Impact Factor Value: 4.029 ISSN: 2349-7084
International Journal of Computer Engineering In Research Trends
Volume 4, Issue 10, October - 2017, pp. 431-440 www.ijcert.org

Two Step Factor Based Authentication Control to Access Cloud Services

[1] Mr. Mohammed Shuja Ur Rahman, [2]Mr. Mohammed Khaleel Ahmed, [3]Dr. G.S.S Rao
[1] MTech(CSE), [2] Associate Professor, [3]Professor & HOD
[1,2,3] Nawab Shah Alam khan College of Engineering and Technology,Hyd
Email ID: mrshuja456ify@gmail.com, ahmedkhaleelmohammed@gmail.com ,profgssrao@gmail.com

---

Abstract: The innumerable points of interest of distributed computing have conveyed an enormous change to the way of life and the best approach to adapt to the world today, yet the cloud needs to achieve development. Be that as it may, the primary boundary to it's across the board appropriation is the security and protection issues. So as to make and keep up common trust among the clients and the cloud specialist co-ops, a well-characterized trust establishment ought to be executed. The information put away in the cloud remotely by the singular client or an association, so they lost control over the information, in this way making a security issue. The most difficult and hot research region in distributed computing now daily is the information security and access control. A powerful measure to ensure distributed computing assets and administrations in the begin is to execute an entrance control system. In this paper, the highlights of different access control systems are examined, and a novel structure of access control is proposed for distributed computing, which gives a multi-step and multifaceted confirmation of a client. The model proposed is an efficient and provably secure arrangement of access control for remotely facilitated applications.

Keywords: Cloud Security, Access Control, Cloud Trust, Data Control, Multi-Factor Authentication

---

1. Introduction

Despite the fact that distributed computing stage with a ton of advantages that comprise of the economic measure, dynamic stipulating, and increased flexibility and close to the ground essential costs, yet it additionally gets an assortment of unique security dangers. The across the board worries in connection to distributed computing are the protection and security. A cloud client can get to cloud administrations from any area. It is of most significance that to reveal new methods for protection and security to ensure information and protection for the distributed computing. One of the methodologies ordinarily being used is the regular validation strategy in which a client needs just a username and watchword, in other to make utilization of a confirmation and approval framework in which each customer has the privilege to get to the information and applications which are just suitable for his or her activity [1, 2]. Each cloud has focal server organization frameworks, which oversee the structure and operation of the cloud; make an adjust among the supply and requests of the customer assets and screen in going and active movement. One of the worries of the client is about the capacity of information in the cloud. It is a widespread way to deal with store information of a few clients in a single basic place in distributed computing; other concern is the entrance to the information in the cloud condition. The cloud administrations are given by business specialist co-ops, and the previously mentioned concerns are

exceptionally regular from the clients, as it is outside the trust area of the clients [3]. It is the duty of the cloud specialist organization to execute a well – composed component of information privacy and access instrument. The proprietor of the data has an awesome worry over the danger of information misfortune when they free the data for preparing to the cloud since they do not have the control over the data. The clients have no physical control over the framework of the server farm and data, and this expansion assuagement of information impressively [4]; then again, points of interest (decrease in the general working expenses and opened up accessibility of profiting the administrations of distributed computing might be sufficiently groundbreaking to legitimize the dangers [5].

For the most recent twenty years, numerous endeavors are made, and various arrangements have been given to secure information, messages and different assets accessible on PC systems. Endeavors are additionally made that the security of the clients, respectability, accessibility, and unwavering quality could be guaranteed for registering situations. Regardless of every one of these necessities, exercises, persevering endeavors, or more every one of the arrangements that we have, it is a typical conviction that the trust in the present cloud application is not adequate. In this paper, a novel system of access control is proposed for distributed computing, which gives a two-advance multifaceted confirmation of the client. The model proposed is efficient and provably secure and can likewise give a solitary sign-on answer for remotely facilitated applications [6].

