ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Towards Achieving Data Security using FIE and Double Encryption

Rupa Thanuja Darla
Department, of CSE,
MVGR College of Engineering,
Vizianagaram, India.

Aruna Kumari B
Assistant Professor,
Department, of CSE,
MVGR College of Engineering,
Vizianagaram, India.

Abstract:
For Cloud Computing Offering real-time data security for petabytes of data is important. A recent survey on cloud security states That Highest priority in a cloud is the security of users data. This can only be able to achieve with an approach that is adoptable ,systematic, and well-structured. Therefore, this paper has developed a framework known as FIE and Double Encryption which has been customized for securing cloud users data. This paper explains the rationale, overview and components in the FIE to protect the data security.

Introduction:
Cloud Computing is a type of computing infrastructure that consists the collection of inter-connected computing servers, nodes and other hardware and software services and applications that are dynamically provisioned among competing users. Services are delivered over private networks or through the Internet or both. The cloud services are accessed over these networks based on their performance like availability, Quality of Service (QoS) and capability, requirements. The aim is to deliver fault-tolerant, secure, scalable, reliable, and sustainable services, infrastructures to the end-users and platforms. These systems have goals of providing virtually unlimited computing and storage and hiding the complexity of large-scale distributed computing from users. A new way of delivering services can be done by the cloud computing. There always remain Security, trust and privacy issues challenges for organizations which adopt Cloud Computing and big data.

Now a days there are several demands for the businesses to move their data in to the Cloud and centralize management for data centres, services and applications and they are designed to achieve cost savings and operational efficiencies and security. At the same time, policies andsystem design and deployment based on its current security practices should be ensure all data and services are security compliant with up-to-date patches. A Security program have to develop a risk-based approach that recognizes appropriate controls will ensure that all.The users can be protected, and that data can be confidential, have integrity and be available to the users all the time. The FIE and DE has been developed to ensure that all implementations and service deliveries can meet all the technical challenges in order to meet the requirements for Business Clouds.

Software as a service (SaaS) is particularly in demand with the rapid rise in cloud computing. The data centres are facing several challenges in increasing the data. Focus on the data security while experiencing a large increase of data, if users or clients accumulate hundreds of terabytes of data per day, weather they are from the external sources or from the internal sources such as attack of viruses or trojans . This is a research challenge for data security which is essential for the better management of the data centre to handle a rapid increase in the data. Apart from the data center security management for rapid growth in data, the software engineering process should be enough robust to withstand the attacks and unauthorized access to the user's data stored in the data centres.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Furtherly, the entire process can be done with the development of framework to tighten up the technical design and implementations, governance and policies associated with good practices to help organizations achieving good Cloud design, deployment, migration and services.

Literature Survey:

As a service applications, existing literature defined cloud application service security as threat, vulnerabilities and software protection of cloud operational service. Here, explained some selected literatures which are relevant to the cloud applications and security. They are different types of security frameworks, First, Zhang et al. [1] propose their Usage-Based Security Framework (UBSF) for the Collaborative Computing Systems. They explain their motivation, techniques and architecture, conditions for experiments. Usage decision of the USFB is based on the objects, subjects, obligations, authorization, and conditions. They explain how their model can do work in collaborative ways supported by their literature and hypotheses.

The usage-based authorization architecture uses policy decision point (PDP), sensors, directory service, and usage monitor (UM) to functions. Steps have been described to justify how the USFB can function effectively. Define cloud application service security as threats, vulnerabilities and protection of cloud operational services and software as a service applications. Liu et al. [2] has proposed an agent-oriented modelling framework for analysing the security requirements. However, it is as yet another modelling language than security requirements capturing the framework. [2] provides a detailed definition and description on various cloud security and privacy issues. However, there is no clear framework to follow from security requirements. Cebula and Young [5] further classify cloud applications security engineering and its implementation into two major groups:

systems & software development security (which include the security specifications in all processes to develop information systems) and software acquisition security (which includes the security specifications in all processes to buy, rent, or interchange software to use in an enterprise) However, there is no clear framework to be adopted to classify security requirements and then to feed towards implementation. Mather et al[3] which provides a detailed description and definition on various cloud privacy and security issues which were occur in the data centres and cloud storage. However, there is no clear framework to follow from security requirements. Ko et al [5] presents how to make trust and investigate the trust for Cloud computing and propose a Trust Cloud Framework focused on the accountability. They have three layers:

(1) System layer, which covers all the core hardware and platform; (2) Data layer, which contains the data for the work and (3) Workflow layer, which uses workflow to execute all the services and requests. This framework is considered as a conceptual framework which was focused on the recommendations and the best practice, since they do not have any computational demonstration, quantitative analyses, and case studies in their paper.

