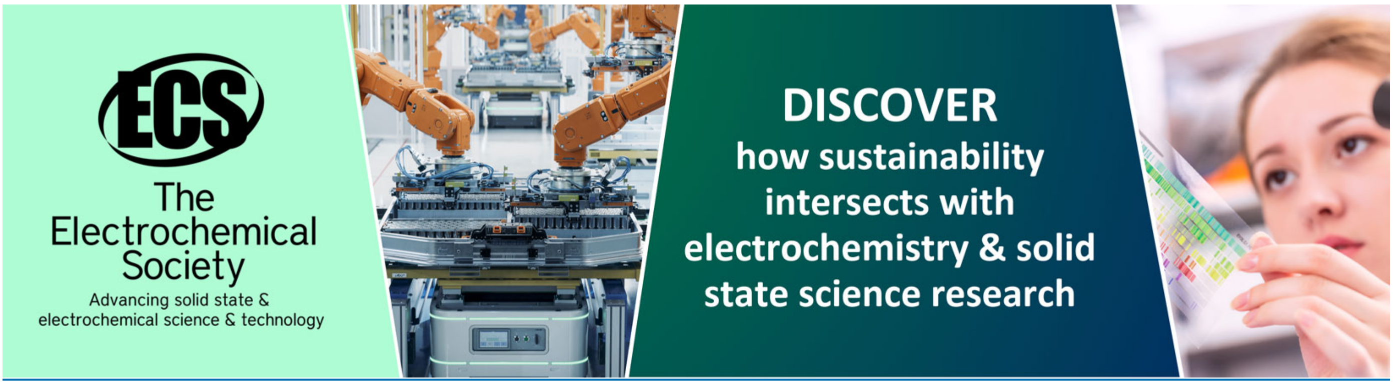
Journal of Physics: Conference Series

PAPER • OPEN ACCESS

Review of Access Control Mechanisms in Cloud Computing

To cite this article: Muhammad Rizwan Ghori and Abdulghani Ali Ahmed 2018 *J. Phys.: Conf. Ser.* **1049** 012092

View the article online for updates and enhancements.



Review of Access Control Mechanisms in Cloud Computing

Muhammad Rizwan Ghori, Abdulghani Ali Ahmed

Faculty of Computer Systems and Software Engineering, University of Malaysia Pahang, Gambang Campus, Kuantan, Malaysia

rizwanghori@outlook.com, abdulghani@ump.edu.my

Abstract. Cloud Computing is an evolving technology in the field of IT. People are using this technology vastly as it reduces the storage and other services burden of the users as they use the services provided by the cloud. There are many advantages related to this technology like unlimited storage, cost effectiveness but lacking the strong authentication process. Many researchers are working on the security issue of cloud like user confidentiality, integrity and authenticity etc. However, in this paper we have reviewed and discussed several papers that are related to the authentication in cloud environment. Moreover, after studying different authentication system made by the researchers, we have critically analysed them and found advantages and disadvantages along with some suggestions for the future work.

1. Introduction

Cloud Computing (CC) is a growing field nowadays as it is being used commonly and is generally provided by the third party. The most prominent feature is accessibility of the data. Data kept in the cloud can be retrieved any time and at any place if there is a network access. The benefit of using this technology is that you get worry free related to equipment purchase, data storage capacity, accessibility speeds etc. as these are the concerns of service providers. In view of aforesaid, sharing of data has become more convenient with cloud storage. Moreover, the companies or industries are also taking advantages of the cloud for data management tasks as it becomes cheaper for the companies instead of purchasing the expensive hardware's and software's.

SPI is the most common CC service model for Software, Platform and Infrastructure. Software as a service (SaaS) is a software model in which applications are provided by the vendor or service provider on the requirement of the user on the internet. Platform as a service (PaaS) is a standard for providing the operating system to the customer on the internet without downloading or installation. Infrastructure as a service (IaaS) is provision of storage, hardware etc. facilities to the customer [1-3]. CC is basically providing two major services like data and computational service. With data being the most popular service as all the data management and storage tasks are performed by the cloud service providers. Further the tasks of computations are also managed by the cloud computational services [4-5].

