ISSN 2047-3338

A Customizable Client Authentication Framework (CCAF) Based on Multi-Factor for Cloud Computing Application

Muhammad Kaleem[1] and M. Junaid Arshad[2]

[1,2]Department of Computer Science and Engineering, University of Engineering and Technology, Lahore

[1]kaleemaq06@gmail.com, [2]mjunaiduet@gmail.com

***Abstract*– The advance innovation through which various facilities, such as, access of information, storage of information, applications and platforms can be accomplished by web is called Cloud Computing. While moving expansive amount of information and data on the cloud, it is vital to guarantee suitable security control. User authentication is a main technology for data security, which is a technique to establish proof of identities to get access of data and information in the system. Traditional password authentication does not offer adequate security for data in cloud computing environment. In this research work, we will try to develop and introduce a trusted customizable authentication security framework for cloud environments which improve security. This research work will propose mechanism of multi factor for secure user authentication. There are many technologies for multi-factor authentication and client preferred one method to another. In this research work, we will let the client to choice their preferred factor through Customizable Client Authentication Framework (CCAF) for authentication along with username and password. Based on the clients' requirements, they have to select the preferred type for authentication service. The model will consist of four stages such as Registration stage, Login and authentication stage, Forget authentication credential stage and Change authentication credential stage. By implementing CCAF model will improve the rate of trust and reliability in cloud computing environments as an evolving and influential technology in various industries.**

***Index Terms*– Cloud Computing; Data Security, Authentication and Authorization, Security Threats and Customizable Authentication Security Framework**

I. INTRODUCTION

CLOUD computing is essentially a great type of outsourcing in the dispersion of facilitated administrations by means of the Internet [1]. The cloud goes about as a virtual server that client can access by means of the web on an as required premise. Cloud computing incorporates any membership based or pay-per-use benefit that stretches out IT capacities permitting client to access their stored data and resources remotely [2].

The internet and central remote servers are used by cloud computing to retain data and applications. It is being made possible for the customers by cloud computing to access personal files and applications at any computer without any installation [3].

The three building blocks of cloud computing are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) as shown in Fig. 1. SaaS is a delivery model of cloud computing which offers software applications to online clients on the internet [4]. Client does not need to install software on his PC. In short, it is not required to purchase, establish, sustain or update the software. PaaS is used to permit diverse software to run on similar platform. IaaS is the fundamental corporeal and organizational structures of any organization.

Cloud deployment model offers diverse services such as platform, storage, infrastructure as a service and network on the basis of client's requirement; it can be leveled up or down. Public cloud permits different consumers or clients to approach the cloud from several locations to get numerous services.

Private clouds have recognized and proprietary infrastructure therefore generally these are positioned inside data centers following a firewall within an organization. Hybrid Cloud is a combination of two or more other deployment models of cloud.

Information security and protection are the two important security concerns toward the associations to receive cloud computing services [5]. The organizations are hesitant to store their resources outside their own premises on account of the uncovered security dangers. As organizations lose control over information in the cloud computing environment, they trust that the substance stored in the cloud is more inclined to security dangers [6]. A secure security framework must be given to expand the level of trust between the cloud suppliers and the cloud purchasers. The cloud suppliers must give best in cloud security answers for build up the required level of trust. They need to demonstrate logically that the information stored in the cloud is secure and just the validated and approved work force can access the cloud information [7].

User authentication is a main technology for data security, which is a technique to establish proof of identities to get access of data and information in the system. Traditional password authentication does not offer adequate security for data in cloud computing environment [8]. There are many

