International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

Providing Security Using Fine Grained Two factor Access Control in Cloud Computing Environment

Varsha

Department of Master of Computer Application (MCA), VTU PG Centre Kalaburagi, Karnataka, India

ABSTRACT

Cloud computing has the major security problem. From the cloud the information can be shared easily. Sharing of information only leads big security problem in cloud computing. The data can easily be hacked by the hackers. In this project we are providing more efficient security to the cloud. We are introducing a project of providing security using fine grained two factor access control for cloud computing environment. The main problem is, the user need to login before entering into the server and sharing the same computer between many people. Only password scheme is not much safe for cloud. By considering the problem, we are proposing a concept of 2FA access which means along with the password scheme the user need to keep the safety device which generates the one time password for the user. Through that the user can enter into the server and he can able to download the necessity files from the cloud. Using salt Encryption Algorithm we are solving the problem and providing security to the cloud.

Keywords : Cloud Computing, Encryption Algorithm, 2FA, E-banking, Secret Key

I. INTRODUCTION

Distributed totaling is a computer-generated mass PC framework which allows endeavors for purchasing, lease, deal, disseminate programming with other advanced things over the mesh as an on request use. There is no time in the future trusts on upon a server or various machineries that materially occur, as I said that this is a computer-generated framework. Some of the certain uses of distributed totaling, information distribution, storing enormous information administration, healing data framework and so on are considered as the examples. Finish clients get to cloud based requests through a mesh program, thin customer and versatile application while the busines programing and user's information are kept away on servers on a remote area.

The advantage's of on-line distributed computing directions are huge, which include the easiness of openness, moderated outlays and main uses, stretched functioning proficiencies, flexibility, adaptableness time of prompt advertise.

In a property oriented get to control system all client has a client mystery key hand-out by the expert. By and by, the client mystery key is inside the computer. Consider the previously declared 2nd issue on online administrations, it is normal that PC's might be used by numerous clients particularly in some extensive ventures or associations. Example, let's consider the accompanying 2 situations:

- The PC's are used in a healing center by various members. When Dr. Alice is on obligation in the day time, she utilizes system in area 1 in the mean time Dr. Weave is on the obligation evening time, he uses a same system in that room only.
- PC's in the undergrad workroom are typically used in a college by various understudies.

In such cases, client mystery bases could be effectively taken or utilized by an unapproved person. Despite the fact that the PC might be bolted by a secret key, it can at present be conceivably speculated or taken by hidden viruses. Some more safe path is to use two consider verification. This is extremely normal among online e-saving money governments. Notwithstanding a

username or secret key, the client need to have a gadget to generate a one-time watchword.

The real time example of our project is E-banking. In E-banking there has two fctor's one is userid and password and the one time password is sent to the cell phone or any device. Through that the user can made transaction successfully. If the user enter's the wrong one time password or userid or password his transaction will be failed.

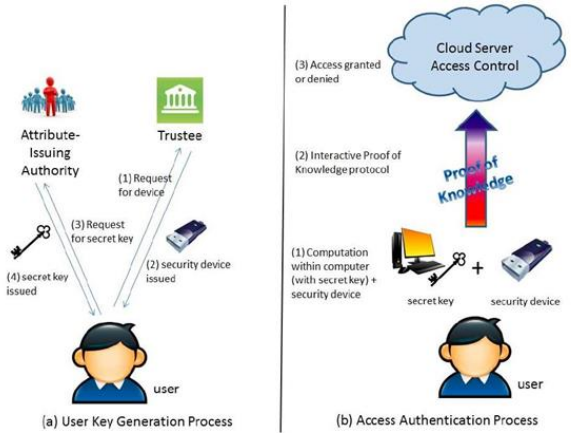

Figure 1. General Architecture of Project

The architecture shows the 2FA concepts which means the user need to keep along with the password scheme the user need to keep the user safety device which generates the one time password for the user. Then the user can be able to download the files.

1.1.1 Problem statement:

There are 2 problems in the customary record/secret key oriented framework. Initially, the usual record/top-secret key oriented confirmation is not that much security safeguarding.it may be that as, it is all around identified that safety is a fundamental component which is considered in distributed totaling frameworks. 2, it is regular to use computer within certain individuals. from the web program it is informal for developers for presenting some spyware to take in the login catchphrase. It is late proposed get to control display known as characteristic oriented get to control is a dressed contender to grip the primary problem. If we consider the last mentioned 2nd issue on electronic managements, it is basic that PC's might be used by more number of clients especially in few vast undertakings or relations

1.1.2 Scope of the project:

There is another fine graiined two figure verification acquire to switch outline for automated distributed computing managements. Here, we are proposing 2 factor get to control outline, a quality oriented acquire to switch system is actualized in the need of both a client unidentified key and a frivolous retreat gadget. The user cannot acquire to the outline if they not keep both, the instrument will upgrade the safety of the outline, especially in the situations of numerous clients share the same computer for electronic cloud managements.

