International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 06 | June -2018 www.irjet.net p-ISSN: 2395-0072

Design and Analytical Study of Id based pixel secured cloud enablement model

Ankur Pan Saikia[1], Dr.L.P.Saikia[2]

[1]M.Tech Scholar, Computer Science & Engineering, Assam down town University
[2] Professor, Computer Science & Engineering, Assam down town University

---

Abstract - *Cloud computing in the 21st century has developed from Workstation to dispersed workplace. The present pattern of Cloud Computing (CC) permits getting to business applications from anyplace just by interfacing with the Web. Proof demonstrates that, changing to Associations' yearly use and support are being decreased to a more prominent degree. In any case, there are a few difficulties that join different advantages of CC. This paper on the whole depicts Cloud Computing security challenges as a rule and portrays the alleviation rehearses that have been proposed to deal with the distinguished difficulties. Be that as it may, there are still a few difficulties with no relief techniques, which may remain as a hazard and a worry for some energetic CC lovers. Through this investigation the creator attempted to center around one such test `incompatibility' and moderation hones from CC specialists. There are approaches to give interoperability between different cloud Service suppliers (information/work stack/examples/application), however there is no appropriate standard or standard interface saw by cloud clients. Every one of them has composed a progression of ventures through which this is interconnectivity is built up. It can likewise be watched this independently planned advance by clients could have as they are not institutionalized. Subsequently, the recommended strategies should be sent with extraordinary alert to avoid security dangers (can be seen by the reactions from the review that propose the utilization of different encryption methods at different levels to forestall information spillage) For the on-premise confirmation (IDM's) being good with cloud security, the conclusions can be that there are no appropriate consistent combination systems existent and the vast majority of the cloud clients need to rely upon sellers. What's more, there are some arrangement of on-start confirmation methodologies should be recognized which can be coordinated with cloud specialist organizations that are specified.*

Key Words: *Cloud Computing, External Cloud, Data Integrity, Security Threats, Cloud Computing, Identity Based, Cued Click Point, Cipher Text*

1. INTRODUCTION

Cloud computing is a method to convey programming, stockpiling and handling. It builds framework's capacity without changing the current foundation, or taking permit for the product. It enhances the current programming abilities and expands the Information Technology assets. Regardless of the considerable number of accomplishments in Cloud computing, Security is as yet a basic test in Cloud Computing worldview. These difficulties incorporate client's mystery information misfortune, spillage and uncovering of protection .In this paper we will propose a Cloud Enablement Model to keep information more secured without losing their genuine substance particularly for External Cloud Services which will give client side Encryption.

1.1 CLOUD COMPUTING SECURITY THREATS

Top seven security dangers to Cloud computing found by "Cloud Security Alliance" (CSA) in 2009 are:

i. Mishandle and Nefarious Use of Cloud Computing: Attackers can invade an open cloud, for instance, and figure out how to transfer malware to a large number of PCs and utilize the energy of the Cloud framework to assault different machines.

ii. Uncertain Application Programming Interfaces: As programming interfaces or APIs are what clients use to collaborate with Cloud benefits, those must have to a great degree secure validation, get to control, encryption and movement observing components - particularly when outsiders begin to expand on them.

iii. Malicious Insiders: The vindictive insider danger is one that increases in significance the same numbers of suppliers still don't uncover how they employ individuals, how they give them access to resources or how they screen them.

iv. Shared Technology Vulnerabilities: Unfortunately, the parts on which this foundation is based were not intended for that.

v. Data Loss/Leakage: Be it by cancellation without reinforcement, by loss of the encoding key or by unapproved get to, information is dependably in threat of being lost or stolen.

vi. Record, Service and Traffic Hijacking: Account administration and activity commandeering is another issue that Cloud clients should know about. These dangers go from man-in-the-center assaults, to phishing and spam battles, to disavowal of administration assaults.

vii. Obscure Risk Profile: Security ought to be dependably in the upper bit of the need list. Code refreshes, security hones, defenselessness profiles, interruption endeavors – everything that ought to dependably be remembered.

