Secure Data Sharing using Decoy Technology

Sonali Karale
Research Scholar
Department of Computer Science and Engineering, RGPV University,
Shri Balaji Institute and Technology, Betul, India
kcc.sonali15@gmail.com

Sachin Choudhari
Associate Professor
Department of Computer Science and Engineering, RGPV University,
Shri Balaji Institute and Technology, Betul, India
choudhari.sachin1986@gmail.com

Abstract--Cloud computing is a virtualized compute power and storage delivered via platform-agnostic infrastructures of abstracted hardware and software accessed over the Internet. Data sharing is an important functionality in cloud storage. Describe new public-key crypto systems which produce constant-size cipher texts such that efficient delegation of decryption rights for any set of cipher texts are possible. Show how to securely, efficiently, and flexibly share data with Decoy technology in secure cloud storage. Cipher texts are possible. The novelty is that one can aggregate any set of secret keys and make them as compact as a single key, but encompassing the force of all the keys being aggregated. So provide formal security analysis of our schemes in the standard model and describe other application of our schemes. In other words, the secret key holder can release a constant-size aggregate key for flexible choices of cipher text set in cloud storage, but the other encrypted files outside the set remain confidential. It Decoy technology provide security, Flexibility and confidentiality in data sharing.

Keywords- Encryption, Decryption, Cloud storage, Key aggregation, data sharing, key-aggregate encryption, REA.

I. INTRODUCTION

Cryptography is a science of secret writing. It is the art of protecting the information by transforming it into an unreadable format in which a message can be concealed from the casual reader and only the intended recipient will be able to convert it into original text .Cryptography renders the message unintelligible to outsider by various transformations. Data Cryptography is the scrambling of the content of data like text, image, audio and video to make it unreadable or unintelligible during transmission. Its main goal is to keep the data secure from unauthorized access. Information security has been provided by physical security and operating system security. As far as we know, neither of these methods sufficiently provides a secure support on storing and processing the sensitive data. Cryptographic support is another important way of database security. In database encryption mechanism could provide the following security. Encryption mechanism can prevent users from obtaining data in an unauthorized manner. Encryption mechanism can verify the authentic origin of a data item. Encryption mechanism also prevents from leaking information in a database when storage mediums, such as disks, CD-ROM, and tapes, are lost. This usually implies that the system has to sacrifice the performance to obtain the security. When data is stored in the form of cipher, we have to decrypt all the encrypted data before querying them. It is impractical because the cost of decryption over all the encrypted data is very expensive. For this purpose, we design the innovative encryption algorithm, called as “Reverse Encryption Algorithm (REA)”. Our new encryption algorithm (REA) is efficient and reliable. It has accomplished security requirements and is fast enough for most widely used software. Reverse Encryption Algorithm limits the added time cost for encryption and decryption. We also provide description of the proposed. The internet is a most popular one in recent years. It provides many services to users. One of the important service is cloud computing. Cloud computing is an on demand computing technology that delivers the resources as a service to the users over the internet. In cloud computing the main concern is to provide the security to end user to protect files or data from unauthorized user. Security is the main intention of any technology through which unauthorized intruder can't access your file or data in cloud. The important service provided by cloud computing is cloud storage. The local users can store their data in the remote cloud storage servers, from that the users can access the data from anywhere in the world. But storing data in a third party cloud system may affect the data confidentiality. For avoid this issue the data’s are encrypted before storing in to storage server. In the general encryption system the data owner encrypts the data by using cryptographic methodology and stores the encrypted data at the cloud storage server. It provides data confidentiality but it does not provide high security and dynamic data modification for that reason

used decoy technology.