Regardless of CC advantages, it has also increased the risk of the attacks and unauthorized access to the data as it is distributed and stored in different location. Moreover, as storage is shared among many users so there are chances of the illegal user access to the data which can be due to many reasons like device problems, bad intention of some user etc. To overcome these issues the data security must be provided. In network, the protection to the information can be provided with the help of encryption of the data or information. There are different aspects of security in CC such as data confidentiality, integrity and availability which is also known as CIA triad [5-12].

Data confidentiality can be called as the privacy. It is basically to prevent the sensitive information from reaching the wrong person. As said above that data encryption is the standard method for provision of data security. Other include the user id and password protection authentication. Moreover, biometric verification constitutes the other method for certification. Data integrity means that data should not be changed during transmission and steps must be taken to ensure that data cannot be altered by illegal intent of any person [2]. Availability can be defined as the system should always be available for the use. It can be best assured with timely hardware equipment maintenance and keeping up the system with upgrades to avoid any conflict. Authentication and access control is done with the matching of the credential provided by the user with the stored one in the relevant server.

With the advent of CC, user can custom the storage or service without having any idea of the location of the infrastructure. For example, if you are in country A and using the CC service for data storage. It might be possible that your data is being stored in the CC server which is in country B. Thus, keeping your data secure in such huge environment is difficult as CC service can store the data regardless of the location. CC being a convenient service have some disadvantages as well in terms of security as discussed. As the term security is quite vast, the major issue nowadays in CC is the management of access controls and authentications for users related to data sharing etc. [13]. Data authentication and access control in CC is the latest ongoing research topic. In this review, we have discussed and reviewed different aspect related to cloud data security in terms of authentication in detail.

The rest of the paper is organized in a manner that in Section 2, the data authentication and access controls in CC along with the classification of authentication methods are discussed while Section 3 will discuss in detail the comparative studies related to CC and at last with Section 4 we conclude the paper.

2. Data Authentication and Access Control in Cloud Computing

People are using CC commonly these days. Many small as well as large organizations use CC for managing their large amount of data as well as for using different applications etc. As far as customers are concerned data security is the main worry. There are many aspects of security but as told above the authentication and access control of data is now a debating topic among the IT professionals. As the hackers are becoming more advanced, the normal user id and password authentication is never remained reliable [22]. Additionally, security can be compromised when a member of Cloud Service Provider (CSP) can steal information for some financial benefits. Moreover, if you are using biometrics for the security checks it can also be stolen by the aforesaid staff. So, there is a strong need of data authentication and access control techniques to be implemented in CC to fully secure the cloud user. Subsequently, Fig.1 is showing the classification of authentication methods.

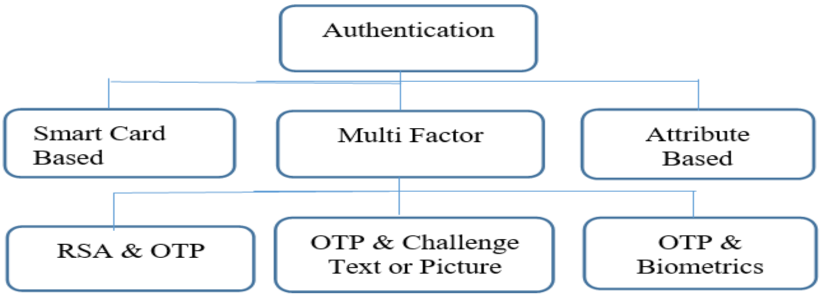


Fig.1: Classification of Authentication Methods

In [14], the author presented a hierarchical authentication model by modifying Anti Statistical Block Encryption (ASBE). The system consisted of five parties i.e. CSP, data owners, data consumers, domain authority and trusted party. In the system data owners, can encrypt the file and will store it in the cloud. Consumers can use the file stored in cloud by decrypting it. Data owners are managed by the respective domain authorities and domain authorities are administered by the trusted parties. The Fig.2 is showing the hierarchical view of system model in which the same process is being followed as discussed.