The real issue defined by the vast majority of the association concerning the appropriation of the cloud design is the security. A lot of procedures and advances have been created and actualized to guarantee an abnormal state of security in the cloud. A considerable measure of cryptographic strategies are utilized to acknowledge security, however attributable to the unpredictability of achievement; it appears that the exhibitions diminish. Just a couple of strategies are available that play out the enrollment and arrangement as well as play out the checking and following of clients' exchanges.

Keeping in mind the end goal to give the information or applications in a cloud domain, a thorough component of security is, stops the unapproved access in the initial step, which is conceivable by actualizing a solid approval system for the client. When all is said in done, the standards or course of activities that hold back, permit or restrict access to a framework is known to the entrance control.

It might potentially, too, watch and record all endeavors made to get to a framework, and distinguish the clients who are unapproved and endeavoring to get to the framework. It is thought to be the most critical instrument of assurance in PC security [7]. The way toward distinguishing a client remarkably through the check of their qualifications is called verification, and upon the approval of the character, a trust relationship is built up for facilitating associations.

The validation of the client is compulsory, when, the client tries to get to the administrations or information. Indeed, even in some cases, while, the applications make a connection to far off administrations or endeavor to get to information held locally. On the off chance that the arrangement chose is key for information or an application, at that point it needs more significance to be secured, like this, it must be open to approved clients. The servers are required to confirm the clients initially to see whether they are the approved to get to information/administration or they are not the genuine clients. The dominant part business undertakings which are security – insightful, utilized different sorts of validation and approval systems keeping in mind the end goal to get to registering assets over a system. The upsides of the approach are clear

Validation can be incorporated by various techniques. The noteworthiness of picking an appropriate validation procedure is possibly the most basic judgment in conspiring ensured frameworks. Various confirmation plans depend on basic secret word verification, which needs easy execution, aside from primitive and ordinarily feeble. A portion of the validation strategies which might be more muddled and require added time to created and protected, aside from offer extreme and dependable methods for confirmation [2].

Regularly the elements which can be utilized for validation fall into three classes; each verification

include swathe up a variety of angles, use to confirm, or demonstrate a man's uniqueness going before to build up an entrance, supporting an operation request, denoting an archive, giving endlessly ideal to others, and discovering a series of forces. These variables of confirmation comprise of the things which are in the responsibility of a client, the things which are identified with the learning base of the client, and individual inherent components [8, 9].

Approval is the following stage after verification, which allows or limits the rank of the privilege to utilize and use reason to that unit, which depends on the character of the client. The primary goal of both of the entrance control system is to make accessible a provable plan for guaranteeing the wellbeing of data from dishonorable access. This is finished by utilizing a few arrangements in regards to security direction. In expansive, the approach to the use of access control methods depends on the kind of strategy. However, it will incorporate no less than one of these control, i.e., either the secrecy or honesty.

2. Related Work

There are different sorts' of access control procedures that additionally uses cryptographic calculations relying upon the accessibility of the registering assets. Various cryptographic access plans have been characterized and executed in distributed computing. A cryptographic-based access control show is proposed, and the premise of our model additionally relies upon the model portrayed in [9, 10]. The framework model of the cryptographic-based access control appears in Figure 1.

