Journal of Contemporary Issues in Business and Government Vol. 27, No. 3,2021
https://cibg.org.au/

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.240

A MULTILEVEL USER VALIDATION FRAMEWORK FOR ACCESSING CLOUD SERVICES

Swetha Gadde [1] Janaki .K[2]

[1] Department of Information Technology, RVR&JC College of Engineering, Chowdavaram, Guntur, Andhra Pradesh, India

[2] Department of Computer Science and Engineering, Rajarajeswari College of Engineering, Bengaluru, Karnataka, India

ursgadde@gmail.com, karur.janaki@gmail.com

ABSTRACT: Cloud computing is a paradigm that offers enormous advantages to cloud users for example, huge memory, adaptable processing abilities, security to the data and boundless registering capabilities. To utilize the maximum capacity of Cloud computing, information is moved, handled and stored by Cloud Service Providers (CSP). Be that as it may, information owners are suspicious to put their information in cloud that is outside their own control. The main issue with Cloud computing is the manner by which to provide the security and protection of cloud user information being prepared and additionally stored in a Cloud computing condition. With regards to cloud information assurance, the techniques utilized can be fundamentally the same as ensuring information inside a conventional server group. To perform user validation for accessing cloud services, a strong cryptography method is introduced along with a multi factor verification process. Moving information into the cloud implies that the clients have less authority over their information, this implies the cloud clients must believe the CSP to secure the information from both outside and inside attacks. In the proposed work, a Multi Level User Authentication (MLUA) framework is introduced for accessing cloud services. The unauthorized users are not allowed to access cloud resources. The cloud user, data owner and cloud service providers are involved in multi factor authentication. The CSP will generate a Digital Unique Authentication Identity (DUAI) number along with general verification for undergoing multi level verification process. The proposed method is compared with the traditional methods and the results show that the proposed method is better in performance and accuracy in identification of valid cloud users.

Keywords: Cloud Data Security, Cloud User Validation, Multi Level user Validation, Digital Unique Authentication Identity, Unauthorized User Identification, Validation Accuracy.

Journal of Contemporary Issues in Business and Government Vol. 27, No. 3,2021
https://cibg.org.au/

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.240

1. Introduction

Cloud computing is one of the applied advances for data storage and for accessing its services user validation process must be done [1]. It dependents on the idea of on-request sharing services over the web. These services are systems, servers, storage, applications, and administrations [2]. Cloud computing is accessible in pay more only as costs arise. Security of Cloud computing is one of the essential issues and difficulties. It is imperative to convey a protected cloud and impervious to assaults. Cloud Service Providers should actualize a dynamic access control system for their framework. Services and information in the cloud are profoundly delicate. When a client needs to get to any of cloud's service ought to validate users to guarantee that approved clients can get access to the cloud's services [3] [4]. A very much planned access control arrangements should be received so as to forestall unapproved access to the cloud [5]. As innovative advances proceed, the range and impact of Cloud computing keep on rising. All things considered, when associations re-appropriate information and business applications to CSP, security and protection issues develop as essential concerns. The cloud computing models are depicted in Figure1.

