BEST: International Journal of Management Information
Technology and Engineering (BEST: IJMITE)
ISSN (P): 2348–0513, ISSN (E): 2454–471X,
Vol. 7, Issue 08, Aug 2017, 23–26
© BEST Journals

HYPER ATTRIBUTE BASED CRYPTOGRAPHIC METHOD TO SECURE CLOUD STORAGE

K. VASUMATHI[1] & R. KALAISELVI[2]

[1]Department of Computer Science, Prist University, Thanjavur, Tamilnadu, India

[2]Assistant Professor, Department of Computer Science, Prist University, Thanjavur, Tamilnadu, India

ABSTRACT

Many researchers have grabbed attention on cloud computing, due to its popularity and demand in the software market. This paper offers various strategies to protect or secure data at the database storage level in cloud based environments or virtualized environments. The sensitive data which is called as hyper-attribute must be carefully monitored to ensure that it is always protected from the attacker or hacker. To overcome these sorts of issues, we had proposed an approach called hyper-attribute based encryption mechanism in which the administrator of the database or user has the full rights to define hyper sensitive data. Hyper Attribute Based Encryption (HABE) algorithm is used to encrypt the hyper sensitive data depending on the user requirement. The obtained result shows the effectiveness and efficiency of our proposed approach.

KEYWORDS: Hyper-Attributes, Hyper-Attribute Based Encryption & ABE Algorithm

1. INTRODUCTION

A database which is accessible by the client from the cloud and delivered to ‘n’ number of users on demand via the internet from cloud database provider servers is referred to as Database-as-a-Service (DBaaS). Cloud database offers significant advantages over traditional approaches like very high accessibility, fast recovery from failures and better performance. Cloud databases drawbacks are security and privacy issues, data loss or inability to access data in the event of a natural disaster or by attacks. Nowadays, the cloud application deals with direct consumer and small business people rather than very large business application because the impact of security breaches for large scale business application will be considerably very high compared to small scale business application.

In this paper, we address the problem of security using Hyper Attribute Based Encryption (HABE) algorithm. It deals with encryption and decryption of data based on user-defined attributes. Cloud service provider has to provide full assurance of security in terms of confidentiality, privacy, etc. The hyper attribute based encryption is the best way to secure hyper sensitive data, when compared to other types of encryption techniques like user role based access control.

2. PRELIMINARIES

2.1. Secure Hyper-Sensitive Data

Both virtualization and cloud computing provides greater flexibility and efficiency by providing the ability to move servers and add or remove resources in order to maximize the use of your systems and reduce expense. The cloud database servers holding your sensitive data are can be provisioned and de-provisioned from cloud instances which in turn provided a target for attackers/hackers. Monitor activity on these dynamic database servers is very difficult without management involvement.

2.2. Wide Area Network (WAN)

Database activity monitoring solutions is not feasible in cloud environments where internet is essentially required. Network sniffing model is used to identify the malicious queries in cloud environments. In distributed computing the local sensor is able to analyze the network traffic of the cloud database. Cloud computing resources are likely to be connected to Wide Area Network (WAN) in order to get connected to internet. The time and resource spent while sending every transaction to a remote cloud server for analysis will slow down network performance and prevent timely interruption of malicious activity.

2.3. Data Access Privilege

The activity of monitoring privileged users in any database implementation is very difficult one. DBAs and system administrators will have admin rights to copy the sensitive data from the database with the provided privileges to them. You cannot conduct background checks on third parties as you do for your own staff, and it’s very difficult to protect against inside threats. One way to resolve this problem is activities of privileged third parties are monitored by your own staff only.

3. HYPER ATTRIBUTE BASED ENCRYPTION

Hyper attribute based encryption is one among the type of public key encryption in which the cipher text is generated based on the secret key of the user. Only the user predefined attributes can be encrypted by the secret key and the attributes for each and every user can change accordingly. Decryption of the cipher text is possible only if the secret key of the user matches perfectly and it got expired when the user generates a new secret key instead of the old one. In order to provide fine-grained access control of outsourced data attributes in cloud computing, we had implemented hyper attribute based encryption.