II. LITERATURE SURVEY

Cryptography tries to prevent the eaves droppers from understanding the message. The message in its original form is called plaintext. The transmitter of a secure system will encrypt the plaintext in order to hide its meaning. This meaning will be revealed only after the correct recipient tries to access it. This reversible mathematical process produces an encrypted output called cipher-text. The algorithm used to encrypt the message is a cipher. The unauthenticated user can also try to access the information. The analysis is carried out to check if cipher's security is satisfactory from unauthorized access. Cloud is a market-oriented distributed computing system consisting of a collection of inters - connected and virtualized computers .In cloud computing, users can outsource their computation and storage to servers using Internet. The field of cryptography deals with the techniques for conveying information securely. The goal of cryptography is to allow the intended recipients of a message to receive the message securely. Cryptanalysis is the science of breaking ciphers, and cryptanalysts try to defeat the security of cryptographic systems. A cipher -text can be transmitted openly across a communications channel. Because of its encrypted nature, eavesdroppers who may have access to the cipher-text will ideally be unable to uncover the meaning of the message. Yong Cheng, Jiangchun Ren, Zhiying Wang, Songzhu Mei, Jie Zhou,In this paper presents a novel technique, attributes union, for promoting the CP-ABE algorithm's applications in cryptographic access control systems. Attributes unionizing means that I can reduce the number of components in cipher text and private secret keys. And I can reduce the storage and computational overhead to a constraint by unionizing attributes. The attributes union can be also used for modifying other existing CP-ABE algorithms. We benefit a lot from attributes union, since the number of attributes only has a mini effect on it. Only the intended recipient, who has the valid key, can decrypt the message to recover the plaintext and interpret. Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, In this paper authors explain about How to protect users' data privacy is a central question of cloud storage. With more mathematical tools, cryptographic schemes are getting more versatile and often involve multiple keys for a single application. In this article, I consider how to "compress" secret keys in public-key cryptosystems which support delegation of secret keys for different cipher text classes in cloud storage. No matter which one among the power set of classes, the delegate can always get an aggregate key of constant size. Our approach is more flexible than hierarchical key assignment which can only save spaces if all key-holders share a similar set of privileges.

III. PROPOSED WORK

In modern cryptography, a special type of public-key encryption is called key-aggregate cryptosystem. In KAC, users encrypt a message not only under a public-key, but also under an identifier of cipher text called class. key aggregate policies is use to make a decryption of key more powerful in the sense that it allows decryption of multiple cipher texts, without increasing its size. The key owner holds a master-secret called master-secret key, which can be used to extract secret keys for various classes. More importance, the extracted key have can be an aggregate key which is as compact as a secret key for a single class, but aggregates the power of many such keys, i.e., the decryption power for any subset of cipher text classes. The sizes of cipher text, public-key, and master- secret key and aggregate key in our KAC schemes are all of constant size. The public system parameter has size linear in the number of cipher text classes, but only a small part of it is needed each time and it can be fetched demand from large cloud storage. The data owner establishes the public system parameter via Setup and generates a public/master-secret key pair via Key Gen. Messages can be encrypted via Encrypt by anyone who also decides what cipher text class is associated with the plaintext message to be encrypted. The data owner can use the master-secret to generate an aggregate decryption key for a set of cipher text classes via Extract. The generated keys can be passed to delegates securely (via secure e-mails or secure devices) finally any user with an aggregate key can decrypt any cipher text provided that the cipher text class is contained in the aggregate key via Decrypt. By monitoring data access in the cloud and detect abnormal data access patterns User profiling is a well-known Technique that can be applied here to model how, when, and how much a user entrances their information in the Cloud.