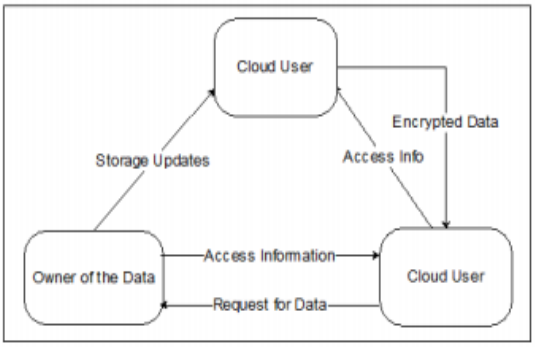

Figure 1. Encrypted Data Access Model

There are three donors in the model represented above, i.e., the Owner of the Data, the supplier of the Could Services, and Cloud User. The proprietor outsourced its information to the cloud administrations, as the cloud is a multitenant domain and the information outsourced by the proprietor is encoded, and the cloud client wants to get to the information. The proprietor of the information sends the keys and a validation endorsement required to get to and unscramble information when it gets the demand from the client of the cloud. The confirmation testament is then displayed to the CS for the check; upon the fruitful approval by cloud benefits, the client gets the information in scrambled shape. The model delineated above guaranteed that the privacy will be accomplished, trustworthiness will be kept up, and verification will not be traded off, yet it endures. The proprietor will dependably be online keeping in mind the end goal to engage the demand of the client, which is the primary shortcoming of the model [11]. It is hard to keep up keys and authentications for all the imparting elements. The circumstances even deteriorate when the proprietor has poor registering abilities.

A framework to fulfill a secured, fine-grained and equipped for being effectively overhauled or extended and to give on-request get to control was presented for distributed computing condition [3]. This framework depended on the distinctive strategies for encryptions which are, intermediary re-encryption, characteristic based encryption, and apathetic re-encryption. The highlights which are importantly affecting each other are coupled to a document in the circumstance of client's worry. The instruments for each client, to be approved to get to have a particular consistent articulation in light of the highlights, which demonstrates the limit of the information petition for which the client is validated to get to. For each characteristic, an open key component is created. These open keys are utilized to scramble the greater part of the information records practically equivalent to the properties. The clients are allowed private practically equivalent to keys to the entrance rights, to make them fit for decoding a ciphertext if and just if the trait of the information record validate his entrance rights. A key issue concerning this component is the induction of an unmistakable consistent articulation for all clients because the cloud store a tremendous measure of information legitimate articulation gave the trait of the

document ends up noticeably multifaceted. Besides, the re-encryption likewise turns into an issue as the refreshing of the client mystery key for each client barring the denied one is extreme methodology when the there is a considerable measure of clients.

An arrangement of verification which depends on the mix of personality and joined key and equipment encryption innovation is proposed, executed and tried [12]. This component is made out of web – server subsystem, confirmation subsystem and customer subsystem.

A powerful ID-Based framework on Elliptic Curve Crypto System (ECCS) for remote client verification is proposed in [13]. The model proposed is a framework isolated into three stages; the principal stage is the framework statement stage, the second stage is about the enlistment of the client, stage and in the third stage the validation of the client alongside the common key understanding happens. The validation framework given ECCS has a few impediments. The first: a key validation focus is expected to keep up a declaration for client's open keys. The second: an extensive storage room is required when the quantity of clients is expanded as on account of the cloud to store people in general keys and authentication of the clients. The calculation and vitality cost of the gadgets turn out to be high, as the clients require extra calculations with a specific end goal to confirm the testament of others.

Another model given the dynamic firewall operation and utilizing the three-way TCP handshake for the verification of the clients is proposed in [14]. The firewall abuses the accessible data to endorse the foundation of relationship amid the sessions which are upheld by client's shown uniqueness. The insufficiency of the model is the origination and stronghold of the endorsements, which is wrong for the cloud condition. The execution of the general framework is lessened because of complex cryptographic techniques

The utilization of endorsement at various levels which empower the protected exchange and access of information is uncovered by the model displayed in [15]. The distinctive sorts of testament show the kind of client, the kind of utilization and the sort of equipment. The fundamental shortcoming of the system is the support of the testaments at different levels and to make a confide in the connection between these declarations.

The model of the multitenant stage that certifications to obstruct any defective or malevolent code from any inhabitant, which meddles the ordinary execution of the other occupant or code or the stage itself is proposed in [16]. The testing concerns are detachment, conceivable damages like the permeability of protest introduction from fluctuating position of classes and congestion all through collective information structures.

Access control on accessible XML archives by the utilization of different cryptographic keys on an alternate level of XML tree is introduced in [17]. Unique hubs of metadata were additionally acquainted in the procedure with force get to control. The key administration and the age of the XML tree are the main complexities of this approach.