1.1.3 Objective of the project:

- Our main aim of our project is to provide security to the cloud.
- We are using the 2FA concept which is using the user's identity that is nothing but along with the user's password scheme the user should keep his safety device for the login and accessing the necessity information from the cloud.

II. METHODS AND MATERIAL

Salt Encryption algorithm

A salt is arbitrary information thatis used as an additional influence to a limited volume that confusions a confidential key or passphrase.

Salts exist resolutely recognized with the hint of nonce. The important point of salt is to protect beside each word situation is the volume of salt against its hashed comparable, a preregistered multicolored bench assault. These are used to protect watchwords.

Historically a secret key was kept aside in plaintext on a outline, however after few time

A new salt is randomly created for every furtive word. In an average setting, the salt and the secret key are linked and ready with a cryptographic hash work, and the subsequent yield is with the salt is kept away in a database.

Chopping takes into account later confirmation without charge and along these lines pleasing a chance with the

plaintext top-secret key if the validation info store is imported off.

Advantages of salt:

Likewise saltss make word reference assaults and savage compel assaults for splitting vast quantities of passwords much slower (however not in the situation of breaking only one secret word).

Another (lesser) advantage of a salt is as per the following: two clients may pick an indistinguishable string from their secret key, or a similar client may utilize a similar watchword on two machines. Without a salt, this secret key would be put away as a similar hash string in the watchword document. This would uncover the way that the two records have a similar secret key, permitting any individual who knows one of the record's passwords to get to the next record. By salting the passwords with two irregular characters, regardless of the possibility that two records use a similar catchphrase, nobody can find this fair by perusing hashes.

III. Literature Survey

In this paper[1] presented accepting software as a account archetypal of billow which is acclimated to call the aegis challenges in Software as a Account (SaaS) archetypal of billow accretion and aswell end eavors to accommodate approaching aegis analysis directions.From this cardboard we accept referred the band-aid On Billow Accretion Security.

In this paper[2] presented framework for defended billow computing. A billow aegis archetypal and aegis framework that identifies aegis challenges in billow computing. From this cardboard we accept referred the band-aid for aegis challenges in billow accretion andproposed a aegis archetypal and framework for defended billow accretion ambiance thatidentifies aegis requirements, attacks, threats, apropos associated to the deployment of the clouds.

In this paper[3] proposeda abstraction on affidavit and admission ascendancy for billow computing.The aegis issues are still in bend of solutions, because of that so abounding organizations are cat-and-mouse for acceptance of billow accretion services. This is a analysis cardboard for affidavit and admission ascendancy for billow computing. From this Paper, we accept referred a acceptable band-aid affidavit and admission ascendancy for the billow computing.

In this paper[4] presented admission ascendancy archetypal for billow platforms application multi-tier graphical authentication. This proposed arrangement has been evaluated beneath assorted situations. Both of the graphical countersign schemes accept been evaluated alone with assorted countersign combinations. The new multi-level graphical countersign arrangement can be advised as a defended arrangement for billow platforms. FromthisPaper, we accept referred the archetypal will be added with added functionality and college akin of affidavit security; it would be implemented by application aegis questions, angel based aegis for the login aegis and at the endure akin User Identification Number (UIN) would be acclimated to admission or appearance the abstracts in billow platforms on adaptable accessories and software systems for computers Joseph K.

In this paper [5] proposed k-times attribute-based bearding admission ascendancy for billow accretion which is decidedly advised for acknowledging billow accretion environment. From this Cardboard , We accept referred an attribute-based admission ascendancy apparatus which can be admired as the alternate anatomy of Attribute Based Signature.

In this paper [6], "PERM: Practical notoriety based boycotting without TTPS," in Proc. ACM Conf. Comput. Commun.Secur.(CCS), Raleigh, NC, USA, Oct. 2012, pp. 929–940.

In this paper [7], "BLACR: sans ttp blacklistable mysterious accreditations with notoriety," in Proc. nineteenth NDSS, 2012, pp. 1–17.

In this paper [8], "Steady size dynamic k-TAA," "A protected distributed computing based system for enormous information data administration of brilliant network," IEEE Trans. Cloud Comput.

In this paper [9], “Receipt-free electronic voting schemes for large scale elections,” in Proc. 5th Int. Workshop Secur. Protocols.

