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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Ranking Based Shared Authority Privacy Preserving Authentication Protocol in Cloud Computing

Yerragunta Harshada [1], K.Janardhan [2]

M-Tech Student, Department of C.S.E., INTELL Engineering College, Anantapuramu, Andhra Pradesh, India

Associate Professor, Department of C.S.E.,INTELL Engineering College, Anantapuramu, Andhra Pradesh, India

ABSTRACT: Cloud computing is rising as a prevailing data interactive model to take in users' data which has been remotely stored in an online cloud server. On-demand cloud applications is offered by the cloud services without any local infrastructure limitations. Multiple users may wish to access and share another user's authorised data fields to achieve successful benefits. whenever user request another users for information sharing, Access request itself may uncover the client's security regardless of whether it can obtain the data access permissions or not. The option of granting/revoking data access and ranking at the admin level for the number of times the particular file has been requested is not present in the existing system .In a Proposed System Ranking Based shared authority privacy-preserving authentication protocol (RSAPA) address the above privacy issue for cloud storage. And provide ranking at the Admin level .In the RSAPA,1) shared access authority is achieved by the anonymous access request matching mechanism, without out revealing the user's privacy for a data demand 2) user can access his own data fields by attribute based access control 3) Data sharing between the different users is achieved by proxy re-encryption in cloud server In the mean time, universal compose capability (UC) model is built to demonstrate that the SAPA hypothetically has the outline accuracy .It demonstrates that the proposed protocol acknowledging privacy-preserving data access authority sharing, is keen for multi-user collaborative cloud applications. In our model, privacy is achieved by encrypting the data it can prevent the unapproved access. Also, we are going to raise the security level of the owner of the data and confidentiality of the information by giving access to the users

KEYWORDS: Cloud computing, authentication protocol, privacy preservation, shared authority, universal composability.

I . INTRODUCTION

cloud computing may be a promising data technology design for each enterprises and people. It launches a formidable storage and interactive paradigm by the total of actual advantages, together with on-demand self-services, throughout network access, and placement freelance resource pool . A typical business design towards he cloud computing is something as a engagement in activity application (XaaS)., all over infrastructures, platform, software, et al. are applied for throughout interconnections. Recent studies are worked to market the cloud computing grow towards the web of services [2], [3]. later on, security and privacy problems are getting key considerations with the increasing quality of cloud services. standard security approach predominantly specialise in the robust authentication to grasp that a user can remotely access his own data in demand mode. alongside the range of the appliance necessities, users might want to access and share every other's authorised data fields to attain productive benefits, which bring new privacy challenges and security for the cloud storage.

An example has been introduced to mark the most motivation. With in the cloud storage primarily based supply chain management, there are different significance groups (e.g., Retailer, carrier, and Supplier) within the system. every member owns its users that area unit permissible to access the authorised data fields, and totally different users own comparatively freelance access authorities. It implies that any two users from various teams ought to access totally different information fields of an equivalent file. There into, a supplier deliberately might want to access a carrier's information fields, however it's unsure whether or not the carrier can authorize its requested access. If the carrier will refuses its request, the supplier's access need are obvious in conjunction with nothing obtained towards

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

the desired data fields. Actually, the supplier might not send the access request or withdraw the unacceptable request ahead if it firmly is aware of that its request are refused by the carrier. it's unreasonable to completely disclose the supplier's non-public info with none privacy concerns. Fig. one illustrates 3 revised cases to address above undetectable privacy issue.

Case 1: The carrier or the Third party auditor additionally needs to request and access the supplier's data fields, and also the cloud server ought to inform one another and broadcast the shared access authority to the each users;

Case 2: The carrier doesn't have interest on alternative users' data fields, thus its authorised data fields ought to be properly protected, meantime the supplier's access request will be concealed.

Case 3: The carrier might want to access the retailer's data fields, however it's not sure whether or not the owner or supplier can settle for its request or not. The owner's authorised data fields shouldn't be public if the retailer doesn't have interests within the carrier's information fields, and also the carrier's request is additionally in camera hidden. In the above three cases, privacy preservation and security protection are both considered without revealing susceptible access desire related information.

