ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Secure Data Sharing and Preventing Key Recovery Attack in Cloud Environment

Nayan Asane, Prof. S.S.Vairagar

M.E. Student, Department of Computer Engineering, Siddhant College of Engg., Pune, Maharashtra, India

Professor, Department of Computer Engineering, Siddhant College of Engg., Pune, Maharashtra, India

ABSTRACT: Nowadays Data sharing, maintenance, its security are major challenges in global world. User in the data sharing system upload their file with the encryption using private key. This property is especially important to any large scale data sharing system, as any user leak the key information then it will become difficult for the data owner to maintain security of the information. In this system provide a concrete and efficient instantiate of scheme, prove its security and provide an implementation to show its practicality. There are lots of challenges for data owner to share their data on servers or cloud. There are different solutions to solve these problems. These techniques are very much critical to handle key shared by the data owner. This system will introduce how to reduce burden of data owner, authenticate those who have the access to the data. The advancement of cloud computing and a radical increment in data size are making the outsourcing of image storage what's more, handling an appealing business show. In spite of the fact that this outsourcing has many focal points,guaranteeing data classification in the cloud is one of the fundamental concerns. There are state-ofthe- art encryption plans for guaranteeing classification in the cloud. Be that as it may, such
plans don't permit cloud datacenters to perform operations over encrypted data. The attacks are extremely efficient, showing that it is reasonably easy for an attacker to recover the key in any of the two settings discussed. Finding out the unauthorized user and blocking their access also detecting malicious activities of authorized user and blocking them and recovering the by resignature concept. Data owner continuously monitor the activities of the user.Data Owner has all the rights to grant and revoke the access of the user.

KEYWORDS: Key, Encryption, Black Box, Gray Box, Recovery, Resignature.

I. INTRODUCTION

Cloud computing is a virtual host PC framework that empowers ventures to purchase, rent, offer, or disseminate programming and other advanced assets over the web as an on request benefit. It no longer relies on upon a server or a number of machines that physically exist, as it is a virtual framework.End clients get to cloud-based applications through a web program, thin customer or versatile application while the business programming furthermore, client's information are put away on servers at a remote area. The advantages of electronic cloud registering administrations are tremendous, which incorporate the simplicity of openness, diminished expenses furthermore, capital consumptions, expanded operational efficiencies, versatility,adaptability and prompt time to advertise. Despite the fact that the new worldview of cloud figuring gives awesome points of interest, there are then additionally worries about security and privacy particularly for electronic cloud administrations. As delicate information might be put away in the cloud for sharing reason or helpful get to; and qualified clients may likewise get to the cloud framework for different applications and administrations, client verification has turned into a basic segment for any cloud framework. A client is required to login before utilizing the cloud benefits or getting to the touchy information put away in the cloud. There are two issues for the conventional record/password based framework. To begin with, the customary record/secret word based confirmation is not privacy-saving. Be that as it may, it is well recognized that privacy is a fundamental component that must be considered in cloud figuring frameworksSecond, it is basic to share a PC among various individuals. It possibly simple for programmers to introduce some spyware to take in the login secret key from the web-program. An

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

as of late proposed get to control show called attribute-based get to control is a decent candidate to handle the primary issue. It not just gives mysterious confirmation additionally characterizes get to control approaches based on various attributes of the requester, environment, or the information protest. There are two broad classed of classifiers that use a key:first one is known as randomized classifiers, this is entirely public. KIDS belongs to a second group, that we call keyed classifiers.

.

