IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 36-40

A Theoretical model for Privacy-Preserving Multi-keyword over Encrypted Cloud Data

Vikash Kolhe , Prahlad Kolhe, Bhagyasri Milmile Prof Rasika Kachore, Pranali Manapure

Dept. of computer science Engineering AbhaGaikwad-patil College of Engg Nagpur,Maharashtra India, 2018-19

Dept. of computer science Engineering GH-RaisoniUniversity,saikhaeda MP India 2018-19
2018-19

Dept. of computer science Engineering AbhaGaikwad-patil College of Engg, Nagpur,Maharashtra India 2018-19

Abstract:*The major aim of this paper is to give a theoretical approach model for the multi-keyword over encrypted cloud data that will be used in many areas like software applications used in multi-pal sectors like medical, banking, scientific research and many other private as well as government sectors and many more. The Internet has to provide rice to many privacy issues. But due to the emerging new technologies, the privacy is at risk from the perpetrators, thus preserving the privacy and security is more important. In present scenarios, the cloud has provided many security models of the cloud computing that provides the users to outsource the data onto the cloud, which is stored via encrypting the data before storing the data on the cloud. theservice techniquelike K-NN (k-nearest neighbor) secure outsourcing protocol used. Within the rising technologies, artificial intelligence and cloud are hot zones and thus could be used in security and privacy purposes. My model depicts the use of artificial intelligence in a security model. The model contains the three-level sequential security filtration of encrypted data over the cloud and thus making the cyphertext much complex to crack via preceptors. Thus, it involves database and data management aspects, data pre-processing model and hashcode, artificial intelligence, inference considerations, interestingness metrics, complexity considerations, post-processing of discovered structures, visualization, qualitative matrix, and online updating. A theoretical model for privacy-preserving multi-keyword over encrypted cloud data*

Keywords : *Matrix coder, Privacy preserving data mining, multiple clouds, Multi-keyword over encrypted cloud data.*

I. Introduction

Cloud computing is an interdisciplinary subfield of computer science, is the computational process of managing data and its services through the cloud. which matches mostly with internet computing involving methods at the intersection of artificial intelligence, machine learning, statistics, and database systems. The cloud computing has a futureinformation technology architecture and could be evaluated more in future for enterprises, on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk [1]. the future technology in cloud computing could be more advanced in terms of privacy and security. Cloud Computing is a kind of computing technique where IT services are provided by massive low-cost computing units connected by IP networks [2]. thus, this could lead to data breaches and attacks via preceptors. Artificial intelligence is has grown much at present and will be developing more in the future. this increase in technology could be used in different purpose in cloud computing mainly in the security and privacy sectors of this field. The privacy is the key issue as data should be confidential sectors like banking and other government as well as private sectors need the security and privacy most to their data. various data models are used to keep the data confidential, algorithms like ciphertextCryptographic Algorithms and more complex model are used to filter the data to change is structure and meaning. This is a pay-as-you-goso there will no relation with the internal structure and longtime bond with the user.The issues related to cloud computing we focus on the issues of user's privacy and data securities [3].Researchers point out cloud security and user privacy issues. Some threats are enlisted over here.

* Sensitive private information can be disclosed while exchanging the data with cloud services.
* Once the data is given to cloud service user do not have control over the data and its security.
* Data is vulnerable to different network attacks such as DOS and DDOS [4]. [5]

security and privacy issues present a strong barrier for users to adapt to cloud computing systems and we have investigated several cloud computing system providers about their concerns on security and privacy issues[6]. thus applications and services glitter the workings of the cloud.

II. Related work

Highly Secured Log Management System over Cloud. Implies The log management system over the cloud in a highly secured manner and additionally for dealing the problems to access cloud-based storage with the increase in the privacy of the data several cryptographic algorithms used. Thus,overcoming the drawbacks of the cloud-based log management system [7]

many of the algorithms exist up till now for the data security and privacy includes symmetric and asymmetric key algorithms like DES, AES, and Triple DES. These are symmetric key algorithms in which a single key is used for encryption and decryption whereas RSA, Diffie-Hellman Key Exchange, and Homomorphic equations are asymmetric, in which two different keys are used for encryption and decryption. [8]

increase in privacy also alarms security and confidentiality of data. thus techniques of encryption and security algorithms like Extensible Authentication Protocol-CHAP and Rijndael encryption Algorithm [9]

data consistency quires data to be worked on a certain basis of hash adding impurity in terms of security is important. thus, Hash functions are versatile building blocks and are used to critically analyze existing hashing algorithms in the cloud computing environment.[10]