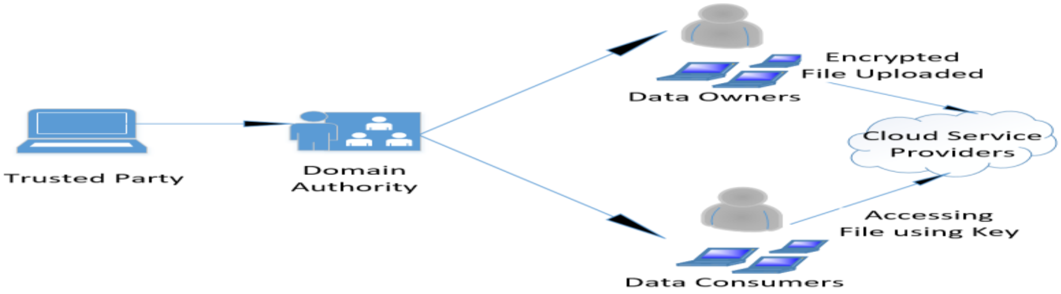


Fig.2: Hierarchical Authentication Model (Z. Wan et al. 2012)

Basically, according to the author, the domain authorities are represented by the organization or department and the user and consumers are under the aforesaid authority. With the permission of domain authority user or consumer can upload and download the file to and from the cloud respectively. As per system shown in Fig.2, it is lacking the proper authentication for user's security. According to the author, the users are dependent only on the trusted party, if the said party plays bad then there will be no security.

Another scheme was proposed by [15], that used Smart Card and Single Sign on (SSO). In the scheme, a combination of smart card and third party authentication was used to attain SSO in inter cloud environment. Moreover, [16] also presented the same model. The drawback of these models is that they have used a special smart card reader for the authentication purpose.

In [17], the writer has given a model scheme in which two factor authentications, Ron, Ravist and Adi (RSA) and one time password (OTP) for CC accessibility has been used. The connection establishment to the cloud consisted of three phases such as setting up for the connection, registration and finally the authentication phase. According to the author, first two steps will be performed by the user only for once. But the authentication step is mandatory every time for the user to access the cloud services. In this scheme, no extra devices have been utilized such as special purpose smart card readers etc. The scheme presented was good for authentication but [19] used the elliptic curve cryptography which is more faster and having smaller key sizes than RSA.

In [18], the system was proposed consisting of the Data Owners, CSPs and the Reputation Centers (RCs). Data owners were the users that request or use the services provided by the CSPs. RC was the trustworthy party with a good reputation and a system consisted of multiple RCs. Moreover, as per the system, CSP will pass stored data to the user on the directives of RC as it will be always available for the authorization of the data access. But according to the system proposed, RC is not given permission to access the data stored in the cloud. The system is shown in Fig.3.

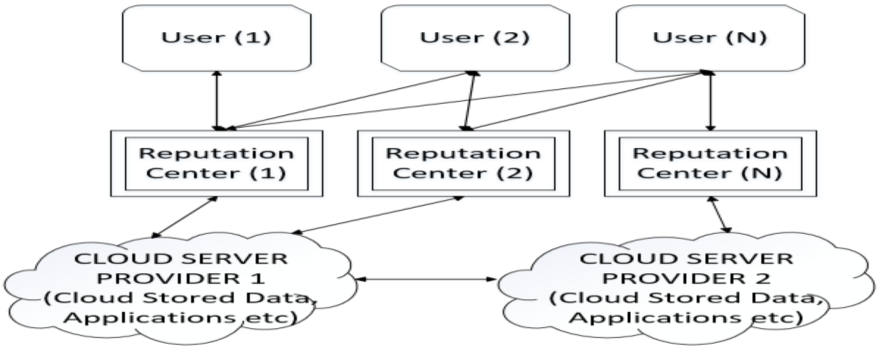

User (1)
User (2)
User (N)
Reputation Center (1)
Reputation Center (2)
Reputation Center (N)
CLOUD SERVER PROVIDER 1 (Cloud Stored Data, Applications etc)
CLOUD SERVER PROVIDER 2 (Cloud Stored Data, Applications etc)

Fig.3: Architecture for Flexible Access Control in CC (Z.Yan et al. 2015)

The system for authentication was developed by [19] using A3 algorithm. According to the author, first step is the establishment of the connection between the cloud server and the user. For registration, the user must fill in the form with personal details. After the registration, Elliptic Curve Diffie Hellman (ECDH) equivalent key exchange will be established with the server. Furthermore, the server will create One Time Password (OTP) which will be send to the user according to the given details by using A3 algorithm. With the help of ECDH and OTP user id will be generated using A3 algorithm. Moreover, after every log in, the new password will be generated for the use. The model presented by the author is efficient as ECDH is faster and have small key sizes. Moreover, according to [22] multifactor authentication with biometrics proven more authenticated.

