Journal of Computer Science and Applications.
ISSN 2231-1270 Volume 7, Number 1 (2015), pp. 39-44

http://www.irphouse.com

A Novel Frame Work For Cloud Computing Security By Using Abe

P.Srinivas Kumar and Dr S.Venkateswarlu

M.Tech, Department of CSE, Vaddeswaram, Gunture
Professor, Department of CSE, Vaddeswaram, Guntur

Abstract:

Cloud computing is a revolutionary computing ensample, which enables ductile, on demand, and low cost usage of computing collateral, but the data is redistribute to some cloud servers, and various seclusion deportment disembark from it. Various pragmatic based on the attribute-based engraving have been proposed to defended the cloud storage. However, most work limelight on the data contents privacy and the access control, while less attention is paid to the concession control and the coherence privacy. In this paper, we extant a semi anonymous appendage control contrivance AnonyContprivacyrol to address not only the dossier concealment, but also the user identity concealment in existing connection control contrivance. Anony Control apportions the central jurisdiction to limit the identity gush and thus enact semi anonymous. Besides, it also theorize the file access control to the privilege control, by which privileges of all operations on the cloud data can be managed in a fine-grained idiosyncrasy. Consequently, we present the AnonyControl-F, which fully prevents the coherence effusion and dispatch the full anonymity. Our security dissection shows that both Anony Control and Anony Control-F are impenetrable under the arbitrational bilinear DiffieHellman assumption.

Index Terms— Cloud computing, DepSky, Secret Sharing algorithm, LaGrange's basis polynomial, multi-clouds and ABE(Attribute based encryption).

I. INTRODUCTION

Cloud computing in its most righteous form can be called the next generation of computer technology. Cloud computing offers limitless complaisance, better reliability, aggrandize collaboration, portability, full-blown storage but how

immune is it after all? If the safety of dope cannot be assured when it is testimony in our privy server how can we be sure of its sanctuary over the cloud? Dope stored in the cloud can be arbitrate or lost. So, we have to come up with a way to guarded those files. We can encrypt them before storing them in the cloud, which sorts out the disclosure aspects. Despite, what if the data is lost due to some adversity befalling the cloud service provider? We could store it on more than one cloud appropriateness and encrypt it before we send it off. Each of them will have the same file. A lot of delve has been carried out for the same, and to a large extend has helped to invigorate cloud computing security.

II. NEED FOR CLOUD SECURITY

Hassan Takabi et al. [3], in their paper have sculpt a complete survey on the issues related to cloud computing security. Cloud computing is both propitious and pat. Despite of the attractive economic and technological eminence it has, businesses still think of the imaginable security threat before allot their data. Security is the most desperate aspect of everyday computing; this is very well applicatory to cloud computing itself. There are many security concerns in cloud computing security; a few can be listed as follow: A. Detrimental Attacker Hackers these days can breach the strongest security provender and hijack hushed data. Detrimental attacker can inject worms(virus) into the database, and destroy or corrupt the data that is of value to the company. B. Service Shanghai Service shanghai is nothing but gaining illegitimate services. It includes various techniques like barratry, phishing and software profiteering. This is prepense to be one of the top most threats. C. SQL Injection Attack A SQL code is interpolated into the model code. By doing this the intruder can gain entree to a database and to other unauthorized dossier. SQL cross contrive is a well-known tool for hackers, wherein on use of special complexions the hacker can mutate rows and columns. D. Confidentiality Confidentiality is preventing the unwarranted disclosure of information. Preserving confidentiality is one of the important issues faced by cloud systems, since the dossier is stored at a remote location that the Service Provider has full control to. Therefore, there has been some disposition of preserving the confidentiality of data stored in the cloud. The main disposition used to preserve memorandums confidentiality is memorandums encryption; however encryption brings about its inherent issues, some of which are discussed later.

III. IMPLEMENTATION :

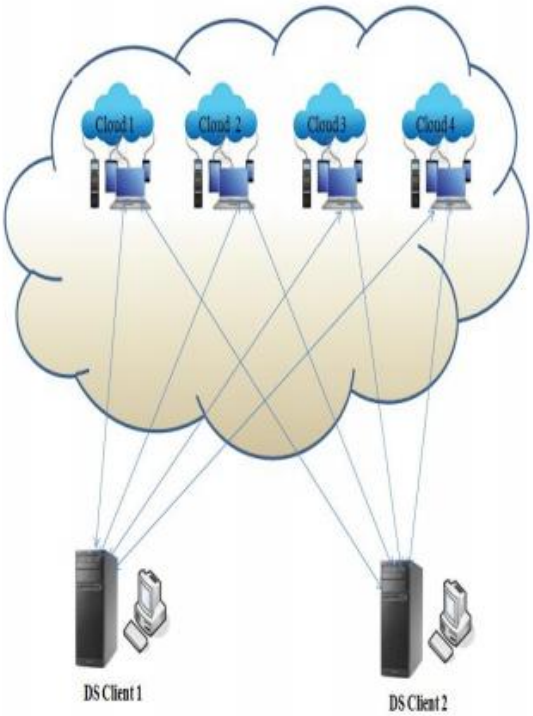
Data Integrity: It is not an accessible task to firmly maintain all cardinal data where it has the need in many appositeness for applicant in cloud computing. To perpetuate our data in cloud computing, it may not be fully trustworthy considering client doesn't have copy of all stored info. But any authors don't tell us data honorableness through its user. So we have to establish new proposed system for this using our data reading conventions algorithm to check the rectitude of data before and after the data insertion in cloud. Here the security of data before and after is checked by client with the help

of CSP using our "effective automatic data reading protocol from user as well as cloud level into the cloud" with truthfulness[8]. Data Intrusion:

The tenor of data intrusion detection systems in a cloud computing aura. We find out how intrusion detection is discharge on Software as a Service, Platform as a Service and underpinning as Service offerings, along with the available host, network and hyper visor-based intrusion detection options. Attacks on systems and data are a reality in the world we live in. Detecting and responding to those attacks has become the benchmark and is considered due diligence when it comes to security[8].

Service Availability Service whack is most important in the cloud computing security. hellion already mentions in its licensing agreement that it is adventitious that the service might be unavailable from time to time. The user‟s web service may adjourn for any reason at any time if any user‟s files break the cloud storage policy. In addition, if any damage occurs to any Amazon web service and the avail fails, in this case there will be no charge to the Amazon Company for this failure. Association pursuing to protect services from such failure need measures such as backups or use of multiple providers [8][11].

DepSky System Model Architecture: The DepSky system model comprehend three parts: readers, writers, and four cloud storage providers, where readers and writers are the client‟s nuisance. Bessanietal. explain the difference between readers and writers for cloud storage. Readers can fail arbitrarily (for example, they can fail by crashing, they can fail from time to time and then splash any behavior) whereas, writers only fail by crashing [8][14].



IV Attribute Based Encryption:

Global Setup → It takes as forewarning a pawn guideline and outputs the system criterion params.

Authority Setup → Each dominion generates his secret-public key pair and an access structure.

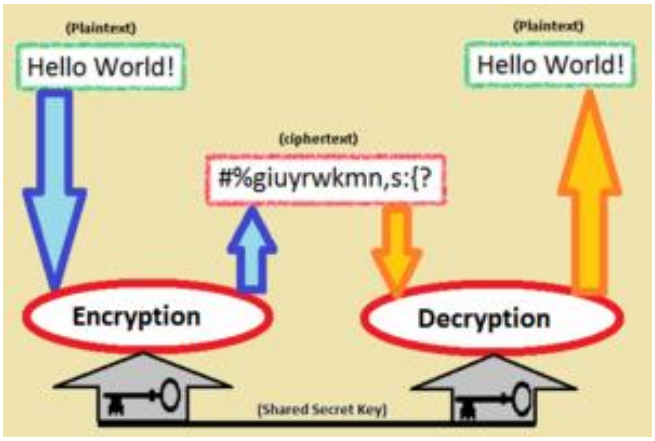
KeyGen → Each authority takes as input his secret key, a global identifier and a set of attributes and outputs the secret.

Encryption → It takes as input the system parameters params, a message and a set of attributes and outputs the ciphertext.

Decryption → It takes as input the global identifier, the secret keys and the ciphertext and outputs the message.

Cryptography

The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography artistry are fundamentally indestructibly.