In this paper [10], "Efficient attribute-based signatures for non-monotone predicates in the standard model," in Public Key Cryptography.

Existing System:

A user has to login before entering into the cloud and to access the information stored onto the cloud server. There are 2 problem's in userid and password system. That is, Firstly, accessing the information using only userid and password system is not much safe. So that, we all well known that safety is more crucial impact on cloud computing process. Secondly, the single computer can be shared by many people in an organization, this is the easy way for the hackers to crack the userid and password using few spyware softwares.

Disadvantage:

1. Accessing the information using only userid and password does not provide safety to the cloud.
2. Sharing the same computer between many people in an organization.

Proposed System:

Our proposed system is a property based mechanism which is implemented with the user's userid and password along with the user safety device. The user should keep both the thing along with him/her to enter into the cloud. If in case the user does not keep both with him, he cannot access the information from the cloud. This provides more security especially in the situations of sharing the same PC's in an organization. The property base mechanism also limits from accessing the information. In this, we need only proof of the user rather than identity of the user.

Our gadget has the some features. Gadget can operate some frivolous calculations, That is, hashing and exponentiation are the examples .Gadget is alter safe, that is, it is assume that no body can br.eak into it to acquire the mystery data kept left inside. With this gadget, our convention gives a 2FA safety. Start with the client mystery key is necessary. What's more, the safety gadget must to be likewise joined to the system with a detailed finish area to confirm the client of receiving to the cloud.

Advantage:

1. This Procedure bolsters fine grained characteristic depend to get to that gives an awesome adaptability to the framework to set diverse get to approaches as indicated by various situations.
2. At a similar time, the security of the client is also protected.
3. This cloud framework just feels that the user forms few necessary characteristic, but not the original personality of the customer.
4. To demonstrate the common sense of our framework, we reenact the model of the convention.

IV. RESULTS AND DISCUSSION

System Design

The framework configuration is an idea that gives plan of the framework. The framework configuration ought to be done in a way where configuration ought to satisfy the requirements the client. The framework configuration ought to likewise incorporate the viewpoints, adaptability, security and intricacy of the framework. The framework configuration must be composed in the way which can take care of the current issue of the framework and furthermore answer for the issues which may happen later on. The primary concentration of the framework configuration is to actualize the framework in detail. Consequently framework configuration is a way of describing and producing framework to fulfill the client necessity.

System Perspective

The compositional outlines fundamentally focus on the plan of the framework which characterizes a structure, conduct and perspective of the framework.