The Identity – Based Hierarchical Model for Cloud Computing is proposed in [18]. This component is utilized for the confirmation of cloud clients. The progressive encryption and mark instrument are utilized to have the capacity to get to the administration of the cloud. The main issue with the technique is that it devours a considerable measure of transmission capacity.

The activity for confirmation of the client through charging data by the mists specialist organizations, and influence utilization of X.509 to endorsement or PKI/SSH foundation [19] [20]. The model just permits picked a working framework and parts to run, which is the main downside.

To secure information on depended servers another strategy is proposed, which depends on the encryption of information with a symmetric key and the greater part of the clients are allocated discharge keys [21]. The proprietor of the information at that point makes a public token, which contains the decoding key which is determined by the client utilizing his mystery key.

The quantity of mystery keys and encryption keys are quite diminished in this approach, yet it has experienced the issue of many-sided quality in operations, i.e., the quantity of record creation and

client get to demands is straightforwardly relative to various clients, which prompts the non – adaptability issue.

The connected instrument for client verification and approval are distinctive safety efforts to spare the stages. The methods which are utilized to delimit the entrance of a procedure in one working framework and not to come surprisingly close to the alternate process are proposed in [22]. The arrangement proposed has not a mind-boggling calculation on the customer side, the verification and approval are performed at specialist co-op and server farm's area.

The Internet is thought to be the framework of all-inclusive correspondence for the suppliers of the cloud administrations [23]. It utilizes the well-characterized TCP/IP conventions for the recognizable proof of the clients' on the cloud. The downsides of this approach are same as to tend to the component of the physical PC on the web; the virtual machines additionally have IP addresses. A malignant substance, independent of its character, can find this address. In this circumstance, the physical server running the virtual machine can be found, and the malicious client embeds a false virtual machine at that physical area to start an assault.

A secured arrangement of dispersed stockpiling given the strategies of intermediary re-encryption is proposed in [24]. The square of information is scrambled with symmetric content keys by the proprietor of the information; the greater part of the substance keys are then encoded by the proprietor with an ace open key. The intermediary re-encryption keys are created by the proprietor of the information by utilizing the client's open key and his private key. The issue looked at this component is that even a solitary depended on the server or noxious client could uncover all the unscrambling keys for the figure content and the general security of the framework is bargained.

3. The Proposed Model

In our proposed demonstrate, it is expected that the segments which make the framework administrator is made out of a proprietor of the information, elements which will utilize the information made by the proprietor of the information called the client of the information and the supplier of the cloud administrations and server farm. The confirmation of the client is a multistep procedure, and after the fruitful validation, the client will just access the information record put away by the proprietor, in a private way by the execution of the advanced testament. It is additionally expected that it is not important for the client or proprietor to be online constantly. The proprietor comes online when it needs to enlist another client or make some refresh to the authentication accessible on the supplier of cloud benefit, and the supplier of cloud administrations is thought to be online all an opportunity to give access to the information stored at the server farm. Another suspicion that we make is that the proprietor of the information will have the capacity to perform/execute paired codes at cloud administrations for the organization of information alongside the putting away of such information in the encoded sort. All the correspondence, regardless of whether it is the cloud administration and client or between the client and proprietor and the other way around will utilize cryptographic means, i.e., the utilization of RSA for encryption and alongside a computerized endorsement. The thought behind the decision of RSA encryption including the client and the cloud benefit is since RSA encryption will require all relationship to create an advanced testament for all clients, and which is just a single of its kind for each client. By actualizing this system of RSA encryption we can achieve a secured information correspondences for all most recent session.

The RSA is thought to be more efficient, protected, and sound mean of encryption, and furthermore, the computerized endorsement is made utilization of an encoded session, subsequently, whatever remains of the clients cannot watch the information or data which is in travel over the system. The client is abstaining from getting to other's information documents, as the entrance gate by the proprietor has put some confinement on the client on account of their abilities.

