ISSN 2319-2720

Volume 7, No.2, April – June 2018

International Journal of Computing, Communications and Networking

Available Online at http://www.warse.org/ijccn/static/pdf/file/ijccn20722018.pdf

https://doi.org/10.30534/ijccn/2018/20722018

ACCESS CONTROL FOR TIME SENSITIVE DATA BY USING TIME AND ATTRIBUTE FACTORS IN PUBLIC CLOUD

Prof. Prasanna Kumar M[1], Mythri V[2],Nandini S[3] ,Pallavi P[4],Pruthvika BU[5]

[1]Associate Professor EWIT, India, prasannamysoru@gmail.com
[2]Student,EWIT, India, mythrigowda96@gmail.com
[3]Student, EWIT, India, nandinisept9@gmail.com
[4]Student EWIT, india,pallaviprasannakumar@gmail.com
[5]Student EWIT, India, bupruthvika@gmail.com

ABSTRACT

Cloud storage benefit has critical points of interest on both advantageous information sharing and cost lessening. Therefore, an ever increasing number of endeavors and people outsource their information to the cloud to be profited from this administration. Nonetheless, this new worldview of information stockpiling postures new difficulties on information secrecy conservation. As cloud benefit isolates the information from the cloud benefit customer (people or substances), denying their immediate control over these information, the information proprietor can't believe the cloud server to lead secure information get to control. In this way, the safe access control issue has turned into a testing issue out in the open cloud storage.

Keywords: About four watchwords or expressions in order arrange, isolated by commas

I. INTRODUCTION

Cloud computing is the utilization of figuring assets (equipment and programming) that are conveyed as an administration over a system (normally the Internet). Cloud computing endows remote administrations with a client's information, programming and calculation. Cloud computing comprises of equipment and programming assets made accessible on the Internet as oversaw outsider administrations. These administrations normally give access to cutting edge programming applications and top of the line systems of server PCs. The objective of cloud computing is to apply conventional supercomputing, or elite figuring power, typically utilized by military and research offices, To perform many trillions of calculations for every second, in purchaser arranged applications, for example, money related portfolios, to convey customized data, to give information stockpiling or to influence extensive, immersive PC amusements. The cloud computing utilizes systems of huge gatherings of servers normally running minimal effort buyer PC innovation with specific associations with spread information handling errands crosswise over them. This common IT foundation contains extensive pools of frameworks that are connected together. Frequently, virtualization systems are utilized to expand the energy of cloud computing.

Characteristics and Services Models:

The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

On-demand self-service: A buyer can singularly arrangement figuring abilities, for example, server time and system stockpiling, as required naturally without requiring human collaboration with each specialist co-op's

Broad network access: Capabilities are accessible over the system and got to through standard instruments that advance use by heterogeneous thin or thick customer stages (e.g., cell phones, workstations, and PDAs).

Resource pooling: The supplier's processing assets are pooled to serve numerous purchasers utilizing a multi-inhabitant demonstrate, with various physical and virtual assets powerfully doled out and reassigned by buyer request. There is a feeling of area freedom in that the client for the most part has no control or information over the correct area of the gave assets however might have the capacity to indicate area at a more elevated amount of deliberation (e.g., nation, state, or server farm). Cases of assets incorporate capacity, handling, memory, organize data transfer capacity, and virtual machines.

Rapid elasticity: Capabilities can be quickly and flexibly provisioned, at times consequently, to rapidly scale out and quickly discharged to rapidly scale in. To the customer, the abilities accessible for provisioning regularly give off an impression of being boundless and can be acquired in any amount whenever.

Measured service: Cloud systems naturally control and advance asset use by utilizing a metering capacity at some level of reflection suitable to the kind of administration (e.g., capacity, handling, data transfer capacity, and dynamic client accounts). Asset utilization can be overseen, controlled, and detailed giving straightforwardness to both the supplier and shopper the used administration.

