VOL. 10, NO. 7, APRIL 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

ENHANCED SECURITY FRAMEWORK TO PROTECT ORPHANAGE SENSITIVE DATA USING CLAIM-CARRY-CATCH METHOD IN CLOUD ENVIRONMENT

N. Jayapandian[1], A. M. J. Md. Zubair Rahman[2] and A. Sowntharya, V. Nivedha[1]
[1]Knowledge Institute of Technology, Salem, India
[2]Al-Ameen Engineering College, Salem, India

ABSTRACT

Cloud computing is well developed popular option for renting of computing and storage infrastructure services. Cloud computing is a computing resource in which tasks are assigned to a different set of connections, services and software that can be accessed over internet. This paper proposes the security methods provided in orphan home secure system. The main aim of this project is to protect sensitive data of orphans using claim carry catch method (CCC). The Orphan Home Management System is going to be secured to overcome the problems that occur in the orphan home. We proposed a secure cloud storage model that addresses security and storage issues for cloud computing environments. In this paper Security is achieved by anonymous authentication which ensures that cloud users remain anonymous while getting duly authenticated. Cloud gives more storage area to the system. The cloud computing relies on the internet. We used cryptographic and claim carry catch method to enhance security in cloud.

Keywords: cloud computing, claim-carry-catch (CCC), orphanage management system, anonymous authentication, cryptographic techniques.

1. INTRODUCTION

Cloud computing is a set of scalable resources and computing infrastructure which provides services to users with the "pay as you use" strategy. Cloud computing is so named because the information being accessed is found in the clouds, and does not require a user to be in a specific place to gain access to it. This type of technology helps users in handling resources effectively on-site. The data which is stored in the cloud are often sensitive in nature. For example, orphan records and user-driven data generated in social networks are often stored in public or private clouds. Ensuring privacy and security of such data is important for users to trust the service providers. For achieving that, anonymous authentication and access control techniques must be employed. A high level security system also ensures that only verified and valid services are provided to authorized users. Indeed, the process of authentication must be initiated for all valid transactions that are performed through the cloud.

The first goal of our work is to implement anonymous authentication of users. In [1], the authors discuss anonymous authentication of users and highlight its importance. The privacy settings of users must be followed in such a manner that the identity of the user should not become evident to either the cloud service providers or to other users. Thus, the anonymity of users is preserved. For achieving anonymous authentication of users, cryptographic techniques and protocols are used. The Cryptographic techniques can be employed to protect the data in cloud environment. In this article, we present the opportunities for cryptography to address some of these security challenges in cloud.

2. LITERATURE SURVEY

We now take a brief survey of the existing approaches for handling various security issues such as key distribution, access control and authentication.

a) Anonymization techniques

There are several techniques available to anonymize the data such as Encryption, substitution, shuffling, number and date variance and nulling some fields. We have discussed some anonymization techniques to obscure data in database [2].

1. Data hiding

It suppresses a data value by replacing it with a value '0'. It is also called as Black marker anonymization. For example, while considering hospital database, an age of a patient may not be required for processing, so it is replaced with constant '0'.

2. Hash calculation

It finds a hash value of either one field or several fields. It takes a variable input and produces fixed size hash of input. The MD5 or SHA can be used. For example, hash of first name and last name can be calculated.

3. Shifting

Shifting shifts a field or data value by specific value. It adds some offset to data value. Shift value is the only key to shift function, so that is kept secret. For example, an offset value 10 is added in age field.

4. Data enumeration

Enumeration is also a substitution technique. It retains the chronological order in which events takes place. It is useful for applications demanding strict

sequencing order. For example, salary field is enumerated while maintaining the order of execution.

