ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Improving Security Using Arbitrary State Attribute Base Encryption

Surah Kumar[1], Rohitrai[2], Abhishek Poddar[3]

B. E Student, Department of Computer Engineering, Dr D Y Pail Institute of Engineering and Technology, Ambi, Pune, Maharashtra, India[1]

B. E Student, Department of Computer Engineering, Dr D Y Pail Institute of Engineering and Technology, Ambi, Pune, Maharashtra, India [2]

B. E Student, Department of Computer Engineering, Dr D Y Pail Institute of Engineering and Technology, Ambi, Pune, Maharashtra, India[3]

ABSTRACT: Dynamic Proof of Storage (Pops) could be a helpful scientific discipline primitive that allows a user to see the integrity of outsourced files and to with efficiency update the files in a very cloud server. Though researchers have planned several dynamic PoSschemes in single user environments, the matter in multi-user environments has not been investigated sufficiently. A sensible multi-user cloud storage system wants the secure client-side cross-user reduplication technique, that permits a user to skip the uploading method and procure the possession of the files now, once alternative house owners of an equivalent files have uploaded them to the cloud server. To the simplest of our data, none of the present dynamic Poss. will support this system. during this paper, we have a tendency to introduce the conception of deduplicatabledynamic proof of storage associated propose an economical construction referred to as Depose, to realize dynamic PoS and secure cross-user duplication, at the same time. Considering the challenges of structure diversity and personal tag generation, we have a tendency to exploit a unique tool referred to as Homomorphism genuine Tree (HAT). We have a tendency to prove the protection of our construction, and therefore the theoretical analysis and experimental results show that our construction is economical in follow.

KEYWORDS: Deduplication, Proof of ownership, Dynamic proof of storage, Cloud Computing

I. Introduction

In cipher text attribute base secret writing theme (CP-ABE) might be a secure secret writing technique use in cloud computing. throughout this theme info owner has full authority to assign all access permission .But In recent state of affairs info user square measure increase, therefore with the increasing vary of cloud users there is a risk of users secret key square measure instrument. Key of data owner square measure manage or instrument as a results of the key authority or cloud service provider every do not appear to be honest. Therefore to manage key of data owners and implement attribute with arbitrary state. Therefore we have a tendency to tend to propose an issue with a pair of party key provision mechanism with weighted attribute. Therefore every storage value and secret writing quality for cipher text square measure solves. The weighted attribute is introduced to not only extend attribute expression from binary to arbitrary state, but to boot to change access policy. Thus, the storage value and secret writing value for a cipher text are mitigated. We have a tendency to tend to use the next example to extra illustrate our approach. The weighted attribute is introduced to not only extend attribute expression from binary to arbitrary state, but to boot to change access policy. Thus, the storage value and secret writing value for a cipher text are mitigated. We have a tendency to tend to use the next example to extra illustrate our approach.

We propose Associate in nursing attribute-based info sharing theme for cloud computing applications, that's denoted as cipher text-policy weighted ABE theme with removing instrument (CP-WABE-RE). It successfully resolves a pair of kinds of problems: key instrument and arbitrary-sate attribute expression.

We propose Associate in Nursing improved key provision protocol to resolve the key instrument drawback of CP-ABE in cloud computing. The protocol can forestall Hindu deity and CSP from knowing each other's master secret key therefore none of them can manufacture the whole secret keys of users on a personal basis thus, the entirely honest Hindu deity are semi-trusted. Data. We have a tendency to divide a traditional attribute in a pair of parts first is attribute and second is its value. For example, the quality attributes are denoted as. The improved attributes square measure denoted as: , where "Career" represents Associate in Nursing attribute and "Doctor", "Professor" and "Engineer" denote the values of the attribute "Career" Time server is supplemental in whereas uploading the file and specify time with that file therefore file is accessible to users only for time assign by time server.

