Secure Login Using Multi-Tier Authentication Schemes in Fog Computing

Awais Manzoor, Abdul Wahid, Munam Ali Shah, Adnan Akhunzada, Faisal Fayyaz Qureshi

Department of Computer Science
COMSATS Institute of Information Technology
Islamabad, Pakistan
malik.awaismanzoor@yahoo.com, abdulwahid@comsats.edu.pk, a.qureshi@comsats.edu.pk, mshah@comsats.edu.pk,

Abstract

Security threats are major barriers in authentication process in Fog Computing. Identification of a user through single sign-on process like simple password-based authentications are no longer considered secure. Different multi-tier authentication schemes exist in literature that overcome the weakness of single sign-on. This paper surveys state-of-the-art multi-tier authentication techniques, their vulnerabilities, security threats and their solution proposed over the period of 2012-2016. We compare the performance of existing multi-tier authentication schemes on three parameters, i.e., cost, usability and level of security. Multi-tier authentication schemes have been categorized into groups according to the factors involved in the authentication process. Lastly, we aim to provide an easy and concise view of the underlying authentication model adapted by each approach.

Keywords: Authentication, Multi-tier Authentications, Cloud computing, Multifactor authentications, cloud security.

Received on 28 May 2017, accepted on 08 July 2017, published on 26 July 2017

doi: 10.4108/eai.26-3-2018.154382

1. Introduction

Cloud computing is emerging technology providing on-demand services including online storage, platform and software as service. Security threats have also raised with advancement of cloud technologies like malicious insider attack, data loss and privacy breach. Security of cloud computing has become a major area of research since last few decades [1]. Cloud networks are vulnerable to a variety of attacks and security challenges. Cloud server must identify users before allowing them access to cloud resources. Authentication schemes are the key procedure to identify users, which may be implemented through different techniques like password, biometric verification, public key infrastructure, and symmetric key based authentication schemes [2][3]. Single sign-on authentication schemes are insecure and vulnerable to variety of attacks like Man-in-the-Middle attacks and dictionary based attacks [4]. When users are allowed to choose their own passwords, they choose easily rememberable passwords and that can be easily guessed. 75% people use same password for multiple resources and 50% of users are hacked via phishing attack [5]. Dropbox passwords were hacked in 2015 and user lost their confidentiality [6]. In 2013, 44% of cloud service providers lost their data due to brute force attack [7].

Since 2011, security is taken as high priority task [4]. Some authors suggest using multi-tier authentications to improve security infrastructure. Multi-tier authentication schemes are more secure than single sign-on schemes, as user has to pass multiple steps before accessing cloud resources. Figure 1 shows the working flow of multi-tier authentication schemes. Multi-tier authentications keep victim's account secure even if a hacker has obtained victim's password but he has not hold of next authentication factor [8][9]. This has reduced the incidence of security theft because password is not enough to give hacker access to information. The objective of multi-tier authentication schemes is to provide a layered defense making it difficult for an attacker to access the target. If one factor is compromised, there is at least one more barrier for an attacker to breach before successfully entering into the target.

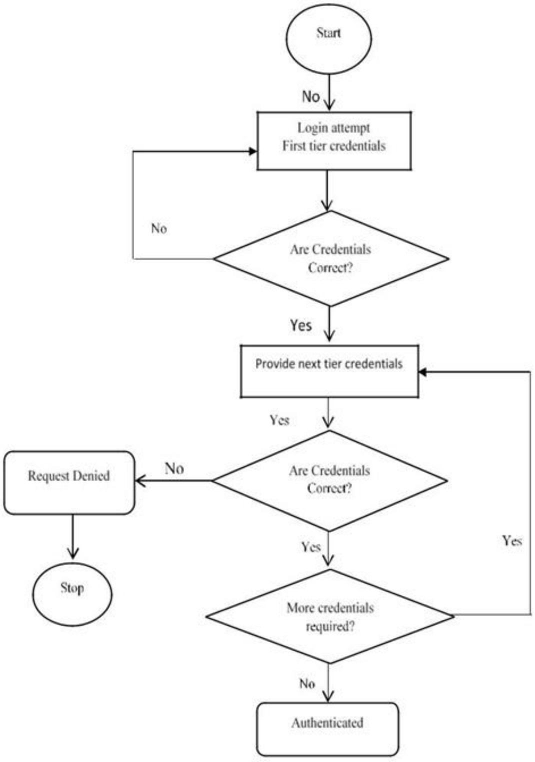


Fig. 1 work flow of Multi-tier

This paper focuses on secure and highly usable authentication techniques, based on multi-tier architecture. Each technique comes up with certain advantages and limitations. A detailed analysis of surveyed techniques performed in this paper and these techniques have been evaluated based on cost, complexity and usability. The rest of the paper is organized as follows. Next section contains literature review. Then evaluation and analysis of surveyed techniques is given in section III and finally section IV contains results and future work.