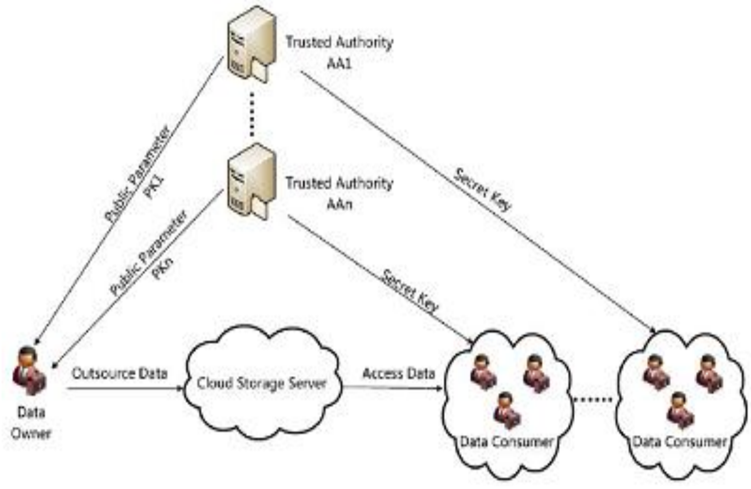

Figure 1: Architecture of Algorithm.

4. RESULTS AND DISCUSSIONS

The proxy re-encryption technique is used for decryption of the cipher-text and the size of cipher-text can vary in size according to the input data. The performance of the proposed algorithm hyper attribute based encryption is relatively very high. Due to process of encryption, when the number of user increases there will be slowness in the performance of the system. The security of the real time applications is very high in number when compared to other applications which are not using our proposed algorithm. We had conducted experiment with 10,000 users accessing the same application at varying time gaps with a concurrency of 10 users. In our stimulation, we had observed 95% accuracy while decrypting the cipher-text which was encrypted by our proposed algorithm.

5. CONCLUSIONS

In this paper, we had proposed hyper attribute based encryption to encrypt all the user pre-defined attributes and provide security to the outsourced data. The proposed algorithm will be suitable for application that needs high level security; it also consumes less access time and reduces cost consumption. The proposed algorithm is provides very high security from malicious insiders and threats during processing of the encrypted data. The security of the outsourced data is measured against the cryptographic proofs with 100% certainty. The results obtained show the efficiency and effectiveness of our proposed algorithm.

REFERENCES

1. Ruilin Liu, Hui Wang, Anna Monreale, Dino Pedreschi, Fosca Giannotti, and Wenge Guo. Audio: An integrity auditing framework of outlier-mining-as-a-service systems. In ECML/PKDD, 2012.
2. Bryan Parno, Mariana Raykova, and Vinod Vaikuntanathan. How to delegate and verify in public: verifiable computation from attribute based encryption. In TCC, 2012.
3. Al-Waily‘Theoretical, M. (2013). „Theoretical and Numerical Analysis Vibration Study of Isotropic Hyper Composite Plate Structural. International Journal of Mechanical and Production Engineering Research and Development, 3(5), 145–164.
4. Michael T. Goodrich, Charalampos Papamanthou, Duy Nguyen, Roberto Tamassia, Cristina Videira Lopes, Olga Ohrimenko and Nikos Triandopoulos Efficient Verification of Web-Content Searching through Authenticated Web Crawlers in PVLDB, volume 5, pages 920–931, 2012
5. Siavosh Benabbas, Rosario Gennaro, and Yevgeniy Vahlis. Verifiable delegation of computation over large datasets. In CRYPTO, 2011.
6. Vijay, P. M., & Prakash, A. M. A. R. (2014). Analysis of sloshing impact on overhead liquid storage structures. International Journal of Research in Engineering & Technology, 2(8).
7. Ran Canetti, Ben Riva, and Guy N. Rothblum. Verifiable computation with two or more clouds. In Workshop on Cryptography and Security in Clouds, 2011.
8. Fosca Giannotti, Laks V. S. Lakshmanan, Anna Monreale, Dino Pedreschi, and Wendy Hui Wang. Privacy-preserving data mining from outsourced databases. In Computers, Privacy and Data Protection, pages 411–426. 2011.
9. Fudalla, A. S., Magtoof, M. S., & Auda, M. A. Synthesis and Characterization Of Mono/Bis B-Lactams by using [2+ 2] Cycloaddition Reaction and Study Antihyperglycemic Activity.
10. Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos. Optimal verification of operations on dynamic sets. In CRYPTO, 2011.

11. Dario Fiore and Rosario Gennaro. Publicly verifiable delegation of large polynomials and matrix computations, with applications. In CCS, 2012.
12. Ran Canetti, Ben Riva, and Guy N. Rothblum. Practical delegation of computation using multiple servers. In CCS, 2011.
13. Srinath Setty, Andrew J. Blumberg, and Michael Walfish. Toward practical and unconditional verification of remote computations. In HotOS, 2011.