SCOPE **-** Redesigned Associate in Nursing attribute-based info sharing theme in cloud computing and improved key activity protocol for to resolve the key instrument disadvantage. It enhances info confidentiality and privacy in cloud system against the managers of deity and CSP more as malicious system outsiders, where deity and CSP square measure semi-trusted. to boot, the weighted attribute improves the expression of attribute, which could not only describe capricious state attributes, but put together prune the complexity of access policy, so as that the storage worth of cipher text and continuance in secret writing is saved

II. RELATED WORK

2.1 Improving Privacy and Security in Multi-Authority Attribute-Based Encryption

Authors: Melissa Chase, Sherman S.M. Chow

Description: it's surreal to assume there is one authority which could monitor every single attribute of all users. Multi-authority attribute-based coding permits a heap of realistic activity of attribute-based access management, mere entirely totally different completely different} authorities area unit responsible for supplying different sets of attributes. The primary answer by Chase employs a trustworthy central authority and conjointly the utilization of a world image for each user, which means the confidentiality depends critically on the protection of the central authority and conjointly the user-privacy depends on the honest behaviour of the attribute-authorities.

2] **Randomizable Proofsand Delegable Anonymous Credentials**

Authors: Mira Blankly, Jan Camenisch, Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and HovavShacham

Description: Users can anonymously and unlink aptly acquire credentials for several authorities, delegate their credentials to different users, and prove possession of a certificate L levels faraway from a given authority. We have a tendency to tend to revise the entire approach to constructing anonymous credentials and confirm randomizable zero-knowledge proof of knowledge systems as a result of the key building block. We have a tendency to tend to formally define the notion of randomizable non-interactive zero-knowledge proofs, and provide the first instance of controlled re-randomization of non-interactive zero-knowledge proofs by a third-party.

3] **Improving Privacy and Security in Multi-Authority Attribute-Based Encryption**

Authors: Melissa Chase, Sherman S.M. Chow.

Description: it's unreal to assume there is one authority which could monitor every single attribute of all users. Multi-authority attribute-based coding permits a heap of realistic preparation of attribute-based access management, such entirely completely different completely different} authorities unit of measurement in control of issuing different sets of attributes. The primary resolution by Chase employs a trustworthy central authority and thus the utilization of a world image for each user that suggests the confidentiality depends critically on the protection of the central authority and thus the user-privacy depends on the honest behaviour of the attribute-authorities. Approaches.Finally, we have a tendency to gift some recommendations for the event of next-generation cloud security and assurance solutions

III. PROPOSED SYSTEM

No Such system of Dynamic proof of storage will achieve cross user deduplication. To remove these drawbacks we implement Deduplicatabledynamic proof of storage. We propose associate attribute-based information sharing theme for cloud computing applications, that's denoted as cipher text-policy weighted ABE theme with removing legal document (CP-WABE-RE). We tend to tend to propose associate improved key issue protocol to resolve the key legal document drawback of CP-ABE in cloud computing. The protocol can stop Ka and CSP from knowing each other’s master secret key so as that none of them can manufacture the full secret keys of users on a private basis so, the completely reliable Ka are going to be semi-trusted. Information confidentiality and privacy are going to be ensured. We tend to tend to gift weighted attribute to spice up the expression of attribute. The weighted attribute cannot only specific arbitrary-state attribute (instead of the traditional binary state), but collectively trim the standard of access policy. So the storage worth of cipher text and computation quality in committal to writing is going to be reduced. Besides, it'll specific larger attribute house than ever below constant condition. We tend to tend to conduct and implement comprehensive experiment for the planned theme. The simulation shows that CP-WABE-RE theme is economical every in terms of computation quality and storage worth. To boot, the security of CP-WABE-RE theme is to boot established below the generic cluster model. Time server is introducing for distribution an amount with file at time of uploading. So this file is accessible to user only for time such by time server.

1] CP-WABE-RE (Cipher text policy-Weighted attribute base encryption revisited in cloud)

In Cipher text- policy attribute base cryptography Associate in Nursing improved key supply protocol to resolve the key legal instrument downside of CP-ABE in cloud computing. The protocol can stop divinity and CSP from knowing each other’s master secret key so as that none of them can turn out the overall secret keys of users severally thus, the wholly trustworthy divinity is semi-trusted. Information confidentiality and privacy is ensured. We have a tendency to tend to gift weighted attribute to spice up the expression of attribute. The weighted attribute cannot only specific arbitrary-state attribute (instead of the traditional binary state), but to boot reduce the standard of access policy.

2] Key Authority (KA).

