Security framework of KCABE in SAAS model

M Sangeetha[1] . Neela V[2]

[1] Department of Computer Science and Engineering, Fatima Michael College of Engineering and Technology, Anna University, Madurai, Tamil Nadu, India.
[2] School of Computing and Information Technology, REVA University, Bangalore, Karnataka, India

Received: 12 August 2022 / Revised: 22 August 2022 / Accepted: 09 September 2022

Abstract — Cloud computing extends its usage to the public in enormous ways. Basically cloud computing is manufactured by three service models. Each model provides its application based on user requirements. This is the cause of reaching cloud computing to the public in short period. Especially to provide data security is used as main aspect . it assures to provide security in IT sectors,business,hospital,administration ..etc. in this paper we focus and rectify security issues of SAAS model by applying KCABE algorithm. The main security threat of SAAS are data access, authorization and authentication. these security threads are overcome by KCABE because of associating set of user attributes with access tree structure. By this concept, client does not depend on providers security measures during data access.

Keywords — KCABE, SAAS, authorization and authentication

I. Introduction

Cloud computing takes to fulfill on-needs server farm. By having on-needs of information center, it needs for controlling all, like buying and presenting machine tools, virtualization, presenting functioning structure, some of needed requests, to set for association, orchestrating firewall, , to set for limit with respect to data. It will make responsible to maintain it via for what seems like forever framework.

In any case, when it picks Cloud Computing, data distributor is liable for the gear obtaining and backing. It is similarly give to extensive combination of programming , stage by way of an assistance. It yields some fundamental organizations on charge. The distributed computing organizations can excite ward to be arranged. This cloud climate gives effectively open available gateway which varieties helpful to the client for dealing with register, stockpiling, organization, request assets.

Public Cloud: The cloud properties which moved by a pariah data centre expert association are named as open fogs. It passes on figuring resources like laborers, software design, limit done in net.

Private Cloud: The appropriated figuring resources which is just used private a lone business or affiliation called as a private cloud. A private cloud might really be arranged on the association's on the spot cloud or worked with via third-social affair expert centre.

Hybrid Cloud: This is mix of public and private fogs, that is restricted composed through advancement that licenses information requests for split between the vendors. Blend cloud gives versatility ,additional noteworthy plan choices in contrast to professional.

Types of service model

Infrastructure as a Service (IaaS): In IaaS, it will charge IT establishments such specialists ,computer-generated machines (VMs), amassing, associations, working systems through a cloud organization merchant. We can make Virtual Machine is operating all operating windows that present everything that needs on it. By means of IaaS, we don't need to regularly ponder the gear or virtualization programming, but other than that, it have to administer the wide range of various things. Using IaaS, we get most outrageous versatility, and simultaneously, we need to put extra vigour interested in upkeep.

Platform as a Service(PAAS): It helps an on-demand environment for making, trying, passing on, and supervising software design requests. The originator responsible to all application, PaaS merchant enables for passing on the track it. Using PaaS, flexibility becomes reduce, but organization of environment managed through data center vendors.

Stage as a Service (SaaS): This springs halfway worked with and supervised software design organizations for end-customers. The situation passes on software design done by web, on-demand, and generally scheduled a participation principle. KCloud advances offer an assortment of freedoms to organizations, autonomous engineers, analysts, teachers, and understudies. By understanding the various administrations, models, advantages and dangers offered by the cloud, clients can settle on educated choices about how to best exploit its contributions.

II. LITERATURE SURVEY

Cloud computing utilizes three kinds of transmission replicas in that various kinds of managements have taken for last users. The three transmission replicas of cloud are SaaS, PaaS and IaaS that gives various kinds of administrations like application stage, foundation assets, and software design as managements towards buyer. There are three sorts of management replicas require distinctive degree of safety administrations in the cloud climate. IaaS contains all cloud benefits as it is called as the establishment of all cloud administrations, Data security issues and dangers are acquired as the abilities are acquired from one assistance model to another. There are distinctive compromises in each assistance model in the terms of intricacy versus extensibility, incorporated highlights what's more, security.

