Secure Framework of Authentication Mechanism Over Cloud Environment

Ramesh Shahabadkar[1(✉)], S. Sai Satyanarayana Reddy[1], Chinthakunta Manjunath[2], Ugranada Channabasava[3], and Krutika Ramesh Shahabadkar[4]

[1] Vardhaman College of Engineering, Kacharam, Shamshabad, Hyderabad, Telangana 500018, India
ramesh.shahabadkar@gmail.com
[2] Faculty of Engineering, Christ University, Bangalore, India
[3] K S School of Engineering and Management, Bangalore, India
[4] RNS Institute of Technology Channasandra, Bangalore, India

Abstract. Cloud computing offers a cost effective virtual infrastructure management along with storage and application-oriented services to its customers. This innovation quickly turns into a generally very widely accepted worldview for conveying administrations through web. In this way, this administration expert provider must be offer the trust and information security, on the grounds that there is a most vital and profitable and most delicate information in extremely secure using cryptographic techniques to secure the data in cloud. So for ensure the privacy of essential information, it must be secured utilizing encryptions algorithms and afterward transferring to cloud. This paper presents a novel technique for electronic distributed computing administrations utilizing two-variable validation (2FA) access control framework. The prime target of the projected framework is to guarantee a optimal security for all the actors involved in the component design of proposed authentication system. Furthermore, property based control in the framework likewise authorize cloud servers to maximum the access to those clients with the same arrangement of properties while saving client privacy. At long last, we additionally do a reproduction to show the practicability of our proposed framework. The assessment work is done by utilizing expense of communication, data transfer capacity and proficiency of the framework as an execution metric.

Keywords: Access control · Attributed-based control system · Cloud computing · Two-Factor authentication (2FA) · Web services

1 Introduction

Cloud computing has turns into a generally utilized worldview for dispersing services through the internet. Along these providers, this server must be giving the trust and the information security, on the grounds that significant and extremely delicate information are put away in substantial sum in clouds. To ensure the imperative data present in cloud, it must be encoded before transferring to the clouds utilizing cryptographic strategies. We have predominantly three distinctive trademarks in cloud administration,

R. Silhavy et al. (eds.), *Software Engineering Trends and Techniques in Intelligent Systems*, Advances in Intelligent Systems and Computing 575, DOI 10.1007/978-3-319-57141-6_30

which are unique in relation to routine facilitating. Basically, sold on interest, actually by minutes or 60 min; Elasticity, a client could have as much as of administrations they need at various circumstances by provider [1]. Cloud registering gives a critical enhancement in virtualization and scattered processing, and it enhances access to rapid of web alongside weak economy. There are numerous uses of distributed computing, for example, information. Sharing, information stockpiling, enormous information administration, medicinal in-arrangement framework and so forth. End clients entrance cloud-based purposes during a web plan, delicate customer or transportable submission whereas the commerce programming and client's in sequence are set away on servers at a distant district. The advantages of electronic distributed computing administrations are huge, which incorporate the simplicity of openness, decreased expenses and capital consumptions, expanded operational efficiencies, adaptability, adaptability and prompt time to advertise. Although, the superior features of cloud computing offers a new arena of distributed clock, but it also suffers from security loopholes. There are in the interim additionally worries about security and protection particularly for electronic cloud administrations. As delicate information might be put away in the cloud for sharing reason and qualified clients might likewise get to the cloud framework for different applications and administrations, client validation has turned into one of the most important factor of safety over cloud interface [2]. In order to utilize cloud services, should access their privilege account using standard authentication mechanism of user ID and password. Unfortunately, such conventional mechanism of authentication is no more secure in cloud that uses internet protocol shrouded with massive number of Trojans. To begin with, the conventional record/secret word based authentication is not security saving. Nonetheless, it is all around recognized that protection considered in distributed computing frameworks. Second, it is regular to share a PC among various individuals. It perhaps simple for programmers to introduce some spyware to take in the login secret word from the web-program. An as of late proposed access control model called characteristic based access control is a decent candidate to handle the primary issue. It gives unknown validation as well as further characterizes access control strategies in view of various properties of information object. In a quality based access control framework, every client has a client master key issued by the power. Practically speaking, the client master key is put away inside the PC. When we consider the aforementioned second issue on online administrations, it is normal that PCs might be shared by numerous clients particularly in some extensive endeavors or associations. The point of this dad per is to outline a novel procedure for electronic distributed computing administrations utilizing two-variable verification (2FA) access control framework. Accurately, in our plan 2FA air conditioning access control framework, a characteristic based access control component is executed client mystery key and a lightweight security gadget. Lastly, we additionally complete to show the practicability of our proposed framework. The evaluation work is carried out by using cost of communication, bandwidth and efficiency of the system as a performance metric. This manuscript has been prearranged as follow. Segment 2 explains the related works done by different authors. Segment 3 explains proposed framework as well as implementation part. Segment 4 provides consequences and discussion then, finally Sect. 5 concludes this paper along with future research direction.