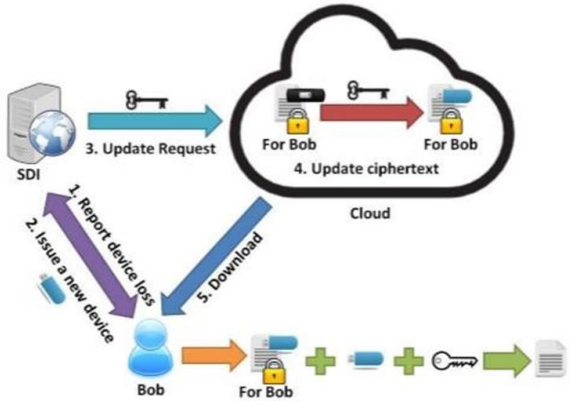

Figure 2. An overview of our project

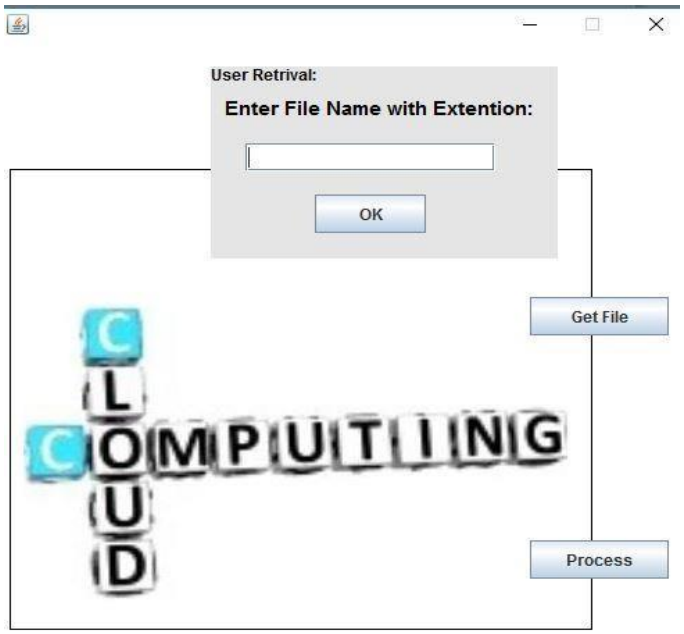

Figure 3. Getting file from the cloud

Figure 4. files available for user to download

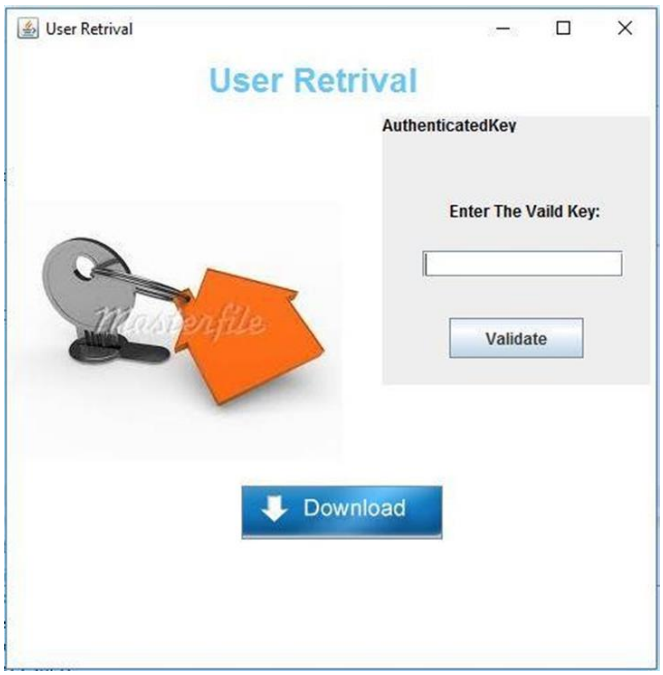

Figure 5. Download the file

Figure 6. Secrete key generation

Figure 7. Upload the file

V. CONCLUSION

We have introduced a new fine garined two factor access control mechanism for web based cloud computing services. The main problem is, the user need to login before entering into the server. Password scheme is not much safe for cloud.

Using salt Encryption Algorithm we are solving the problem and providing security to the cloud. we are proposed a concept of 2FA access which means along with the password scheme the user need to keep the safety device which generates the one time password for the user. Through that the user can enter into the server and he can able to download the necessity files from the cloud.

VI. FUTURE ENHANCEMENT

In future enhancement a huge future extent of work. It is exceptionally extensible. The security issues are expanding step by step. Since the advances and its safe utilize is an essential concern we utilize diverse and secure get to control and validation system. The tangible fear is more easy to understand and profoundly secure measures must be created and executed. So the future work has an extension on this region where more easy to understand safety efforts must be concentrated.

VII. REFERENCES

[1]. M. H. Au and A. Kapadia, "PERM: Practical notoriety based boycotting without TTPS," in Proc. ACM Conf. Comput. Commun.Secur.(CCS), Raleigh, NC, USA, Oct. 2012, pp. 929- 940.

[2]. M. H. Au, A. Kapadia, and W. Susilo, "BLACR: sans ttp blacklistable mysterious accreditations with notoriety," in Proc. nineteenth NDSS, 2012, pp. 1-17.

[3]. M. H. Au, W. Susilo, and Y. Mu, "Steady size dynamic k-TAA," inProc. fifth Int. Conf. SCN, 2006, pp. 111-125. 4] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang, "A protected distributed computing based system for enormous information data administration of brilliant network," IEEE Trans. Cloud Comput., vol. 3, no. 2, pp. 233-244, Apr./Jun. 2015.

[4]. M. Bellare and O. Goldreich, "On characterizing evidences of learning," I Proc. twelfth Annu. Int. CRYPTO, 1992, pp. 390-420.

[5]. J. Be, and B. Waters, "Ciphertext-approach attributebased encryption," in Proc. IEEE Symp.Secur. Security, May 2007, pp. 321-334.

[6]. D. Boneh, and Shacham, "Short gathering marks,"

[7]. in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2004, pp. 41-55.

[8]. D. Boneh, X. Ding, and G. Tsudik, "Fine-grained control of security abilities," ACM Trans. Web Technol., vol. 4, no. 1, pp. 60-82, 2004.

[9]. J. Camenisch, "Aggregate mark plans and installment frameworks in view of the distinct logarithm issue," Ph.D. exposition, ETH Zurich, Zürich, Switzerland, 1998.

[10]. J. Camenisch, M. Dubovitskaya, and G. Neven, "Negligent exchange with get to control," in Proc. sixteenth ACM Conf. Comput.Commun.Secur.(CCS), il, USA, November. 2009, pp. 131-140.