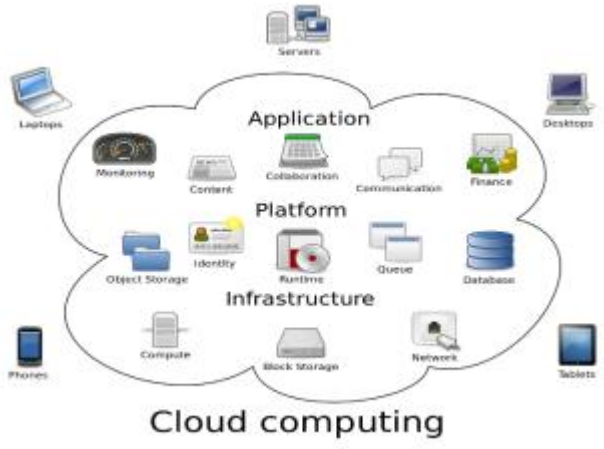

Fig 1: Cloud Computing Models

CC has a few advantages by allowing clients to utilize framework, stages, and programming arranged by CSP. One of the advantages of utilizing CC is decreasing the expenses for introducing virtual products just as equipment [6] [7]. Another preferred position is that, you no more need to help the basic models. Identification of client's is the most significant objective behind verification. Individual ID is frequently received as the main security component for cell phones [8]. Clearly, ID isn't extremely secure component for verifying clients in light of its impediment, just as it is hard to confirm that the interest is from the original data owner [9] [10]. A efficient technique for validation that is proposed should cover one or a few different components of distinguishing proof to improve security. These components are something client know; something client have; something client are. The security model introduced can be deployed in any of the cloud model that is depicted in Figure 2.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.240

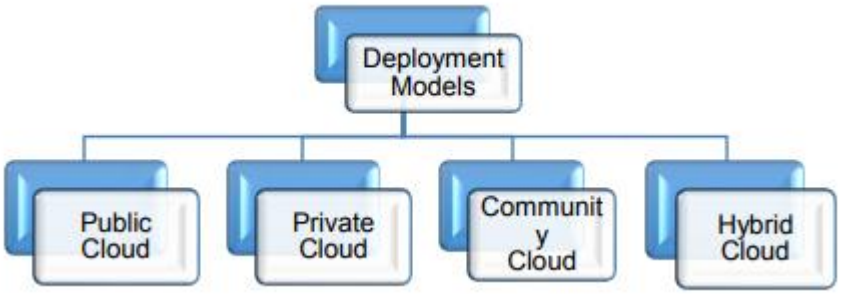

Fig 2: Cloud Deployment Models

Multi Level User Authentication (MLUA) can be characterized as the utilization of more than one lot of verification stages in different stages that are utilized for performing validation of users [11] [12]. Commonly, one classification of 'factors' is something that is recognized, for example, a client ID, data owner ID and Cryptography Key. Another factor that is added to this is frequently something that have a Digital Unique ID token that when combined with the primary factor builds the authenticity of confirming users to access the cloud services [13] [14].

MLUA is one of the most dynamic and significant regions inside data security. The utilization of passwords to verify has been suspected specifically for high worth exchanges and utilization of basic uncertain and regularly reused, handily speculated or passwords are sufficiently bad. Requiring different factors to get to significant substance or to lead high-esteem exchanges is progressively required and is the focal point of this model [15] [16]. MLUA is a subset of the verification model and is frequently suggested dependent on versatile validation verification dependent on security strategy or potentially logical information in regards to the individual cloud access [17].

The test with MLUA is to adjust the requirement for security effortlessly of utilization. The more information that is gathered on the side of the client's side includes what their identity is, the key that they have, and their behavior. Cryptography techniques are utilized for generating keys that has to be shared between the cloud user, data owner and CSP [18]. The Keys are communicated among them for accurate user validation and allowing to access cloud services [19]. In the proposed strategy for encryption, the keys are generated and then while user login the keys are checked for accurate validation. In the proposed work, the users are validated.

2. Literature Survey

Validation is the demonstration of affirming reality of a characteristic of a user for using of information or data stored in cloud. Validation is applicable to

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.240

numerous fields and it is significant in cloud computing. In cloud computing, confirmation is the procedure through which programming, PC, client, or framework checks the character of a user that desires to use some service. Validation is unique in relation to approval for allowing to user services of a cloud.

Jignesh S et. al. [1] proposes a system where the cloud environment is used to achieve access restrictions, and simultaneously used to ensure the protection for the data. The data created utilizing the SID in the secured information are all different in any event, for a similar user for every one of their electronic clinical record numbers. It has the unlink ability trademark. What's more, a onetime key is utilized for data encryption to upgrade the security of the encoded segment. The use of the cloud environment not just permits emergency conditions with fewer services to get the data administration and electronic clinical records, yet additionally permits to survey their own records at home.