2 Related Work

This segment studies is mostly cantered around looking into the current systems and contributory considers talked about by earlier literary works, it is vital for examination that what the current status in the same area is. There are different specialists who have utilized this system on different issues spaces of cloud computing. This paper demonstrates existing condition of research paper, its year of publications, and the name of the distributers. Along these lines, we audit the current number of exploration papers and investigated the viability in them (Table 1).

Table 1. Existing survey on data mining classification methods

Authors	Problem focused	Techniques used	Performance parameters
Fotiou et al. [3]	Security problems and to offers data owners flexibility	Lightweight access control	Lifetime, Number of messages exchanged, Average number of Token
K. Punithasurya et al. [4]	To enhance the Security on cloud	Analysing various access control mechanism	User's convenience, Reusability, Node overhead, Authentication failure
R. Wu et al. [5]	To achieve highly configurable security requirements of cloud	Role-based access control	Activation & Deactivation time, Network traffic
V. Harika et al. [6]	Security and privacy challenges in cloud	Hierarchical attribute based encryption	Execution & Decryption time
A. Sirohi et al. [7]	Data security at cloud	Hash based message authentication, Dual substantiation & access management	Confidentiality, Overhead, Authorization, Encryption, Cost effective
Pandey et al. [8]	Improve cloud security	Trust dependent ciphering process, policy of key management, encryption	Throughput, Time to generate secret generation time, High end reliability
Rashmi et al. [9]	Security challenges in Software	Software as a Service model	Data confidentiality, Authentication
F. I. Oyeyinka et al. [10]	Security challenge and to reduce cost of services	Modified things Role Based Access Control model (T-RBAC)	Network traffic, Cost effective, Confidentiality

(*continued*)

Table 1. (*continued*)

Authors	Problem focused	Techniques used	Performance parameters
S. Kshatriya et al. [11]	Data sharing and security challenges in cloud computing	Survey on data sharing utilizing different encryption technique	Confidentiality
P. Kuppuswamy et al. [12]	Securing cloud storage systems	Partitioning and Role based access control	Client security, Identity and Access management, Authentication
Talib [13]	Distributed data access control, security in cloud computing	Formula-Based Cloud Data Access Control (FCDAC)	Round trip time, security, confidentiality
V. Echeverría et al. [14]	Security in cloud and privacy preserving	Permission as a Service (PaaS), attribute based encryption (ABE)	Confidentiality, Client security
Z. Iqbal et al. [15]	Service access policies representation	Enhance attribute based access manager and rule based representation method	Throughput, high end reliability and confidentiality
S. Yu et al. [16]	Data security & to reduce heavy computation overhead	Ciphering based on attributes	Confidentiality, highly efficient for security
D. A. Gondkar et al. [17]	Protected health record sharing process over cloud	Ciphering based on attributes	Confidentiality, highly efficient for security
Z. Liu et al. [18]	Data security and data for sharing on cloud	Identity-based access control	Overhead, Authorization, Confidentiality