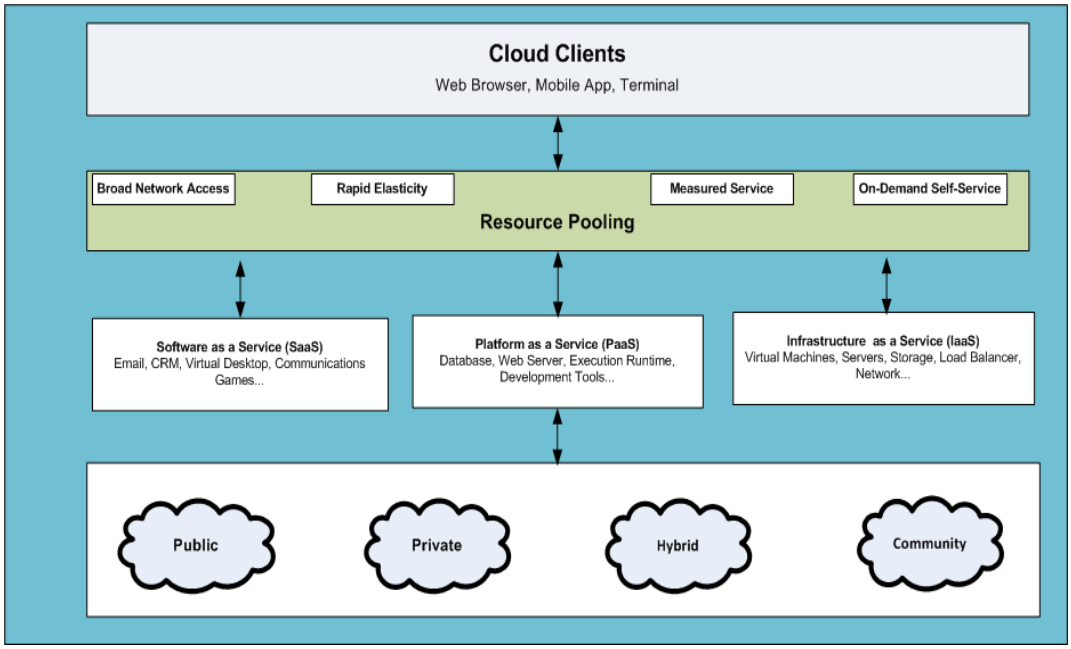

Fig. 1: Cloud Computing Delivery and Deployment Model

technologies for multi-factor authentication and client preferred one method to another. It's better to decide clients to choice their preferred method for Multi-Factor Authentication.

The authentication mechanism plays a vital role in security enhancement [9]. Authentication mechanism is like an entrance door and will allow only the trusted individuals to enter in the cloud premises. The mechanism should be robust enough to ensure availability by letting the right person in, any time and any place. Authentication mechanism can be combined with cryptographic techniques to ensure confidentiality of data [10]. Having the best possible authentication mechanism along with a complete security plan can mitigate most of the security concerns of cloud consumers.

From the above readings and concerns, it is understood the significance of security in cloud. As a solution for this issue, this research work will look at how to oversee verification and authentication frameworks in cloud situations and offer a methodology of cloud security framework for giving confirmation and approval managements to cloud based administrations. In this research work, we will let the client to choice their preferred factor through Customizable Client Authentication Framework (CCAF) for authentication along with username and password. In the meantime, the task will concentrate on the best way to convey those services and resources in an interoperable and secure way.

II. RELATED WORK

All the application utilizes any validation method to secure the clients' data in multi-occupancy way. By and large, username and password are the straightforward approach to accomplish validation, yet this method is not that much secure to shield the data from the unapproved access of the client. Numerous security assaults are conceivable to break this single-level authentication framework like brute-force attack, password guessing, man-in-the-middle attack and so on. Along these lines, [11], [12], [13] depicts authentication procedure that is called multi-level authentication or multi-factor authentication. [14] depicts distinctive authentication and approval framework which expresses that all the application must utilize more than one-level for authentication to secure the data. [14] additionally determines that utilization one time produced secret key which will be sent to the email address or cell number.

Sarbjeet Singh and Maninder Singh proposed a multi-authentication mechanism for cloud security in which validation process is done in two levels [15]. First place level uses general username and secret password. Second level is pre-decided arrangement of steps. The upside of this plan is that it doesn't require any extra equipment like software and hardware. So this can be utilized and accessed from anywhere and anytime over the globe. They inferred that the quality of any authentication strategy relies on the likelihood of breaking that method.