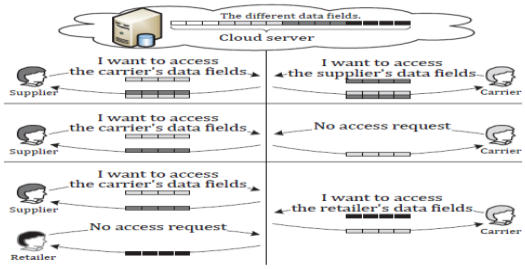


Fig. 1. Three possible cases during data accessing and data sharing in cloud applications.

II. RELATED WORK

In the cloud environments, a reasonable security protocol should achieve the following requirements.

1) Authentication*:* a authorised user may access his own data fields, only the authorised partial or entire data fields can be known by the authorised user, and any forged or tamp data fields cannot deceive the legal user.

2) Data anonymity*:* any inapplicable entity cannot acknowledge the communication state and exchanged data even it intercepts the exchanged messages by an open channel.

3) User privacy*:* any inappropriate entity cannot find a user's access desire, which represent a user's interest in another user's authorised data fields. If and only if the both users have common interests in each other's authorised data fields, the cloud server will intercommunicate the two users to recognize the access permission sharing.

4) Forward security*:* any opponent cannot correlate two communicating sessions to derive the preceding interrogations according to the presently captured messages. Most researches have been worked on and privacy preservation and security protection in cloud applications. and there are diverse cryptographic algorithms to handle potential security and privacy problems. However, most previous researches target the authentication to understand that solely a legal user will access its approved information, that ignores the case that totally different users might want to access and share every other's approved data fields to know productive advantages. once a user challenges the cloud server to request alternative users for data sharing, the access demand may itself reveal the user's privacy regardless of whether or not or not it will get the data access permissions. during this work, we have a tendency to aim to handle a user's sensitive access want connected privacy throughout data sharing within the cloud environments, and it's important to style a humanistic security theme to at the same time accomplish, access authority sharing, data access control and privacy preservation. which shows a user's interest in another user's authorised data fields., the cloud server will inform the two different users to recognise the access permission sharing.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

- The current securities outcome principally focus on the authentication to interpret that a user's non-public data cannot be lawlessly accessed
- When a user demand the cloud server to request different users for data sharing, the access demand may itself reveal the user's privacy despite whether or not or not it will get the data access permissions
- It is vital to style a humanistic security theme to at the same time succeed knowledge access management, access authority sharing, and privacy preservation.
- Hence the present System doesn't have the choice of granting/revoking knowledge access and ranking at the Admin level

III. PROPOSED METHODOLOGY

In a Proposed system specifies a Ranking based shared authority based privacy-preserving authentication protocol (RSAPA) for the cloud data storage, which realises authentication and authorisation without compromising a user's private information. The main contributions are as follows.

- To identify and address a refined privacy issue throughout a user difficult the cloud server for data sharing, within which the challenged request itself will not reveal the user's privacy despite whether or not it can acquire the access authority.
- Proposed an authentication protocol to increase a user's access request related privacy, and also the shared access authority is achieved by anonymous access request matching mechanism.
- Apply cipher text-policy attribute primarily based access control to understand that a user will faithfully access its own data fields, and adopt the proxy re-encryption to supply temporary worker authorised knowledge sharing among multiple users.
- Shared access authority is achieved by anonymous access request matching mechanism with security and privacy concerns while not out revealing the user's privacy to a different user for a data request
- User will access his own knowledge fields by attribute primarily based access control
- Based on proxy re-encryption in cloud server the sharing of data between multiple users has been achieved
- Ranking is provided at the Admin level to specify number of times the particular file has been requested. Particular user can view on his/her dashboard about the number of times he accessed particular file and can get the suggestions if any extensions or particular file is uploaded onto cloud server
- Web Application is developed based of Bootstrap which is most popular Html, CSS and JavaScript framework for developing responsive mobile-first websites Hence the screen resolution is adaptable to mobile, tablet, Pc.

SYSTEM MODEL

Fig. illustrates a system model for the cloud storage architecture, which contains three main network entities: . users (U_x), a cloud server (S), and a trusted third party

A. User*: A* group entity or an Individual, which stores its data in online cloud storage for computing. Multiple users may be affiliated with a communal organization, and are assigned with independent authorities on certain data fields.

B. Cloud server*:* an entity, which is maintained by a particular cloud service provider to provide data storage and computing services. The cloud server is considered as an entity with unlimited storage and computational resources.