Moreover, [20] made an authentication system based on attributes for Cloud Server (CS). Attributes Based Signature (ABS) is a technique in which signer is identified by a set of attributes rather having a single attribute defining the signer identity. In this paper, the author has proposed an effective and dynamic signature generation scheme for ABS in which CS provides the half of the signature for the user and other half a user will generate and with less computational cost. Cost effectiveness along with security has made the ABS an emerging technique in the field of authentication and proving itself.

A study was made by [21] on factors that boosted privacy concern in CC environment. He collected 340 cases from the student population and concluded that CC security has to be improved to overcome the privacy concerns of the users.

In [22], the multifactor authentications such as user id, password, OTP and biometrics have been used. As per the system, the user id and password judges the knowledge of the user, fingerprints shows the users identity and OTP along with nonce, master and session keys used for the verification of user identity to the server and vice versa.

Additionally, for management of session keys, station to station Diffie-Hellman key exchange has been used for exchanging one time session key. Furthermore, the said keys will not be stored in server etc. for security concerns. Nonce has basically been used for handshaking for the avoidance of any undependable server encounters.

In addition, for preservation of privacy related to user identifications, the hashed credentials have been used for the verification by cloud server in place of original keys. Also, for symmetric encryption and decryption of the data communication between the user and server Advanced Encryption Standard (AES) has been implemented. The Fig.4 is showing the system scenario depicting that client will register with the third-party authentication server and all the server involved including CS and Authentication Server (AS) must get registered with each other by sharing a secret key.

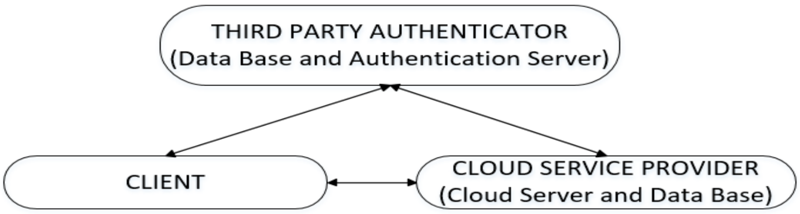

THIRD PARTY AUTHENTICATOR
(Data Base and Authentication Server)
CLIENT
CLOUD SERVICE PROVIDER
(Cloud Server and Data Base)

Fig. 4: Multi-Factor Authentication for CC (S.Nagaraju and L.Parthiban 2016)

Cloud Cat tool was developed by [23] for flexible, protected and effective management of multiple user accesses in cloud environment. The aforesaid model was based on the combination of Cyphertext Policy-Attribute-Based-Encryption (CP-ABE) and access control model based on roles (RBAC).

The model consisted of four modules such as Authentication Manager responsible to control access to the data in the cloud database According to the model, Authorization Manager controls the administration and implementation of security policies. Moreover, policy deployment can only be done by data owners or administrators. Another module included in the system is the User Access Control Management which provides access to the data and the last is Collaborative Ciphertext Policy Attribute-Role Based Encryption Model C-CP-ARBE access control algorithm which is used to provide the cryptographic processes for the users.

Also, in healthcare systems the authenticity is of great concern. In view of aforementioned, [24] has made a framework for Electronic Health Record (EHR) system over cloud. The system was made in a manner that patient report can be shared through cloud with the doctors in such a way that privacy of the patient should not be compromised. In addition, the requested EHR encryption is done using symmetric keys for the communication between the two doctors. The model was made in a way that an individual EHR server was placed on each health care provider side and finally they were connected to the cloud shared environment.

The Fig.5 is showing the EHR cloud system proposed by the author. For instance, two health servers are shown. As per the system, the doctors can share the information through the cloud server with more authentication as it is dedicated cloud for the EHR. Moreover, this system is typically for the health care, not very much reliable for the sensitive data.