III. Proposed theory

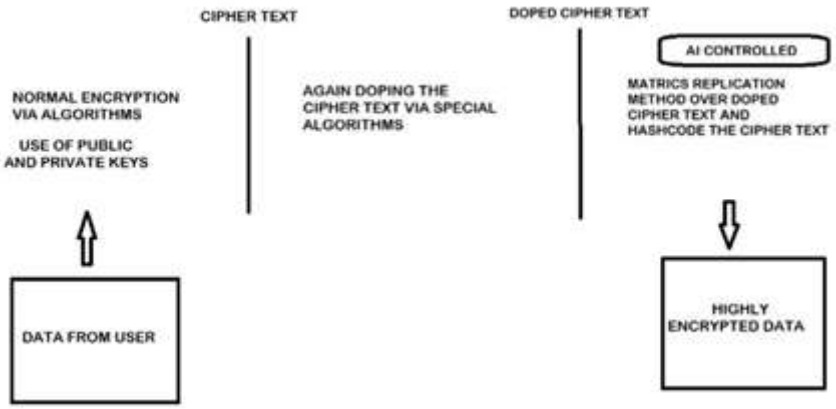
The cloud is an uplink of the storage where the data is stored the data need to be secured in all way every security paradigm consists of levels so that if the data is hacked he must have to crack each level to get the data

The cloud data is also one of the important measures to take care off. the data need to be secured within the cloud with emerging new technology the data on the cloud is at risk with the harmful ransomware and DDOS attacks[15]. New crackers and hackers are more hazardous with their technics to rob data plus its much more important to secure data before giving access to the third party.

This model consists of a sequential security plan. LikeMES [11]Which will depict with the two clouds .one with the data stored on the cloud and another with the key and AI or key computing on the cloud data. the future(21st century) world will be on AI [16]. Firstly, the data will be encrypted using the public and private key which will be reliable for the security of the cloud [13]. There would present a default key which will decode the data of anything goes wrong, the backup key stored in the cloud.

Thus, this model proposes three level security paradigms

1. The data is encrypted via existing algorithms like One Time Pad Cipher with Rail Fence and Simple Columnar Transposition Cipher[14], to ciphertext.
2. The ciphertext will be doped with the strings of data controlled by AI
3. Thus, the doped data will again be encrypted with matrices replication methods and hash function controlled by AI.



This doping will consist the encryption onto the same encrypted text again increasing privacy and security three times.

Working

The user across the globe will access the cloud over the process of authentication and securities issues thus the security protocols will give access to the user to access the cloud.

Now user can access the cloud as per his subscription and can use services provided on type of user. The stored data will go on a few security processes and then will be stored on the cloud with the public key.

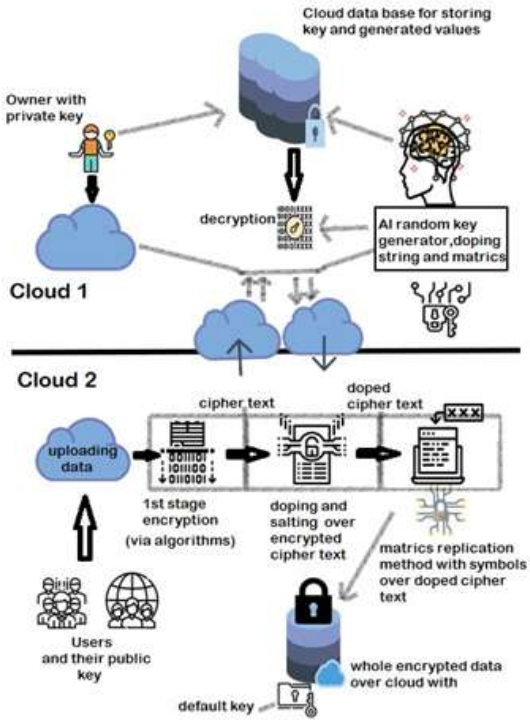
The public key of the user givesa balance security to the user with not providing full access to data to the third party. The owner of the cloud 1(special cloud of storing key values and generated random bits storage) will be having its key .thus while uploading the data on the cloud 2(data storing cloud) the cloud will mix the public and private key using algorithms such to make a 3rd key this key will help to encrypt the data over cloud using encryption algorithms like DES, AES, Triple DES, RSA, Diffie-Hellman Key Exchange thus encrypting the data will make it inconvenient to use.

Now this added ciphertext will continue to next step the code will be salted with impure or random data generated by artificial intelligence.Example: The salting of passwords using hash function[12]This code will be doped as per the algorithm. The code would get mixed with the data and make it again impure and thus doping key will be saved to the last bits of the data.