The proposed structure and its operational design are exhibited in this area. The general all working model is displayed in Figure 2. The information which will contain demand of the client for the information and his ID accreditations are sent to cloud benefits and checked it with the access data in the approval data at the server farm, and furthermore, the

correspondence amongst proprietor and supplier of cloud administrations should be secured amid the exchange, to contradict any assault. The structure proposed, will clear up the best approach to achieve the level of security required and controlled the instrument of access.

The confirmation of the client is a multi-step process. In the initial step, the client can sign in to CS by giving her/his username and secret word, alongside the IP address of the terminal. At that point, the client will be requested entering the biometric (Finger Prints) information. Upon the valid confirmation, the client will be sent an email containing the entrance code for the session, which includes an additional layer of security around the client account. In the wake of finishing the login procedure, each client will get an approval endorsement based the quality. The abnormal state chart of the proposed structure appears in Figure 2, and the detailed outline appears in Figure 3. The means required for the enlistment of new clients involves a demand for enrollment send to the proprietor of the information with personality subtle elements, i.e., Client ID, IP address/Terminal ID, timestamp and the privilege to get to the information document. This appears in Figure 4.

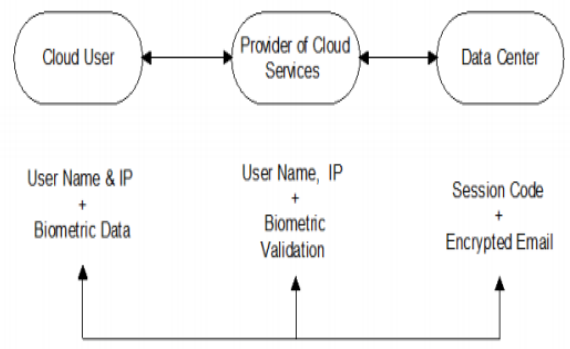

Figure 2. High Level Diagram of the Proposed Scheme

The legitimacy of the demand is checked by the proprietor of the information after the formal receipt of the information. To influence the things quietly, we to expect that the proprietor has a different game-plan to check the legitimacy of the customer's demand. The new client data is currently refreshed by the proprietor at the specialist organization. In the wake of refreshing the data at cloud administration and server farm, the server farm now create sends an answer message to the customers encoded by MD5. The man – in – the – center assault can be maintained a strategic distance from by the utilization of timestamp and IP address in the answer message.

In the accompanying arrangement of operation, it is clarified how the information could be influenced more to secure. The proprietor of the information scrambles each document accessible in the edge of reference utilizing MD5. The proprietor of the information utilized MD5 a 128 – bit hash rather than a few another component, i.e., SHA – 1. It is done to guarantee the honesty of information and due to the putting this process close to the record with by methods for a symmetric key. The record is again encoded with the general population of the proprietor of the information, which brings about more quality and security of the information rather than just utilizing the SHA – 1. The information respectability and classification of information is guaranteed by this implies between the client and the proprietor of the information.

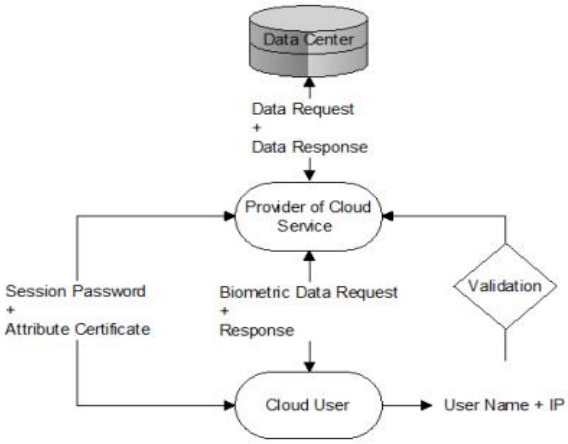

Figure 3. Multi – Step Authentication of Cloud User

The proprietor of the information like this drives the entire part of the information, encoded with his private key, and after that utilizing the specialist co-op open key keeping in mind the end goal to keep up the classification and confirmation among the supplier of the cloud administration and proprietor of the information. After getting the encoded documents the supplier of cloud administration will utilize general society key of the proprietor of information and its private key to unscramble the message and send the scrambled records to the server farm for capacity. The

quality of our model is that the supplier of the cloud administrations cannot know the genuine substance of the information as the symmetric shared key is just known to the client and the proprietor. The outline objective is refined by utilizing this model as the real information/data is just accessible to the information client and proprietor and not to the supplier of cloud benefit since it is to be had in a space which isn't reliable.