IV. REVERSE ENCRYPTION ALGORITHM

We recommend the new encryption algorithm, "Reverse Encryption Algorithm (REA)", because of its simplicity and efficiency. Reverse Encryption Algorithm limits the added time cost for encryption and decryption. In this section we provide a comprehensive yet concise algorithm. Our new Reverse Encryption Algorithm is a symmetric stream cipher that can be effectively used for encryption of data. It takes a variable-length key. The REA algorithm decipherment and decipherment consists of the same operations, except the two operations: added the keys to the text in the decipherment and removed the keys from the text in the decipherment. Executed divide operation on the text by 4 in the decipherment and executed multiple operations on the text by 4 in the decipherment. We execute divide operation by 4 on the text to narrow the range domain of the ASCII code table at converting the text. The details and working of the proposed algorithm REA are given below

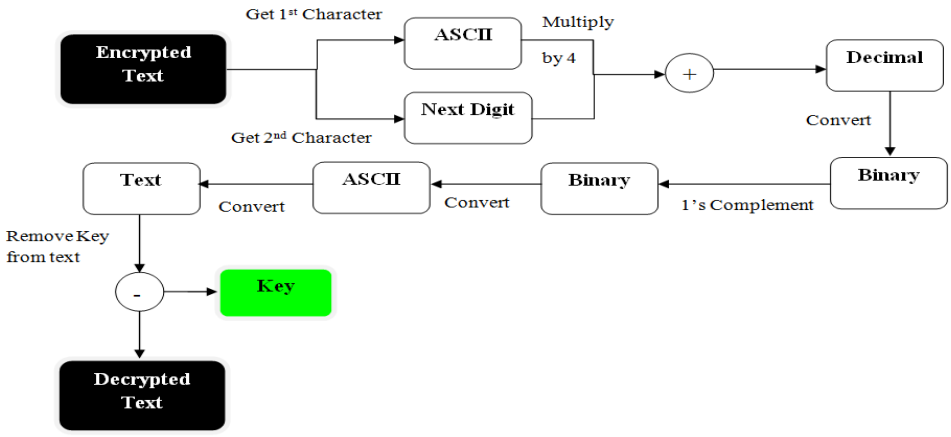

Figure1. Example of Reverse encryption algorithm

In this figure used Reverse Encryption algorithm. It used for encrypted text in ASCII value and then converted in decimal and binary. It used to convert data and used encrypt and Decrypt Key.

V. DECOY TECHNOLOGY

Several products are available to assist in creating a decoy system, each of which has its own interpretation of what a decoy system is and how it should be used. The overall process of installing decoy systems on a network infrastructure is relatively simple. The main components are commonly an extra interface on the firewall to control data communications and the deception system. In choosing a form of decoy system, an organization's defence posture and financial situation must be taken into consideration. The Man Trap decoy system also uses a hardware token to digitally sign and time stamp log files to guarantee non-repudiation in the event they are needed for prosecution or legal actions. Man Hunt and Man Trap products offer extensive customer support and carry an expensive price tag. Decoy technology is the technology which is providing the decoy information to the unauthorized user or the attacker. Decoy technologies for example honey pot, or the generating The useless data files on the demand of the system to do attack against the attacker. Using this technique the original information gets changed in unexpected format so that the ex-filtering of the document or information is becomes impossible. Decoy means the relative disinformation, Fake information about the respective data documents. This technology is mainly stores some of the decoy data files in the database of the customer as the part of his database. As the decoy files are in same database of the user so that the attacker is gets failed to verify between the actual documents and decoy documents. So the Fake documents getting receive to the attacker in the much more amount. As the Fake data is gets downloaded by the attacker he gets confused among which data is the actual targeted data. But all the documents are of the Fake types so the original data is gets secured from the malicious insider attack.

Securing Clouds

The basic idea is that we can limit the damage of stolen data if we decrease the value of that stolen information to the attacker. We can achieve this through a 'preventive' disinformation attack. We posit that secure Cloud services can be implemented given two additional security features:

Give bogus information from attacker

We posit that the combination of these two security features will provide unprecedented levels of security for the Cloud. No current Cloud security mechanism is available that provides this level of security. We have applied these concepts to detect illegitimate data access to data stored on a local file system by masquerades, i.e. attackers who impersonate legitimate users after stealing their credentials. One may consider illegitimate access to Cloud data by a rogue insider as the malicious act of masquerades. Our experimental results in a local file system setting show that combining both techniques can yield better detection results, and our results suggest that this approach may work in a Cloud environment, as the Cloud is intended to be as transparent to the user as a local file system.