This doped data will again be encrypted in the next step of matrix replication method the data will be divided as per the matrix and will be computed as per the algorithm. the algorithm [17]will tend the data to covert the data to special symbols thus making it again incontinent.

This all process will be separated with their respected clouds the cloud 1 will store the random keys and key values generated by AI in its database and cloud 2 will store the highly encrypted data on to the cloud database.

The default key generated at the end of the key if any problem willoccur in the cloud due to malfunction. Thus, this key will have potential regenerate and decrypt the whole data as same as the data saved by the user.



Example

Suppose the user 1 want to upload data and verification as a user

Cloud 1 =>

The user data be

User 1: Bob is a good boy.

Public key: g8db6.

Data upload cloud 1.

Cloud 2=>

The administrator cloud owner

Private key: p9ghn4b6o

Cloud 1 =>

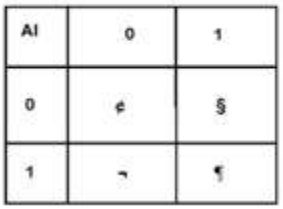
Let via an algorithm to join public and private key

Encryption key: gp89dgbh6n040b060o

stored in the default stack(database).

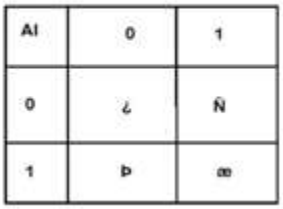
Step 1:
Now with the encryption algorithm, the data is encrypted
Encrypted data (ciphertext): h5j43i59tri59gj849jgd2g9k3hy&M%BS322l^G7n4Fn3DdN0f5vUf7BsdfTkYHg6
Step 2: let the data flow to the doping and salting algorithm
Doping bits: rjsf
Salting algorithm salts the encrypted data.AI encryption random doping
Ai Random: after 6 bits
Doping bits and Ai random stored in default stack(database).
Doped Cipher text:rjsf h5j43irjsf 59tri5rjsf 9gj849rjsf jgd2g9rjsf k3hy&Mrjsf %BS322rjsf l^G7n4rjsf Fn3DdNrjsf 0f5vUfrjsf 7BsdfTrjsf kYHg6rjsf.
Step 3: The AI generated random matrix with symbol
Examples of the matrix via AI

Generated 1:



AI	0	1
0	¢	§
1	¬	¶

Generated 2:



AI	0	1
0	¿	Ñ
1	Þ	œ

Encrypting the doped cipher text using Ai Random generated matrix
Matrix 1: Generated 1
Strings bit used: ¢ £ ¤ ¥ ¦ § ¨ « ¬ ® ¯°
Ai random matrix stored in default stack(database).
Matrixgenerated doped ciphertext:
3¢£§®¤ ¯¦¢¬¢¥3°¤«¢®§¢¥¨£ ¯¢®2¢°¢«£¦¢¬¢£¢®¢§¥¢®¢6¤¢¥ ¯¢£¢§¢2¢¬¢¥¢¦¢ ¯°¢§¢£4®C¥ ¯¢«8¢6¢«¢£¢«¦§¢¥«¢4¢°¢A ¯¤£4§¢¥¢¬¢¢L5«¢S ¯§¥¢¦5£¢¬¢« ¯¥°k0
This code will be securely stored in the database of cloud 2.
The key will get recorded into the default stack database and will be used to decrypt the data.
If the key inputted wrong by the user, the AI will generate random fake data and publish it to the user and remind the user to input the correct key.
Cloud 1 =>
Public key:gh9b6
Default stack keys: all keys stored.
Cloud 2 =>
Decrypting the data with the decrypting algorithm
With the help of Artificial intelligence.
Cloud 1 =>
Data decrypted
User 1: Bob is a good boy

IV. Conclusion

In this paper, we mainly focus on encryption privacy with the help of artificial intelligence. Over the cloud, the cloud has its properties and security to secure the data. This model is a multi-stage encryption system. It encrypts data within three levels, firstly normal encryption using cipher algorithm, the doped code generated by artificial intelligence is used to again encrypt the code. Then, again encrypting the code using an AI matrix

generator code. Thus, making the code much inconsistent to crack via preceptors and cybercrime data seekers. This provides additional security over cloud data,plus makes a balance between the public data via public key with accessing it to the third party. The default key also provides a backup plan for the users this will give CSP(Cloud Service Provider) a Business profit for more having users.

V. Future scope

In the future, this model could be more evaluated and upgraded. Overcoming its cons more multistage algorithms and tactics could be used. This theory could be used in Real-time practical usage with algorithms and Artificial intelligence. More algorithms could be used to refurbish the same.