It is a semi-trusted entity in cloud system. Namely, Ka is honest-but-curious, which may honestly perform the appointed tasks and come back correct results. However, it'll collect as several sensitive contents as potential. In cloud system, the entity is chargeable for the users’ enrolment. Meanwhile, it not solely generates most a part of system parameter, however additionally creates most a part of secret key for every user.

3] Time Server

In our system we tend to propose a Time Server. We tend to use Time server in our system for assignment a time to a file that is uploading in cloud. By assignment a time to file we tend to outline a time base access permission to file. By assign a time to file specific user access this file for that point amount solely .After assign time is completed file is mechanically unavailable for user for access.

4] Advantages of propose system:

2.4.1 Proposed an arbitrary-state ABE to solve the issue of the dynamic membership management.

2.4.2 The attributes are divided into multiple levels to achieve fine-grained access control for hierarchical attributes, but the attributes can only express binary state.

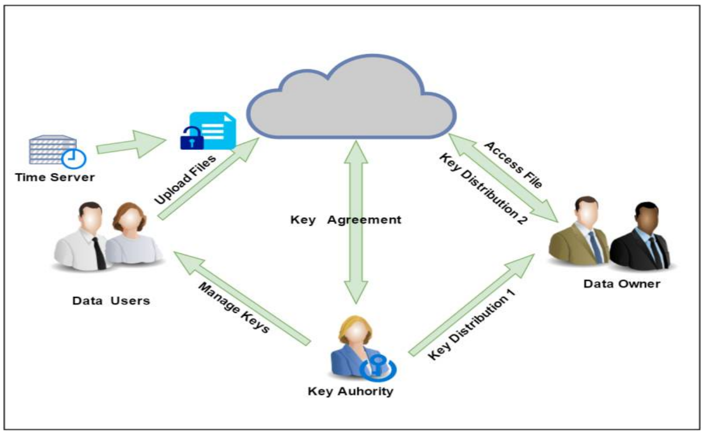


Fig.1. System architecture

Mathematical Model

Phase 1: System Initialization. {SI}
It includes: **KA**.**Setup and**CSP.**Setup.**
(1) **KA**.**Setup**(1κ). KA runs the algorithm which inputs a security parameter κ. Then, KA chooses random α1, β ∈Zapandcomputes h= goand u1 = ˆe (g, g) α1. Lastly, it obtains PP1 and MSK1 as the formula
: PP1 = {G0, g, h, u1}, MSK1 = {α1, β}
(2) **CSP**. **Setup** (**1**κ). CSP executes the operation which inputs a security parameter κ. Based on the κ, CSP chooses a random number α2 ∈Zapand calculates u2 = ˆe (g, g) α2. Then, it sets PP2 and MSK2 as the formula:
PP2 = {u2}, MSK2 = {α2}
Finally, the public parameter and master secret key of system
Are denoted as PP = {G0, g, h, u = u1 · u2 = ˆe (g, g) α},
Whereα = α1 + α2, and MSK = {{α1, β}, {α2}}.