3 Proposed System with Implementation

The projected scheme develops an apparatus of the secret key management over cloud. Owing to insecure cloud environment, the proposed systems divide the secret key. The mechanism that perform localization of each of these two secure splits of key, where one part of the secure key resides over the client's machine while second part of the split key is stored over the secured device. The system performs further security incorporations by using two factor authentication processes which lets attacks know that there are multiple dependencies to perform cryptanalysis. Hence, attackers find it near to impossible to locate another split of the secured key even if compromised the first key split. Hence, the proposed data over the security device where work for further encrypting the client's secret key. There is additionally a connecting relationship

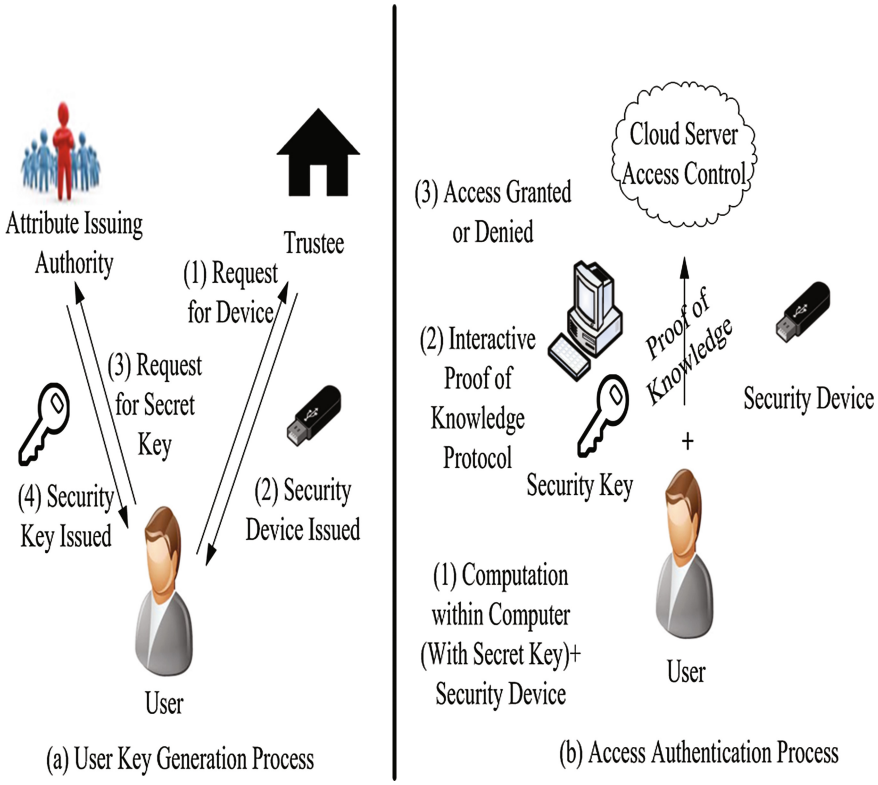

Fig. 1. Overview idea of proposed method

between the client's gadget and the mystery key so that the client can't utilize another client's gadget for the verification. The correspondence overhead is negligible and the calculation required in the gadget is only some light-weight calculations, for example, hashing or exponentiation over gathering. All the substantial computations, for example, matching is done on the PC. The thought of our framework is illustrated in Fig. 1.

4 Results and Discussion

This section, gives the assessment of the proposed strategy is being assessed and authorised. Assume the aggregated number of features in the framework is 100. At the day end, the features universe A $= \{1...100\}$. The analysis processing of the services in order to validate the client is highlighted in Fig. 2. In case of normal strategy, say, comprising of 2 conditions with 2 properties for every statement for a sum of 4 qualities, the time is under 0.3 s. For an approach of 10 conditions with 10 traits for every statement, the processing time is found to be approximately 3 s. Similar trends of the outcomes related to processing time can be seen in the server side too. The outcome