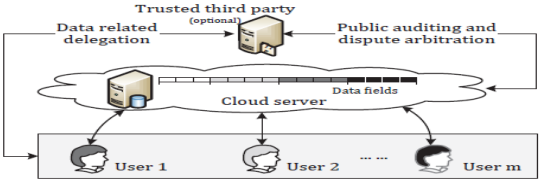
C. Trusted third party*:* a neutral and an optional entity , which has progressive capabilities on behalf of the users, to do data public auditing and dispute arbitration.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015



.

IV. DESCRIPTION OF PROPOSED ALGORITHM

A. Authentication

An authorized user can access his own data fields, only the authorized partial or entire data fields can be identified by the authorized user, and any forged or tamp data fields cannot delude the authorized user. The cipher text-policy attribute based access control and bi linear pairings have been introduced for identifying between Uθ and S, and only the authorized user can derive the cipher texts. Additionally, Uθ checks the re-computed cipher texts accordant to the proxy re-encryption, which relies flexible data sharing rather than publishing the interactive users' secret keys

B. Data Anonymity

Any inapplicable entity cannot recognize the communicating state and exchanged data even it point the exchanged messages by an open gateway the pseudonym PIDU_ are hidden by the hash function so that other entity cannot derive the real values by the inverse operations. Meanwhile, U~θ's temp authorized fields _D U~_ is encrypted by k__ for anonymous data transmission. Hence, an opponent cannot identify the data, even if the opponent captures the transmitted data, it will not crack the complete cryptographic algorithms.

C. User Privacy

Any inapplicable entity cannot identify a user's access tendency, which shows a user's interest in another user's approved data fields. Only if the both users have common interests in each other's authorized data fields,the cloud server will intercommunicate the two users to recognize the access permission sharing The access request pointer (e.g.,RUxU_) is draped along with H(sidS_ ?PIDU_) for privately revealing S about Uθ's access desires. whenever both users are interested in each other's data fields, The re-encryption key kU_ has been set up by S to know authority sharing between Ua and Ub. S will temporarily store the in demand access requests for a certain period of time, and cannot be able to exactly conclude which user is keenly interested in the other user's data fields.

D. Forward Security

Any opponent cannot compare two communication sessions to derive the previous interrogations according to the presently captured messages. The double session identifiers {sidS_ ,sidU_ } and pseudorandom numbers are presented as session variation operators to assure the communications dynamically. An opponent regards the preceding session as random even if {S, Uθ} get corrupted, or the opponent obtains the PRNG algorithm. The existing security compromises cannot correlate with the previous interrogations

E. Attribute based access control

Attribute based access control Specifies a new access control prototype whereby access rights are granted to users through the use of policies which pool attributes together. The policies can use any type of attributes(user attributes, resource attributes, environment attribute etc.). Attribute values can be set-valued or atomic-valued. Set-valued attributes hold more than one atomic values. Examples are role, project. Atomic-valued attributes has only one atomic value. Examples are clearance, sensitivity. Attributes can be compared to static values or to one another Hence enabling relation-based access control.
Ua first extracts its data attribute access list AUa= [aij] (aij? {0; 1}, aij? pij)
to re-structure an access list