5. Ip prefix-preserving

This method preserves the n-bit prefix on IP-address. Two anonymized IP addresses match on prefix of n-bits, if and only if two real IP addresses match on prefix of n-bits. The IP address is prefix preserved here.Prefix-preserving anonymization belongs to Typed Transformation, which uses single anonymized value for each unique value of original data. We surveyed few anonymization methods to protect sensitive data in cloud. Formal models of security for anonymization are also discussed. Anonymization is a viable technique to secure cloud computing. It limits the misuse of sensitive data, but is not a complete solution to preserve confidentiality. These techniques which are currently safe for anonymization may fail in future. In future, the privacy preserving in cloud needs many efforts.

b) SIMD implementation

As our protocol is designed to work well in the SIMD model we did our implementation in CUDA, which is a platform that supports both explicit programming of SIMD execution, along with cheap hardware, GPUs, which supports SIMD execution. More specifically we implemented our protocol in ANSI C using the CUDA extension by NVIDIA. Some parts of our implementation is based on the code from which gave very efficient construction and evaluation of garbled circuits (including handling of the possible selective failure attack on Bob's input), along with an "OT extension", using a consumer GPU. It should be noted that a recent result by Husted et al. Their scheme is up to a factor 3 faster than the scheme in computation on the same hardware, but increases the size of each gate with another cipher text (both xor and non-xor gates). Unfortunately their result was not published until after we had completed our implementation and thus we do not know whether their scheme would be faster when used with our protocol. However, a study of this would be interesting for future work[3].

c) Cryptographic techniques

In the beginning of the Cloud Computing, common encryption Technique like Public Key Encryption was applied. This traditional technique does not provide expected result as it support one to one encryption type communication. Public Key Encryption is not highly scalable. This gave rise to move forward to some advanced encryption methods. The advanced cryptographic methods includes the below encryption methods.

- Identity Based Encryption
- Homomorphic Encryption
- Attribute-based Encryption

- KP-ABE
- CP-ABE
- MA-ABE

These Cryptographic methods gave a very good progress in the field of Cloud Computing.

d) Authentication techniques

In [1], the authors describe anonymous authentication where users are authenticated without their identity being revealed. This approach is very useful in a real time scenario where users want to post some sensitive information without being recognized. Nevertheless, users should be able to prove that he/she is a valid user who has posted the information. For achieving anonymous authentication of users, cryptographic techniques and protocols are used. None of these techniques are quite feasible solutions for providing authentication for cloud users as the number of users is typically very large. Group signatures are also not possible in cloud services since predefined groups should be assumed which is usually not the case in cloud services. Similarly in mesh signatures, the identification of the exact source of information is not possible which makes the system vulnerable to colluding attacks.

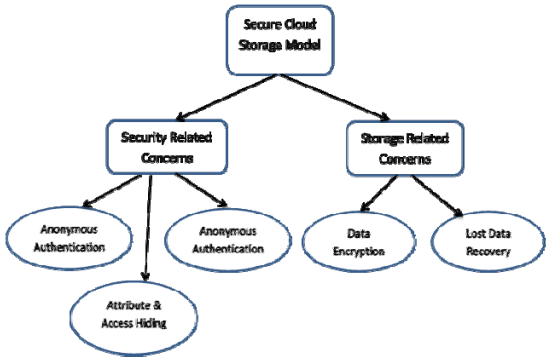

Figure-1. Anonymous authentications.

1. Identity based encryption

Identity Based Encryption cryptographic scheme has been developed by Shamir [4] in 1984. Major issue is the inability to build Identity Based Encryption system which is based on RSA. Later in 2001 an efficient Identity Based Encryption has been developed by Boneh and Franklin [5]. In Identity Based Encryption, an identity of the user plays a vital role. The sender who sends the message only needs to know the receiver's identity attribute in order to send the encrypted messages. Email Encryption is one of the major applications for Identity Based Encryption. However, key revocation is not achieved in Identity Based Encryption

2. Homomorphic encryption

Ronald Rivest Michael Dertouzos and, Leonard Adleman put forth the concept of the Homomorphic encryption [15] in the year 1978. Homomorphic Encryption scheme is used to protect the data in the cloud

environment. This encryption scheme permits to perform computations on the data which is encrypted. This encryption scheme comes under the advanced cryptographic technique. A study on homomorphic encryption is gathered in [6]. However, this encryption has a snail-like processing time which is its major drawback.