The achievement of an enhanced and ensured information access for a cloud situation; an elite access control is given by methods for another kind of advanced testament known as the property authentication. The information structure of the credit authentication is practically equivalent to the personality declaration; then again, it does not contain any open key rather than character endorsement. Despite the fact that the kind of support information perhaps is situated inside extra fields of personality declarations, because does as such, it has some basic causes.

Above all else, the specialists who issue these authentications are by and large not responsible for the approval data of this sort. Therefore, some extra advances are required to be taken by the authentication issuing experts to secure the data required for the entrance control from the sources. Then again, the data required for approval may maybe give different life expectancy to the imperative of an open key and the character. If the data of access control is put in the augmentation of the personality testament then it will abbreviate the life expectancy of the declaration, while life expectancy/legitimacy essential for the characteristic authentication allow short and seemingly perpetual endorsements.

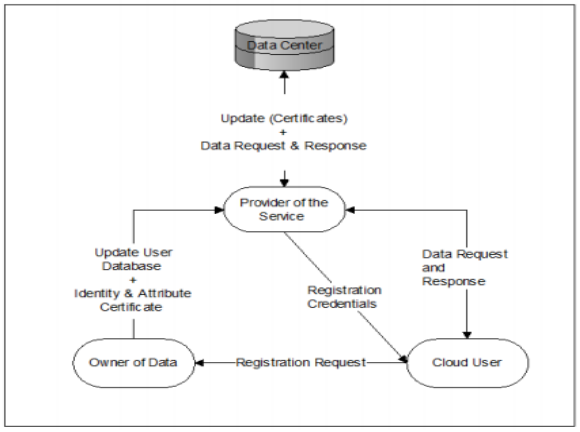

Figure 4. User Registration

The legitimacy times of property authentication, by and large, may maybe be ascertained in hours, on as opposed to character endorsement, for which the time figured, is in months and years. The authorizations for short legitimacy periods trait testament can be changed in a little adaptable way on the off chance that it is utilized as a part of such a system, to the point that no disavowal is required. The trait authentication which requires a more extended life maybe be utilized for approval those are relatively static. In such cases, a typical testament issuing expert is at risk to give trait and character endorsements. It is suggested that the quality essential for approval is kept partitioned, yet now and again when the issuing specialist is basic, it kept in the augmentation field of the character testament.

Ensuring the active login of the client onto the cloud benefits, the testament issuing specialist issues character, and property. The client asks for the information access to the server farm through cloud benefits, the cloud benefit after a check of the quality and personality declaration with the issuing expert, approve the client to get to information in the server farm.

Presently the client can get to the scrambled information as asked for by the client. The client needs a decoding doohickey that is available in her/his client account. The thingamabob will require a secret key to play out the unscrambling, which is naturally sent to the substantial email address of the customer which the entrance is conceded to the customer. The unscrambling thingamabob will begin the age of the private key for the information scrambled and after that decode the

information. The process is figured with the assistance of needs to capacity and check for the respectability of the message utilizing the new process, and the one got the message.

4. Analysis of the Proposed Framework

The proposed scheme is being analyzed for the characteristics of security in this section.

4.1. Authentication and Authorization

The client is verified and approved by a multi-factor and multi-step approach at the cloud benefit focus. Every one of the connections with the proprietor of the information and cloud benefit is likewise confirmed, the system took after is, the proprietor utilizes his private key for the encryption of the mixed information document, and the Cloud Services utilizes his open key to verify the proprietor of information. The confirmation client of the information is performed with claim private key while including another customer, while the proprietor validation is performed at cloud benefit by the private encryption at cloud benefit with possessing private key.