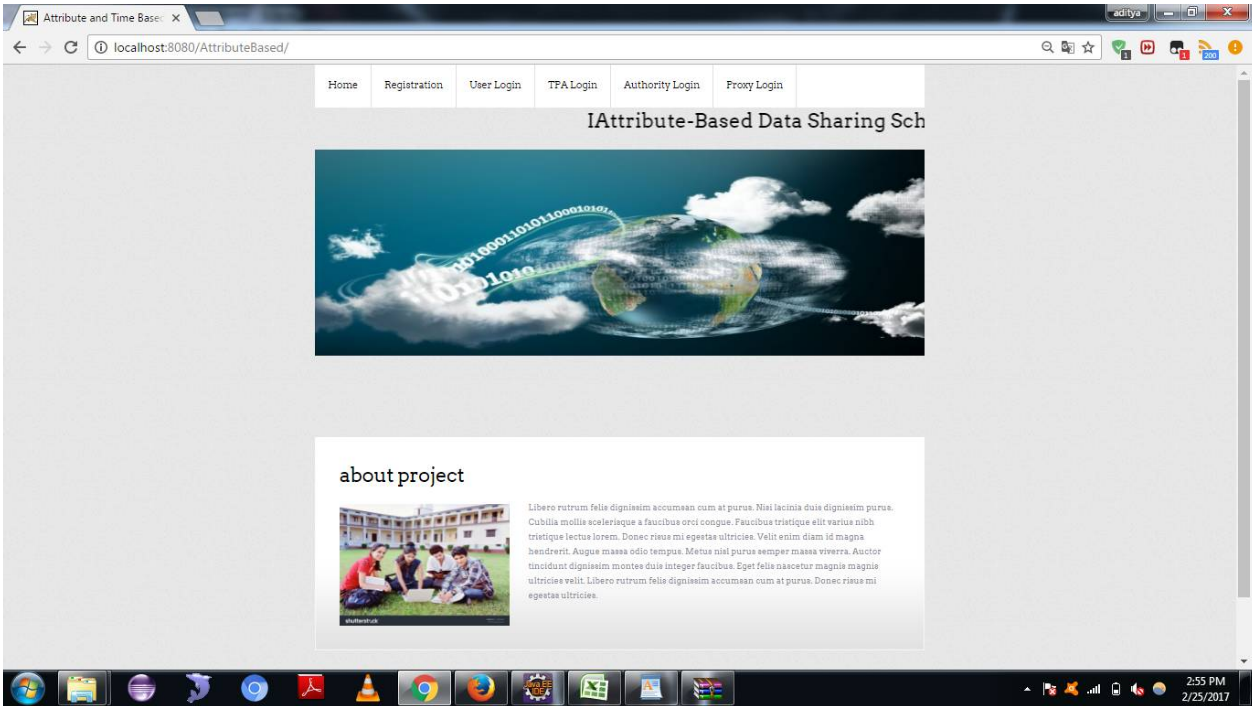
Phase2: DataEncryption {De} :(
The improved algorithm is executedby DO which inputs PP, ck and T. It outputs CT. beginning from the root node R, DO sets or (0) =s(s ∈Zap), where s is randomly selected. And DO randomly selects dryother points of the polynomial or to define it completely. For each non-root node x, it sets ox (0) parent(x) (index(x)) and randomly chooses doother points to completely define ox. Meanwhile, each leaf node denotes an attribute with weight.
Finally, DO send the integrated cipher text{ID, CT, Eck(M)} to CSP.

Phase 3:User Key Generation {Kg}. This phase consists of **KA**.**Eigen** and **CSP**.**KeyGen .**
KA.**KeyGen:** (MSK1, r, S): input to KA is r ∈Zpchosen randomly. For each weighted attribute j ∈S, itpossesses weighted value job (job∈W). Finally, it computesSK1 described by S as the formula:
SK1 = {L = g^{o}, $\forall_j$∈S:D_o= H (j) ^{raj}}and complete key is
SK= {D = $g^{\alpha}h^{r,}$L=g^{o}, $\forall_j$∈S:D_o= H (j) ^{raj}}

CSP.**KeyGen**. We provides an improved key issuing protocol between KA and CSP to execute the work of CSP.
KeyComKA↔CSP (MSK1, It, r, MSK2).Assume that user t needs a secret key
KA choose r ∈Zapfor users, CSP selects a random number ρ1 ∈Zap to calculate
X1 = $g^{o/\rho1}$ = g $^{(\alpha1+\alpha2)\ \beta/\rho1\ \text{and}}$ transmits {X1,PoK(ρ1, x)} to KA.
CSP calculatesD = Y $^{1}{}_{3}{}^{/\rho2}$ = g $^{(\alpha1+\alpha2)}$ hr= $g^{\alpha}h^{r}$and sends a personalized key component SK2 = {D = $g^{\alpha}h^{r\}}$to the corresponding user t.

Phase 4: DataDecrypt {De} (Eck (M), ck):
User inputs file cipher textEck (M) and content key ck
Deckdenotes a symmetric decryption operation with the key ck.
Deck [Eck (M)] = M.
.