References

[1]. A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep, 2009.

[2]. Ling Qian, Zhiguo Luo, Yujian Du, and Leitao Guo, "Cloud Computing: An Overview", Springer-Verlag Berlin Heidelberg CloudCom, LNCS 5931, pp. 626631, 2009

[3]. M. D. Ryan, "Cloud Computing Privacy Concerns On Our Doorstep", Communications of the ACM (CACM), vol. 54, no. 1, pp. 36–38, 2011.

[4]. D. Chen and H. Zhao, "Data Security And Privacy Protection Issues In Cloud Computing", in Proceedings of the International Conference on Computer Science and Electronics Engineering (ICCSEE), 2012, pp. 647– 651.

[5]. Pramila Kharat, Amar Buchade "Survey on Privacy Preserving and Data Security Techniques" Computer Engineering, Pune Institute of Computer Technology, Savitribai Phule Pune University,Volume 4 Issue 7, July 2015 www.ijsr.net.

[6]. Santosh Kumar and R.H.Goudar, "Cloud Computing –Research Issues, Challenges, Architecture, Platforms, and Applications: ASurvey" International Journal of Future Computer and Communication, Vol. 1, No. 4, December 2012

[7]. Rajebhosale Sagar S.1, Pawar Anil B.2, "Implementation of Highly Secured Log Management System over Cloud" SRES's College of Engineering, Kopargaon,Volume 4 Issue 3, March 2015

[8]. T.Ramaporkalai, "Security Algorithms in Cloud Computing"Madurai Sivakasi Nadars Pioneer Meenakshi Women's college, Poovanthi, Tamil Nadu. Volume 5 Issue 2, Mar-Apr 2017.International Journal of Computer Science Trends and Technology (IJCST)

[9]. Sanjoli Singla, Jasmeet Singh, "Cloud Data Security using Authentication and Encryption Technique"International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)Volume 2, Issue 7, July 2013

[10]. Meena Kumari, Dr. Rajender Nath, "One-Way Hash Algorithms in Cloud Computing Security- A Systematic Review"Department of Computer Science & Applications, Kurukshetra University, Kurukshetra, Haryana International Journal of Scientific & Engineering Research, Volume 7, Issue 12, December-2016

[11]. Chengqing Li∗, Xinxiao Li†, Shujun Li‡§ and Guanrong Chen, "Cryptanalysis of a Multistage Encryption System" Conference Paper · January 2005http://www.hooklee.com.

[12]. Pritesh N. Patel1, Jigisha K. Patel2 and Paresh V. Virparia3, "A Cryptography Application using Salt Hash Technique" Institute of Science and Technology for Advanced Studies and Research (ISTAR), 2&3Department of Computer Science, Sardar Patel University, Vallabh Vidyanagar, Gujarat, India.Volume 2, Issue 6, June 2013

[13]. Akashdeep Bhardwaja*, GVB Subrahmanyamb, Vinay Avasthic, Hanumat Sastryd , "Security Algorithms for Cloud Computing" International Conference on Computational Modeling and Security (CMS 2016)

[14]. Jawad Ahmad Dar1, Sandeep Sharma2, "Implementation of One Time Pad Cipher with Rail Fence and Simple Columnar Transposition Cipher, for Achieving Data security" Computer Science and Engineering, Kurukshetra University Kurukshetra, Haryana, India. Volume 3 Issue 11, November 2014 www.ijsr.net

[15]. Aaqib Iqbal Wani1, Janaki Raman V.2, N. Priya, "Identification and Avoidance of DDoS Attack for Secured Data Communications Cloud" B.Tech Computer Science and Engineering, and M. Tech Computer Science and Engineering, Assistant Professor, Bharath University. Volume 4 Issue 4, April 2015 www.ijsr.net

[16]. JIAYING LIU1, XIANGJIE KONG 1, (Senior Member, IEEE), FENG XIA 1, (Senior Member, IEEE), XIAOMEI BAI 2, LEI WANG1, QING QING1, AND IVAN LEE3, (Senior Member, IEEE), "Artificial Intelligence in the 21st Century" Received February 3, 2018, accepted March 9, 2018, date of publication March 26, 2018, date of current version July 12, 2018. VOLUME 6, 2018

[17]. Sayed Tathir Abbas1, Ravindera Kumar2, "Analytical Study of AES and Proposed Variant with Enhance Block Length and Key Length" Al-falah School of Engineering & Technology, Faridabad Haryana, India,Volume 2 Issue 8, August 2013 www.ijsr.net