II. RELATED WORK

Attribute-based encryption (ABE) is the foundation of attribute-based cryptosystem. ABE empowers fine-grained get to control over encoded information utilizing get to arrangements and partners attributes with private keys and ciphertexts. Inside this unique circumstance, ciphertext-arrangement ABE (CP-ABE) [6] permits a versatile method for information encryption with the end goal that the encryptor characterizes the get to strategy that the decryptor (and his/her attributes set) needs to fulfill to decrypt the ciphertext. Subsequently, unique clients are permitted to decrypt diverse bits of information as for the pre-characterized strategy. This can dispose of the trust on the capacity server to forestall unapproved information get to. Intervened cryptography was initially presented in [8] as a strategy to permit quick disavowal of open keys. The fundamental thought of interceded cryptography is to utilize an on-line go between for each exchange. This on-line go between is alluded to a SEM (SEcurity Go between) since it gives a control of security abilities. In the event that the SEM does not collaborate then no exchanges with the general population
key are conceivable any more. As of late, an attribute-based form of SEM was proposed.The idea of SEM cryptography was further altered as security intervened certificateless (SMC) cryptography . In a SMC framework, a client has a mystery key, open key and a personality. In the marking or decryption calculation, it requires the mystery key and the SEM together. In the signature check or encryption calculation, it requires the client open key and the relating character. Since the SEM is controlled by a power which is utilized to handle client repudiation, the power declines to give any participation for any disavowed client. In this way denied clients can't produce signature or decrypt ciphertext. Take note of that SMC is not quite the same as our idea. The principle reason for SMC is to tackle the renouncement issue. Accordingly the SME is controlled by the power.Boyang Wang, Student Member, IEEE, Baochun Li, Senior Member, IEEE, and Hui Li,Member, IEEE has proposed a paper on Public Auditing for Shared Data with Efficient User Revocation in the Cloud. Where it gives information of Shared data with efficient user revocation in the cloud.The cloud can improve the efficiency of user revocation. But it has disadvantage as Network Connections Dependency. Cost is more Cheng-Kang Chu, Sherman S.M. Chow, Wen- Guey Tzeng, Jianying Zhou, and Robert H Deng proposed a paper on Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage.. More flexible than hierarchical key assignment which can only save spaces if all key-holders share a similar set of privileges.Allows efficient and flexible key delegation. Network Connections Dependency. Here also has disadvantage that Cost is more and algorithm used are Key Aggreegate Encryption,Decryption. Seung-Hyun Seo, Member, IEEE, Mohamed Nabeel, Member, IEEE, Xiaoyu Ding, Student Member, IEEE, and Elisa Bertino, Fellow, IEEE proposed a paper on An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds. Securely share sensitive data in public clouds.Improve efficiency. here also has disadvantage that Network Connections Dependency and Cost is more algorithm used are public key encryption algorithms. Mohamed Nabeel and Elisa Bertino, Fellow, IEEE proposed a paper on Privacy Preserving Delegated Access Control in Public Clouds. Decomposition ACPs used to privacy preserving fine-grained delegated access control to data in public clouds.The Owner has to handle a minimum number of attribute conditions while hiding the content from the cloud here also has disadvantage thatNetwork Connections Dependency. Cost is more algorithm used are optimization algorithms, gen graph, random cover, policy decomposition.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