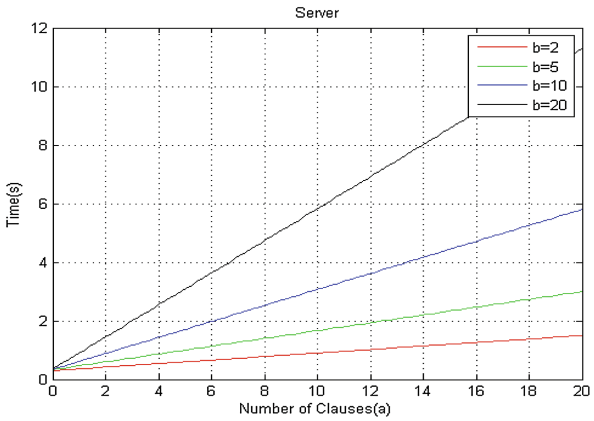

Fig. 2. Time consumption during service-side authentication (sec)

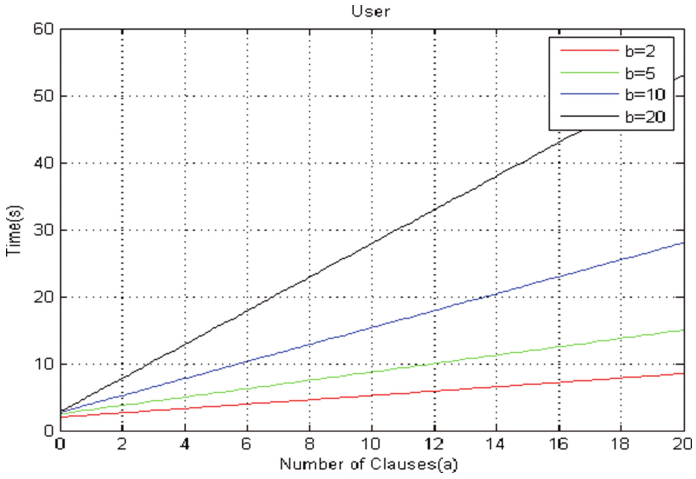

Fig. 3. Time consumption during client-side authentication (sec)

shows that time consumed for operating the client-side application is approximately five times slower owing to the usage of poor security devices for registration.

The outcome shown in Fig. 3 highlights the interesting trends of the processing time for authentication over client side application. Considering more than 100 charecteristics, the cumulative validation time is found to be approximately 18 s. Similar trend is also observed in Fig. 2 where the aggregate data transfer capacity prerequisite is around 45 KB, which is satisfactory throughout today's system. One could accomplish that our protocol is conceivable for extremely straightforward arrangement is still not functional yet for strategy of medium size.

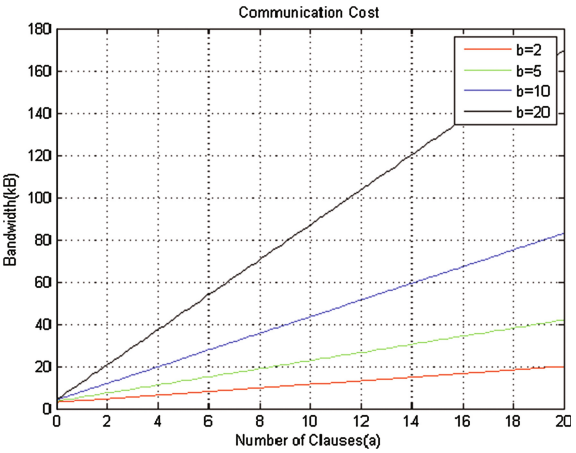

Fig. 4. Communication expense of the Auth protocol (KB)

The correspondence expense of our convention is portrayed in Fig. 4. Specifically, for a policy of 100 qualities, the aggregate data transmission prerequisite is originate to be in the order of 45 KB which is found to be within acceptable limit.