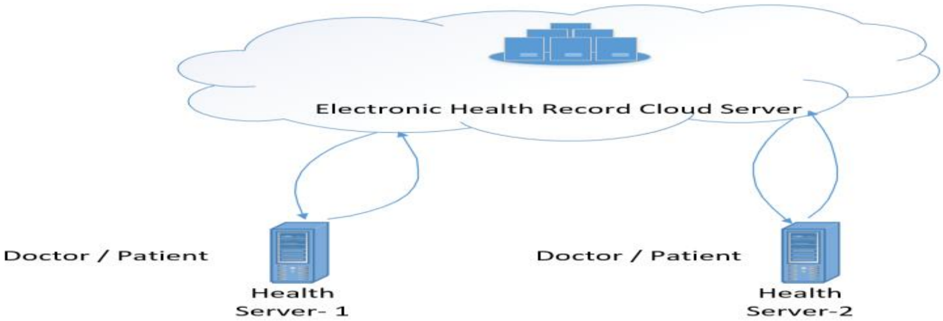


Fig. 5: Framework for Sharing EHR over Clouds (A. Ibrahim et al. 2016)

In other study, [25] proposed a security architecture for CSP to check the data integrity with user authentication system. For the said purpose, the authors used One Time Password (OTP) and modified SHA-2 hash function for authentication and integrity checks respectively. The system architecture along with steps is shown in Fig.6.

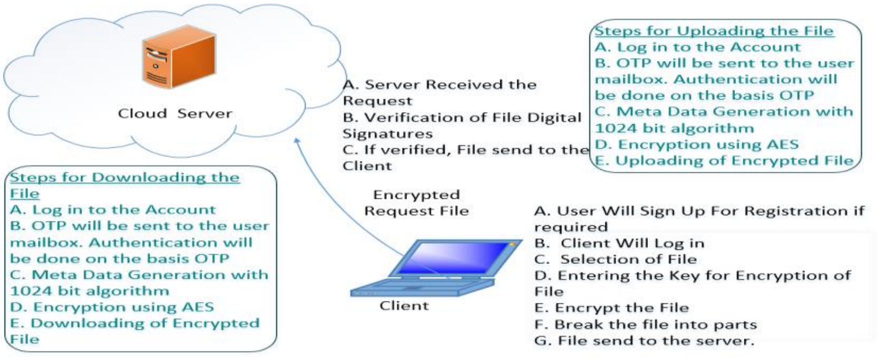

Cloud Server
Steps for Uploading the File
A. Log in to the Account
B. OTP will be sent to the user mailbox. Authentication will be done on the basis OTP
C. Meta Data Generation with 1024 bit algorithm
D. Encryption using AES
E. Uploading of Encrypted File
A. Server Received the Request
B. Verification of File Digital Signatures
C. If verified, File send to the Client
Encrypted Request File
Steps for Downloading the File
A. Log in to the Account
B. OTP will be sent to the user mailbox. Authentication will be done on the basis OTP
C. Meta Data Generation with 1024 bit algorithm
D. Encryption using AES
E. Downloading of Encrypted File
Client
A. User Will Sign Up For Registration if required
B. Client Will Log in
C. Selection of File
D. Entering the Key for Encryption of File
E. Encrypt the File
F. Break the file into parts
G. File send to the server.

Fig. 6: Security Architecture for CSP (N.R.Patil and R.Dharmik 2016)

The model in Fig.6 has used single authentication method in which only OTP was required for the file encryption and decryption.

In [26], another authentication scheme was produced consisting of pass generator. The system was designed in such a way that user must pass through different phases like registration, login, image update as shown in Fig.7.