Pal et al. [6] presents their proposed Cloud security that has been developed on the architecture and steps of interactions between different services and models. They explain how each and every role in each major user, their agents and all the fifteen steps involved. They use UML diagram to justify their approach and use architecture to explain relationship between the user, proxy server, provider, user agent and provider agent. They present their two algorithms and their experimental results. Using “Trust Value Updation”, they validate their approach. and proposed the cloud security. All these examples have the security framework which is used for the cloud security.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

However, those proposals do not demonstrate their assistance for business clouds. In other words, when businesses adopt Cloud Computing solution, they should be able to provide architecture, approaches for their framework, validity of the framework and steps and experiments to support the robustness of the framework or the system.

FIE & DE Multilayered Security:

Firewall, Intrusion Detection System, and Encryption(FIE) & Double Encryption(DE) were used for achieving data security in cloud. To provide security to the users data which is highest priority for the data security in cloud. In this paper to provide the data security FIE uses four modules and were explained as follows and the double encryption concept were also used in this paper.the four modules used in his paper are Admin, Data Owner, Data User and IDS Manager.

Admin:

Here admin is the person who has only the features like activating the data owners and data users at the time of first time registration. Once if admin activates them we get an mail alert for the respective Owner or User an message like "He/ She is activated and we get an Secret code" which is used for login into the system along with their Id and Password Admin has the facility like de-activating the users at the time of continuous wrong attempt if the user try to do..(I.e if the user try to access illegally files for those he is not having permission for more than or equal to 3 times ,automatically account should be blocked and once account is blocked ,the user should get an acknowledgement like account blocked due to suspicious activity.)So if the admin want to again re-activate the account for login he has the facility to activate the blocked user accounts from his login side. The admin while doing activation or de-activating the users. He can specify the access rights for the cloud users like:

1) Partial rights : Only View or read the files, 2) Semi Rights : Can view and Download, 3)Complete Access: like read,update/modify and Download.

These rights are only for user but for data owner there is no rule to specify roles because he is the owner who has only facility like uploading and giving permission for users while downloading ,no other job is there for owner Finally in this project the admin has a facility to re-encrypt the files which is uploaded by admin.This indicates that admin can able to re-encrypt all the table data not only original data but also the details which represents that identity of data like :DATE ,TIME,UPLOADED By ,FILENAME and so on they should also be encrypted in that representation ,because the hackers should not find out the information about that file.That is known as re-encryption. Initially the admin can view the table in this way after he gets requests from the data owners

S.No	File Name	Upload Date and Time	Encrypted Status	File Downloaded Link	Request for Re-Encrypt
1	test.txt	12:05:06 07/08/2016	Yes	test.txt	Send
2	qwerty.txt	12:15:06 07/08/2016	Yes	qwerty.txt	Send

S.No	File Name	Upload Date and Time	Encrypted STtaus	File Downloaded Link	Re-Encrypted Status
1	!#!$!$.txt	@$@$@$$!	@$@$@$@$@	#!!#!#!#!(&(*&	Yes
2	!@#$$.txt	@$@$@$$!	@$@$@$@$@	#!!#!#!#!(&(*&	yes

Once the Admin selects the last field like RE-Encrypt then he can view the table in this way

Data Owner:

Here the data owner is a separate type of login account. Once the data owner is registered with his own user id and password along with some basic details. He will be activated by the admin, then he has a facility to login into his account with his Username and password along with the Key that was reached that was send to the owner mail id. Once the data owner is login into his account. He has following features like:

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Initially he has a facility like

i) He can upload any text or .doc files or even try for images into the cloud server

ii) Once he choose an file he must able to encrypt that file initially from his side and then try to upload that into the BOX. At this stage we use Convergent Encryption Technique(I.e It means at a time we must check encryption of data should be done as well as we must able to verify that duplication of keys should not be done like same key should not be assigned for more than one file .I.e Just like assigning hash function for each and every file and every key .The data owner can also view the list of files which are available in his list like total files what he uploaded into the application by doing encryption

S.No	File Name	Upload Date and Time	Encrypted STtaus	File Downloaded Link	Forward TO Admin
1	test.txt	12:05:06 07/08/2016	Yes	**test.txt**	**Send**

iii) He can also view the list of data users who are registered in his cloud application with their individual type of access also.

iv) He can also view the requests that was came from data users for downloading the files. This is represented as follows