In cloud computing environment, there are several multitier authentication mechanisms, however they do not give security against virtualization attacks and insider attacks. In cloud computing environment, entire authentication mechanism lies in the server side. In this way, it is difficult to trust the outsider server in cloud framework. Ashish et al. [7] proposed a secured and more progressed multi-level authentication framework for accessing cloud resources and services.

Nayak, Sanjeet Kumar, Banshidhar Majhi and Subasish Mohapatra, et al. [16] recommended an authentication technique in the cloud computing. This structure shows mutual validation and session key understanding between the confirmed client and the cloud service provider for the fulfillment of the authentication procedure. The security

examination of this methodology shows that it is safe from the reply attack.

M.S. Shashidhara et al. [17] proposed a multi-client verification system for distributed computing. In this system, client distinguishing proof is confirmed before signing into the cloud server. Proposed convention can oppose interloper assault and DOS (Denial of Service) assault. Sultan Ullah et al. [18] proposed multi-level, multi-factor verification methodology is utilized for the confirmation and approval of the users. This plan builds the privacy and trustworthiness of the information. This model proposed the blend of cryptography and access control to keep the information safe from vulnerabilities.

Another scheme proposed by Liao etal. [19] in which they have used public key cryptography. But they send the password and user ID in plaintext. Plaintext data can be easily intercepted by intruders. This scheme doesn't care about the confidentiality and privacy of users. In addition to this the scheme doesn't provide password change option which can be a flaw during real time environment.

III. PROPOSED WORK

In this research work the algorithm and implementation of various phases and activities of secure authentication will be discussing in detail. Figure 2 represents the proposed framework for Customizable Client Authentication Framework (CCAF).

Table 1: Comparison with Existing Authentication Technique

Authentication Method	Security From Insider Assault	Presence of Authentication Factor Selection Control Towards CSP or Client	Additional Software Hardware Required	Number of Security Levels
Customizable Client Authentication Framework	Yes	CSP and Client	Depends on Client's Requirement	Multiple
Multi-tier Authentication Scheme in Cloud	Yes	CSP	No	2
Mutual Authentication Framework For Cloud Computing	No	CSP	Yes	2
Proactive Model For Security In Cloud Computing	No	CSP	Yes	1