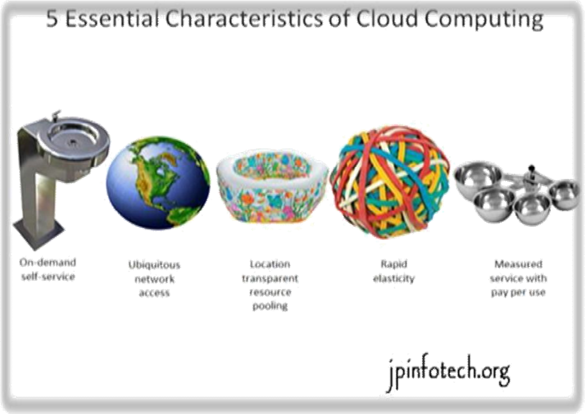
5 Essential Characteristics of Cloud Computing
On-demand self-service
Ubiquitous network access
Location transparent resource pooling
Rapid elasticity
Measured service with pay per use
jpinfotech.org

Fig.1. Characteristics of cloud computing

Services Models:

Cloud computing involves three diverse administration models, to be specific Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three administration models or layer are finished by an end client layer that typifies the end client point of view on cloud administrations. The model is appeared in figure underneath. On the off chance that a cloud client gets to administrations on the framework layer, for example, she can run her own applications on the assets of a cloud foundation and stay in charge of the help, support, and security of these applications herself. On the off chance that she gets to an administration on the application layer, these undertakings are ordinarily dealt with by the cloud specialist organization.

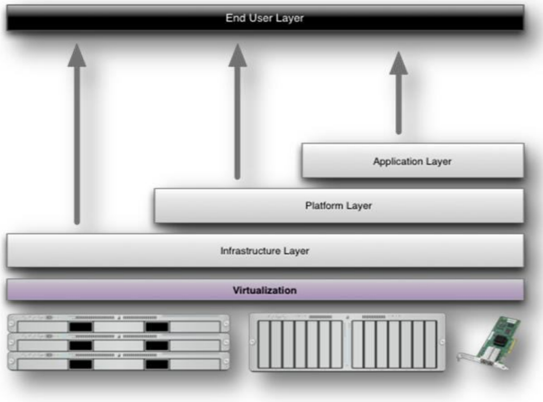

Fig.2. Structure of service models

Benefits of cloud computing:

1. Achieve economies of scale – increment volume yield or profitability with less individuals. Your cost per unit, task or item plunges.

2. Reduce spending on innovation foundation.-Keep up simple access to your data with negligible forthright spending. Pay as you go (week after week, quarterly or yearly), in view of interest.

3. Globalize your workforce at little to no cost-Individuals worldwide can get to the cloud, if they have an Internet association.

4. Streamline procedures- Accomplish more work in less time with less individuals.

5. Reduce capital expenses-There's no compelling reason to spend huge cash on equipment, programming or permitting charges.

6. Improve openness- You approach whenever, anyplace, making your life so significantly simpler!

7. Monitor ventures all the more adequately- Remain inside spending plan and in front of finishing process durations.

8. Less faculty preparing is require-. It takes less individuals to accomplish more work on a cloud, with an insignificant expectation to absorb information on equipment and programming issues.

9. Minimize permitting new programming- Extend and develop without the need to purchase costly programming licenses or projects.

10. Improve adaptability- You can alter course without genuine "individuals" or "money related" issues in question.

Advantages:

1. Price: Pay for just the assets utilized.
2. Security: Cloud occasions are disengaged in the system from different examples for enhanced security.
3. Performance: Instances can be included immediately for enhanced execution. Customers approach the aggregate assets of the Cloud's center equipment..
4. Scalability: Auto-send cloud occasions when required.
5. Uptime: Uses various servers for most extreme redundancies. If there should arise an occurrence of server disappointment, examples can be naturally made on another server
6. Control: Able to login from any area. Server preview and a product library gives you a chance to send custom cases.
7. Traffic: Deals with spike in rush hour gridlock with snappy organization of extra cases to deal with the heap.

2. PREVIOUS WORK

Ciphertext-approach quality based encryption (CP-ABE) isa valuable cryptographic technique for information get to control in distributed storage . All these CP-ABE based plans empower information proprietors to acknowledge fine-grained and adaptable access control without anyone else information. Nonetheless, CP-ABE decides clients' entrance benefit construct just in light of their intrinsic traits with no other basic components, for example, the time factor. In all actuality, the time factor normally assumes a critical part in managing time-delicate information (e.g. to distribute a most recent electronic magazine, or to uncover an organization's future strategy for success). In these situations, both the component of access benefit planned discharging and fine-grained get to control ought to be as one considered.