3. Attribute-based encryption

Attribute-based Encryption is one of the cryptographic techniques used in Cloud Computing Environment. Attribute-based Encryption is first brought into use by Sahai and Waters [7] in the year 2005. The main focus of this Attribute-based Encryption scheme is to provide security to the data stored in the cloud. The four steps in Attribute Based Encryption are Setup, KeyGen, Encrypt, and Decrypt. The KenGen() algorithm is used to the create private key of the user for secret sharing. The users who are authorized can decrypt the information using their private key. Attribute-based Encryption comes up with access control. In Attribute Based Encryption, data owner uses a set of attributes to encrypt the data and only the authorized users who has the predicted or certain attributes can decrypt the data. This encryption scheme makes the cloud environment more secure. The various classes of Attribute-based Encryption are summarized.

3.1. Key-policy attribute-based encryption

KP-ABE is introduced by Vipul Goyal and Omkant Pandey [8] to achieve fine-grained access control [12] in one-to-many communications. In Key-Policy Attribute-based Encryption, the encrypted data is constructed with the set of attributes. The person is authorized to decrypt the ciphertext if and only if the attributes that are built with the cipher text satisfy the access structure of their private or secret keys. The four steps in Key-

Policy Attribute Based Encryption are Setup, KeyGen, Encrypt, Decrypt. The KeyGen and Decrypt algorithms get differed from the Attribute Based Encryption. In Key-Policy Attribute-based Encryption, private key of the user is cognated with the access structure. However unauthorized access may occur, the people may decrypt the information. This can be overcome in the Ciphertext Policy Attribute Based Encryption which construct the access policy in the encrypted data ie, ciphertext and employs a set of attributes to narrate the private key of the user. Also in some applications that uses this scheme, owner of the data must have a firm belief with the key issuer.

3.2. Ciphertext policy attribute based encryption

In 2007, Bethencourt *et al* [9, 11] proposed a cryptographic technique named cipher text policy attribute-based method. The access policy is built with the data that has been encrypted. In CP-ABE the cipher text is identified with access structure and the private keys with the attributes. In Key-Policy Attribute Based Encryption, the major disadvantage is that the access policies were not created by the encryptor. This provided a route to the establishment of Ciphertext Policy Attribute Based Encryption which allows the access policies to be built with the encrypted data. The owner who encrypt the data model the access policy. A proposal was made in [16] for the use of CP-AB technique. The data owner is in charge of defining the access policies. This prevents unauthorized access and promotes security. In CP-ABE, revocation is not achieved efficiently. Thus it is not so easy for the data owner to modify the access polices whenever needed.

3.3. Multi-authority attribute based encryption

Multi-Authority Attribute Based Encryption is introduced by Chase [10, 13]. The Multi-Authority Attribute Based Encryption (MA-ABE) is also a cryptographic technique which consists of many authorities to manage the attributes and the distribution of the secret keys. The user who wishes to download the information will request the decryption keys from the attribute authority. The attribute key generation is one of the algorithms in MA-ABE. This algorithm is run by the authority and in turn the authority will distribute the keys to the users. An authorized user who has the appropriate decryption keys can view the information. The algorithms involved in this scheme include Set up, Attribute Key Generation, Central Key Generation, Encryption, and Decryption. This cryptographic scheme handles more number of users. Data confidentiality can be achieved on using this type of technique in cloud environment. As it is suitable for multiple authorities' scenario, this cryptographic technique is most suitable for the applications which contain various sectors. This cryptographic scheme improves security and reduces key management complexity which is the major advantages.

3. EXISTING SYSTEM

The security level in existing system is not up to the mark. As we do not have any back up, consider the case of Orphanage project data reliability is not assured. As we store our data in database there are several issues in security. Some problems are lack of security, low data retrieval, data redundancy and consistency and no backup and recovery. For example attackers can easily steal the important details and financial reports of orphan home and sell it to other third party. As there is no backup of orphan's data if data lost, the orphan home center will face a bad impact where they may lose their important information for future analysis.