Zkik Ornahou et al. [2] proposed Cloud Proof as a safe storage framework to ensure secrecy, respectability and compose serializability utilizing obvious verifications of intrusion by outsiders. Classification is guaranteed by private keys that are known uniquely to the owner of the information that will be encoded. The fundamental thought behind Cloud Proof is the utilization of the verification system. Authentications give verification of stability of clients, information owners and cloud service providers. Information owners utilize a identifier to procure the substance of a open place. This system empowers clients to store information by putting a identifier and the substance of the identity in the cloud.

Y. Zhang et al. [4] proposed a model that empowers clients to confirm the integrity of Virtual Machines VMs in the cloud. The arrangement is known as the trusted Cloud computing stage, and the entire IaaS is viewed as a private framework rather than accessible to all. In this methodology, all hubs run a trusted virtual machine screen to seclude and secure virtual machines. Clients are offered access to cloud benefits through the cloud administrator segment. The outside confided in element is another part that gives a trust facilitator administration so as to monitor the trusted VMs in a cluster.

H. Kwon et al. [5] proposed Swap and Play as a methodology for live refreshing of hypervisors without the need to reboot the VM for high accessibility. The proposed plan is adaptable, usable and material in cloud conditions and it has been executed in Xen as one of the most well known hypervisors. Swap and Play gives strategies to move the in-memory condition of the running hypervisor to the refreshing state, notwithstanding refreshing the basic host. Swap and Play comprises of three free stages: readiness, appropriation and update. In the readiness stage, data for the later state move is gathered. The appropriation stage

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.240

conveys the update data on the objective host for refreshing. In the last advance, the update data is fixed to singular has in the cloud.

K. V. Pradeep et al.[6] address the issue of trust between information owner and CSP, by disposing of trust prerequisite between them. They propose a protected information storage plan where security of the information will be constrained by information owner as it were. Information owner indicates get to rights for his/her own information and oversees disavowal, assuming any. Clients may look through the records in a scrambled database, in a protected way, with the assistance of positioned keyword search. Their method follows a Client/Server model, where cloud user plays out every single cryptographic activity, though server performs search tasks over the scrambled information. Also, cloud user application informs the information owner if there should be an occurrence of any security break through.

Z. E. Dawahdeh et al.[7] propose a hybrid control model using Attribute Based Encryption (ABE), intermediary re-encryption. Records contain characteristics and open key comparing to these traits. Access structure of records is characterized by the intelligent articulations over public key qualities. Information document sets are characterized for every client. Documents are encoded by symmetric keys. Symmetric keys are scrambled with attribute based encryption comparing to key strategy. To reject a client, information owner indicates insignificant arrangement of traits and alters open and secret key as indicated by the predefined properties.

The greatest difficulties cloud and specialist organizations faces are secure information storage, fast access to the Internet, and normalization. Storing a lot of information that is arranged around client security, personality, and application-explicit inclinations in unified areas raise numerous worries about information insurance. These worries, thus, offer incline to questions with respect to the legitimate system that ought to be actualized for a cloud-arranged condition.

A two-factor verification model for Cloud computing is introduced in [9] by utilizing USB token with a mix of various procedures, for example, hash model and Diffie-Hellman key understanding. It comprising of three stages: Registration, login, validation stage, and two exercises: a difference in secret phrase and USB token reinforcement. In examination with the current strategies, the current technique is demonstrated increasingly more powerful in Cloud computing since it accomplishes both usefulness and security prerequisites. The usefulness prerequisite it gives, includes shared confirmation, no check table, client protection, key exchange, and picking and refreshing the secret phrase unreservedly.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.240

3. Proposed Method

Techniques for confirming individuals contrast from those used to verify machines or projects, because of significant contrasts in the capacities of individuals and PCs. Approaches for human validation depend on the accompanying variables:

- Information factors something the client knows (for example a secret key) - the most well-known type of confirmation
- Ownership factors something the client has (for example a token) - frequently an equipment or programming token
- Inherence factors something the client is (for example unique mark) - verification depends on something secretly validated.