2. Literature review

With the advancement of technology, there is a tremendous need of strong authentication schemes. Researcher proposed different multi-tier and multifactor authentication schemes to provide strong security for cloud computing networks. Some multi-tier authentication schemes use one-time password while others are based on biometric scan, QR code or graphical pattern. A review of most recent multi-tier authentication schemes from period of 2012-2016 is given below.

A. One-time Password (OTP)

OTP can be implemented using various techniques and valid for short time period and can be used just for one login session. *R. K. Banyal et al.* classified cloud services and resources into three levels i.e. low, medium and high level [3]. This scheme uses arithmetic captcha, OTP and IMEI number of registered for authentication.

- *Low level authenticatio*n: Low level authentication is based on username, password and arithmetic captcha and user is granted access to use low level resources.
- *Medium Level authentication:* In addition to user name, password and arithmetic captcha, one-time password (OTP) for accessing medium level cloud resources and services.
- *High level authentication*: This level uses all three factors for authentication. First is arithmetic captcha, second is OTP and third is IMEI of registered mobile phone. IMEI is divided into small chunks of two digits and ask user to provide three random segments. On verification user is granted full access to all cloud resources and services.

K. Hussein et al. secured OTP by adding another security layer to ensure identity of the user[10]. User proves his identity by providing his personal information previously registered with system i.e. mobile number, IMEI and PIN to receive OTP. Single mobile number and IMEI can't be associated with multiple accounts. Strength of this scheme is that if hacker manage to get username and password and steals configured mobile, still unable to access user's account but extra hardware is required for sending OTP and IMEI is also not very secure as it is known to mobile network operators[11].

Image based OTP (imOTP) proposed in [12] requires out of band channel for sending imOTP on smart phone which is pre-registered with cloud server but author has not addressed confidentiality and integrity.

B. Smart phone for Authentication

S. Kumar et al. [13] authentication scheme is based on OTP using personal registered device interface for entering OTP. On verification of OTP through registered device interface, direct communication starts between client and server.

Authentication scheme in [14] for financial transactions, which is using near field communication (NFC), biometric and PIN . For making transactions, smart phone app is used to enter amount and then receiver's details are fetched through NFC. Face picture of sender will be taken and on successful verification, 4 digits PIN are used for authentication to complete transaction. User inconvenience is limitation of this scheme.

K. Virgile *et al.* [15] make use of App stored in smart phone for generating OTP and sending to cloud server. User will get access if OTP come from registered MAC address.

C. Risk based authentication

Risk based authentication calculates risk score associated with login information. Risk is calculated for device specific information or behavioral and location based information [16]. Access manager sends script to device using webserver and gathers device information and calculates risk score. If risk is below the threshold value, then user is allowed to access cloud services otherwise multilevel authentication is carried out. If risk score is higher, QR-code is transferred to user through user through email or SMS service. Pseudo random number generator algorithm generates dynamic QR code with randomness. Limitation of risk based authentication scheme is user's connection profile has to be detected for calculating risk score and improper detection may lead to unauthorized access.

D. Biometric authentication

Biometric authentication may be based on physical, psychological or behavioral characteristics. Biometric scanner is required for scanning person's physical biometric characteristics. Biometric characteristics include finger print, voice recognition, iris scan, or face recognition.

E. Osei et al. [17] used registered mobile phone for biometric input. Authentication server embeds login link to registered mobile phone to allow biometric scan. In case of registered mobile lost, email account is used as alternative. Login link is send to email account and any computing device with embedded biometric scanner can be used for authentication. This scheme is resistant to many type of attacks as it requires predefined mobile device for scanning biometric information.

M. M Mohammad et al. [18] added SMS based authentication as an additional layer to biometrics for online transactions. This scheme out of band channel for sending OTP which can result is delays in case of network failure. It also adds hardware cost.