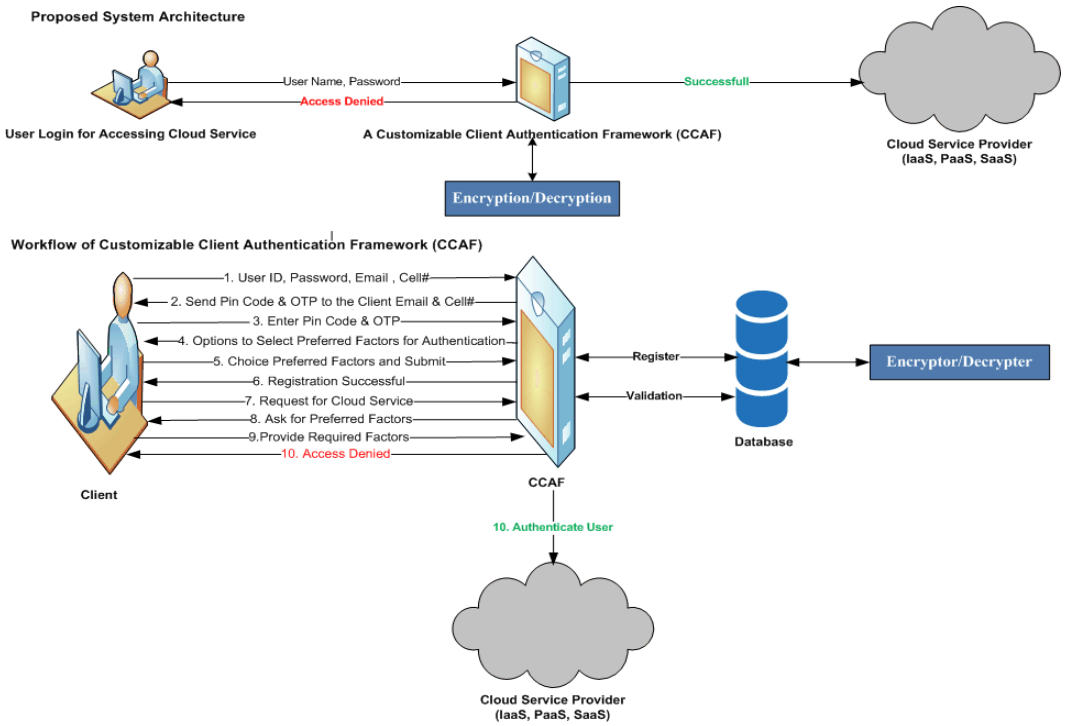

Fig. 2: Proposed Customizable Client Authentication Framework

A) Components of CCAF

The framework will consist of four main components. These are as follows:

Client: Client has limited access to the resources from the cloud offered resources, application and services. The client demands for cloud services to the CSPs. Clients are required to prove themselves during login and authentication stage by giving exact and real identification details for getting cloud services, application and resources.

Customizable Client Authenticator: Customizable Client Authenticator (CCA) will decide whether a client should be allowed to access cloud services, application and resources or not. The idea of insisting CCA in cloud computing is to certificate the user to access services through the service provider. CCA has two stages, one is Registration Stage and another is Verification and Authentication stage. The CCA has a database server which store registered clients' information and authenticate the registered user to access cloud services.

Encryption/Decryption: Cryptography is the process of preventing private data from stolen []. Cryptography is the important process that can be used to authenticate the sender of the message whether it is the actual sender or not. Encryption is commonly used for secure your data. Encryption is a process of converting data to a form that cannot be used in any meaningful manner without special knowledge. It is preventing unauthorized access [25]. Decryption is a reverse process of encryption. This component is utilized to encrypt the information of clients. It utilizes a key for encryption and decryption.

Cloud Service Provider (CSP): A Service Provider that offers clients software or storage services accessible by means of a private cloud or public cloud. As a rule, it implies the capacity and software is accessible for access through the Internet.

B) Work Flow of CCAF

The framework flow work will consist of four stages. These are as follows:

Registration Stage: Whenever a new client wants to access cloud services, client has to register first on to the cloud. Client should have a valid Email ID, mobile phone and provide right information in order to complete registration.

Login and Authentication Stage: Login and Authentication stage enables client to provide its active login ID and password for verification and provide their preferred authentication factor to access cloud application according to the services provided by CSP.

Forget Authentication Credential Stage: This stage will provide the facility of forget password with the help of which a new system generated password has been sent at client's email address.

Step Wise Work Flow of Proposed CCAF Framework Process: The overall working steps in the CCAF authentication process is explained in eleven steps. They are:

Step 1: The client sends User ID, Password, Email ID and Cell# to the CCAF authenticator for new registering.

Step 2: CCAF validate the user credentials for uniqueness. If unique, sends Pin Code & OTP to the client email address & Cell phone number else it goes to Step 1.

Step 3: Client provide Pin Code and OTP to the CCAF authenticator.

Step4: CCAF verify Pin Code and OTP provided by the client, if validated, CCAF provides the options to the client to choose other factors for authentication.

Step 5: Client choose their preferred factors according to their interest and submit.

Step 6: CCAF register the client identifications, client credentials information is stored in the database and sends a message of registration successful.

Step 7: After the successful registration, the client sends a request of a cloud service to the CCAF authenticator.

Step 8: CCAF validate the client credentials and redirect the client to a page, where the client enters the preferred factors for high-level authentication.

Step 9: Client provide required factors to the CCAF authenticator.

Step 10: CCAF authenticator performs validation and if accept CCAF provides the entry of the client request.

Step 11: Client gain the cloud service according to the demand.

C) Forget Authentication Credential Stage

This feature allows the client to recover their password in a few simple steps. On clicking forget your password system open a new screen on which user will provide required information. If the information is correct then system will have sent password and generate a successful delivery message on screen.

The forget authentication credential process is shown in the Fig. 3.

The working steps in the forget authentication credential stage is explained below:

Step 1: Client clicks "Forget Password ". System will open a new screen.