1.2 RECOMMENDED CURES BY THE CSA

Recommended cures by the CSA to diminish these dangers are**:**

i. Stricter starting enlistment and approval forms.

ii. Guarantee solid verification and access controls are actualized working together with scrambled transmission.

iii. Transparency into general data security and administration hones, and in addition consistence detailing.

iv. Advance solid verification and access control for authoritative access and tasks.

v. Scramble and secure respectability of information in travel.

vi. Use solid two-factor confirmation strategies where conceivable.

vii. Exposure of appropriate logs and information.

The Objectives of this paper is to enhance information classification in Cloud storage conditions while upgrading dynamic sharing between clients. For sure, the proposed security instruments ought to guarantee both heartiness and effectiveness, in particular the help of adaptable access control, proficient client denial and exhibitions.

Tending to the issue of provable information ownership in Cloud storage conditions for information trustworthiness check bolster, following three significant viewpoints:
Security level, open questionable status, and execution, and thinking about the constrained stockpiling and preparing limits of client gadgets.

Actualizing the proposed systems utilizing models and broadly conveyed conspires, and approving their practicality and effect on genuine equipment.

2. EXISTING SOLUTION FOR SECURITY THREATS

Notwithstanding CSA, S.Hanna et al. In 2009 recognize Other Security Dangers:

i. Failures in Suppliers Security

ii. Attacks by other client

iii. Availability and dependability issues

iv. Legal and Administrative issues

v. Perimeter security demonstrate broken

vi. Integrating Supplier and Client Security Frameworks

J. Wei, et al. In 2009 proposed "Mirage Image Management System".
The general engineering of Mirage Image Management System that it comprises of 4 noteworthy parts:

i. Access Control: This system directs the sharing of VM pictures. Each picture in the store has an exceptional proprietor, who can impart pictures to trusted gatherings by giving access authorizations.

ii. Image Change by Running Channels: Channels expel undesirable data from pictures at distributing and recovery time. Channels at distribute time can expel or conceal touchy data from the distributer's unique picture. Channels at recovery time might be indicated by the distributer or the retriever.

iii. Provenance Following: This instrument tracks the deduction history of a picture.

iv. Image upkeep: Archive support administrations, for example, intermittent infection filtering, that distinguish and fix vulnerabilities found after pictures are distributed.

Confinements: Enormous execution overheads, both in space and time. Channels can't be 100% exact and thus the framework does not wipe out hazard altogether.

Miranda.M and S. Pearson.in 2010 proposed "Client Based Privacy Manager"

The general engineering of the security director have fundamental highlights of the protection chief are:

i. Obfuscation: This component can naturally muddle a few or the majority of the fields in an information structure before it is sent off to the cloud for preparing, and interpret the yield from the cloud again into de-jumbled shape.

ii. Preference Setting: This is a technique for enabling clients to set their inclinations about the treatment of individual information that is put away in an un-muddled shape inside the cloud. This element permits the client more noteworthy control over the utilization of his information.

iii. Data Access: The Protection Supervisor contains a module that enables clients to get to individual data in the cloud, keeping in mind the end goal to perceive what is being held about them, and to check its exactness. This is an inspecting instrument which will recognize protection infringement once they have happened.

iv. Feedback: The Input module oversees and shows criticism to the client with respect to use of his own data, including warning of information utilization in the cloud.

v. Personae: This element enables the client to pick between different personae while associating with cloud administrations.

Confinements: the specialist organization does not give full participation; the highlights of the Protection Administrator other than obscurity won't be powerful, since they require the legit collaboration of the specialist organization.

Like shrewd in later years ,Flavio.L et al. in 2010 proposed "Transparent Cloud Protection System"

Weichao.W, et al. In 2011 proposed "Secure and Efficient Access to Outsourced Data" approach .But because of precision issues those model couldn't be adequate for longer time.

As the awareness of the cloud privacy issues is going to increase, but still small work has been done in this area. Recently, Pearson et al. has proposed accountability mechanisms to address privacy concerns of end users [2015] and then develop a simple solution, a privacy manager, relying on obfuscation techniques [2016]

The Advantages of their User-oriented Ranking Model:

i. Privacy preservation is high at user end.

The Disadvantages of their User-oriented Ranking Model:

i. Processing cost (end-user and overall) is high.
ii. Communication cost (end-user and overall) is high.
iii. Privacy preservation at service provider side is low.
iv. Additional requirements required at user end and having high processing capability.