Biometric scan along access code presented in [19] where all communication is encrypted with RSA algorithm. User provides provide biometric scan and receives access code in email. On verification user will be authenticated and issued authorization certificate. Author has made certain assumption about owner of data that he has knowledge of binary code implementation. Physical biometric characteristics may change or damage and may by photographed [20].

E. Graphical password

Graphical password is based on selecting images in specific order or forming certain patterns. Graphical passwords are more secure than textual passwords but require more space for storing images.

R. Kaur et al. [21] technique allow overlapping pattern and shuffling geometric shapes. In first step 3X3 image grid where user selects four images combination while in second step 3X3 grid containing 9 clue point is displayed. User is required to combine these points to draw password pattern to get high level authentication. This scheme is based on overlapping pattern which reduce the risk of surfing attack but pattern is statics.

S.M Gurav et al. [22] uses combination of username and image based password. Alphabetic images are provided in same order as position of characters in username. A number of series is generated based on alphabetic images which are used for authentication purpose.

F. Smart card based authentication

N. Harini et al. [23] proposed two factor authentication "2CAuth" by integrating smart card and QR based authentication. Smart card generates random number and encrypts it into QR-code. Registered mobile phone decrypts QR-code by getting one pin from registered mobile and other from user. This decrypted QR-code is used for completing transactions.

In [24] authors proposed "3CAuth" and integrated smart card, secret pin, biometric and mobile phone based authentication. User insert smart card and provide finger print, then decrypts QR-code using his registered mobile phone to obtain OTP. It also takes into account timestamp for submitting QR-code. It is secure to replay, phishing and denial of service attack.

S. Ahmad et al. encoded textual password and biometric information in smart card [25]. Client inserts smart card into card reader and provides his textual password and biometric scan. Cloud server matches user information with information encoded in smart card. Possession of smart card is limitation of this technique as user has to carry it with him.

G. 3D password

3D password is combination of recognition and recall based attributes. *T. Naik et al.* [26] proposed a novel method for authentication which is based on combination of textual, graphical and biometric password. This scheme contains many options for multi-level authentication like sequence of activities, graphical password, textual password or biometric scan. User is free to choose any number of combination among the available option.

3D password scheme proposed in [27] where user performs sequence of activities while navigating through a 3D virtual environment. 3D quick hull algorithm is used for point selection which is based on convex hull algorithm. No additional hardware is required for this scheme.

P. C. Talhan et al. presented 4D password in [28] to strengthen 3D password with gesture recognition. User perform gestures for entering into 3D environment. Time window is associated with gestures to ensure the legitimacy of user. Authentication schemes based on 3D virtual environment are slower and require more disk space.

H. Sequence of activities

Authentication scheme based on sequence of activities, where activities include menu activity, mouse activity or text field activity proposed in [29]. This scheme focuses on secure use of third party server. User first enters his user name and password which are send to server for verification and initiate application program. Data from fake database is taken to load fake screen into browser where user perform sequence of predetermined activities. If sequence performed by user is correct then original screen is loaded and direct communication between client and server begins. Advantage of this scheme is that no extra hardware is needed.

In [30] puzzle solving scheme proposed, based on textual password and predetermined activities. User solve puzzle in a specific pattern in given time stamp. If sequence matches, then user get authenticated to use cloud services. Predetermined activity based schemes use static pattern which can be identified by attacker.

I. Multilevel authentication

Authentication scheme proposed in [31] and [32] generates and use password at multiple levels to access cloud services.

In [31], author categorizes cloud administrative panel into multiple levels according to critical administrative areas. Decision logic is responsible for accepting for denying login request. Level 1 uses password and unique identification number whereas in level 2, grid of 3x3 is displayed for graphical pattern. User select image in sequence and then provide unique identification number to access services.

H. A. Dinesha et al. [32] proposed multilevel authentication scheme for cloud platform. This scheme generates password at multiple levels and is acts as middleware authentication technique. To enable strict authentication and authorization, passwords are generated at multiple levels of organization.

- First level is the organization level. Organizational password is required at this level for authentication. After successful authentication second level authentication is required.
- Second level is the team level. Team password is required at this level for authentication. After successful authentication, user level authentication is carried out.
- Third Level is last level of authentication which is the user level. User is required to provide his password for gaining full access to resources.