5 Conclusion and Future Research Direction

This article displayed a new 2FA access control framework for online distributed computing administrations. The presented technique not only enhances the mechanism of secure authentication but also leverages the communication system over cloud environment. Point by point security examination demonstrates that the proposed 2FA access control framework accomplishes the coveted security necessities. Through execution assessment, we exhibited that the development is "feasible". The future work to facilitate enhances the effectiveness while keeping every decent element of the framework.

References

1. Nelson, M.R.: Building an open cloud. Science **34**(5935), 1656–1657 (2009)
2. Zhiguo, W., Liu, J., Deng, R.H.: HASBE: a hierarchical attribute-base solution for flexible and scalable access control in cloud computing. IEEE Trans. Inf. Forensics Secur. **7**(2), 743–754 (2012)
3. Fotiou, N., Machas, A., Polyzos, G.C., Xylomenos, G.: Access control as a service for the Cloud. J. Internet Serv. Appl., 6–11 (2015). Springer
4. Punithasurya, K., Jeba, P.S.: Analysis of different access control mechanism in cloud. Int. J. Appl. Inf. Syst. (IJAIS) **4**(2), 34–39 (2012)
5. Wu, R., Zhang, X., Ahn, G.-J., Sharifi, H., Xie, H.: Design and Implementation of access control as a service for IaaS cloud. Automot. Serv. Excell., 1–16 (2013)

6. Harika, A.V., Haleema, P.K., Subalakshmi, R.J., Iyengar, N.Ch.S.N.: Quality based solution for adaptable and scalable access control in cloud computing. Int. J. Grid Distrib. Comput. **7**(6), 137–148 (2014)
7. Sirohi, A., Shrivastava, V.: Implementing data storage in cloud computing with HMAC encryption algorithm to improve data security. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **5**(8), 678–684 (2015)
8. Pandey, V.K., Patel, S.K., Bedre, S.: A novel trust dependent attribute based encryption (TD-ABE) for improving the cloud security. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **4**(12), 875–881 (2014)
9. Rashmi, Sahoo, G., Mehfuz, S.: Securing software as a service model of cloud computing: issues and solutions. Int. J. Cloud Comput. Serv. Archit. (IJCCSA) **3**(4), 1–11 (2013)
10. Oyeyinka, F.I., Omotosho, O.J.: A modified things role based access control model for securing utilities in cloud computing. Int. J. Innov. Res. Inf. Secur. (IJIRIS) **5**(2), 21–25 (2015)
11. Kshatriya, S., Chaware, S.M.: A survey on data sharing using encryption technique in cloud computing. Int. J. Comput. Sci. Inf. Technol. **5**(4), 5351–5354 (2014)
12. Kuppuswamy, P., A-Khalidi, S.Q.Y.: Analysis of security threats and prevention in cloud storage: review report. Int. J. Adv. Res. Eng. Appl. Sci. **3**(1), 1–10 (2014)
13. Talib, A.M.: Ensuring security, confidentiality and fine-grained data access control of cloud data storage implementation environment. J. Inf. Secur. **6**, 118–130 (2015)
14. Echeverría, V., Liebrock, L.M., Shin, D.: Permission management system: permission as a service in cloud computing. In: IEEE 34th Annual IEEE Conference on Computer Software and Applications Conference Workshops (COMPSACW), pp. 371–375 (2010)
15. Iqbal, Z., Noll, J.: Towards semantic-enhanced attribute-based access control for cloud services. In: IEEE Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 1223–1230 (2012)
16. Yu, S., Wang, C., Ren, K., Lou, W.: Achieving secure, scalable, and fine-grained data access control in cloud computing. In: IEEE Proceedings on INFOCOM, pp. 1–9 (2010)
17. Gondkar, D.A., Kadam, V.S.: Attribute based encryption for securing personal health record on cloud. In: 2nd International Conference on Devices, Circuits and Systems (ICDCS), pp. 1–5 (2014)
18. Liu, Z.: A secure anonymous identity-based access control over cloud data. In: Fourth International Conference on Emerging Intelligent Data and Web Technologies (EIDWT), pp. 292–295 (2013)