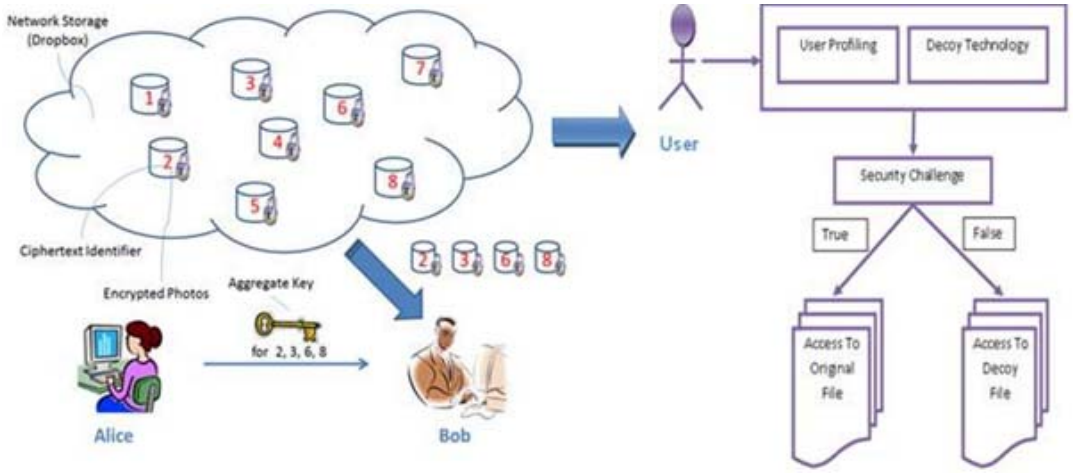

Figure 2.Example of Decoy Technology

A. User profiling behaviour module:

In this module, admin will going to record log record of all users so that he can easily set working baseline for legitimate user. Admin monitor data access in the cloud and detect abnormal data access patterns User profiling will a well known Technique that can be applied here to model how, when, and how much a user accesses their information in the Cloud. Such 'normal user' behaviour can be continuously checked to determine whether abnormal access to a user's information is occurring. This method of behaviour based security will commonly used in fraud detection applications. Such profiles would naturally include Volumetric information, how many documents are typically read and how often. We monitor for abnormal search behaviours that exhibit deviations from the user baseline the correlation of search behaviour anomaly detection with trap-based decoy files should provide stronger evidence of malfeasance, and therefore improve a detector's accuracy.

B. Decoy documents module:

We propose a different approach for securing data in the cloud using offensive decoy technology. We monitor data access in the cloud and detect abnormal data access patterns. We launch a disinformation attack by returning large amounts of decoy information to the attacker. This protects against the misuse of the user's real data. We use this technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless.

C. Secure from vendor:

If legal user does not want to give access to the vendor so we can prevent that access form vendor. In earlier system, vendor can directly access the personal or corporate data which is stored on to the cloud. There is no any provision for security of data which is stored on to the cloud. So in our proposed system, all the data which is stored on the cloud is secured, it is totally depend on the user to assign access permission to its data. In case, if vendor want to access the data which is stored on the cloud, it has to gain the private key of that particular user to decrypt the information and this process is get done via secure key exchange algorithm.

D. Block the Malicious user:

If we will found any malicious user from his user profile behaviour we can directly block that user or we can ask a security questions. For ex. User consecutively fails in login, Brute search attack, uploads files which contains .exe files with in it etc. so, All this log of the all user will maintained in the user profiling behaviour, so as soon as system detects any malicious behaviour, it directly block that user in case, if any authorized user try to search any other publicly stored files then according to our scenario our system blocks that client, but during blocking system asks security questions to that user to avoid authorized user blocking.

E. Differentiate user:

We can differentiate user by using access privileges. We can assign privileges at the time of uploading. For example low user have only read permissions, high user has all permissions like modification. By categorizing different users on the cloud, we obtain fair and flexible control on managing resources on the cloud.