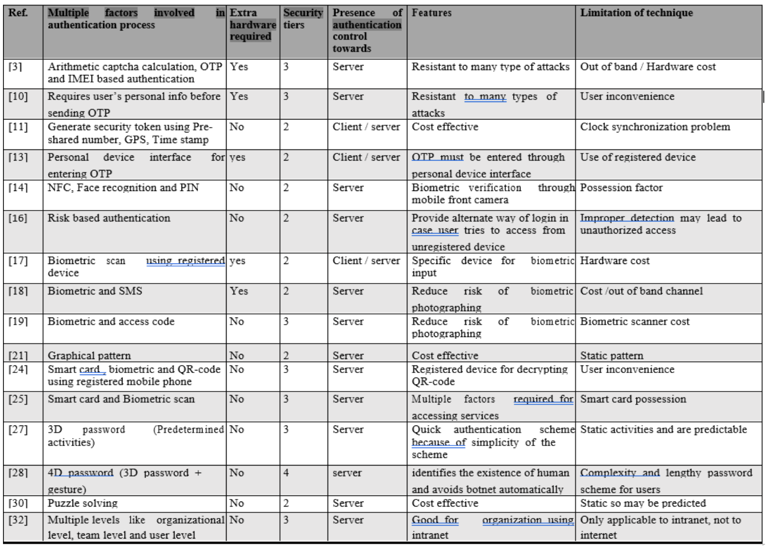
This technique is only applicable at organizational level and can’t be deployed for daily life internet users.

3. Evaluation analysis

As different authentication techniques have been proposed for enhancing security mechanism, but each authentication scheme came up with its own advantages and limitations. So we have used cost, space and user convenience as parameters for evaluating performance of different multi-tier authentication techniques.

Surveyed techniques that are based on OTP using out of band channel provide costly solution. This scheme is also effected by low network coverage and also suffers from delays due to network failure. Another problem with OTP based authentication is that OTP is not very secure as OTP algorithm may be exposed to hacking [33, 34, 35, 36, 37, 38]. Biometric alone authentication techniques are not very secure as physical characteristics of biometric may be changed or damaged. Biometric solution also come up with certain limitations like extra hardware requirement and may be photographed. Different researcher secured biometric by adding other factors to biometric as discussed above but adding more factor compromises usability and user convenience.
Some authors proposed image-based solution using specific pattern for authentication. Although solutions are cost effective and don’t require extra hardware but storing images requires a lot of space. Pattern based authentication schemes are also prone to hacking as static pattern may be predicted. Authentication techniques using 3D virtual environment takes a lot of time and add to user inconvenience Authentication scheme based on sequence of predetermined activities also provides cost effective solution and security to many types of attacks [39, 40,41, 42, 43, 44, 45].

Table 1 given below provides a detailed analysis of authentication schemes discussed so far. It should be noted that adding more security factors add to user inconvenience and is not an appropriate solution. Adding more factors increases cost and complexity of authentication technique and usability is also compromised by adding more factors.



Ref.	Multiple factors involved in authentication process	Extra hardware required	Security tiers	Presence of authentication control towards	Features	Limitation of technique
[3]	Arithmetic captcha calculation, OTP and IMEI based authentication	Yes	3	Server	Resistant to many type of attacks	Out of band / Hardware cost
[10]	Requires user’s personal info before sending OTP	Yes	3	Server	Resistant to many types of attacks	User inconvenience
[11]	Generate security token using Pre-shared number, GPS, Time stamp	No	2	Client / server	Cost effective	Clock synchronization problem
[13]	Personal device interface for entering OTP	yes	2	Client / server	OTP must be entered through personal device interface	Use of registered device
[14]	NFC, Face recognition and PIN	No	2	Server	Biometric verification through mobile front camera	Possession factor
[16]	Risk based authentication	No	2	Server	Provide alternate way of login in case user tries to access from unregistered device	Improper detection may lead to unauthorized access
[17]	Biometric scan using registered device	yes	2	Client / server	Specific device for biometric input	Hardware cost
[18]	Biometric and SMS	Yes	2	Server	Reduce risk of biometric photographing	Cost /out of band channel
[19]	Biometric and access code	No	3	Server	Reduce risk of biometric photographing	Biometric scanner cost
[21]	Graphical pattern	No	2	Server	Cost effective	Static pattern
[24]	Smart card , biometric and QR-code using registered mobile phone	No	3	Server	Registered device for decrypting QR-code	User inconvenience
[25]	Smart card and Biometric scan	No	3	Server	Multiple factors required for accessing services	Smart card possession
[27]	3D password (Predetermined activities)	No	3	Server	Quick authentication scheme because of simplicity of the scheme	Static activities and are predictable
[28]	4D password (3D password + gesture)	No	4	server	identifies the existence of human and avoids botnet automatically	Complexity and lengthy password scheme for users
[30]	Puzzle solving	No	2	Server	Cost effective	Static so may be predicted
[32]	Multiple levels like organizational level, team level and user level	No	3	Server	Good for organization using intranet	Only applicable to intranet, not to internet