The Advantages of Pearson's Service-provider-oriented Ranking Model:

i. Processing cost at user end is medium.
ii. Communication cost (user end and overall) is medium.
iii. Low processing capability at user end.
iv. Privacy preservation at service provider side is high.

The Disadvantages of their Service-provider-oriented Ranking Model:

i. Overall processing cost is high.

The Advantages of Agent-based Ranking Model:

i. Processing and communication cost at user end and overall cost is low.
ii. Privacy preservation at user end and service provider side is medium

3. PROPOSED MODEL

To overcome all those challenges following Algorithm may be considered as a proper solution:

3.1 ID BASED PIXEL SECURED ALGORITHM

Let, if 'L' be the numbers of bits in the plain text, then 'i' range from 1 to L in the following definitions:
Pi= ith bit in the plain text string
Ci= ith bit in the cipher text string
Ki= ith bit in the cipher text string
P(Pi) =the probability that pi was sent
P(Pi |Ci)=the probability that Pi was sent given that Ci was observed

INPUT

Step1: INITIALIZE plain text string Pi.
Step2: Consider One Time Pad Token (OTP Token_ID)Oi; designed such that as long as the Pi.

ENCRYPTION:

Step6: Calculate One's Complement of Fi and Pi such that values will be Fi and Pi respectively.
Step7: Perform the following:

Stage1 Cipher: Ci1 = Pi XOR Oi ……..(5)

Step8: Key Generation:

Ki1 = S XOR Oi ……..(6)

Ki2 = Fi XOR S …….. (7)

Ki= Ki1 XOR Ki2 …… (8)

Hence, Final Cipher, Ci = Ci1 XOR Ki … …….. (9)

DECRYPTION:

Our system encoded everything in 64 bits length. Hence, our OTPs are 64 bits strings in length as long as 8 decimal digits. This possible brute force attacks succeed with probability close to (108-8).

Step9: If Successful login Exists System get the S and Oi.
Step10: Put Fi.
Calculate: Ki1 and Ki2
Find Ki
Now Calculate,

Ci1 = Ci XOR Ki.....(10)

Pi = Ci1 XOR Oi .....(11)

Result Pi

3.2 MATHEMATICAL PROOF AND DISTRIBUTION

A System can be called perfectly secret when
P(Pi)= P(Pi |Ci).(Alferd Menezes in 2007)

This Section will prove that Cipher of our System is perfectly secret.
Suppose the sender makes Cipher text Ci by performing XORing Pi and Ki and Key one bit at a time. We can assume the following proof for each individual equation (5),(6),(7),(8) and (9).

Ci = Pi XOR Ki……..(12)
Where Ci, Pi, Ki are as defined earlier.
P(Ki) = the probability that Ki was used to create Ci

The first conclusion can be written as
P(Ki=1) = P(Ki=0) = 1/2 for all i……..(13)

Equation (12) leads to the observation: knowing of any two { Pi , Ci , Ki } determines the third.

Likewise, given one of { Pi , Ci , Ki }, a second one can be written in terms of the third.
For example,

P(Ci=1 | Ki=0) = P(Pi=1);

In order to show that P(Pi | Ci) = P(Pi), we first need to show P(Ci) = P(Ci | Pi).

Using equation (12), we will do this explicitly by first deriving the distribution of P(Ci). Next, we will derive the distribution of P(Ci | Pi) given that the plain text bit is a 0 and then given that it is a 1.

3.2.1 Distribution of P(Ci)

P(Ci=1) = P(Ci=1 | Ki=1) P(Ki=1) + P(Ci=1 | Ki=0) P(Ki=0)…….(14)

by the definition of conditional probability
= P(Pi=0) P(Ki=1) + P(Pi=1) P(Ki=0)……..by equation (12)

= P(Pi=0) (1/2) + P(Pi=1) (1/2)……..by equation (13)

= (1/2) [P(Pi=0) + P(Pi=1)]…… ……..regrouping
= ½……since Pi can only be 1 or 0

P(Ci=0) = P(Ci=0 | Ki=1) P(Ki=1) + P(Ci=0 | Ki=0) P(Ki=0)……..(15)

by the definition of conditional probability

= P(Pi=1) P(Ki=1) + P(Pi=0) P(Ki=0)……..by equation (12)
= P(Pi=1) (1/2) + P(Pi=0) (1/2)…… ……..by equation (13)
= (1/2) [P(Pi=1) + P(Pi=0)]…… ……..regrouping
= ½……since Pi can only be 1 or 0