F. Combining User Behaviour Profiling and Decoy

The correlation of search behaviour anomaly detection with trap-based decoy files should provide stronger evidence of malfeasance, and therefore improve a detector's accuracy. We hypothesize that detecting abnormal search operations performed prior to an unsuspecting user opening a decoy file will corroborate the suspicion that the user is indeed impersonating another victim user.

VI. ACKNOWLEDGEMENT

In this paper, we present a different approach to securing personal and business data in the Cloud. We propose a system to monitor data access patterns by profiling user behaviour to determine if and when a malicious insider illegitimately accesses someone's documents in a Cloud service. Decoy documents stored in the Cloud alongside the user's real data also serve as sensors to detect illegitimate access. Once unauthorized data access or exposure is suspected, and later verified, with challenge questions for instance, we inundate the malicious insider with bogus information in order to dilute the user's real data. Such preventive attacks that rely on disinformation technology could provide unprecedented levels of security in the Cloud and in social networks. Monitoring the activity of the cloud storage user in Infrastructure as a service cloud environments is an important work. The authors proposed several techniques for identifying the misuse or attacker in the cloud. But there are no efficient profiling strategies for cloud storage area protection and there are no clear distinguishing strategies for identifying the attacker's activity. Hence, proposing an efficient strategy for quickly adopting the user's behaviour.

VII.REFERENCES

[1] M. Van Dijk and A. Juels, "On the impossibility of cryptography alone for privacy-preserving cloud computing," in Proceedings of the 5th USENIX conference on Hot topics in security, ser, USA, "USENIX Association", pp. 1–8.2010

[2] H. H. Ngo, X. Wu, P. D. Le, C. Wilson, and B. Srinivasan, "Dynamic key cryptography and applications" International Journal of Network Security, vol. 10,pp. 161-174, May 2010.

[3] Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng, "Key-Aggregate Cryptography for scalable data sharing in cloud storage", IEEE Transactions on parallel and distributed system,Volume-25,pp.468-477,Feb-2014.

[4] Y. Sun and K. J. R. Liu, "Scalable Hierarchical Access Control in Secure Group Communications, "org by-at The convention and exhibition centre ,Hong Kong in Proceedings of the 23th IEEE International Conference on Computer Communications . March 7-11, 2004.

[5] D. Godoy, "User profiling for web page filtering," IEEE Internet Computing, vol. 9,pp. 56–64, Jul. 2005.

[6] [6] A. Ceselli, E. Damiani, S. D. C. D. Vimercati, S. Jajodia, S. Paraboschi, and P. Samarati, "Modeling and assessing inference exposure in encrypted databases," ACM Transactions on Information System Security, vol. 8,pp.119–152, 2005.

[7] J. Daemen and V. Rijmen, "Rijndael: The advanced encryption standard (AES)," Dr. Dobb's Journal, vol. 26,pp. 137-139, Mar. 2001.

[8] E. Damiani, S. D. C. D. Vimercati, M. Finetti, S. Paraboschi, P. Samarati, and S. Jajodia, "Implementation of a storage mechanism for untrusted dbmss," IEEE Security in Storage Workshop pp. 38-46, 2003.

[9] M. R. Doomun and K.M.S. Soyjaudah,"Analytical comparison of cryptographic techniques for resource-constrained wireless security", vol. 9, pp. 82-94, 2009.

[10] D. S. A. Elminaam, H. M. A. Kader, and M. M. Hadhoud, "Evaluating the performance of symmetric encryption algorithms", International Journal of Network Security, vol. 10, pp. 213-219, 2010.

[11] D. S. A. Elminaam, H. M. A. Kader, and M. M. Hadhoud, "Evaluating the effects of symmetric cryptography algorithms on power consumption for different data types" International Journal of Network Security, vol. 11, pp. 78-87, Sep. 2010.