The kinds of validation accessible contrast in their degree of security. Also, by joining factors from the at least one of the three classes of elements the degree of security can be additionally raised. The decision of the various techniques for validation relies upon numerous variables, for example, ease of use, the significance of the data that must be ensured, and the expense of the framework. Some of the time a procedure called common verification is utilized, where the two gatherings verify one another.

In this proposed work the calculation and usage of different stages and exercises of multi level secure validation is introduced. All the clients and cloud specialist organizations should be straightforward in the enrollment stage. After enlistment stage is finished, no client, cloud specialist co-op is trusted. Clients are required to check themselves during login and verification stage by giving genuine and definite ID subtleties for getting to cloud administrations, applications and services. To get to cloud information administrations, if validation plays a key security job then client can have a sense of security to utilize frameworks. So keeping validation as our fundamental center, we have proposed here security design which offers confirmation as a administration to cloud information owners and clients. The design too comprises of cloud information security

Customary verification methods don't function admirably for cloud as cloud is exposed to different assaults. So watching the cloud powerlessness, it needs very much organized and all around characterized security. The arrangement is execution of MLUA, which consolidates more than one autonomous component for dynamic validation process. The goal of MLUA is to make a strong assurance and make it all the more trying for an unapproved individual to get to target and restrict them to access cloud services.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.240

In the Cloud User (CU) Registration Level, CU needs to enroll to the CSP by giving suitable recognizable proof data. The CSP Registers the CU information and generates a Digital Unique Authentication Identity (DUAI) number and the CU has to submit the DUAI whenever and where ever required. The authentication process is done in multiple levels for accessing cloud services. The process for user Registration is discussed clearly

1. CU Sends Membership Request (MR) to CSP.
2. CSP creates a secret key for the CU using his identity and based on the secret key CSP generates the DUAI number and assigns to CU along with basic login credentials. The key is generated as

   - Select 2 numbers Pr(X) and Pr(Y) where X and Y are even and odd numbers and X must be greater than Y.
   - PubKey(CU(i)) = Pr(X) | Pr(Y) * K +T(i)
     Where K is constant and T(i) is the time instance at registration.
   - PrKey(Cu(i)) = Pr(X)/Pr(Y) + PubKey(Cu(i))
   - PrKey(Cu(i)) = PrKey(Cu(i)) & PubKey(Cu(i))
   - DUAI(Cu(i)) = PrKey(Cu(i)) | Pr(X) + PrKey(Cu(i)) & Pr(Y)
   - DUAI(Cu(i)) = DUAI(Cu(i)) + PubKey(CU(i)) + T(i)

3. CSP server updates the DUAI, PubKey and PrKey and allots the permissions to CU to access cloud services.
4. Every time CU request for a cloud service, Cu has to submit the DUAI number for getting permissions.
5. CU gives every necessary authorization credential and submits.
6. CSP allots permissions to access cloud services.

After registration of CU with CSP, if it requests to store data in cloud, the CU becomes Data Owner (DO). The DO if needs to store the data in the cloud, it has to send a DATA-STORE request to CSP. The Process of Validation of users is depicted clearly.

1. DO send DATA-STORE request to CSP
2. CSP request for basic login credentials.
3. After successful validation, CSP requests to submit DUAI number and Identity submitted during registration from the user and it validates it whether it is received from genuine user or not based on the identity.

   DO (i) → DUAI(CU(i)) + ID
   CSP→ Record Time Instance T(i)
   - PrKey(Cu(i)) = PrKey(Cu(i)) | PubKey(Cu(i))

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.240

- DUAI(Cu(i)) = PrKey(Cu(i)) & Pr(X) + PrKey(Cu(i)) | Pr(Y)
- DUAI(Cu(i)) = DUAI(Cu(i)) + PubKey(CU(i)) + T(i)
- If (DUAI(CU(i)) = = (DUAI(DO(i))
  Allowed to access the cloud services.
  else
  Remove the CU from cloud service accessing list.