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

LUa= [lij]n×mfor lij= pij? aij. Ua
also defines a polynomial
FUa(x;LUa)
according to LUaand TUa.
FUa(x;LUa) = nΠ,mi=1,j=1 (x + ijH(TUa))lij(mod q).
It turns out that FUa(x;LUa) satisfies the equation.
FUa(x;LUa) = nΠ,mi=1,j=1 (x + ijH(TUa))pij?aij=FSa(x; PUa)=FSa(x;AUa):
Afterwards, Ua chooses _ ?Zq, at random and the decryption key kAUafor AUacan be obtained.
kAUa= (g(β+1)/FSa(α,AUa); hβ?1)
Ua further calculate a set of values {NUa1, NUa2, NUa3}. Here, fSaiis has been used to symbolise xi's coefficient in FSa(x; PUa),
and fUaiis used to represent xi's coefficient in FUa(x;LUa).
NUa1 = e(MSa21; Πni=1 (hi)fUaihfUa0); NUa2 = e(Πni=1 (MSa2i)fUai ; hβ?1);
NUa3 = e(g(β+1)/FSa(α,AUa);MSa1):
It turns out that e(g; h)MSa0 satisfies the equation.
NUa1 =e(gαiMSa0 ; Πni=1 (hi)fUaihfUa0) =e(g; h)αMSa0 Σni=1(αi?1fUai+fUa0) =e(g; h)MSa0FUa (α,LUa);
NUa2 =e(Πni=1 gαiMSa0fUai ; hβ?1) =e(g; h)MSa0(Σni=1 αifUai+fUa0?fUa0)(β?1) =e(g; h)MSa0βFUa(α,LUa)?MSa0fUa0 ;
NUa3 =e(g(β+1)/FSa(α,AUa); hfSa0MSa0 Πni=1
(hi)fSaiMSa0) =e(g; h)(β+1)/FSa(α,AUa)FSa(α,PUa)MSa0 = e(g; h)MSa0βFUa(α,LUa)+MSa0FUa (α,LUa);
(NUa1NUa2=NUa3) ?1/fUa0 =(e(g; h) ?MSa0fUa0) ?1/fUa0 =e(g; h)MSa0 :
Ua internally re-computes {_?, M? Sa0 }, derives its own authorized data fields DUa, and checks whether if the cipher text
CSa is encrypted by M? Sa0. If it holds, Ua will be a authorized user who can decently decry-pt the cipher text CSa; otherwise,the protocol will terminate.
_? = MSa3 ?H(e(g; h)MSa0);
M? Sa0 = H(PUa?TUa?_?);
DUa= MSa4 ?H(sidUa?_?):
Ua therefore extracts its pseudonym PIDUa, a session sensible access request RUb
Ua, and the public key pkUa. Here, to let S know its data access ,Rub Ua is set up
desire. It results in that Rub Ua makes S know the facts: 1) Ua wish to access Ub's temporary authorized data fields _D *Ub*;
2) Ra will also accept to share its temporary authorized data fields _D Ua with Ub in the circumstance that Ub grants its request.
Later on , Ua randomly chooses rUa
?Z*q , calculate a set of values {MUa0, MUa1, MUa2, MUa3} to perform a cipher text CUa, and reassigns CUa to S for furthermore access request matching.
MUa0 = H(sidSa?PIDUa) ?Rub Ua ;
MUa1 = gpkUarUa ;
MUa2 = e(g; h)rUa ;
MUa3 = hrUa :
Similarly, Ub execute the related operations, consider that Ub take out AUb, and decide {LUb,FUb(x;LUb), fUbi}. Ub therefore chooses _' ?Zq, at random and calculate the values {NUb1, NUb2, NUb3, _'?, M? Ub} to derive its own data fields DUb. Ub also extracts its anonym PIDUb and an access request RUaUb to establish a cipher text CUb with the elements *{MUb*0*;MUb*1*;MUb*2*;MUb*3*}.*

F. Proxy Re-Encryption

In the RSAPA, To recognize {Ua, Ub}'s access authority sharing ,S act as a semi-trusted proxy . Throughout the proxy re-encryption, {Ua, Ub} respectively set up cipher texts {MUa1, MUb1} by their public keys {pkUa, pkUb}, and S generates the subsequent re-encryption keys {kUa, kUb} for {Ua, Ub}. Supported there-encryption keys, the cipher texts {MUa1, MUb1} are re-encrypted into {M' Ua1, M' Ub1 }, and {Ua, Ub} can decipher the composition cipher texts {M' Ub1, M' Ua1 } by their own private key {skUa, skUb} without disclosing any sensible information. Till now,

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

{Ua, Ub*}* have recognised the access authority sharing in a situation that both Ua and Ub has an access needs on each other's data fields. Meanwhile, there could also be multiple cases when Ua shows interest in Ub's data fields with a challenged access request Rub Ua. 1) In the case that Ub has no interest in Ua's data fields, it seems that Ub's access request *Rub* Ub and Rub Ua satisfy that F(Rub Ua(Rub Ub)T) = *F*(1). For Ua, *S can* extract a dummy data fields *D null* as a response. Ub will be clued-up that a certain user is showing intrest in its data fields, but cannot find Ua's detailed identity for privacy issues. 2) With In the case that Ub has an interest in Uc's data fields instead of Ua's data fields, however Uc doesn't have interest in Ub's data fields. It seems that the challenged access requests Rub Ua, RUcUb, and *R* U~ bUc satisfy that F(Rub Ua(RUcUb)*T*) = F(RUcUb(R U~bUc)T) = *F*(1), in which U~b show that the user is not Ub. *D* null will be sent to {Ua,Ub, Uc} without data sharing