Limitations of existing system:

1. No schemes can support both fine-grained access control and time-sensitive data publishing.
2. Not explored ,simultaneously achieve both flexible timed release and fine granularity with lightweight overhead

3. PROPOSED WORK

In Proposed System, Our plan consistently joins the idea of coordinated discharge encryption to the engineering of figure content approach characteristic based encryption. With a suit of proposed instruments, this plan furnishes information proprietors with the capacity to adapt ably discharge the entrance benefit to various clients at various time, as indicated by an all around characterized get to approach over characteristics and discharge time. We additionally contemplated get to strategy outline for all potential access necessities of time touchy, through reasonable position of time trapdoors. The examination demonstrates that our plan can save the classification of time-delicate information, with a lightweight overhead on both CA and information proprietors. It along these lines well suits the down to earth substantial scale get to control The proposed work is Highly proficient and fulfills the security prerequisites for time touchy information stockpiling in broad daylight cloud and Time related unscrambling can be outsourced to the cloud without losing confidentiality.

Our scheme possesses two important capabilities:

1) It inherits the property of fine granularity from CP-ABE;

2) By introducing the trapdoor mechanism, it further retains the feature of timed release from TRE. Note that in TAFC, the introduced trapdoor mechanism is only related to the time factor, and only one corresponding secret needs to be published when exposing the related trapdoors. This makes our scheme highly efficient, which only brings about little overhead to the original CP-ABE based scheme.

IV . SYSTEM ARCHITECTURE

Similar to most CP-ABE based schemes, the system in this paper consists of the following entities: a central authority (CA),data owners (Owner), many data consumers (User), and a cloud service provider (Cloud).

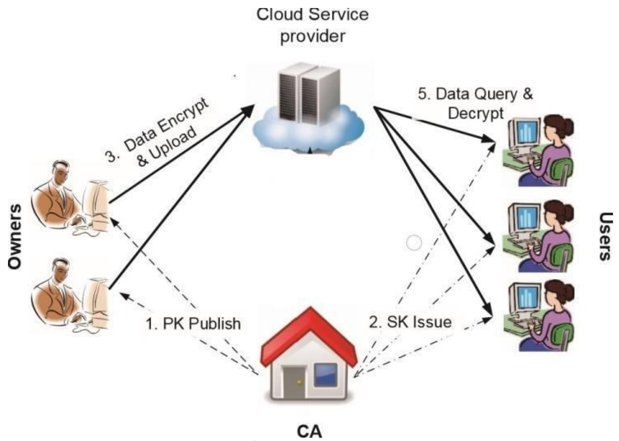

Fig 3. Architecture of Time and Attribute Factors

• The central authority (CA) is responsible to manage the security protection of the whole system: It publishes system parameters and distributes security keys to each user. In addition, it acts as a time agent to maintain the timed-releasing function.

• The data owner (Owner) decides the access policy based on a specific attribute set and one or more releasing time points for each file, and then encrypts the file under the decided policy before uploading it.

• The data consumer (User) is assigned a security key from CA. He/she can query any ciphertext stored in the cloud, but is able to decrypt it only if both of the following constraints are satisfied:

1) His/her attribute set satisfies the access policy;

2) The current access time is later than the specific releasing time.

•Cloud service provider (Cloud) includes the administrator of the cloud and cloud servers. The cloud undertakes the storage task for other entities, and executes access privilege releasing algorithm under the control of CA. The ciphertexts are transmitted from owners to the cloud, and users can query any ciphertexts. CA controls the system with the following two operations: 1) It issues security keys to each user, according to user's attribute set; 2) At each time point, it publishes a time token (T K), which is used to release access privilege of data to users.

5. MODULE DESCRIPTION

Data Owner

In this module, there are n quantities of information proprietor are available. Proprietor should enroll before doing a few tasks. What's more, enlist Owner points of interest are put away in Owner module. After enrollment effective he needs to login by utilizing approved client name and secret word. Information

Owner, in light of the qualities of clients to create diverse access control methodology, scramble transferred records utilizing the comparing encryption technique and afterward send to the cloud server.

In this module, we do the accompanying capacities:

1. Enlist
2. Login
3. Transfer File

Cloud Server Provide one Time Key to Data Owner. That Key Used for transfer Process. After Data proprietor Session Time Finished the Key will naturally lapsed.