4.2. Data Confidentiality and Integrity

Keeping in mind the end goal to play out the investigations of the information classification for this proposed approach, it is contrasted and the effectively existing encryption procedures that utilize the symmetric keys. The supplier of cloud benefit cannot imagine the first information and process of the proprietor as the key is symmetric and just shared among the client and information proprietor. The information after encryption with symmetric keys is indeed encoded with the private key of the information proprietor, and people in general key of the supplier of cloud administrations. To wrap up the discourse that information is not accessible to be unscrambled into its unique frame by the cloud administrations.

The trustworthiness is guaranteed for the information under thought by utilizing the MD5 hash calculation. The client of the information figures a new has and after that match it up to the one as of now affixed to the first information document. The uprightness infringement will be accounted for, and the proprietor of the information will be educated in like manner if the hash figured by the client does not match to the first hash display in the message.

4.3. Access Control Based on Attribute Certificates

The validation and approval depend on a multistep procedure including the biometric information, other than that, in our proposed demonstrate, the entrance is a further control on the bases of a moment sort of advanced authentication, i.e., the trait authentication. The personality and trait declaration can be made by the proprietor of the information in authentication issuing specialist focus. The customers have issued testaments as per the idea of their demand after fruitful login to the cloud specialist co-op. The reason of utilizing the quality declaration is that the prior models were utilizing access control records, which may not be practicable for distributed computing condition [22, 23, and 24].

Since the client needs are unique, on the off chance that one access one information record may redundant got to by another customer along these lines, making of access control list for any information protest is troublesome. In our approach, we utilize characteristic endorsement which contains the fundamental information structure of the information documents for the entrance control.

5. Conclusion

The model proposed in this paper offer energy to the proprietor of the information to execute the security procedure on the information to be outsourced and consequently hold the control over the information. The model likewise proposed the blend of cryptography and access control to protect the information from vulnerabilities.

A multistep, multi-factor validation approach is utilized for the verification and approval of the customer, which increment the privacy and uprightness of the information. The paper likewise exhibited the private key, hash and opened scrambled figures among the proprietor, the customer and the specialist co-op which ensure the separation and safe execution of the cloud condition.

References

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, (2008), pp. 50-55.

[2] S. Ullah and Z. Xuefeng, "Cloud Computing Research Challenges," In Proceedings of 5th IEEE International Conference on Biomedical Engineering and Informatics, (2012), pp. 1397-1401.

[3] S. Yu, C. Wang, K. Ren and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," In INFOCOM, 2010 Proceedings IEEE, IEEE, (2010), pp. 1-9.

[4] L. Yousef, M. Butrico and D. Da Silva, "Toward a Unified Ontology of Cloud Computing," Grid Computing Environments Workshop, GCE '08, (2008), pp. 1-10.

[5] Z. Shen and Q. Tong, "The Security of Cloud Computing System enabled by Trusted Computing Technology," In Proceedings of 2nd International Conference on Signal Processing Systems, (2010), pp. 11- 15.

[6] R. L. Grossman, "The Case for Cloud Computing," IT Professional, vol. 11, no. 2, (2009), pp. 23-27.

[7] S. Ullah, Z. Xuefeng and Z. Feng, "TCloud: Challenges and Best Practices for Cloud Computing," International Journal of Engineering Research and Technology, vol. 1, no. 9, (2012), pp. 01-05.

[8] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, vol. 34, no. 1, (2011), pp. 1-11.

[9] Di Vimercati, S. De Capitani, S. Foresti, S. Jajodia, S. Paraboschi and P. Samarati, "A data outsourcing architecture combining cryptography and access control", In Proceedings of the 2007 ACM workshop on Computer security architecture, ACM, (2007), pp. 63-69.

[10]W. Wang, L. Zhiwei, R. Owens and B. Bhargava, "Secure and efficient access to outsourced data", In Proceedings of the 2009 ACM workshop on Cloud computing security, ACM, (2009), pp. 55-66.