Cloud computing is forming what's to come of IT's nevertheless it drastically affects distributed computing development due to the effect of nonappearance of a consistence climate. By utilizing administrations like framework as an assistance, associations favor to test the security and privacy issues for their basic unfeeling applications in business. In cloud it is hard to ensure the security of corporate information, as they give various sorts of administrations like SaaS, PaaS, and IaaS. Every one of these administrations has their own security issues. SaaS is an assistance model to convey programming wherever requests are distantly enabled through the specialist organization or applicaton, complete available for consumers on request, finished the Internet. SaaS model gives a few advantages to the clients with, for example, it increments operational productivity and decreased expenses. SaaS is speedily ascending by way of prevailing transportation model to satisfy requirements of big professional information technology managements.

In SaaS, the significant security issue is that customer needs to rely upon the supplier for all safety efforts. So it is supplier's obligation hold various clients' back from watching and getting to one another's information. So the clients are not guaranteed about the safety efforts on cloud, it gets hard for the clients to guarantee that privilege safety efforts are given to the information and furthermore they are definitely not guaranteed whether the application will be accessible when required. PCs have been spread broadly inside business, while IT administrations and registering has become resource. Popular SaaS model, effort data took on specialist organization's information focus, which has the information of different endeavors. Also, uncertainty the SaaS supplier favors a public distributed computing administration, the endeavor information may be put away alongside the information of other disconnected SaaS applications. The SaaS merchants should have the application all alone private worker to encourage all the works.

Information access issue is identified with the issues in getting to the information put away on cloud. It is identified with the different security strategies gave to the clients during getting to the information on cloud. Each cloud supplier has its own security strategies, for model if a private venture association can utilize a cloud given by some other cloud supplier for completing its business measures then this association will have its own security strategies due to which no representative can get to information of other representative yet approaches a specific arrangement of information. The security approaches may permit some consideration where some of the workers are not offered admittance to certain measure of information.

Not everything except rather the greater part of the organizations are putting away their representative data in Lightweight Directory Access Protocol (LDAP) workers. In SMB organizations, Active Directory (AD) utilized as the most mainstream instrument for overseeing clients [18], when a portion that has the most elevated SaaS reception rate. The majority of the occasions client records are put away in the SaaS suppliers' data sets and not as a component of the corporate IT framework. Likewise with SaaS, the programming is facilitated outside of the corporate firewall

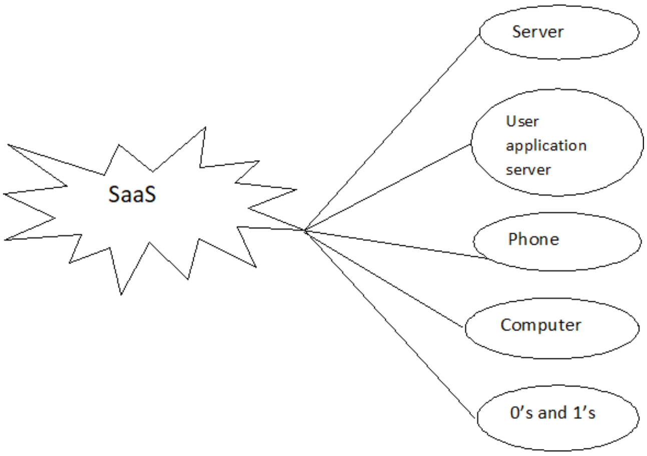

Fig. 1. SaaS system

SaaS Security implies getting customer assurance and corporate data in participation based cloud applications. SaaS applications pass on a ton of tricky data and can be gotten to from for all intents and purposes any contraption by a mass of customers, along these lines addressing a threat to security and sensitive data.it is an on-need, data center based programming movement typical which engages relationship to purchase toward the requests who want short of working with people popular family. SaaS stays single of a couple of characterizations of cloud enrollment organizations, with stage as-a-organization and establishment as-a-organization.