3.3 DISTRIBUTION OF P (CI| PI)

If Pi=0:

P(Ci=0 | Pi=0) = P(Ki=0)……..by equation (12)
= ½……..by equation (13)
P(Ci=1 | Pi=0) = P(Ki=1)……..by equation (12)
= ½……..by equation (13)

If Pi=1;

P(Ci=0 | Pi=1) = P(Ki=1)……..by equation (12)
= ½ ……..by equation (13)
P(Ci=1 | Pi=1) = P(Ki=0)……..by equation (12)
= ½ ……..by equation (13)

It is clear from the distributions derived above that
P(Ci | Pi) = P(Ci)

Now a system can be called perfectly secret when
P(Pi) = P(Pi | Ci)

Using the definition of conditional probability, the joint probability, P(Pi and Ci), the probability Pi and Ci are observed,

P(Pi and Ci) = P(Ci | Pi) P(Pi)……..(16)

and

P(Pi and Ci) = P(Pi | Ci) P(Ci)…… (17)

Combining (16) and (17)

P(Pi | Ci) P(Ci) = P(Ci | Pi) P(Pi)……..(18)

Since
P(Ci | Pi) = P(Ci)
as shown above, these two terms cancel, leaving
P(Pi | Ci) = P(Pi), which is the condition for perfect secrecy.

Hence it is proved that we can go with the System.

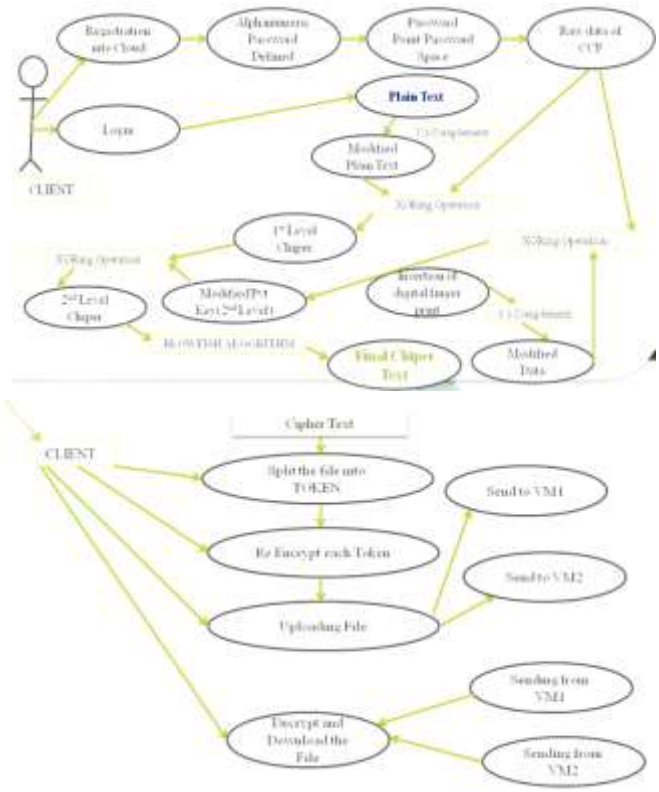

Fig 3.1: USE Case diagram of Proposed Model

4. CONCLUSION

This study and implementation collectively describes cloud computing security challenges in general and describes the mitigation practices that have been proposed to handle the identified challenges. The suggested methods need to be deployed with extreme caution to prevent security risks (can be observed by the responses from the survey that suggest the usage of multiple encryption techniques at various levels to prevent data leakage).The Proposed system can be adopted globally for different types of Cloud.

REFERENCES

[1] A. Hammami, N. Simoni, and R. Salman. Ubiquity and QoS for cloud se-curity. In 2012 41st International Conference on Parallel Processing Work-shops (ICPPW), pages 277 {278, September 2012}.