TABLE 1 Comparison of various multitier authentication schemes

4. Conclusion

In this paper we surveyed different multitier authentication schemes proposed over a period of 2012-2016 and then we analyzed and evaluated these schemes based on different parameters. Multitier authentication schemes provide a layered defense and thus are more secure than single sign on. But there is a tradeoff between user convenience and level of security. Our objective is to achieve high level of security but not on the cost user convenience. Some authors suggested to enhance security by involving more factors to achieve security but adding more factors is not appropriate solution as it arises usability issue and add to complexity and cost. Graphical password provides more user convenience and security on low cost compared to other authentication schemes. Pattern based and pre-determined activities based authentication schemes also provides cost effective solution for daily life internet user, however authentication schemes for online banking must be highly secure. In future, we will work on authentication scheme that will be less costly with high usability and user convenience. We are working on authentication scheme for cloud computing that will provide high security and user convenience.

References

[1] I. Al Rassan and H. Al Shaher, "Securing Mobile Cloud Using Finger Print Authentication," *Int. J. Netw. Secur. Its Appl.*, vol. 5, no. 6, pp. 41– 53, 2013.

[2] N. Khankari and G. Kale, "Survey on one time password," *Int. J. Comput. Eng. Appl.*, vol. 9, no. 3, pp. 1–7, 2015.

[3] R. K. Banyal, P. Jain, and V. K. Jain, "Multi-factor authentication framework for cloud computing," in *Fifth International Conference on Computational Intelligence, Modelling and Simulation*, 2013, 105–110.

[4] A. Singh and K. Chatterjee, "A Secure Multi-Tier Authentication Scheme in Cloud Computing Environment," in *International Conference on Circuit, Power and Computing Technologies*, 2015.

[5] S. Nagaraju and L. Parthiban, "SecAuthn : Provably Secure Multi-Factor Authentication for the Cloud Computing Systems," vol. 9, no., 2016.

[6] R. Thandeeswaran, "Wide-ranging Survey on Authentication Mechanisms," vol. 11, no. 6, pp. 4114–4117, 2016.

[7] M. Kazim and S. Y. Zhu, "A survey on top security threats in cloud computing," *Int. J. Adv. Comput. Sci. Appl.*, vol. 6, no. 3, pp. 109–113, 2015.

[8] A. Sajnani, "Multi-Staged Authentication," *Int. J. Eng. Technol. Manag. Appl. Sci.*, vol. 2, no. 6, pp. 141–143, 2014.

[9] O. S. Adeoye, "Evaluating the performance of two-factor authentication solution in the banking sector," *IJCSI Int. J. Comput. Sci. Issues*, vol. 9, no. 4, pp. 457–462, 2012.

[10] K. W. Hussein, N. Fazlida, M. Sani, and R. Mahmod, "Design and Implementation of Multi Factor Mechanism for Secure Authentication
System," *Int. J. Comput. Sci. Inf. Secur.*, vol. 11, no. 7, pp. 31–37, 2013.

[11] A. A. Usman, K. Mustafa, and M. Jawad, "A new mobile-based multi-factor authentication scheme using pre- shared number , GPS location and time stamp," in *International Conference on Electronics, Computer and Computation*, 2013, pp. 293–296.

[12] A. Abdellaoui, Y. I. Khamlichi, and H. Chaoui, "Out-of-band Authentication Using Image-Based One Time Password in the Cloud Environment," *Int. J. Secur. Its Appl.*, vol. 9, no. 12, pp. 35–46, 2015.

[13] S. Kumar and A. Ganpati, "Multi-Authentication for Cloud Security : A Framework," *Int. J. Comput. Sci. Eng. Technol.*, vol. 5, no. 04, pp. 295– 303, 2014.

[14] A. Adukkathayar, G. S. Krishnan, and R. Chinchole, "Secure multifactor authentication payment system using NFC," in *The 10th International Conference on Computer Science & Education*, 2015, pp. 349–354.