Step 2: Client is requested to enter the required information. These information consists Email ID, Phone No., Preferred security question (selected during registration stage) and Preferred security question answer. This additional level stops clients accepting messages they didn't ask.

Step 3: The client's provided information are checked in the database. If that information is existing in database and correct, then system generate one-time token (UUID) and sent to the client's phone# for confirmation, else generate error message.

Step 4: Client enter the UUID. System checks and verifies the provided UUID. If the information is valid go to the next step, else generate error message.

Step 5: Assuming all the provided information's are correct, system get password from database, and sent plain password to the Client email address and generate successful message on the screen.

D) Change Authentication Credential Stage

This stage is used to provide capability of altering the old password with the new password at any time. Client has to provide his old password and new password to change his old password.

The working steps in the change authentication credential stage are explained below:

Step 1: Client clicks "Change Password ". System will open a new screen.

Step 2: System checks the current session for logged user. If the user is legitimate then system will display change password screen, else system will redirect the client to login screen and display error message.

Step 3: Client enter old password, new password and verify the new password and submit.

Step 4: System check and verify the old password. If old password is correct, then system verifies the new password. if valid then go to the next step, else display the proper error message.

Step 5: system update client password and send confirmation email to the client registered email address for successful update password.

Step 6: System update modified date and time for audit purpose.

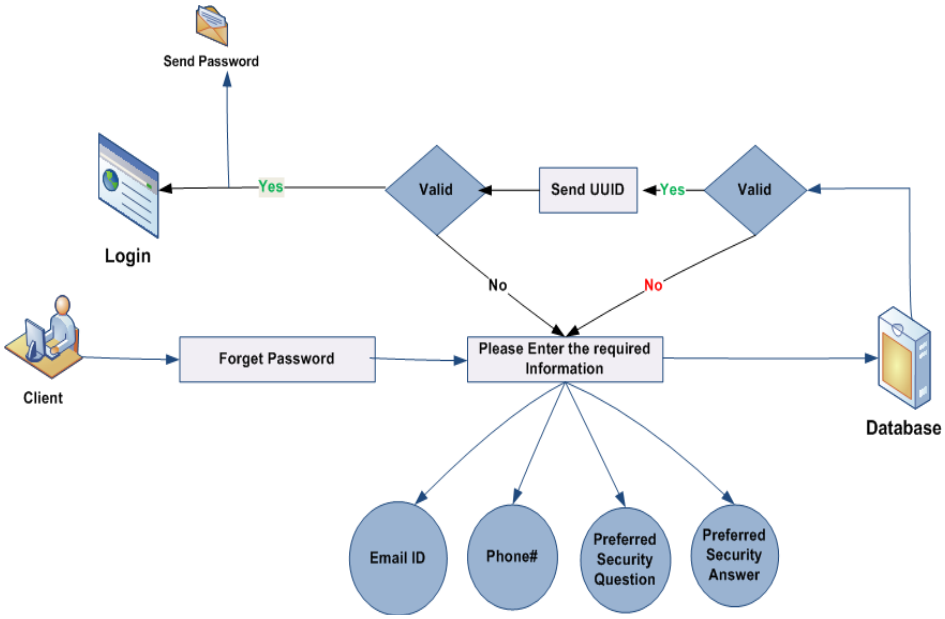

Fig. 3: Forget Authentication Credential Process

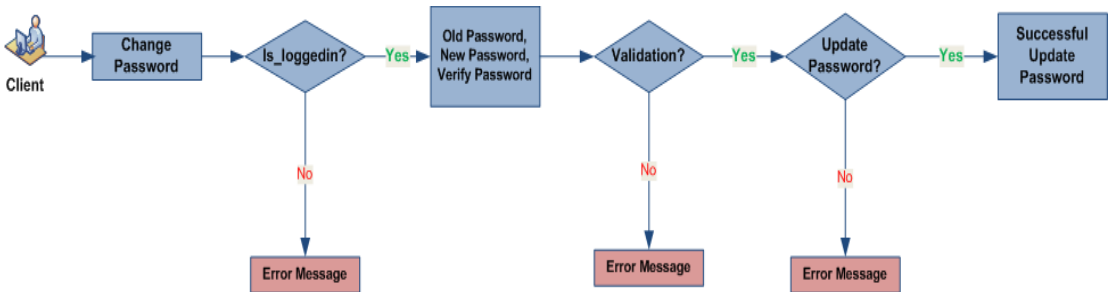

Fig. 4: Forget Authentication Credential Process

E) Implementation of Proposed CCAF Framework

Implementation of proposed authentication framework is as follows:

Fig. 5: Implantation of Proposed CCAF Authentication Framework

F) Implementation of Proposed CCAF Framework

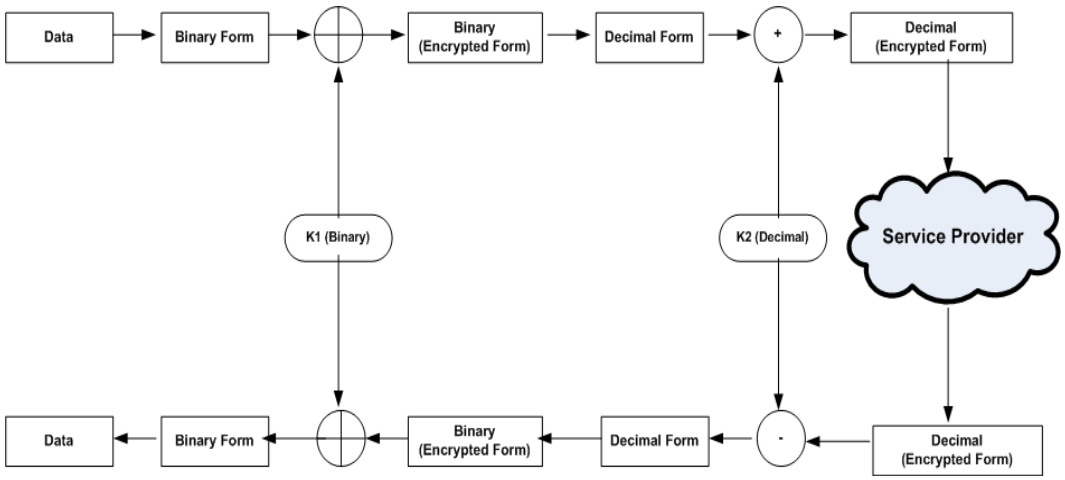

Fig. 6: Block Diagram of Encryption and Decryption for Security

Encryption Process:

Step 1. "Transform data into Binary form by using ASCII values."

For character "K" its ASCII code is "75" and Binary code of "75" is "01001011"

Step 2. "Choice the binary key"

It can be any 4-bit key that repeats two times while performing operation on 8-bit value. Here, binary key is "1101".

Step 3. "Implement binary XOR method on binary data by using selected key"

Binary converted data is "01001011" and binary key is "11011101". After taking XOR operation output binary data is "10010110".

"10010110" is the resulted binary encrypted form of data.

Step 4. "Transform binary encrypted data into Decimal form"

Decimal form of binary encrypted value "10010110" is "150".

Step 5. "Choice the decimal key"

It can be any decimal value so here we take "247" as a decimal key.

Step 6. "Implement Addition operation on decimal data by using selected decimal key"

Decimal converted value is "150" and decimal key is "247". After taking addition operation output decimal data is "397". "397" is the output encrypted decimal data.

Decryption Process:

Step 1. "Select the decimal key"

Key is same which is used for encryption that is "247".

Step 2. "Perform Subtract operation on decimal data by using selected key"

Decimal encrypted data is "397" and key is "247". After performing subtraction operation output value is "150".

Step 3. "Convert decimal data into binary form"

Binary form of decimal value "150" is "10010110".

Step 4. "Select the binary key"

Key is same which is used for encryption that is "1101".

Step 5. "Perform binary XOR method on binary data by using selected key"

Binary encrypted data is "10010110" and key is "11011101". After taking XOR operation output value is "01001011".

Step 6. "Change Binary data into original data with the help of ASCII code."

For binary value "01001011", its ASCII value is "75" which is equal to character "K".