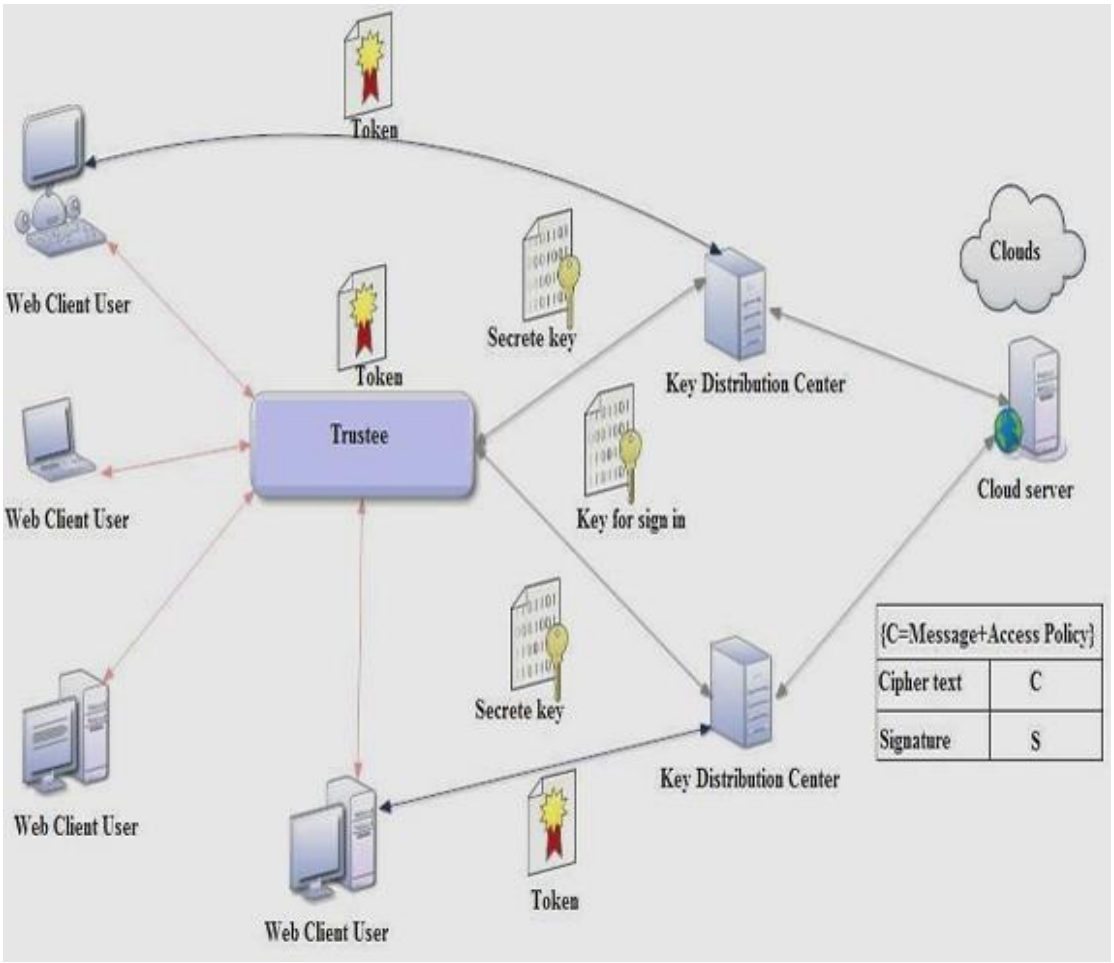


Encryption and Decryption

Encryption: In an encryption contrivance, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning gyrate it into an crabbed cipher text (ibid.). This is usually done with the use of an encryption key, which specialize how the message is to be cryptograph . Any antagonist that can see the cipher text, should not be able to predispose anything about the original message.

Decryption: An authorized party, despite, is able to decode the clip her text using a decryption algorithm, that customarily requires a disguised decryption key, that adversaries do not have access to. For technical inductions, an encryption scheme usually needs a key-generation algorithm, to haphazard green grocery keys.

ARCHITECTURE :



IV. FUTURE WORK:

The amalgamation of multi-clouds and secret sharing algorithm is encouraging, but as of yet it deals with many ambivalence. The current work warrant implementation of only text and relational database. embodiment of images and audio handling capability might increase the size and elaboration of system. The number of data instances depends on user‘s amalgamation with cloud service. The mostest admeasurement of data is again one of the antecedent that we have to conception with in practical implementation. An earnest fling has been made by Alfonso Cevallos Manzano in [20]. So for future work we will try an overcome all these limitations or find an alternative for the same.

VI. CONCLUSIONS:

It is adequately lucid that storing the data over multi clouds is effectual, and when this data is encrypted using Shamir‘s secret sharing algorithm it is ascertained to be more

secure and hardened to compromise. The worst case failing reasonableness of the system is low and the time elaboration of the system is abridged. The purpose of this work is to survey the potentiality of a system that would take the best of both multi-clouds and secret sharing algorithm, to dwelling the present security issues and present a possible solution.

REFERENCES:

[1] D. F. Ferraiolo and D. R. Kuhn, "Role-based access controls," in 15th National Computer Security Conference, 1992.

[2] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to rolebased access control," IEEE Computer, vol. 43, no. 6, pp. 79–81, 2010.

[3] M. Li, S.Yu, K. Ren, and W.Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in SecureComm, 2010, pp. 89– 106.

[4] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ACM ASIACCS, 2010, pp. 261–270.

[5] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in ACM CCS, 2010, pp. 735–737.

[6] F. Zhao, T. Nishide, and K. Sakurai, "Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems," in ISPEC, ser. Lecture Notes in Computer Science, vol. 6672. Springer, 2011, pp. 83–97.

[7] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed access control in clouds," in IEEE TrustCom, 2011.

[8] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures: Achieving attribute- privacy and collusion-resistance," IACR Cryptology ePrint Archive, 2008.

[9] "Attribute-based signatures," in CT-RSA, ser. Lecture Notes in Computer Science, vol. 6558. Springer, pp. 376–392, 2011.

[10] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in EUROCRYPT, ser. Lecture Notes in Computer Science, vol. 3494. Springer, pp. 457–473, 2005.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in ACM Conference on Computer and Communications Security, pp. 89–98, 2006.

[12] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext- policy attribute-based encryption," in IEEE Symposium on Security and Privacy. , pp. 321–334, 2007.

[13] X. Liang, Z. Cao, H. Lin and D. Xing, "Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption," in ACM ASIACCS, pp 343–352, 2009.