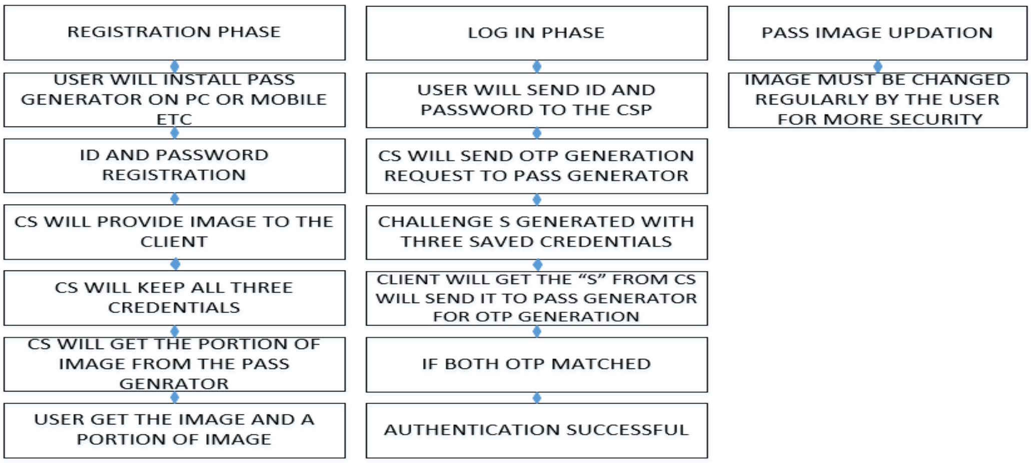

REGISTRATION PHASE
USER WILL INSTALL PASS GENERATOR ON PC OR MOBILE ETC
ID AND PASSWORD REGISTRATION
CS WILL PROVIDE IMAGE TO THE CLIENT
CS WILL KEEP ALL THREE CREDENTIALS
CS WILL GET THE PORTION OF IMAGE FROM THE PASS GENRATOR
USER GET THE IMAGE AND A PORTION OF IMAGE
LOG IN PHASE
USER WILL SEND ID AND PASSWORD TO THE CSP
CS WILL SEND OTP GENERATION REQUEST TO PASS GENERATOR
CHALLENGE S GENERATED WITH THREE SAVED CREDENTIALS
CLIENT WILL GET THE "S" FROM CS WILL SEND IT TO PASS GENERATOR FOR OTP GENERATION
IF BOTH OTP MATCHED
AUTHENTICATION SUCCESSFUL
PASS IMAGE UPDATION
IMAGE MUST BE CHANGED REGULARLY BY THE USER FOR MORE SECURITY

Fig. 7: Strong Password Generator Model (A.Abdellaoui et al. 2016)

According to the Fig. 7, for registration, the user must install the pass generator application in his/her PC or any other device. Then user has to register the id and password for the said phase and that will finally be saved in the Cloud Server (CS). According to the system, CS will assign an image to the client and will save all of the three credentials for the later use. Moreover, for more security the CS will get the image and a portion of image from the pass generator and will send it to the user who will save the aforesaid identifications. In the login phase the user will send the id and password to the CSP. After the authentication, CS will send the OTP generation request to the cloud password generator. In the next step, challenge S will be generated from the previously saved credentials which were id, password and the image. The client will get the challenge S from the CS and will send it to its password generator application which will then generate an OTP for the client. If OTP generated by the client and CS matches, then the client will be allowed to access the cloud for the services. Moreover, in the third phase, the image should be updated or changed by the user often for more security. The aforesaid system is shown in Fig.6 depicting the two-factor authentication with OTP and picture challenge. The stated system provided good authentication. More so, there is a need of a model that should support more layers of authentication for the sensitive data accessing. Moreover, use of additional layers of security can make system a bit slow but security in some cases gets the priority.

Additionally, more layers should be designed in such a way that it should not disturb the systems effectiveness.

3. Critical Analysis

The Table I is showing the latest work done in the field of authentication in CC along with the narration of pros and cons.