4. If the DO is validated then CSP assigns accessing rights and the DO send data to CSP.
5. CSP again request for the DUAI number, verifies it and then stores the data only if the DO is validated successfully.
6. The same process will be continued if CU and DO are different users and for different services also.

The proposed method performs validation of users at different levels and makes the model much stronger to allow only valid users to access cloud services.

4. Results

The proposed MLUA model is implemented in JAVA which performs strong user validation in multiple levels and the cryptography method are applied in key sharing and distribution for performing user validation. The proposed method is compared with the traditional methods and the results are depicted in terms of accuracy, user security level, key generation time, user validation time, data security level.

The key generation time of the proposed MLUA model is compared with the traditional AES model and the key generation time of the proposed method is less when compared to the traditional method. The key generation time intervals are depicted in Figure 3.

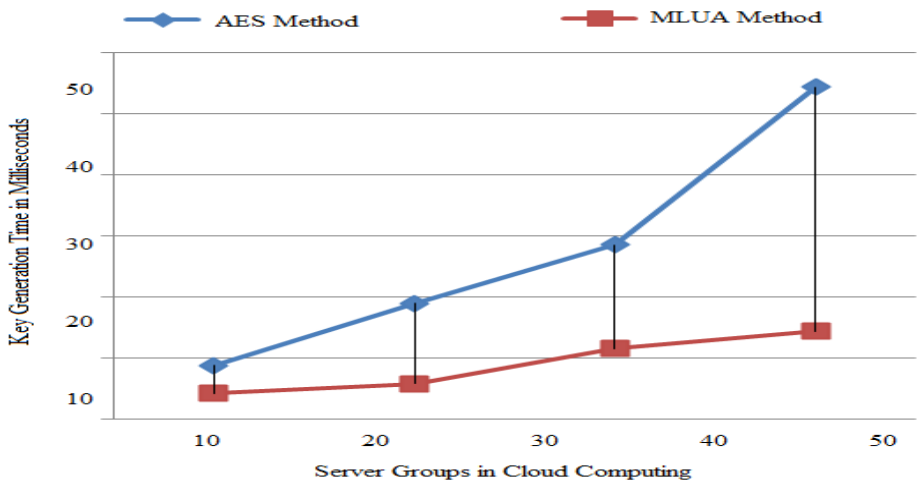

Fig 3: Key Generation Time.

Journal of Contemporary Issues in Business and Government Vol. 27, No. 3,2021
https://cibg.org.au/

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.240

The proposed MLUA model exhibits high security levels for users and allows only validated users to access cloud services. The proposed MLUA model is compared with the existing Trust Level Authentication (TLA) method and the results are depicted in Figure 4.