S.No	File Name	Download Requested By	Users Access RIghts	Accept/Reject	Status
1	test.txt	Data User 1 Name	**Semi**	**Accept/Reject**	Yes
2	qwerty.txt	Data User 2 NAme	**Partial**	**Accept/Reject**	No

v) Here the owner if he think that user is having the access right for downloading that data and if he is okay for that,he willgive access key (I.eDecryption key) for downloading that file from the cloud in a plain text manner..If not the user cant able to download the file in plain manner.

vi) During this stage if the user (I.e Either Semi or Full Access Holder) try to access any file without having valid key with him the attempt will be treated as Hacking stage by the IDS Manager and he will give right or chance for three times then the very fourth attempt it will be treated as Blocked User and The Blocked user details will be displayed in last Module like IDS Manager Module.

vii) Here one thing we should remember while writing the logic like partial access user cant able to participate in the request of downloading a file..For him the option of request should be in disabled manner

Data User Module:

In this module, the user is a person who will initially register with his valid id and Password and if he was activated by the admin he will get an one time token to his mail id ,through which he can be able to participate in the login of his account. Once he login into his account, he will then see the list of files that are available in his list in this manner. Initially the user who is available should see all the files in this way only…I.e Only filename and Only Request for download can be viewed in plain text rest of all the things it should be encrypted

S.No	File Name	Upload Date and Time	Uploaded By	Encrypted File	Request for Download
1	test.txt	&*)_QE(Q)(E_)QE_)	_)@#*_)Q*$*()&@	@)@)$_@))@)	**Send**
2	qwerty.txt	#)_*#_)@*$_)*@$_)*	#_@*$_@*_$*@_*$	**()$)(&$)(@&)($**	**Send**

Here as the re-encryption concept is done the user can only see the file name block in plain text manner and rest of all the columns in an encrypted manner. And the last column represent that he can send the file request for decryption key from the owner..At this case the user who is having semi and Full access only can able to view the request for download option in a enable manner. And the user who is login into the account with partial access cant able to find that last column in a enable manner. He has just a facility to observe whatever the files are there in the cloud but no other means of communication

IDS Manager:

This is the last module where we has a facility like login into the account with a valid login id and password, which is pre-defined earlier by the application.there will be no registration for the IDS because it is treated as an in built module in the

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

application..He has the facility to view only one thing like:

1) List of all Normal users in a separate list view with their access rights
2) List of all Blocked or Attacked users in a separate table with that blocked details like type of file name what they attempted and time and date.
3) If any user who got again activated by admin then that user name should be automatically enter into the normal user list from the blocked user list.

Conclusion and Future work:

Although Cloud computing can be seen as a new phenomenon which is set to transfigure the way we use the Internet, there is much to be cautious about. There are many new technologies budding at a rapid rate, each with technological advancements and with the potential of making human's lives easier. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. Cloud computing is no exception. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future.

Proposed a solution based on arising needs to improve current Cloud security, offers the multilayered security layer for Cloud Computing services. Since each type of security has its strengths and weaknesses, the combination of different security solutions can enhance the strengths and reduce the weakness if only one single solution is deployed.

References:

[1]Marston Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud Computing-The Business perspective Decision Support Systems," vol. 51, no. 1, pp. 176-189, 2011.

[2]L.Liu and E.Yu, "Security and privacy requirements analysis with in a social setting," in IEEE, 2003, pp. 151-161.

[3]T. Mather, "Cloud Security and Privacy," in An Enterprise Perspective on Risks and Compliance. O'Reilly, USA, 2009.

[4]B. Aruna Kumari,J. VenkataRao V. Sreenivas, "Enhancing the Security for Information with Virtual Data Centers in Cloud," springer link, vol. 143, pp. 277-282, 2012.

[5]J. J. Cebula and L. R. Young, ""A taxonomy of operational cyber security," in Software Enginnering Institute , USA, 2010.

[6]S. Roschke, et aI., ss Bowman, ""Intrusion Detection in the Cloud,"" in IEEE, China, 2009.

[7](2010, March) Cloud security Alliance. [Online]. www.cloudsecurityalliance.org

[8]M.A.Morsy, "An Analysis of the Cloud Computing Security Problem," in APSEC, 2010.

[9]Zhang.X, "Toward a usage-based security framework for collaborative computing system," vol. 11, no. 1, 2008.

[10]V. Chang, "Cloud storage and bioinformatics in private cloud deployment," in Springer, New York, 2013, pp. 245-264.

[11]Kedarnadh, B.Aruna kumari Kasamsetty, "Proficient Privacy Keyword Search over Encrypted Cloud Data," IJSRCSAMS, vol. 3, no. 5, september 2014.