TABLE I Summary of Comparative Study

Ref	Year	Advantages	Disadvantages	Suggestions
[22]	2016	It is vigorous and efficient	Device theft can cause a security breach.	Multifactor can be combined with the more challenge so that it becomes stronger
[23]	2016	In Comparison, Secure for the users	Old Technique. No strong password encryption is used	Data and password must be encrypted more strongly
[24]	2016	Secure System for medical use	Not suitable for sensitive kind of data.	With the help of more advanced encryption algorithm it can get more secure and efficient
[25]	2016	Used One Time Password (OTP) Authentication. Easy to Implement	Only one layer of security i.e. OTP	Need to propose more secure technique for the users
[26]	2016	Authentication is done based on Challenge image. Difficult to hack	Time consuming.	Biometrics challenge can also be included for authentication

All the authors in Table I have done well but security and more so authentication in CC requires more research. Because hackers are becoming day by day stronger and equipped. The design of authentication should be in such a manner that to steal an information, a person should pass through different steps to get the information. A system with the combination of multifactor authentication along with the integration of biometrics [22] and a third layer must be implemented like challenge picture [26] can make an authentication system more vigorous and stronger. Moreover, this additional third layer of security will be for the people who are interested in fool proof security for the protection of the data. As far as normal users are concerned OTP and two-layer authentication is good enough.

4. Conclusion

In this paper, we have reviewed several works related to the authentication in CC. Researchers have done well in proposing their work by using different techniques. Still the gaps are there as we did not yet get the perfection in authentication system for cloud CC. After reviewing all the material related with pros and cons, we concluded that a system with multifactor authentication along with biometrics verification and integration of some challenge question for a user can make the CC system more vigorous as far as authentication processes are concerned. Integration of the OTP with biometrics along with the challenge text or image will add a third layer of authenticity for the users who require more security. Moreover, for future works, biometrics of all ten fingers of user hand should be in CS database. Whenever user want to log in he or she will be passed through multi factor authentication and can be asked for specific finger authentication for example when a user log in for the first time the server can ask for the biometric of the left thumb impression. Moreover, as far as data encryption is concerned, AES can be adopted as it is the strongest encryption technique. Additionally, there is no system yet made for authentication which can bypass the service provider staff involvement because they can steal any body's credentials any time. So, there is a need to make such a fool proof authentication system in which involvement of CSP staff should be less.

Acknowledgments

*Funding support was provided by the Ministry of Higher Education in Malaysia (No. FRGS/1/2016/ICT03/UMP/02/1), and the fund of COMSTECH-TWAS joint research grants the program for young scientists in OIC countries No. 14-340 RG/ITC/AS_C.

References

[1] R. Sravan Kumar and A. Saxena, Data integrity proofs in cloud storage. in communication systems and networks (COMSNETS), in Proc. of 2011 Third International Conference on, 2011.
[2] S. Nepal et al., DIaaS: Data Integrity as a Service in the cloud, in Proc. of IEEE International Conference on Cloud Computing, 2011.
[3] S. Subashini and V. Kavitha, A survey on security issues in service delivery models of cloud computing, in Proc. of Journal of Network and Computer Applications, pp. 1-11, 2011.
[4] C. Ning et al., Privacy-preserving multi-keyword ranked search over encrypted cloud data, in Proc. of IEEE Conference, 2011.
[5] F. Jun et al., Analysis of integrity vulnerabilities and a non-repudiation protocol for cloud data storage platforms, in Proc. of 39th International Conference on Parallel Processing Workshop, 2010.
[6] S.M. Khan and K.W. Hamlen, Anonymous Cloud: A data ownership privacy provider framework in cloud computing, in Proc. of IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2012.
[7] F. Sebe et al., Efficient remote data possession checking in critical information infrastructures in Proc. of IEEE Transactions on Knowledge and Data Engineering, vol. 20, pp. 1034-1038, 2008.
[8] A. Juels and J. Burton S. Kaliski, Pors: proofs of retrievability for large files, in Proc. of 14th ACM conference on Computer and communications security, pp. 584- 597, 2007.
[9] G. Ateniese et al., Provable data possession at untrusted stores, in Proc of 14th ACM conference on Computer and communications security, pp. 598- 609, 2007.
[10] Z. Tan, Z. Tang, R. Li, A. Sallam, and L. Yang, Research on trust based access control model in cloud computing, in Proc. of 6th IEEE Joint International Information Technology and Artificial Intelligence Conference (ITAIC), vol.2, pp. 339- 344, 2011.
[11] S. Yu, C. Wang, K. Ren, and W. Lou, Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing, in Proc. of IEEE INFOCOM, pp. 1-9, 2010.
[12] J. Ilanchezhian, V. Varadharassu, A. Ranjeeth, and K. Arun, To improve the current security model and efficiency in cloud computing using access control matrix, in Proc. of Third International Conference on Computing Communications and Networking Technologies(ICCCNT), pp.1-5,2012.
[13] Y.Jin, C.Tian, H.He and F.Wang, A secure and lightweight data access control scheme for mobile cloud computing, in Proc. of IEEE Fifth International Conference on Big Data and Cloud Computing, pp. 172179, 2015.
[14] Z.Wan, J. Liu, and R.Deng, A hierarchical attribute-based solution for flexible and scalable access control in cloud computing, in Proc. of IEEE Transactions on Information Forensics and Security, vol. 7, pp. 743-754, 2012.
[15] M.Hwang and T. Hung Sun, Using smart card to achieve a single sign on for multiple cloud services, in Proc. of IETE Technical Review, September, 2013.
[16] J.W. Tsaur, H.Li and B.W.Lee, An efficient and secure multi-server authentication scheme with key agreement, in Proc. of Journal of Systems and Software, vol. 85, pp. 876882, 2012.
[17] A. Yassin, H.Jin, A.Ibrahim, W.Qiang, and D.Zou, Cloud authentication based on anonymous one-time password, in Proc. of International Conference on Information Technologies and Applications, Netherlands, 2013.