III. PROPOSED SAAS SECURITY

SaaS takes develop continuously renowned since which keeps relationship after hoping for obtaining laborers then additional system or else keep internal provision work. Taking everything into account, a SaaS provider bounces SaaS safety besides backing for item. About striking SaaS requests applications. Greatest endeavor software design venders similarly proposal cloud variations for its submissions, similar to Oracle Financials Cloud.3 layers SAAS security management

A. *Authentication and Data entree manage*

Endorsement is a little part through some of a situation fundings before refutes choice to collect data for its data movement. Entree manage devices kind out for errands the client work through upended out the client's person since a passageway switch slant . Entree manage incorporate:Record consents, like the option to make, read, alter or erase a document,Program authorizations, like the option to execute a program,Information authorizations, like the option to recover or refresh data in a data set.

B. *User data and user approval controls*

The Person object in a corporate information store normally contains an assortment of business data. For instance, data incorporates a room and building number, and office. Data may incorporate a rundown of abilities, current undertaking name, telephone number, and other helpful data. To make a client, you utilize the GUI to interface the User object to an example of individual information for a Person object.

The Person object is not normal for other information objects in the Tivoli Identity Manager information model. The substance of a Person object are connected to a corporate information archive and are recovered dependent upon the situation.

The Identity Manager item doesn't need a prior corporate information storehouse. You can then again design Identity Manager to characterize and store Person object information in the Identity Manager fundamental information storehouse.

C. *Security controls*

Security controls are shields or countermeasures to keep away from, distinguish, balance, or limit security dangers to actual property, data, PC frameworks, or other assets. In the field of data security, such controls ensure the classification, uprightness and accessibility of data. Frameworks of controls can be alluded to as systems or principles. Structures can empower an association to oversee security controls across various kinds of resources with consistency.

In this security architecture diagram, client starts initially to do the user application. It connects with authentication and data access management . In this part , it checks the new user whether they are authorized or not by entering user name and password. If they are authorized only it grants the access control to data. In this paper that access control is taken over by KCABE algorithm. In KCABE algorithm , access tree has specified with usual of user qualities of data. It agree and describe top-secret vital to clients.

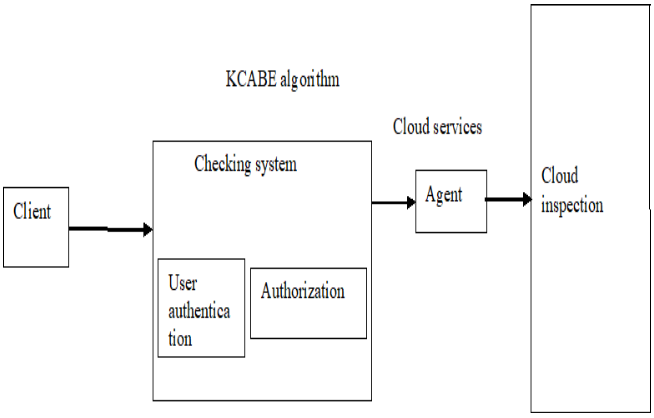

Fig .2. Proposed SaaS security architecture

This means user choose who will encrypt or decrypt data. This will reduce collusion too. So the first management control is totally done by KCABE. Next it goes to user data and user application control. In this area it checks by providing cloud agent whether it does cloud services in right way or not. Cloud agent is acted as intermediate between services and user. It gives right direction to reach user application and checks its availability. So it is used to avoid traffic between the users. It is totally controlled by cloud service agent . it provides more security applications created by API.

Finally it goes to security controls. SaaS security architecture follows ended with this control . cloud is inspected the user logging system and monitored the unauthorization. After inspecting all elements it leads to satisfy security measures of SaaS. Then only it can applicable to security business platform. It comes under control of security system . still the security checking system of SaaS is unreliable one. We are providing this practiises to minimize risk of SaaS.