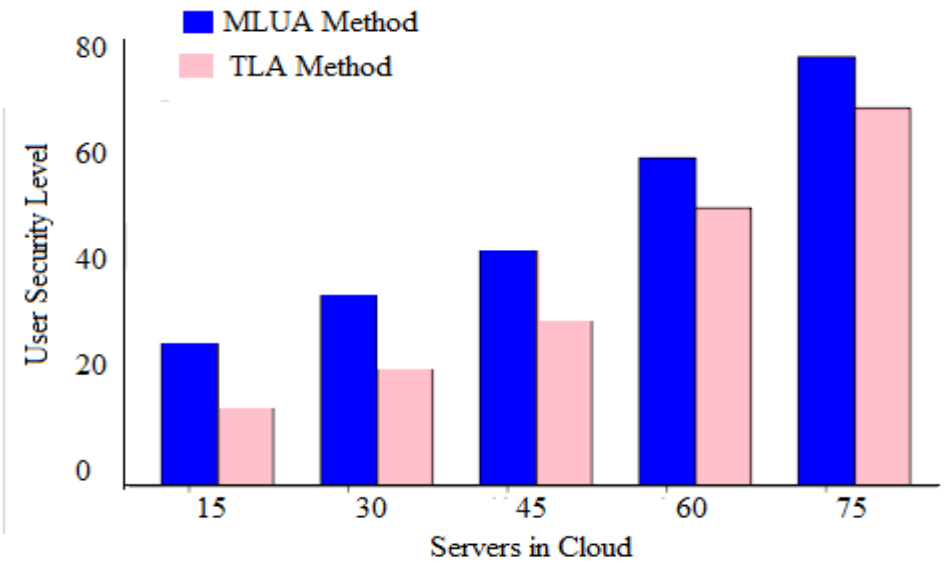

Fig 4: User Security Levels

The proposed MLUA model exhibits high security levels for data stored in cloud and allows only validated users to access cloud services. The proposed MLUA model is compared with the existing Trust Level Authentication (TLA) method and the results are depicted in Figure 5.

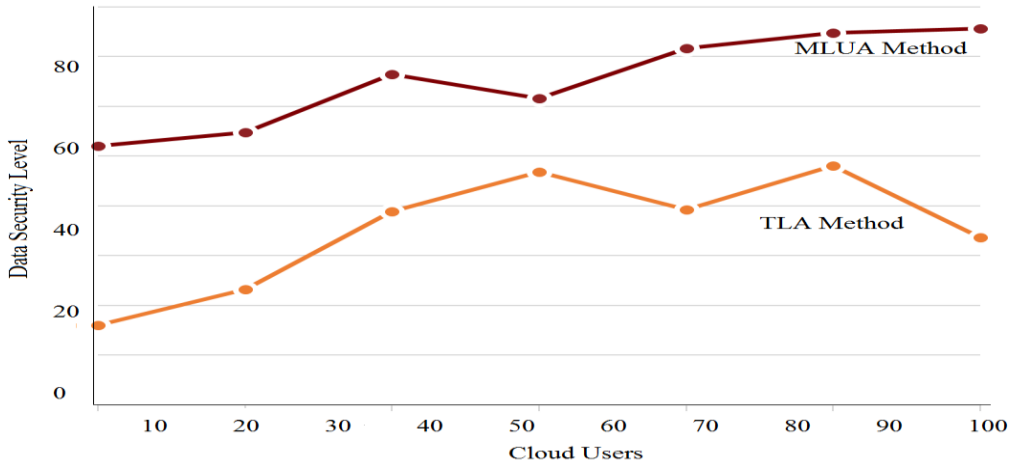

Fig 5: Data Security Levels

Journal of Contemporary Issues in Business and Government Vol. 27, No. 3,2021
https://cibg.org.au/

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.240

The user validation process is done in multiple phases and the successfully validated users are allowed to access cloud services. The user validation process is depicted in Figure 6.