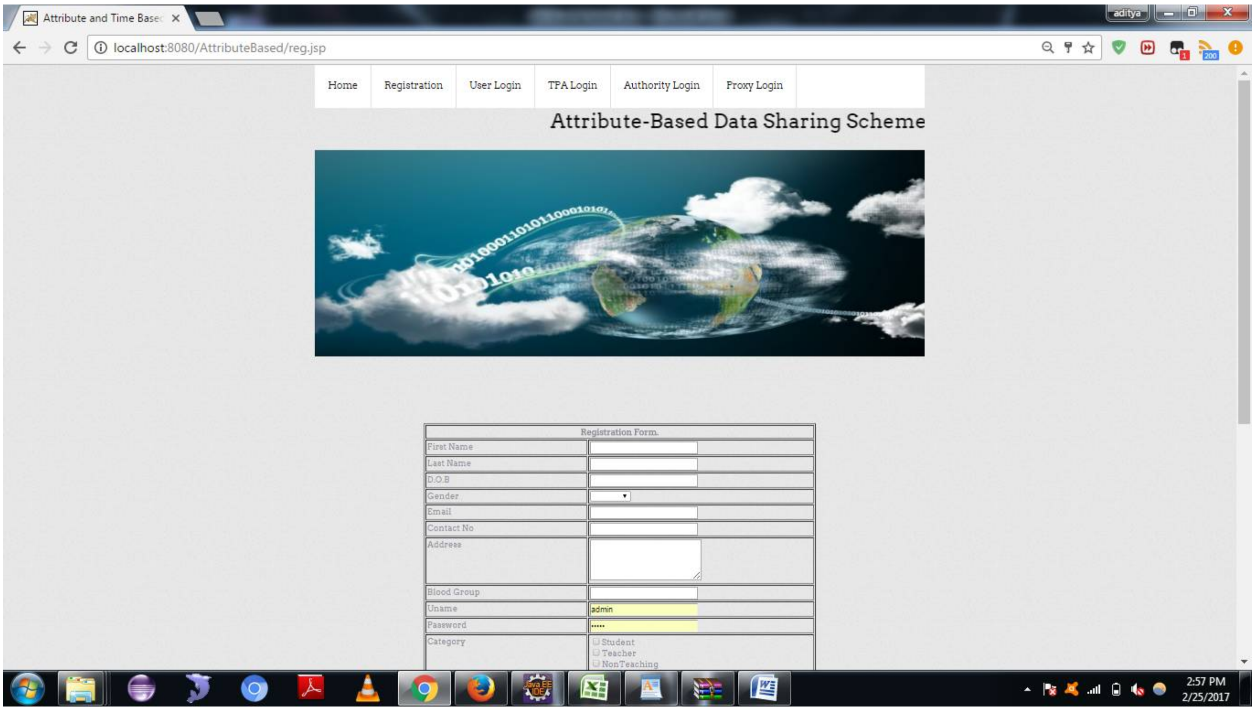
IV. RESULTANALYSIS



IAttribute-Based Data Sharing Sch

about project

Libero rutrum felis dignissim accumsan cum at purus. Nisi lacinia duis dignissim purus. Cubilia mollis scelerisque a faucibus orci congue. Faucibus tristique elit varius nibh tristique lectus lorem. Donec risus mi egestas ultricies. Velit enim diam id magna hendrerit. Augue massa odio tempus. Metus nisl purus semper massa viverra. Auctor tincidunt dignissim montes duis integer faucibus. Eget felis nascetur magnis magnis ultricies velit. Libero rutrum felis dignissim accumsan cum at purus. Donec risus mi egestas ultricies.



Attribute-Based Data Sharing Scheme

Registration Form.	
First Name	
Last Name	
D.O.B	
Gender	▾
Email	
Contact No	
Address	
Blood Group	
Uname	admin
Password	•••••
Category	□ Student □ Teacher □ NonTeaching