[18] Z.Yan, X.Li, M.Wang and A.V. Vasilakos, Flexible data access control based on trust and reputation in cloud computing, in Proc. of IEEE Transactions on Cloud Computing, vol. pp, issue. 99, pp. 1-1, 2015.

[19] S.Singh and V.Kumar, Secured users authentication and private data storage- access scheme in cloud computing using elliptic curve cryptography, in Proc. of 2nd International Conference on Computing for Sustainable Global Development, pp. 791-795, India, 2015.

[20] Z.Liu, H.Yan and Z.Li, Server-aided anonymous attribute-based authentication in cloud computing, in Proc. of International Journal on Future Generations Computer System, Vol. 52, pp. 61-66, 2015.

[21] Z.Asadullah and O.Oyefolahan, Factors Influencing Information Privacy Concern in Cloud Computing Environment, in Proc. of International Symposium on Mathematical Sciences and Computing Research (iSMSC), pp. 238-242 , 2015.

[22] S.Nagaraju and L.Parthiban, Provably secure multi-factor authentication for the cloud computing systems, in Proc. of Indian Journal of Science and Technology, 2016.

[23] S.Fugkeaw and H. Sato, A collaborative access control tool for data outsourced in cloud computing, in Proc. of 10th International Conference on Digital Information Management, pp. 243-248, 2015.

[24] A.Ibrahim, B.Mahmood and M.Singhal, A secure framework for sharing electronic health records over clouds, in Proc. of IEEE International Conference on Serious Games and Applications for Health (SeGAH), pp. 1-8, 2016.

[25] N.R.Patil and R.Dharmik, Secured cloud architecture for cloud service provider, in Proc. of World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), pp. 1-4, 2016.

[26] A. Abdellaoui, Y.I. Khamlichi and H. Chaoui, A novel strong password generator for improving cloud authentication, in Proc. of International Conference on Computational Modelling and Security (CMS), vol. 85, pp. 293-300, 2016.

[27] K. Chauhan, A. Sanger and A. Verma, Homomorphic encryption for data security in cloud computing, in Proc. of International Conference on Information Technology, pp. 206-209, 2015.

[28] R. Mishra, D. P. Mishra, A. Tripathy, and S. K. Dash, A privacy preserving repository for securing data across the cloud, in Proc. of 3rd Int. Conf. Electron. Comp. Tech, pp. 6–10, 2011.

[29] M. S, E. Daniel, and N. Vasanthi, Survey on Various Data Integrity Attacks in Cloud Environment and the Solutions, pp. 1076–1081, 2013.

[30] K. Khan and M. Shaheen, Exploring data security in cloud without encryption, in Proc. of IEEE 16th International Conference on Computational Science and Engineering, pp. 9–14, 2013.

[31] S. Hohenberger, B. Waters, Attribute-based encryption with fast decryption, in Proc. of Public-Key Cryptography, pp. 162–179, 2013.