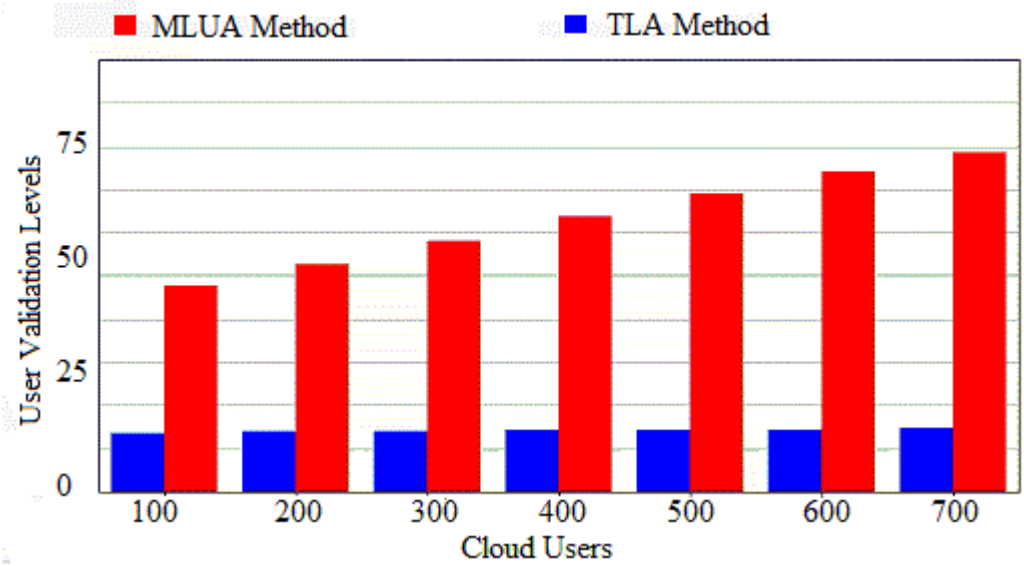

Fig 6: User Validation Levels

The proposed MLUA model performs user validation by allotting a Digital Unique ID for authenticated users. As the validation process undergoes in multiple levels, the authentication is strong. The accuracy levels are depicted in Figure 7.

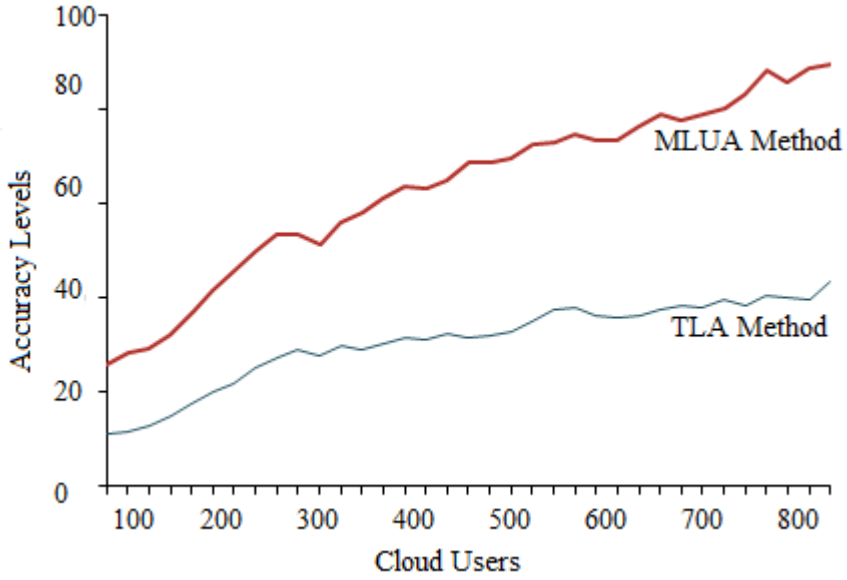

Fig 7: Accuracy Level

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.240

5. Conclusion

Cloud computing is an ongoing method of conveying processing services which acquaints a lot of advantages to the cloud clients. Notwithstanding focal points, it likewise gets new security vulnerabilities, for example, information security, classification, and respectability. To perform user validation for accessing cloud services, a strong cryptography method is introduced along with a multi factor verification process. Moving information into the cloud implies that the clients have less authority over their information; this implies the cloud clients must believe the CSP to secure the information from both outside and inside attacks. MLUA is one of the most dynamic and significant regions inside data security. The MLUA model performs user validations in multiple stages for allowing only valid users to access the cloud resources. Unauthorized users are not allowed to store the data or to access the cloud services. In future, cryptography methods for storing the data in cloud and distributing the data to exact requested users and control on power consumption can be considered for establishing a secured cloud environment for improving customer services, security.

References

[1]. Jignesh S, The 6 multi cloud architecture designer for an effective cloud. https://simform.com/multi-cloud-architecture. 15 Apr 2018.

[2]. Tweaks C, Importance of cloud computing interoperabilitiy. https://cloudtweaks.com/2013/10/importance-of-interoperability-providerlockin. Accessed 15 Nov 2018.

[3]. Zkik Ornahou, Elhajji S (2017) Secure mobile multi cloud architecture for authentication and data storage. Int J Cloud Appl Comput 7(2):213–230.