G) Security Analysis of Proposed Framework

This security analysis clarifies how proposed structure mitigation of possible threat.

S*ecure Identifications Management:* The CCAF server stores all the information of the client in a protected database. Server checks the availability of unique client ID for every client at the time of new enrollment.

Secure Authentication Credential Change Management: Proposed authentication framework encourages clients to change password, cell phone number, IMEI number, and secret key using user friendly and secure way, at whenever as discussed in area 6.6. This change capability makes the CCAF framework essentially stronger as compared to the static password based system.

Man-In-The Middle Attack (MITM): In this proposed framework regardless of the possibility that hackers figure out how to get the client ID and password and are capable to login to the system, they can't get to cloud resources and services, as the client needs authentication which requires client preferred factor like secret key, one-time password (OTP), cell phone and IMEI number, digital signature etc. These privileged are just shared between the client and the server using separate secure channel. Moreover, we used cryptography technique in the proposed framework to secure critical information. Hence the proposed plan is solid and safe against MITM attack.

Stolen Identification Attack and Unapproved Access Attack: In our proposed framework, all verification components are not accessible concurrent. In this way, regardless of the possibility that one credential is stolen or lost, authentication needs other factors for login. Similarly, the system provides the facility to change authentication credentials at any stage and in case of theft, the client can change the required factors. Thus stolen identification attack and unapproved access attack is not fruitful in this authentication framework.

Phishing Attack: In this authentication framework mutual authentication between the client and the CCAF server, in light of multi-factor credentials is performed. More than one factors are required for authentication. only the genuine server can send appropriate authentication information to the client. Also, only genuine server can be verified client response. So, phishing attack is useless in this framework.

Password Guessing Attack: In the proposed system authentication depends on multi-factor based on client interest. In the proposed framework, just password guessing is not sufficient for authentication. It also requires other factors for authentication. Password guessing attack is useless in this framework.

Sniffer Attack: A sniffer is a device or application that can monitor, read, and capture network packets and read sensitive network packets such as account information, password etc. If the network packets are not encoded, a sniffer gives a full view of the information inside the packets. In our proposed framework, cryptography is used to secure sensitive information. Hence the proposed scheme is strong and safe against sniffer attack.

Brute-Force Attack: In the proposed CCAF authentication framework, user account has been locked out after a certain number of login attempts for a specific time period. If the number of failed logins increased to a certain number, CCAF framework block the IP address to prevent brute-force attack. Hence the proposed scheme is strong and safe against brute force attack

IV. CONCLUSION

The proposed framework gives an acceptable and productive arrangement by consolidating the customary client ID and password based verification with element multi-factor based validation approach. It plans secure validation framework which can oppose many sorts of attacks. The fundamental quality of this framework lies in the way that

client is verified robustly instead of statically. CCAF is a client authentication framework that sets up particular level of security for the clients to meet their dynamic prerequisite of security levels for the cloud computing services and resources.

The proposed mechanism resists many popular attacks such as replay attack, password stolen attack etc. Currently, study on some formal security proofing technique is on process, and providing formal security proof to the proposed framework will be the future research goal. Future research also includes preserving the privacy of the user's information provided to the server. In this research work, we proposed a solution in the form of security model with four different security levels. Each level has its own series of steps by using these steps client can secure its confidential data according to desire.

REFERENCES

[1]. N. Xiong, W. Han, and A. Vandenberg, "Green cloud computing schemes based on networks: a survey," IET Communications, vol. 6, no.18, pp. 3294-3300, December 2012.

[2]. Arockiam, L., Monikandan, "Efficient Cloud Storage Confidentiality to Ensure Data Security" IEEE International Conference on Computer Communication and Informatics, ISBN: 978-1-4799-2352-6, pp 355-359, January 2014.

[3]. S. Grzonkowski, and P.M. Corcoran, "Sharing cloud services: user authentication for social enhancement of home networking," IEEE Transactions on Consumer Electronics, ISSN: 1424-1432, vol. 57, no. 3, pp.1424-1432, August 2011.