[2] Arlene G. Fink. Conducting Research Literature Reviews: From Paper to the Internet. Sage Publications, Inc, rst edition edition, April 1998. 19

[3] B. Grobauer, T. Walloschek, and E. St•ocker. Understanding cloud comput-ing vulnerabilities. IEEE Security and Privacy, pages 50{57, 2010)

[4] B. Hay, K. Nance, and M. Bishop. Storm clouds rising: Security challenges for IaaS cloud computing. In 2011 44th Hawaii International Conference on System Sciences (HICSS), pages 1{7. IEEE, January 2011}.

[5] B.R. Kandukuri, VR Paturi, and A. Rakshit. Cloud security issues. In Ser-vices Computing, 2009. SCC'09. IEEE International Conference on, pages 517{520, 2009)

[6] Bansidhar Joshi, A. Santhana Vijayan, and Bineet Kumar Joshi. Securing cloud computing environment against DDoS attacks. In Computer Com-munication and Informatics (ICCCI), 2012 International Conference on, pages 1{5, 2012.)

[7] Baruch Fischho , Paul Slovic, Sarah Lichtenstein, Stephen Read, and Bar-bara Combs. How safe is safe enough? a psychometric study of attitudes to-wards technological risks and bene ts. Policy sciences, 9(2):127

[8] BY Dustin oWens. Securing elasticity in the cloud. Communications of the ACM, 53(6), 2010.

[9] C. Cachin, I. Keidar, and A. Shraer. Trusting the cloud. ACM SIGACT News, 40(2):81{86, 2009.

[10] Cloud cube model: Selecting cloud formations for secure collaboration, April 2009. 25

[11] D.M. Eyers, R. Routray, R. Zhang, D. Willcocks, and P. Pietzuch. Towards a middleware for con guring large-scale storage infrastructures. In Proceed-ings of the 7th International Workshop on Middleware for Grids, Clouds and e-Science, page 3, 2009. 72

[12] Danny Harnik, Elliot K. Kolodner, Shahar Ronen, Julian Satran, Alexandra Shulman-Peleg, and Sivan Tal. Secure access mechanism for cloud storage. Scalable Computing: Practice and Experience, 12(3), 2011

[13] E.J. Goh, H. Shacham, N. Modadugu, and D. Boneh. SiRiUS: securing remote untrusted storage. In Proc. NDSS, volume 3, 2003. 71

[14] F. Farahmand. Risk perception and trust in cloud. Information Systems Control Journal, (4):8 pp., 2010.

[15] Fei Hu, Meikang Qiu, Jiayin Li, Travis Grant, Drew Taylor, Seth McCaleb, Lee Butler, and Richard Hamner. A review on cloud computing: Design challenges in architecture and security. Journal of Computing and Infor-mation Technology, 19(1):25{55, 2011}

[16] Jianyong Chen, Yang Wang, and Xiaomin Wang. On-demand security ar-chitecture for cloud computing. Computer, 45(7):73{78, 2012}

[17] Jin Li, Gansen Zhao, Xiaofeng Chen, Dongqing Xie, Chunming Rong, Wen-jun Li, Lianzhang Tang, and Yong Tang. Fine-grained data access control systems with user accountability in cloud computing. In Cloud Comput-ing Technology and Science (CloudCom), 2010 IEEE Second International Conference on, pages 89{96, 2010}

[18] M. Al Morsy, J. Grundy, and I. M•uller. An analysis of the cloud computing security problem. In the proc. of the 2010 Asia Paci c Cloud Workshop, Colocated with APSEC2010, Australia, 2010.

[19] M. Armbrust, A. Fox, R. Gri th, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, et al. Above the clouds: A berkeley view of cloud computing. EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28, 2009.

[20] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis. The role of trust management in distributed systems security. Secure Internet Programming, pages 185{210, 1999)

[21] M. Blaze, S. Kannan, I. Lee, O. Sokolsky, J.M. Smith, A.D. Keromytis, and W. Lee. Dynamic trust management. Computer, 42(2):44{52, 2015)

[22] Md Tanzim Khorshed, A. B. M. Ali, and Saleh A. Wasimi. A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Generation Computer Systems, 2012.

[23] Michael Armbrust, Armando Fox, Rean Gri th, Anthony D Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. A view of cloud computing. Communications of the ACM, 53:50{58, April 2010. ACM ID: 1721672}.