4. View File
5. Setting course of events for record get to
6. Logout

Search User

In this module, there are n quantities of clients are available. Client should enroll before doing a few activities. What's more, enroll client points of interest are put away in client module. After enlistment fruitful he needs to login by utilizing approved client name and secret word. Login fruitful he will do a few tasks like Search inquiry, SK, record get to, and so forth and so on.

In this module, we build up the accompanying functionalities:

1. Enlist
2. Login
3. Pursuit File
4. Demand File
5. Download

Cloud Service Provider (Admin)

In this module, the Admin needs to login by utilizing legitimate client name and secret word. After login effective he can do a few tasks, for example, View all Owners, View all Users, see records, and so on.

In this module, we build up the accompanying functionalities:

1. Login
2. View All File Information
3. Refresh User and Owner
4. View All Data Owner
5. View All Time Sensitive File

4. ALGORITHM

Advanced Encryption Standard

The Advanced Encryption Standard (AES) was distributed by NIST (National Institute of Standards and Technology) in 2001. AES is a symmetric piece figure that is expected to supplant DES as the endorsed standard for an extensive variety of utilizations. The AES figure (and different hopefuls) shapes the most recent age of square figures, and now we see a noteworthy increment in the piece estimate - from the old standard of 64-bits up to 128-bits; and keys from 128 to 256-bits. The Rijndael proposition for AES characterized a figure in which the square length and the key length can be freely indicated to be 128, 192, or 256 bits. The AES determination utilizes a similar three key size choices yet constrains the piece length to 128 bits.

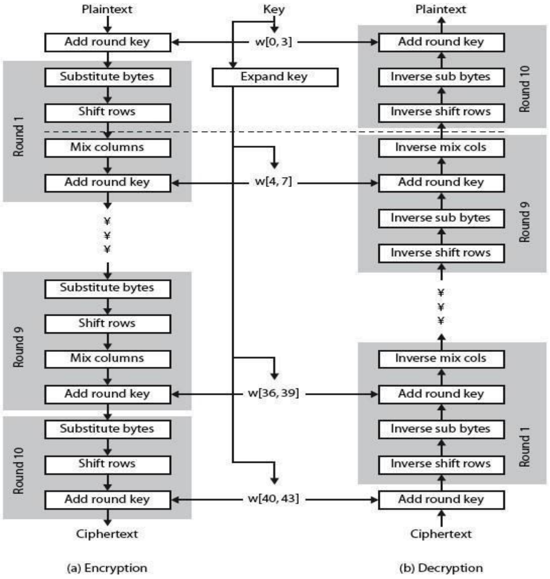

Fig.5. AES structure

Depiction of AES algorithm

1. KeyExpansion-round keys are gotten from the figure key utilizing Rijndael's critical plan.
2. Initial Round
   1. AddRoundKey-every byte of the state is joined with the round key utilizing bitwise xor.
3. Rounds
   1. SubBytes-a non-straight substitution step where every byte is replaced by byte indexed by a row according to a lookup table

   2 . ShiftRows-a transposition step where each column

of the state is moved consistently a specific number of steps.

3. MixColumns-a blending activity which works on the sections of the state, consolidating the four bytes in every segment.
4. AddRoundKey-XOR state with 128-bits of the round key. Again prepared by column (however viably a progression of byte activities).Final Round (no MixColumn)

1.SubBytes
2.ShiftRows
3.AddRoundKey

6. CONCLUSION

This paper goes for fine-grained get to control for time delicate information in distributed storage. One test is to at the same time accomplish flexible coordinated discharge and fine granularity with lightweight overhead, which isn't given in related work. In this paper, we propose a plan to accomplish this objective. Our plan consistently consolidates the idea of planned discharge encryption to the design of figure content arrangement encryption. With a suit of proposed instruments, this plan furnishes information proprietors with the ability to flexibly discharge the entrance benefit to various clients at various time, as indicated by a very much defined get to strategy over traits and discharge time. The examination demonstrates that our plan can secure the confidentiality of time-delicate information, with a lightweight overhead on both CA and information proprietors, in this way well suits the down to earth huge scale get to control framework for distributed storage.