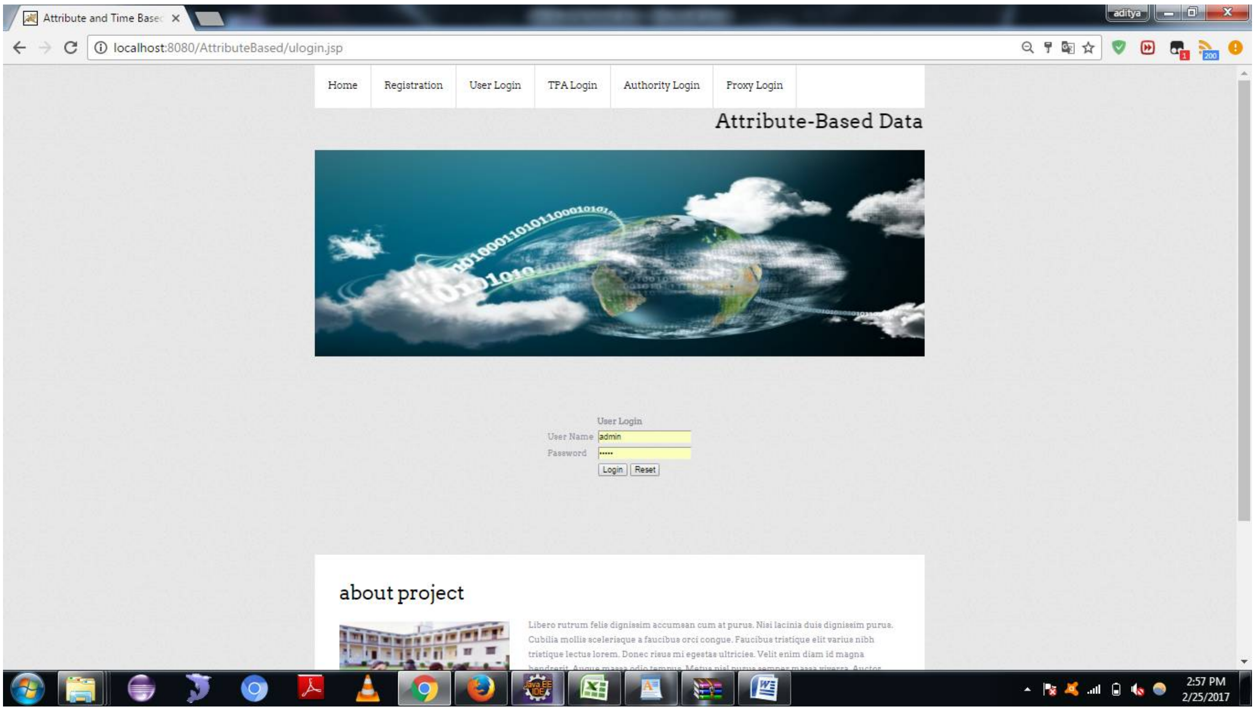
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