[11] S. Kamara and K. Lauter, "Cryptographic cloud storage", Financial Cryptography and Data Security, (2010), pp. 136-149.

[12]J. Dai and Q. Zhou, "A PKI-based mechanism for secure and efficient access to outsourced data", In Networking and Digital Society (ICNDS), 2010 2nd International Conference on, vol. 1, (2010), pp. 640-643, IEEE.

[13]G. Zhao, X. Hu, Y. Li and L. Du, "Implementation and testing of an identity-based authentication system", In Computing, Communication, Control, and Management, 2009, CCCM 2009, ISECS International Colloquium on, vol. 4, IEEE, (2009), pp. 424-427.

[14]E. -J. Yoon and K. -Y. Yoo, "Robust id-based remote mutual authentication with key agreement scheme for mobile devices on ecc", InComputational Science and Engineering, 2009, CSE'09, International Conference on, vol. 2, IEEE, (2009), pp. 633-640.

[15]J. Wiebelitz, S. Piger, C. Kunz and C. Grimm, "Transparent identity-based firewall transition for eScience", In E-Science Workshops, 2009 5th IEEE International Conference on, IEEE, (2009), pp. 3-10.

[16]D. Zissis and D. Lekkas, "Addressing cloud computing security issues", Future Generation Computer Systems, vol. 28, no. 3, (2012), pp. 583-592.

[17]L. Rodero-Merino, L. M. Vaquero, E. Caron, A. Muresan and F. Desprez, "Building safe PaaS clouds: A survey on security in multitenant software platforms", Computers & Security, (2011).

[18]H. Li, Y. Dai, L. Tian and H. Yang, "Identity-based authentication for cloud computing", Cloud Computing, (2009), pp. 157-166.

[19]G. Miklau and D. Suciu, "Controlling access to published data using cryptography", In Proceedings of the 29th international conference on Very large data bases, vol. 29, VLDB Endowment, (2003), pp. 898-909.

[20]D. Naor, A. Shenhav and A. Wool, "Toward securing untrusted storage without public-key operations", In Proceedings of the 2005 ACM workshop on Storage security and survivability, ACM, (2005), pp. 51-56.

[21]E. -J. Goh, H. Shacham, N. Modadugu and D. Boneh, "SiRiUS: Securing remote untrusted storage", NDSS, (2003).

[22]H. Ahn, H. Chang, C. Jang and E. Choi, "User Authentication Platform using Provisioning in Cloud Computing Environment", Advanced Communication and Networking, (2011), pp. 132-138.

[23]G. Ateniese, K. Fu, M. Green and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage", NDSS, (2005).

[24]R. Blom, "An optimal class of symmetric key generation systems", In Advances in Cryptology, Springer Berlin/Heidelberg, (1985), pp. 335-338.

[25] FARZANA, A.HARSHAVARDHAN,"Integrity Auditing for Outsourced Dynamic Cloud Data with Group User Revocation. "International Journal of Computer Engineering in Research Trends., vol.2, no.11, pp. 877-881, 2015.

[26] N. Meghasree,U.Veeresh and Dr.S.Prem Kumar,"Multi Cloud Architecture to Provide Data Privacy and Integrity. "International Journal of Computer Engineering in Research Trends., vol.2, no.9, pp. 558-564, 2015.

[27]A.Shekinah prema sunaina,"Decentralized Fine-grained Access Control scheme for Secure Cloud Storage data. "International Journal of Computer Engineering in Research Trends., vol.2, no.7, pp. 421-424, 2015.

[28]P.Rizwanakhatoon and Dr.C.MohammedGulzar,"SecCloudPro:A Novel Secure Cloud Storage System for Auditing and Deduplication. "International Journal of Computer Engineering in Research Trends., vol.3, no.5, pp. 210-215, 2016.

[29]B.SameenaBegum,.RaghaVardhini,"Augmented Privacy-Preserving Authentication Protocol by Trusted Third Party in Cloud. "International Journal of Computer Engineering in Research Trends., vol.2, no.5, pp. 378-382, 2015.