7. REFERENCES

[1] Jianan Hong, Kaiping Xue, Yingjie Xue, Weikeng Chen, David S.L. Wei, Nenghai Yu and Peilin Hong, "TAFC: Time and Attribute Factors Combined Access Control for Time-Sensitive Data in Public Cloud", IEEE Transactions on Service Computing, 2017 https://doi.org/10.1109/TSC.2017.2682090

[2]E. Androulaki, C. Soriente, L. Malisa, and S. Capkun, "Enforcing location and time-based access control on cloud-stored data," in Proceedings of the 2014 IEEE 34th International Distributed Computing Systems (ICDCS2014), pp. 637–648, IEEE, 2014. https://doi.org/10.1109/ICDCS.2014.71

[3]L. Xu, F. Zhang, and S. Tang, "Timed-release oblivious transfer," Security and Communication Networks, vol. 7, no. 7, pp. 1138– 1149, 2014. https://doi.org/10.1002/sec.845

[4]Q. Liu, G. Wang, and J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," Information Sciences, vol. 258, no. 3, pp. 355–370, 2014. https://doi.org/10.1016/j.ins.2012.09.034

[5]C.-I. Fan and S.-Y. Huang, "Timed-release predicate encryption and its extensions in cloud computing," Journal of Internet Technology, vol. 15, no. 3, pp. 413–426, 2014.

[6]X. Zhu, S. Shi, J. Sun, and S. Jiang, "Privacy-preserving attribute-based ring signcryption for health social network," in Proceedings of the 2014 IEEE Global Communications Conference (GLOBECOM2014), pp. 3032–3036, IEEE, 2014.

[7]Z. Zhou, H. Zhang, Q. Zhang, Y. Xu, and P. Li, "Privacy preserving granular data retrieval indexes for outsourced cloud data," in Proceedings of the 2014 IEEE Global Communications Conference (GLOBECOM2014), pp. 601–606, IEEE, 2014. https://doi.org/10.1109/GLOCOM.2014.7036873

[8] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 1790–1801, 2013. https://doi.org/10.1109/TIFS.2013.2279531

[9] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131–143, 2013. https://doi.org/10.1109/TPDS.2012.97

[10]K. Yuan, Z. Liu, C. Jia, J. Yang, and S. Lv, "Public key timed-release searchable encryption," in Proceedings of the 2013 Fourth International Emerging Intelligent Data and Web Technologies (EIDWT2013), pp. 241–248, IEEE, 2013. https://doi.org/10.1109/EIDWT.2013.47

[11]Z. Wan, J. Liu, and R. H. Deng, "HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 743–754, 2012. https://doi.org/10.1109/TIFS.2011.2172209

[12]Q. Liu, C. C. Tan, J. Wu, and G. Wang, "Reliable re-encryption in unreliable clouds," in Proceedings of the 2011 IEEE Global Communications Conference (GLOBECOM2011), pp. 1–5, IEEE, 2011.

[13]J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proceedings of the 28th IEEE Symposium on Security and Privacy (S&P2007), pp. 321–334, IEEE, 2007. https://doi.org/10.1109/SP.2007.11

[14]E. Bertino, P. A. Bonatti, and E. Ferrari, "TRBAC: A temporal role-based access control model," ACM Transactions on Information and System Security, vol. 4, no. 3, pp. 191–233, 2001.

[15]D. Boneh and M. Franklin, “Identity-based encryption from the weil pairing,” in Advances in Cryptology (CRYPTO2001), pp. 213–229, Springer, 2001.
https://doi.org/10.1145/501978.501979

Mythri V: pursuing B.E in CSE.EWIT (VTU), Bengaluru. Her area of interest are Computer Security, Database, Computer Networking, Web Programming, Computer graphics and Cloud Computing.

Nandini S: pursuing B.E in CSE.EWIT (VTU), Bengaluru. Her area of interest are Computer Security, Database, Computer Networking, Programming the Web, Software Engineering , Computer graphics and Cloud Computing.

Pallavi P: pursuing B.E in CSE.EWIT (VTU), Bengaluru. Her area of interest are Computer Security, Database, JAVA Programming, Programming the Web, Software Engineering, Computer graphics and Cloud Computing.

Pruthvika B U : pursuing B.E in CSE.EWIT (VTU), Bengaluru. Her area of interest are Computer Security, Database, JAVA Programming, Storage area network, Programming the Web, Software Engineering, Computer graphics and Cloud Computing.

Dr. Prasanna Kumar M: Associate Professor, Department of Computer Science and Engineering, East West Institute of Technology(VTU), Bengaluru. Qualification: B.E, M.Tech, Ph.D-Software Engineering, The Research Scholar at VTU. His area of research are Software Engineering, Cloud Computing and Software Engineering