[15] K. Virgile and H. Yu, "Securing Cloud Emails Using Two Factor Authentication Based on Password / Apps in Cloud Computing," *Int. J. Secur. Its Appl.*, vol. 9, no. 3, pp. 121–130, 2015.

[16] D. R. Thorat and S. S. Sonawane, "Risk Based Multilevel and Multifactor Authentication using Device Registration and Dynamic QR code based
OTP Generation," *Int. J. Adv. Res. Comput. Commun. Eng. Vol. 3, Issue 10, Oct. 2014*, vol. 3, no. 10, pp. 8312–8316, 2014.

[17] E. O. Osei and J. B. Hayfron-Acquah, "Cloud Computing Login Authentication Redesign," *Int. J. Electron. Inf. Eng.*, 1, 1, pp. 1–8, 2014.

[18] M. M. Mohammed and M. Elsadig, "A Multi-layer of Multi Factors Authentication Model for Online Banking Services," in *International Conference on Computing, Electrical And Electronic Engineering*, 2013,
pp. 220–224.

[19] S. Ullah, Z. Xuefeng, and Z. Feng, "TCLOUD: A Multi–Factor Access Control Framework for Cloud Computing," *Int. J. Secur. Its Appl.*, vol. 7, no. 2, pp. 15–26, 2013.

[20] T. Pham, W. Ma, D. Tran, P. Nguyen, and D. Phung, "Multi-factor EEG-based user authentication," in *International Joint Conference on Neural Networks Beijing, China*, 2014, pp. 4029–4034.

[21] R. Kaur and A. Kaur, "Multi-Factor Graphical Password for Cloud Interface Authentication Security," *Int. J. Comput. Appl.*, vol. 125, no. 7,
pp. 32–35, 2015.

[22] S. M. Gurav, L. S. Gawade, P. K. Rane, and N. R. Khochare, "Graphical password authentication: Cloud securing scheme," in *International Conference on Electronic Systems, Signal Processing and Computing Technologies*, 2014, pp. 479 – 483.

[23] N. Harini and T. R. Padmanabhan, "2CAuth: A new two factor authentication scheme using QR-code," *Int. J. Eng. Technol.*, vol. 5, no. 2, pp. 1087–1094, 2013.

[24] N. Harini and T. R. Padmanabhan, "3C-Auth : A New Scheme for Enhancing Security," *Int. J. Netw. Secur.*, vol. 18, no. 1, pp. 143–150, 2016.

[25] S. Ahmad and B. Ehsan, "The Cloud Computing Security Secure User Authentication Technique (Multi Level Authentication)," *Int. J. Sci. Eng. Res.*, vol. 4, no. 12, pp. 2166–2171, 2013.

[26] T. Naik and S. Koul, "Multi-Dimensional and Multi-Level Authentication Techniques," *Int. J. Comput. Appl.*, vol. 75, no. 12, pp. 17–22, 2013.

[27] V. Kolhe, V. Gunjal, S. Kalasakar, and P. Rathod, "Secure Authentication with 3D Password," *Int. J. Eng. Sci. Innov. Technol.*, vol. 2, no. 2, pp. 99– 105, 2013.

[28] P. C. Talhan, R. M. Thakare, and P. A. D. Patil, "A survey on secure storage in cloud computing," *Indian J. Sci. Technol.*, vol. 6, no. 4, pp. 4396–4401, 2013.

[29] M. Singh and S. Singh, "Design and Implementation of Multi-tier Authentication Scheme in Cloud," *IJCSI Int. J. Comput. Sci.*, vol. 9, no. 5, pp. 181–187, 2012.

[30] V. Sulochana and R. Parimelazhagan, "A Puzzle Based Authentication Scheme for Cloud Computing," *Int. J. Comput. Trends Technol.*, vol. 6, no. 4, pp. 4–7, 2013.

[31] Y. Sharma and R. Bhatia, "Access Control for Cloud Platforms Using Multi-Tier Graphical Authentication," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 5, no. 8, pp. 361–367, 2015.

[32] H. A. Dinesha and V. K. Agrawal, "Multi-level authentication technique for accessing cloud services," in *International*

Conference on Computing, Communication and Applications, 2012, pp. 1–4.

[33] S. Yoo, S. Shin, and D. Ryu, “An effective Two Factor Authentication Method using QR code,” in *The 7th International Conference on Information Security and Assurance*, 2013, vol. 21, pp. 106–109.