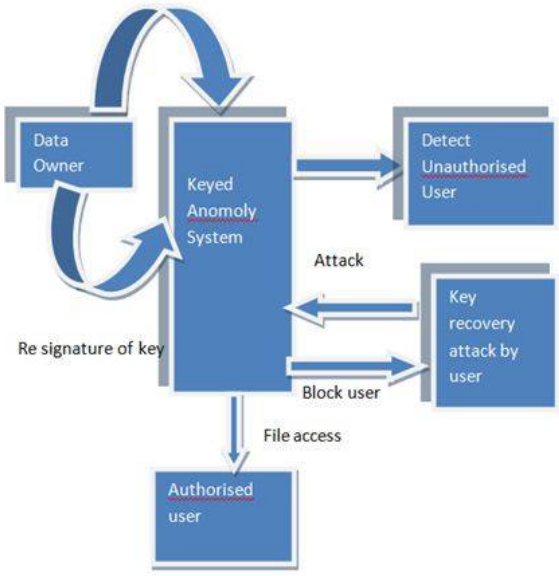

Fig: System Architecture

III. PROPOSED SYSTEM

In this attack we expect the attacker has entry to the abnormality score appointed to a picked payload. Besides,it is sensible to expect that some ordinary payloads are known as well. (Consider, for instance, the instance of an IDS examining HTTP asks for sent to a publicly available web server, where countless payloads will be known by the attacker.) Let p be one such ordinary payload. A clear system to distinguish what components of p have a place with the key D comprises of nourishing KIDS with the main byte of p, at that point with the initial two bytes of p, et cetera. At the point when the nextto the last byte happens to be a delimiter, KIDS will identify a move where the left word is probably going to have been seen amid preparing, while the correct word is frequently obscure (since it is truncated).Now, the abnormality score will endure a slight decrement.By advantageously rehashing the method, all the delimiters exhibit in p can be recovered. Notwithstanding the specialized points of interest, the fundamental disadvantage of the nave technique talked about above is that the attacker will just have the capacity to recover those key components exhibit in the typical payloads accessible, which may well be only a portion of every one of them. In addition, the unpredictability of such an attack is straight in the quantity of payloads and their lengths. We next portray an alternate approach that gets all the key components all the more productively and without specifically depending on typical payloads.In a few regards, this data is less fine grained than the abnormality score, so it is sensible to anticipate that attacks working under this supposition will be marginally more intricate. The focal thought behind our attack is entirely straightforward. We will give KIDS a normal payload connected with a precisely developed tail. Such a tail contains an extensive number of inconspicuous words isolated by the applicant delimiter. On the off chance that the delimiter does not have a place to the key, the whole tail will be handled as only one word and the irregularity score will be generally like that of the first payload. If so, then the payload will be set apart as normal with high likelihood. On the other hand, if the delimiter belongs to the key, the tail will be divided into countless concealed words and moves. This will contrarily affect the peculiarity score, constantly bringing about an odd payload.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

IV. ALGORITHM

1.Key Recovery Black Box
In this payload will be normal with properly structured tail.The tail contain the large number of unseen words separated with delimeter.In Black Box recovery algorithm attacker tries to recover the w1(word 1) and w2(word 2).For this the attacker tries different combination till the length of payload.If w1 recover then the w2 can be easily recoverd.
Algorithm
Input:
Set of payload Q=qi
word w2 s.t. n(w2)=0
Parameter l>1
for each qi belongs Q do
Di ←a
for d=0 to 255 do
p←(qi——d——w2——d——...——d—— w2)
if anom(p)=true then
Di← Di U d
end if
end for
end for
return D=Di.

2.Key Recovery Gray Box
In this attack assume the attacker has access to the anomaly score assigned to a chosen payload. Furthermore,it is reasonable to assume that some normal payloads are known too.
Algorithm
Input:
w1,w2 such that n(w1)¿0,n(w2)=0
D1←a
D2←a
for d=0 to 255 do
p←(w1 —— d —— w2)
if s(p)=S(w1 —— d —— w2) then
D1← D1 U d
else D2←D2 U d
end if
end for
return D2
return D1

V. MATHEMATICAL MODEL

Our problem statement comes under the polynomial class according to denition of polynomial class; the problem is solved in P-time. So above two deterministic algorithms called P-class algorithms.
S=I,P,O
Let S be the proposed system which can be represented as
Input Data:I = fI0(u0,pw0,f0,k0),.....I1(un,pwn,fn,kn) g
u=User Name
p=Password
f=File
k=Key response

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

P= f P1, P2, P3, P4g
Where,
P1=Check Authorized user
P2=Encryption
P2=(f U P2)
P3=Decryption
P3=(f U P3)
P4=Attacker
P= ((I ∩ (f U P2)) U (I ∩ (f U P3)))
Output Data: O (Z) = O1, O2
O1=Block Attacker and prevent the key recovery attack
O1=$((u\,!\,\epsilon\ P1)\epsilon$ P4)
O2= Download File

VI. RESULT

This system can access the data files of any type and maximum size allowed is 5 MB. In this system user can upload the data that data may be text file,word file,image etc. This data is encrypted and stored on cloud.User can share the uploaded files to another registered user.The analysis is generated based on total number of files shared by the data owners and their access by users.To measure the accuracy of files downloaded by the user we have taken three analysis parameters.Precision,Recall,Fmeasure.Precision is calculated as total number of (accurate)times file is access divided by total number of files uploaded by the data owners.
precision=no/tcount;
Here no=Number of times file is downloaded correctly by user
tcount=Total number of file uploaded by the data owner
Recall is calculated as total number of files which are not retrieved or incorrectly accessed by the user divided by the total number of files uploaded by the data owner.
Recall=(tcount-no)/tcount
Fmeasure=2*precision* recall /(precision+recall)