V. EXPERIMENTAL RESULTS

This section shows the screenshots of the website which is basically bookstore where all the books, files are stored in cloud and can be shared between multiple groups like user, retailer and carrier.Fig.1. illustrates the home page , for Bookstore website this consist of Sign up, login , About Us and Contact Us Buttons. About Us and Contact Us buttons is for members feedback and assistance purpose. Books, Textbooks, Audio books, magazines specify the Categories of books available in site.Fig.2. illustrates the Sign up page to Register new account for the Carrier, Retailer, Customer. Fig.3. illustrates the login page for retailer, carrier and Customer. In order to login email-id and password Should be entered and should click on submit button.Fig.4 illustrates Uploading books or files to the cloud by the owner /Retailer. He can add ,delete and can modify the books or files . Fig.*5* illustrates User or customer Requesting for the books to download by adding the selected books to his Cart. He can view all the available books and can place the request .Fig.6 illustrates TPA(Third part auditor) who may approve or revoke the files or books which has been requested by the UserFig.7. illustrates that once the TPA approves the requested book, the secret key will be sent to the customer Mail id.Fig.8. illustrates the download page of the customer. In order to download the requested book, he has to enter the secret key sent to his mail id. After entering the key and by clicking on the download button, the book will be successfully downloaded. Fig.9. illustrates the Ranking of the books based on number of downloads. So user and owner can see number of times the particular book has been downloaded .Fig 10. illustrates that the website is designed based on Bootstrap. If the window is minimized, then the page will accommodate according to screen resolution for Mobile, Tablet or Pc.