[4]. F. Fatemi Moghaddam, N. Memari, A. Hakemi, and H. Latifi, "A Reliable E-Service Framework based on Cloud Computing Concepts for SaaS Applications," in Proc. IEEE Conference on e-Learning, e-Management and e-Services (IC3e), Sarawak, Malaysia, pp. ISBN: 978-1-4799-1573-6, pp. 100–104, December 2013.

[5]. Nuppor M. Yawale, V.B.Gadichcha," Third Party Auditing (TPA) for data storage security in cloud with RC5 algorithm" International Journal of Application or Innovation in Engineering & Management, ISSN: 2319-4847, vol. 3, Issue 3, March 2014.

[6]. M.S. Shashidhara, Jaini.C. P,K.Dayana Devi, "A Study on Multi-User Authentication Framework and Security problems for Cloud Computing" Journal of NanoScience and NanoTechnology, ISSN: 2279-0381 vol. 2, Issue 3, pp.347-352, 2014.

[7]. Ashish Singh and Kakali Chatterjee, "A Secure Multi-Tier Authentication Scheme in Cloud Computing Environment", International Conference on Circuit, Power and Computing Technologies (ICCPCT), IEEE, ISBN 978-1-4799-7075-9, March 2015.

[8]. HA Dinesha and VK Agrawal. Multi-level authentication technique for accessing cloud services. In Computing, Communication and Applications (ICCCA), 2012 International Conference on, pages 1{4. IEEE, 2012.

[9]. N. Veeraragavan, S. Monikandan, Dr. L. Arockiam, "A Novel Framework for an Authentication as a Service in Public Cloud Environment" Proceedings of National Conference on Data Science and Engineering, ISSN: 2278-1021, vol. 5, Issue 03, March 2016.

[10]. [26]. A. N. Jaber and Md. F. B. Zolkipli, "Use of cryptography in cloud computing" IEEE International conference on Control System, Computing and Engineering, Malaysia, pp. 179-184, 2013.

[11]. Trupti Hemant Gurav and Manisha Dhage, Remote Client Authentication using Mobile phone generated OTP. International Journal of Scientific and Research Publications. 2(5): p. 4, 2012.

[12]. Havard Raddum, Lars Hopland Nestas, and K.J. Hole', Security Analysis of Mobile Phones Used as OTP Generators, in international conference on Information Security and Privacy of Pervasive Systems and Smart Devices, International Federation for Information Processing (IFIP), Editor, ACM: Berlin. p. 324-331, 2010.

[13]. Gianluigi Me, Daniele Pirro, and R. Sarrecchia, A mobile based approach to strong authentication on Web, in International Multi-Conference on Computing in the Global Information Technology, IEEE Xplore. p. 67, 2006.

[14]. Jae-Jung Kim and Seng-Phil Hong, A Method of Risk Assessment for Multi-Factor Authentication. Journal of Information Processing Systems. 7: p. 187—198, (2011).

[15]. Sarbjeet Singh and Maninder Singh, "Design and Implementation of Multi-Tier Authentication Scheme in Cloud" Published in International Journal of Computer Science Issues (IJCSI), Vol. 9, Issue 5, No. 2, at Computer Science and Engineering, UIET, Panjab University, Chandigarh, India, September 2012.

[16]. Sanjeet Kumar Nayak, Subasish Mohapatra, and Banshidhar Majhi. An improved mutual authentication framework for cloud computing. International Journal of Computer Applications, 52, 2012.

[17]. Rachna Jain, Sushila Madan and Bindu Garg, "Framework to Secure Data Access in Cloud Environment", ICSI-CCI 2015, Springer, DOI: 10.1007/978-3-319-20472-7, pp. 127-135, 2015.

[18]. Sultan Ullah, Zheng Xuefeng and Zhou Feng, "TCLOUD: A Multi – Factor Access Control Framework for Cloud Computing" International Journal of Security and Its Applications, vol. 7, No. 2, pp.15-26, March 2013.

[19]. LiaoI-En., LeeCheng-Chi., HwangMin- Shiang., "A password authentication scheme over insecure networks," Journal of Computer System Science, vol. 72, issue 4, 2006.