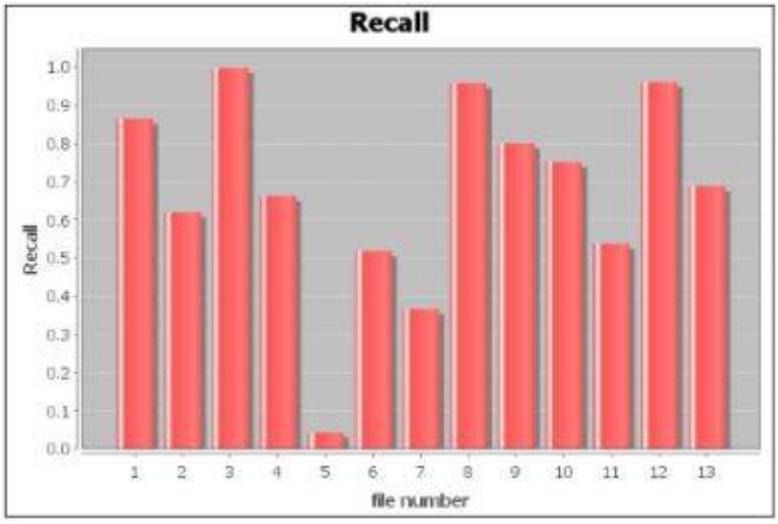

Fig:Recall Graph

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

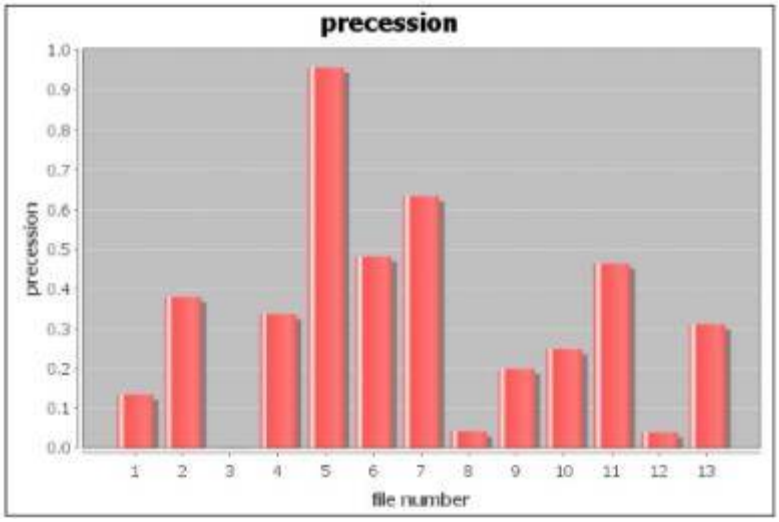

Fig:Precision Graph

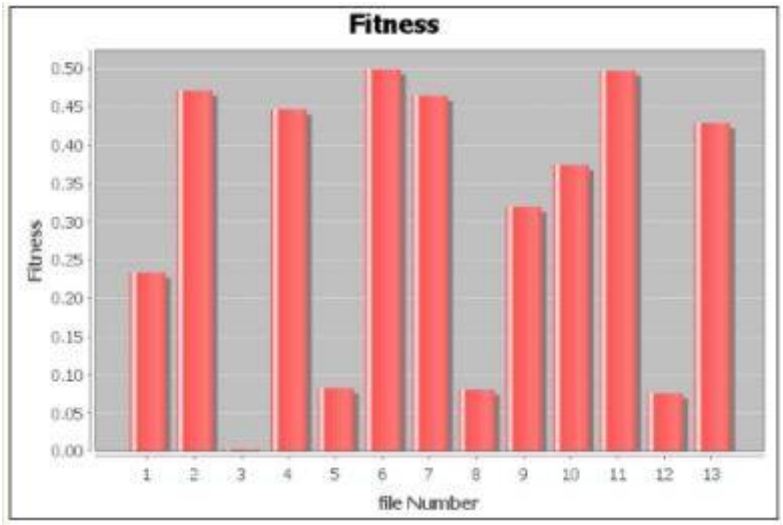

Fig:Fitness Graph

VII. CONCLUSION

In this system we have investigated the quality of KIDS against key-recovery attacks. In doing as such, we have adjusted to the peculiarity identification setting an ill-disposed model obtained from the related field of antagonistic learning.We have displayed key-recovery attacks as per two ill-disposed settings, contingent upon the input given by KIDS to testing inquiries. To the best of our insight, our work is the first to show key-recovery attacks on a keyed classifier. Shockingly, our attacks are amazingly proficient, demonstrating that it is sensibly simple for an attacker to recover the key in any of the two settings talked about. Such an absence of security may uncover that plans like KIDS were basically not intended to avert key-recovery attacks. In any case, we have contended that resistance against such attacks is basic to any classifier that endeavors to block avoidance by depending on a mystery bit of data. We have given discourse on this furthermore,different inquiries in the trust of animating further inquire about around there. The attacks here exhibited could be averted by presenting various specially appointed countermeasures to the framework, for example, constraining the greatest length of words and payloads, on the other hand including such amounts as

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

grouping components.We think, in any case, that these variations may in any case be defenseless to different attacks. In this manner, our proposal for future plans is to construct choices in light of powerful standards instead of specific fixes.