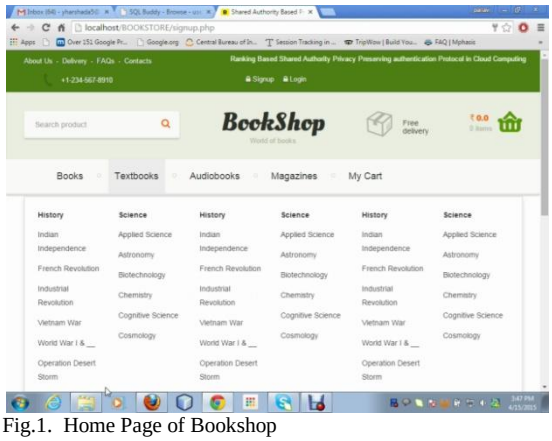


Fig.1. Home Page of Bookshop

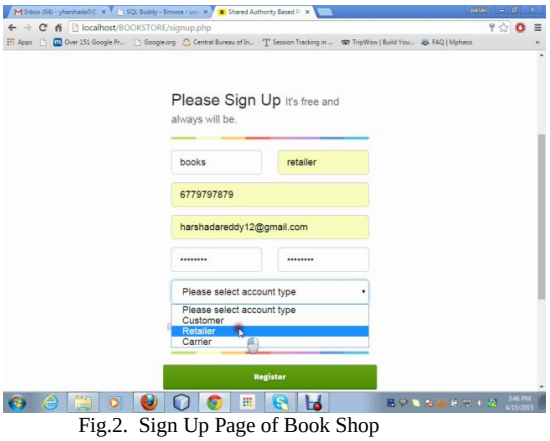


Fig.2. Sign Up Page of Book Shop

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

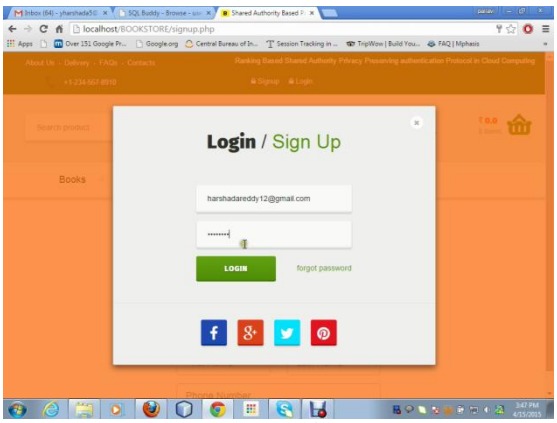


Fig.3. Login Page Of Bookshop

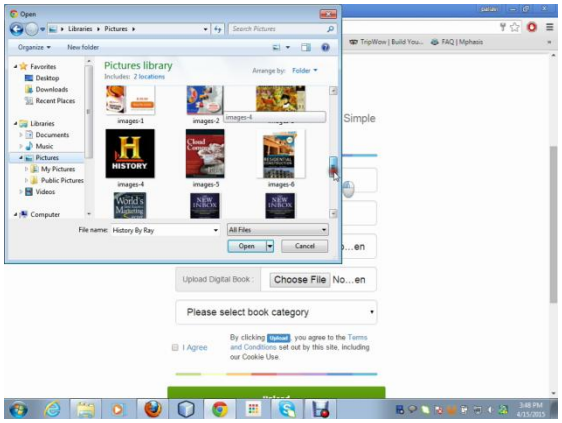


Fig.4. Book Retailer(Owner) Upload the books

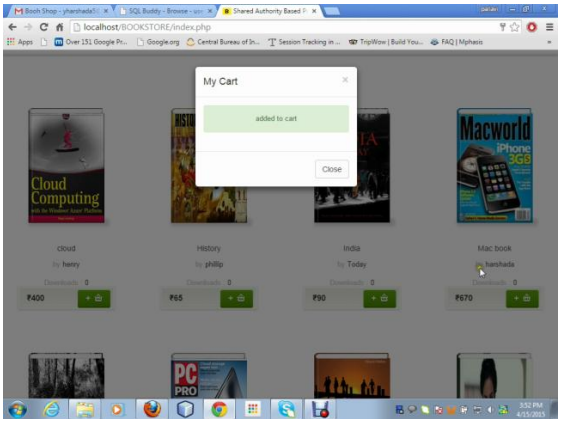


Fig.5. User Request Books by adding the books to his cart

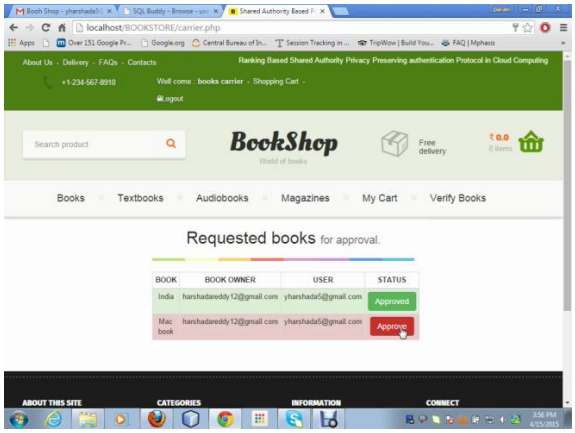


Fig.6. TPA(Carrier) Approves the request

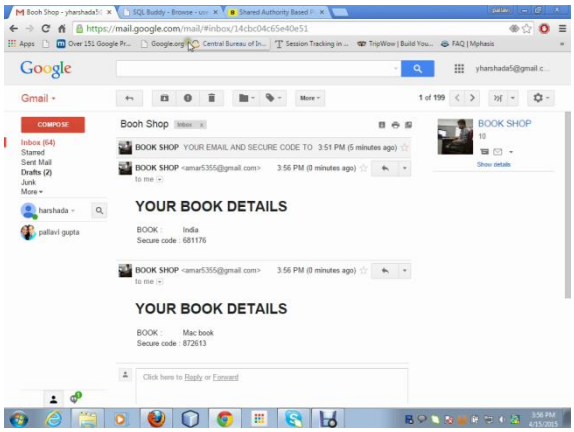


Fig.7. TPA(Carrier) sends the Secret Key to Authorized User's Mail-Id

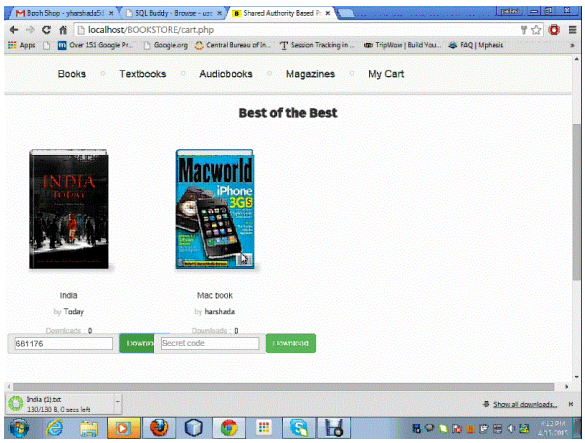


Fig.8.User Must enter the key to download the book or file

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

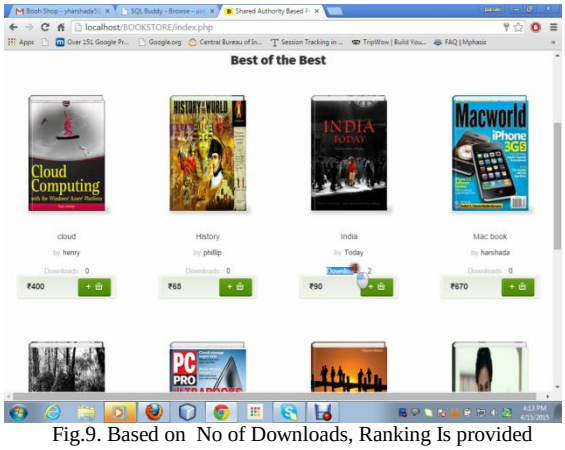


Fig.9. Based on No of Downloads, Ranking Is provided

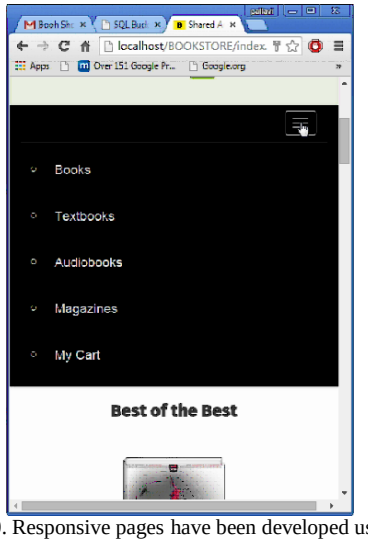


Fig10. Responsive pages have been developed using Bootstrap

VI. CONCLUSION

In this work, a new privacy challenge has been identified during accessing of data in the cloud computing to achieve privacy-preserving access authority sharing. Authentication is implanted to guarantee data confidentiality and data integrity. Since the wrapped values are exchanged during transmission ,data anonymity is achieved. User privacy is increased by anonymous access requests to inform the cloud server in private about the users' access needs. Forward security is accomplished by the session identifiers to stop the session correlation. It shows that the proposed scheme is perhaps applied for increasing privacy preservation in cloud applications. Ranking is provided at the Admin level to specify number of times the particular file has been requested Particular user can view on his/her dashboard about the number of times he accessed particular file and can get the suggestions if any extensions or particular file is uploaded onto cloud server Web Application is developed based mostly of Bootstrap which is most popular Html, CSS and JavaScript framework for developing responsive mobile-first websites Hence the screen resolution is adaptable to mobile, tablet, Pc