IV. RESULT AND COMPARISON

Compared to other system KCABE algorithm provides solution to security issues of SaaS. By applying KCABE algorithm it drawbacks are solved by use of access tree structure. This reduce the users uncertainty during data access. Here after user no need to afraid whether it uses proper safety measures or not. And it makes the availability of application when user needs compared it other solution . it gives better way to avoid security threats of SaaS. SaaS is important building model of cloud computing. We focused and rectified main security aspects of data access. Authentication and access control of SAAS will really improve the importance features of SaaS.

V. CONCLUSION

In cloud security , SaaS does important role to provide many user applications. We applied KCABE algorithm to over come the main drawbacks of SaaS. By associating set of user attributes with access tree structure . user does not depend on safety measures of data owner. The KCABE algorithm is directly applied to Authentication and access control to make good accessibility. Thus how SaaS is renewed with better safety measures.

REFERENCES

1. Patel, N. S., & Rekha, B. S. (2014). Software as a Service (SaaS): security issues and solutions. *International Journal of Computational Engineering Research*, *4*(6), 68-71.
2. Sangeetha, M., & Karthik, P. V. (2017, March). To provide a secured access control using combined hybrid key-ciphertext attribute based encryption (KC-ABE). In *2017 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)* (pp. 1-4). IEEE.
3. Swapnil, C., & BR, M. (2016). Secure Data Retrieval based on Attribute-based Encryption in Cloud. *International Journal of Computer Applications*, *134*(13), 31-35.
4. Ahmed, S. T., Singh, D. K., Basha, S. M., Nasr, E. A., Kamrani, A. K., & Aboudaif, M. K. (2021). Neural Network Based Mental Depression Identification and Sentiments Classification Technique From Speech Signals: A COVID-19 Focused Pandemic Study. Frontiers in public health, 9.
5. Baek, J., Vu, Q. H., Liu, J. K., Huang, X., & Xiang, Y. (2014). A secure cloud computing based framework for big data information management of smart grid. *IEEE transactions on cloud computing*, *3*(2), 233-244.
6. Touati, L., & Challal, Y. (2016, May). Collaborative kp-abe for cloud-based internet of things applications. In *2016 IEEE International Conference on Communications (ICC)* (pp. 1-7). IEEE.
7. Dhanasekaran, S., & Vasudevan, V. (2015). A dynamic multi-intelligent agent system for enhancing the cloud service negotiation. *International Journal of Applied Engineering Research*, *10*(43), 30469-30473.
8. Wang, S., Zhou, J., Liu, J. K., Yu, J., Chen, J., & Xie, W. (2016). An efficient file hierarchy attribute-based encryption scheme in cloud computing. *IEEE Transactions on Information Forensics and Security*, *11*(6), 1265-1277.
9. Xia, Z., Zhang, L., & Liu, D. (2016). Attribute-based access control scheme with efficient revocation in cloud computing. *China Communications*, *13*(7), 92-99.
10. Ma, H., Liu, L., Zhou, A., & Zhao, D. (2015). On networking of internet of things: Explorations and challenges. *IEEE Internet of Things Journal*, *3*(4), 441-452.
11. Dhanasekaran, S., & Vasudevan, V. J. C. C. (2019). A Cognizant agent system for optimizing cloud service searching strategy. *Cluster Computing*, *22*(6), 13381-13386.
12. Ahmed, S. T., Sreedhar Kumar, S., Anusha, B., Bhumika, P., Gunashree, M., & Ishwarya, B. (2018, November). A Generalized Study on Data Mining and Clustering Algorithms. In International Conference On Computational Vision and Bio Inspired Computing (pp. 1121-1129). Springer, Cham.
13. Ahmed, S. S. T., & Patil, K. K. (2016, March). Novel breast cancer detection technique for TMS-India with dynamic analysis approach. In 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT) (pp. 1-5). IEEE.
14. Al-Shammari, N. K., Alzamil, A. A., Albadarn, M., Ahmed, S. A., Syed, M. B., Alshammari, A. S., & Gabr, A. M. (2021). Cardiac Stroke Prediction Framework using Hybrid Optimization Algorithm under DNN. Engineering, Technology & Applied Science Research, 11(4), 7436-7441.

MILESTONE
RESEARCH PUBLICATIONS