ACKNOWLEDGEMENT

I dedicate all my works to my esteemed guide, Prof. S.S. Vairagar, whose interest and guidance helped me to complete the work successfully. This experience will always steer me to do my work perfectly and professionally. I also extend my gratitude to (H.O.D.Computer Department)who has provided facilities to explore the subject with more enthusiasm. I express my immense pleasure and thankfulness to all the teachers and staff of the Department of Computer Engineering, for their co-operation and support. Last but not the least, I thank all others, and especially my friends who in one way or another helped me in the successful completion of this paper.

REFERENCES

[1] Rakpong Kaewpuang, Sivadon Chaisiri ” Cooperative Virtual Machine Management in Smart Grid Environment” IEEE Transactions On Services Computing,Vol.7,No.4,October-December 2014.

[2] Cheng-Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H Deng proposed a paper on ”Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage.” IEEE Transactions On Parallel and Distributed System Vol.25,No.2,February 2014.

[3] Seung-Hyun Seo, Member, IEEE, Mohamed Nabeel, Member, IEEE, Xiaoyu Ding, Student Member, IEEE, and Elisa Bertino, Fellow, IEEE” proposed a paper on ”An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds”. IEEE Transactions on Knowledge and Date Engineering, Vol. 26, No. 9, September 2014.

[4] Mohamed Nabeel and Elisa Bertino, Fellow, IEEE proposed a paper on ”Privacy Preserving Delegated Access Control in Public Clouds”. IEEE Transactions on Knowledge and Date Engineering, Vol. 26, No. 9, September 2014.

[5] Kaitai Liang, Man Ho Au, Member, IEEE, Joseph K. Liu, Willy Susilo, Senior Member, IEEE, Duncan S. Wong” proposed a paper on ”A DFA-Based Functional Proxy Re-Encryption Scheme for Secure Public Cloud Data Sharing”. IEEE Transactions On Information Forensics And Security, Vol. 9, No.10,October 2014.

[6] Kaiping Xue, Member, IEEE and Peilin Hong, Member, IEEE proposed a paper on ”A Dynamic Secure Group Sharing Framework in Public Cloud Computing”. IEEE Transactions On Cloud Computing, Vol.2,No.4,October-December 2014.

[7] Tao Jiang, Xiaofeng Chen, and Jianfeng Ma IEEE. proposed a paper on ”Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation”. IEEE Transactions On Services computing Vol.8,No.1,January/February 2015.

[8] Jiawei Yuan and Shucheng Yu, Member, IEEE proposed a paper on ”Public Integrity Auditing for Dynamic Data Sharing With Multiuser Modification”. IEEE Transactions On Information Forensics And Security,Vol.10,No.8,August 2015.

[9] Wei Zhang, Student Member, IEEE, Yaping Lin, Member, IEEE, Sheng Xiao, Member, IEEE, Jie Wu, Fellow, IEEE, and Siwang Zhou” proposed a paper on ”Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing”. JOURNAL Of Latex Class Files, Vol. 6, No. 1, January 2015.

[10] XinyiHuang,JosephK.Liu,ShaohuaTang,Member,IEEE, Yang Xiang, Senior Member, IEEE, Kaitai Liang, Li Xu, Member, IEEE, and Jianying Zhou” proposed a paper on ”Cost-Effective Authentic and Anonymous Data Sharing with Forward Security”. IEEE Transactions On Computers Vol.64.No.4,April 2015.

[11] Xinfeng Ye” proposed a paper on ” PrivacyPreservingandDelegatedAccessControlforCloud Applications”. ISSN 1007-0214 04/10 pp40-54 Volume 21, Number 1, February 2016

[12] Ovunc Kocabas, Tolga Soyata, Member, IEEE ” Emerging Security Mechanisms for Medical Cyber Physical Systems”. DOI 10.1109/TCBB.2016.2520933.