REFERENCES

1. Mishra, R. Jain, and A. Durresi, "Cloud Computing: Networking and Communication Challenges," *IEEE Communications Magazine*, vol. 50, pp, 24-25, 2012.
2. K. Hwang and D. Li, "Trusted Cloud Computing with Secure Resources and Data Coloring," *IEEE* Internet Computing, vol. 14, pp. 14-22, 2010.
3. J. Chen, Y. Wang, and X. Wang, "On-Demand Security Architecture for Cloud Computing," Computer, vol. 45, pp. 73-78, 2012.
4. Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multi-cloud Storage," IEEE Transactions on Parallel and Distributed Systems, vol. 23, pp. 2231-2244, 2012.
5. C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing, vol. 5, pp. 220-232, 2012.
6. H. Zhuo, S. Zhong, and N. Yu, "A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability," IEEE Transactions on Knowledge and Data Engineering, vol. 23, pp. 1432-1437, 2011
7. Y. Tang, P. C. Lee, J. C. S. Lui, and R. Perlman, "Secure Overlay Cloud Storage with Access Control and Assured Deletion," IEEE Transactions on Dependable and Secure Computing, vol. 9, pp. 903-916, 2012.
8. S. Sundareswaran, A. C. Squicciarini, and D. Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud," IEEE Transactions on Dependable and Secure Computing, vol. 9, pp. 556-568, 2012.

BIOGRAPHY

K. Janardhan is a Associate professor in Computer Science and Engineering Department, Intell Engineering College, Anantapuramu ,Andhra Pradesh, India.

Yerragunta Harshada is a M-tech Student in Computer Science and Engineering Department, Intell Engineering College ,Andhra Pradesh, India. She received Bachelors of Technology (B-Tech) degree in 2012 from Karunya University, Coimbatore,