[4]. Y. Zhang, Q. Chen, and S. Zhong, "Privacy-preserving data aggregation in mobile phone sensing," IEEE Transactions on Information Forensics and Security, vol. 11, no. 5, pp. 980–992, 2016.

[5]. H. Kwon, C. Hahn, D. Koo, and J. Hur, "Scalable and reliable key management for secure deduplication in cloud storage," in Proceedings of the IEEE 10th International Conference on Cloud Computing (CLOUD), Honolulu, HI, USA, June 2017.

[6]. K. V. Pradeep and V. Vijayakumar, "Survey on the key management for securing the cloud," Procedia Computer Science, vol. 50, 2015.

[7]. Z. E. Dawahdeh, S. N. Yaakob, and A. M. Sagheer, "Modified ElGamal elliptic curve cryptosystem using hexadecimal representation," Indian Journal of Science and Technology, vol. 8, no. 15, pp. 1–8, 2015.

[8]. R. Buchade and R. Ingle, "Key management for cloud data storage: methods and comparisons," 2014.

[9]. Arepalli, Gopi & Erukula, Suresh & Gopi, A.P. & Nagaraju, Chiluka. (2016). Secure multicast routing protocol in MANETs using efficient

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.240

ECGDH algorithm. International Journal of Electrical and Computer Engineering (IJECE). 6. 1857-1865. 10.11591/ijece.v6i4.9941.

[10]. K. Sarada, V. Lakshman Narayana,(2020), "Improving Relevant Text Extraction Accuracy using Clustering Methods", TEST Engineering and Management, Volume 83, Page Number: 15212 – 15219.

[11]. K. Sarada, V. Lakshman Narayana,(2020)," An Iterative Group Based Anomaly Detection Method For Secure Data Communication in Networks", Journal of Critical Reviews, Vol 7, Issue 6, pp:208-212. doi: 10.31838/jcr.07.06.39.

[12]. Banavathu Mounika, P. Anusha, V. Lakshman Narayana,(2020), " Use of BlockChain Technology In Providing Security During Data Sharing", Journal of Critical Reviews, Vol 7, Issue 6, pp:338-343. doi: 10.31838/jcr.07.06.59.

[13]. V. Lakshman Narayana, B. Naga Sudheer,(2020)," Fuzzy Base Artificial Neural Network Model For Text Extraction From Images", Journal of Critical Reviews, Vol 7, Issue 6,pp:350-354, doi: 10.31838/jcr.07.06.61.

[14]. V. Lakshman Narayana, A. Peda Gopi,(2020)," Accurate Identification And Detection Of Outliers In Networks Using Group Random Forest Methodoly", Journal of Critical Reviews, Vol 7, Issue 6,pp:381-384, doi: 10.31838/jcr.07.06.67.

[15]. Sandhya Pasala, V. Pavani, G. Vidya Lakshmi, V. Lakshman Narayana,(2020)," Identification Of Attackers Using Blockchain Transactions Using Cryptography Methods", Journal of Critical Reviews, Vol 7, Issue 6,pp:368-375, doi: 10.31838/jcr.07.06.65

[16]. C.R.Bharathi, Vejendla. Lakshman Narayana , L.V. Ramesh, (2020)," Secure Data Communication Using Internet of Things", International Journal of Scientific & Technology Research, Volume 9, Issue 04,pp:3516-3520.

[17]. H. Dinh, A. Dworkin, C. O'Neill et al., "Omnibox: Efficient cloud storage by evaluating dropbox and box," in Proceedings of the 2017 24th International Conference on Telecommunications (ICT) IEEE, Limassol, Cyprus, May 2017.

[18]. Indu, P. M. Rubesh Anand, and S. P. Shaji, "Secure file sharing mechanism and key management for the mobile cloud computing environment," IJST, vol. 9, 2016.

[19]. Armando, R. Carbone, L. Compagna, J. Cuéllar, G. Pellegrino, and A. Sorniotti, "An authentication flaw in browser-based single sign-on protocols: impact and remediations," Computers & Security, vol. 33, pp. 41–58, 2013.