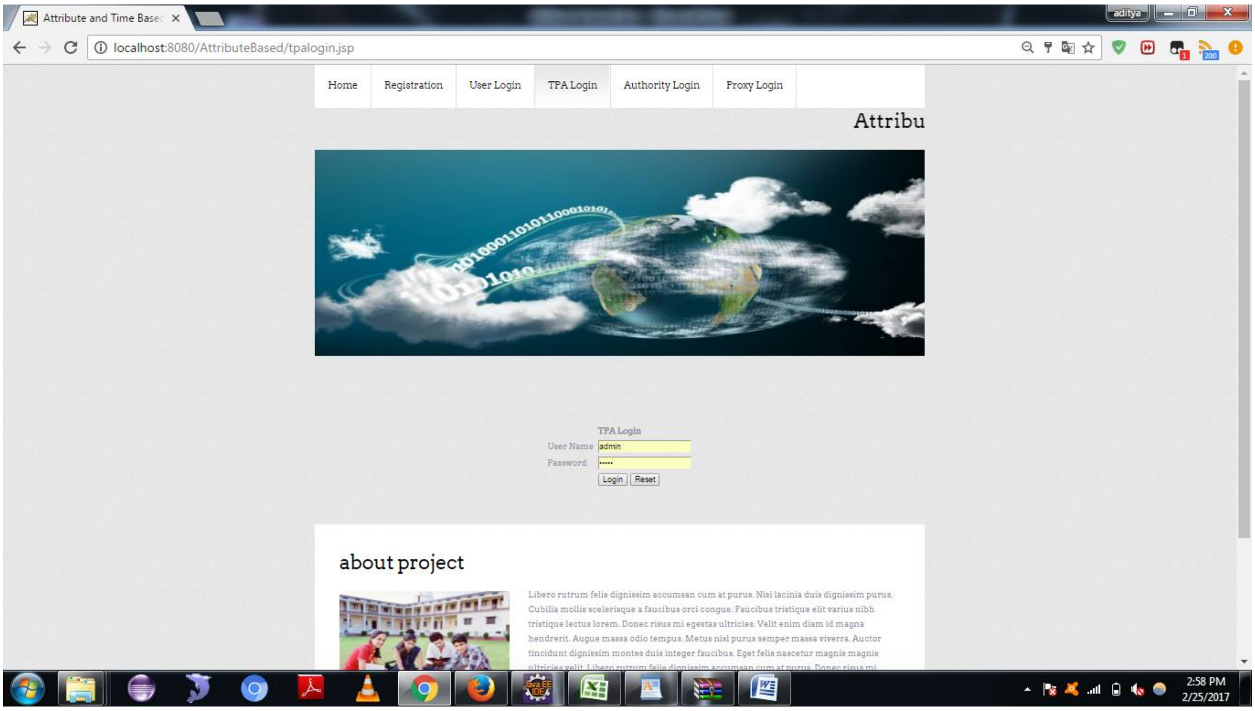


Attribute-Based Data

User Login
User Name admin
Password •••••
Login Reset

about project

Libero rutrum felis dignissim accumsan cum at purus. Nisi lacinia duis dignissim purus. Cubilia mollis scelerisque a faucibus orci congue. Faucibus tristique elit varius nibh tristique lectus lorem. Donec risus mi egestas ultricies. Velit enim diam id magna

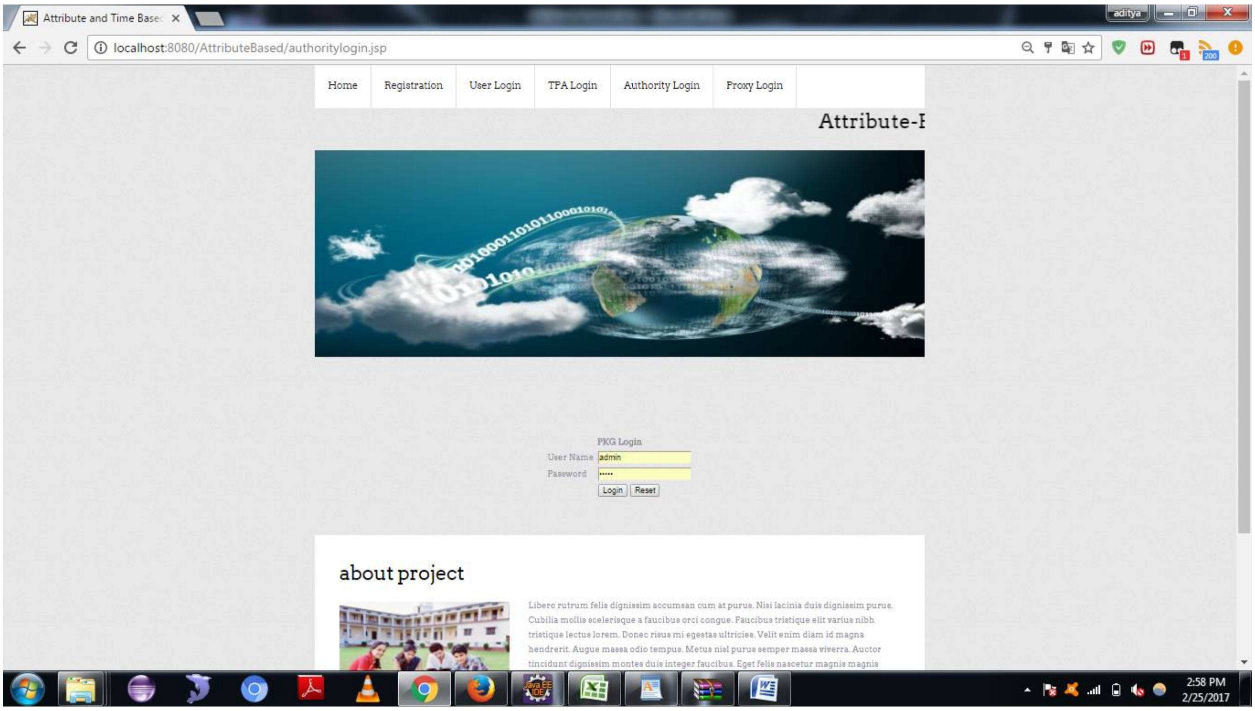


Attribu

TPA Login
User Name admin
Password •••••
Login Reset

about project

Libero rutrum felis dignissim accumsan cum at purus. Nisi lacinia duis dignissim purus. Cubilia mollis scelerisque a faucibus orci congue. Faucibus tristique elit varius nibh tristique lectus lorem. Donec risus mi egestas ultricies. Velit enim diam id magna hendrerit. Augue massa odio tempus. Metus nisl purus semper massa viverra. Auctor tincidunt dignissim montes duis integer faucibus. Eget felis nascetur magnis magnis



