> <li>• The user accesses the cloud, and the authentication algorithm used to encrypt, and decrypt is of Symmetric Encryption Algorithm AES (Advanced Encryption standards).</li> </ul>	<ul style="list-style-type: none"> <li>• Increases the security of the cloud environment, especially authentication from a cryptographic point of view.</li> <li>• The AES algorithm allows only one user to access a service and increases security.</li> <li>• All data that is being transferred is encrypted to increase security.</li> </ul>	<ul style="list-style-type: none"> <li>• Encryption of all data being transferred consumes a lot of time.</li> <li>• The framework proposed needs to incorporate the interoperability issue in the cloud.</li> </ul>
<p><b>M. Zhang et. al. [13]</b></p>	<ul style="list-style-type: none"> <li>• The framework is made up of three processes, the first of which is the 2-D code register.             <ol style="list-style-type: none"> <li>1. It uses two-time 2-D codes for authentication.</li> <li>2. The procedure for authentication of identity</li> <li>3. Authentication of servers</li> </ol> </li> <li>• The open system is used to encrypt data using two-dimensional coding.</li> <li>• The user scans the identification number with a smartphone.</li> <li>• Distinctive identity to determine mutual authentication between the mobile terminal and server, IMEI (international mobile equipment identifying number) is utilized as the identification method and is conducted as secondary encryption.</li> <li>• A 2-dimension codes are employed to achieve dynamic identification of mobile terminals, and QR code technique has been utilized.</li> </ul>	<ul style="list-style-type: none"> <li>• The 2-D code is simple, and feasible and promotes better security due to its complexity.</li> <li>• The security is increased as each user has a different key</li> <li>• The increasing use of server-side in the verification process reduces the leakage of information.</li> <li>• The design can transform the data by itself and doesn't need to bring its encryption function.</li> </ul>	<ul style="list-style-type: none"> <li>• Although the use of 2-Dcode can sometimes lead to reducing the reliability</li> <li>• More attention needs to be given to the possibility of data modification which can create huge threats to the security of user information.</li> <li>• A small amount of data is tampered with in the use of two-time 2-D code so the use of multiple encryptions should be considered to increase security and reliability.</li> </ul>
<p><b>M. Kumari et. al. [14]</b></p>	<ul style="list-style-type: none"> <li>• The proposed model is divided into 3 phases: categorization, storage, and retrieval phase.</li> <li>• In the categorization phase, the sensitivity of the data is calculated and accordingly, the data is classified as public, confidential, or sensitive.</li> <li>• In the storage phase, each type of data uses a different level of security. MAC (Message Authentication Code) hashing is used to ensure data integrity before it is sent to the cloud for storage.</li> <li>• In the retrieval phase user uses different authentication techniques according to the categorization of data (including passwords, graphical passwords &amp; OTP).</li> </ul>	<ul style="list-style-type: none"> <li>• This model provides authentication, confidentiality, integrity, availability, and security from cloud providers.</li> <li>• The data owner does the user authentication itself which reduces the issue of loss and has control over data access.</li> </ul>	<ul style="list-style-type: none"> <li>• The model is theoretical and has not been evaluated and nothing has been mentioned with regards to the time it takes to complete the full process.</li> </ul>

## 6 | 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 environments. Various authentication techniques have been used including password-based authentication, two/three/multifactor authentication, and 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 the advantages and disadvantages are summed up in a comparative format.

## Acknowledgments

The author is grateful to the editorial and reviewers, as well as the correspondent author, who offered assistance in the form of advice, assessment, and checking during the study period.

## Author Contributions

All authors contributed equally to this work.

## Funding

This research has no funding source.

## Data Availability

The datasets generated during and/or analyzed during the current study are not publicly available due to the privacy-preserving nature of the data but are available from the corresponding author upon reasonable request.

## Conflicts of Interest

The authors declare that there is no conflict of interest in the research.

## Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

## References

- [1] 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 Principal Internet of Things (IoT) Security Techniques Framework Based on Seven Levels IoT's Reference Model" Proceedings of the 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 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., "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. 322-333.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 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 environment. Springer International Publishing
- [12] Ji , S., Liu, D., & Jian A. (2024). Exploiting 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 a cloud computing environment. (CrossMark, Ed.) New York: Springer Science and Business Media New York.
- [14] Kurmari, M., & Nath, R. (2022). Data Security Model in Cloud Computing Environment. India: Springer Nature Singapore.
- [15] 1Mona 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] 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., 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] Essam M 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] 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. "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] 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., & 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).

**Disclaimer/Publisher's Note:** The perspectives, opinions, and data shared in all publications are the sole responsibility of the individual authors and contributors, and do not necessarily reflect the views of Sciences Force or the editorial team. Sciences Force and the editorial team disclaim any liability for potential harm to individuals or property resulting from the ideas, methods, instructions, or products referenced in the content.