PKG Login

User Name admin

Password •••••

about project

Libero rutrum felis dignissim accumsan cum at purus. Nisi lacinia duis dignissim purus. Cubilia mollis scelerisque a faucibus orci congue. Faucibus tristique elit varius nibh tristique lectus lorem. Donec risus mi egestas ultricies. Velit enim diam id magna hendrerit. Augue massa odio tempus. Metus nisl purus semper massa viverra. Auctor tincidunt dignissim montes duis integer faucibus. Eget felis nascetur magnis magnis

V. Conclusion

We don't have any text to check? Don't have any text to check? Click "Select Samples" .In this paper, we have a tendency to tend to vogue Associate in Nursing improved attribute base sharing theme is cloud computing. This improved protocol was bestowed to unravel a key agreement draw back in cloud computing. In addition improves a confidentiality and privacy in cloud computing against Key authority and cloud service suppliers and in addition from any outside malicious system. In addition, the weighted attribute was projected to reinforce the expression of attribute, which can not only describe absolute state attributes, but in addition reduce the complexity of access policy, therefore the storage worth of cipher text and duration in cryptography are going to be saved. Finally, we have a tendency to tend to bestowed the performance and security analyses for the projected theme, throughout that the results demonstrate high efficiency and security of our theme.

ACKNOWLEDGMENT

We might need to impart the analysts and conjointly distributers for creating their assets accessible. We have a tendency to in addition appreciative to commentator for his or her vital recommendations what is more imparting the college powers for giving the duty-bound base and backing.

REFERENCES

[1] J. Beak, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang. A secure cloud computing based framework for big data information management of smart grid. IEEE Transactions on Cloud Computing, 3(2):233–244, 2015.
[2] A. Bale and K. Kuppusamy. An expressive and provably secure cipher text-policy attribute-based encryption.Information Sciences, 276(4):354–362, 2014.
[3] M. Belenkiy, J. Camenisch, M. Chase, M., A. Lysyanskaya, and H. Shacham. Randomizable proofs and delegatable anonymous credentials. Proceedings of the 29th Annual International CryptologyConference, pages 108–125, 2009.
[4] J. Bettencourt, A. Sashay, and B. Waters. Cipher text-policy attribute based encryption. IEEE Symposium on Security and Privacy, pages 321–334, 2007.
[5] D. Bone, B. Lynn, and H. Sachem. Short signatures from the Weilpairing.Journal of Cryptology, 17(4):297–319, 2001.

[6] M. Chase. Multi-authority attribute based encryption. Proceedings of the 4th Conference on Theory of Cryptography, pages 515–534, 2007.
[7] M. Chase and S. S. Chow. Improving privacy and security in multiauthority attribute -based encryption.Proceedings of the 16th ACMConference on Computer and Communications Security, pages 121–130,
2009.
[8] L. Cheung and C. Newport. Provably secure cipher textpolicy ABE. Proceedings of the 14th ACM conference on Computer and communicationssecurity, pages 456–465, 2007.
[9] S. S. Chow. Removing escrow from identity-based encryption. Proceedings of the 12th International Conference on Practice and Theory in Public Key Cryptography, pages 256–276, 2009.
[10] C. K. Chu, W. T. Zhu, J. Han, J. K. Liu, J. CSU, and J. Zhou. Security concerns in popular cloud storage services. IEEE Pervasive Computing, 12(4):50–57, 2013.
[12] Ankit Lodha, Clinical Analytics – Transforming Clinical Development through Big Data, Vol-2, Issue-10, 2016
13] Ankit Lodha, Agile: Open Innovation to Revolutionize Pharmaceutical Strategy, Vol-2, Issue-12, 2016
[14] Ankit Lodha,Analytics: An Intelligent Approach in Clinical Trail Management,Volume 6, Issue5, 1000e124