4. PROPOSED METHOD

In the proposed system instead of storing our data in database we are storing in cloud to enhance space and security. our proposed system contains detail about orphans and their sponsors such as address location, phone number and contact details. so information stored in our system is very sensitive. Here we used cryptographic claim-carry-catch method to secure our sensitive data. Claim-carry-catch concept is used to enhance security in public cloud. This is an emerging technology which will bring about innovations in terms of business models and

applications. Anonymity based method is used here it anonymizes the sensitive data before storing in cloud. This system provides safe and secure storing. Cryptography is an essential tool that helps to assure our data accuracy. The Cryptographic techniques can be employed to protect the data in cloud environment.

a) Claim-carry-catch

To handle the unstructured Data, a kind of new technology emerged "NoSQL", which is non-relational database management system for unstructured data. The biggest motivation behind NoSQL is scalability. The data collected from every individual provides a high volume of data at high velocity. Analysis of stored healthcare data in terms of querying leads to early detection, diagnosis and also effective drug can be suggested. A distributed scheme is introduced to detect if a node has violated its rete limit. In DTNs it is difficult to count the number of packets sent by a node, so it is important to introduce the technique called Claim-Carry- Catch. The claim structure uses pigeonhole principle. If the attackers send the packets within the rate limit it is difficult to identify the flooded packets, depends upon the packet count private key should be generated.

b) Claim construction

Two pieces of metadata are added to each packet. Packet count claim (P-Claim) and Transmission count claim (T-Claim) are used to detect packet and replica flood attacks.

1. P-Claim

P-Claim is added by the source and transmitted to later hops along with the packet. When the contacted node receives the packet, it verifies the signature of P-Claim and checks the value of packet count (Cp). If Cp is larger than the rate limit it discards the packet, otherwise it stores as P-Claim.

2. T-Claim

It is generated and processed hop-by-hop. There is a sequence increment in T-Claim (1,2..) it also includes the current transmission count. When the packets transmitted from one hop to another hop (node) it will increase its T-Claim's count.

If there is any inconsistency in both claims, there is a clear indication of an attack. Here sampling is used to reduce the communication cost by exchanging both claims and also to increase the probability of attack detection redirection is used. Both sampling and redirection is used for P-Claim and T-Claim to detect probabilistically in the network. T-Claim should count from starting node and increment continuously.

c) Private key generation

If the attacker send the packets within the rate limit there is no indication of attack. If the packets transmits within the rate limit in the network, private key should be generated by Trusted Authority (TA).Depending upon the packet count TA will generate the private key. If the node transmits the packet in the network, it can able to verify and match the key value; because each node has a private key value. The attacker cannot able to identify the private key. For additional security purpose the private key should be generated.

d) Cryptographic method

The data may get disclosed or modified by any unauthorized access. It is essential that a special care must be taken to protect our sensitive data. A secure storage [3] must be achieved in cloud computing. So we adopt cryptographic techniques for the secure storage. The data is encrypted by the data owner before the data is uploaded to the cloud.

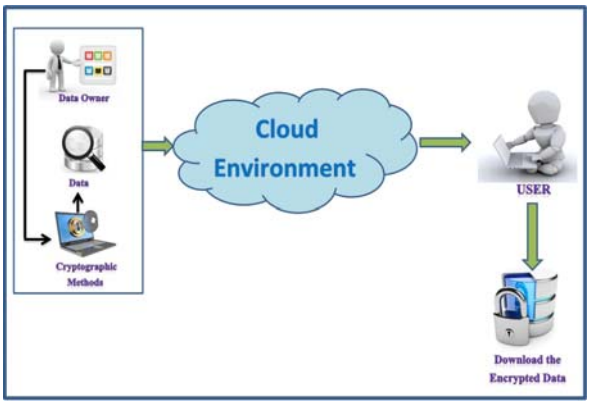

Figure-2. Clouds cryptographic method.

5. RESULT AND DISCUSSIONS

The final result shows that our proposed claim-carry-catch method provides more security than existing model. We defined cryptography techniques here it helps to secure our data in cloud. The above mentioned privacy protection method helps us to protect our data from third parties.

The method shows that our protocol is up to a factor 3 faster than the most comparable method, showing the greatest improvements for the larger the statistical security parameters. As future work the time complexity can be reduced using few scheduling algorithms. This work studies the problem of ensuring the integrity of data storage in Cloud. We consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the data stored in the cloud. This method of algorithm supports to the scalable and efficient public auditing in the Cloud Computing. New techniques can be evolved to minimize the size of the proof of data integrity as well as to reduce the time consumption in cloud. our method supports an external third party auditor to audit sponser's outsourced data in the cloud without learning knowledge on the data content. To the best of our knowledge, We prove the security and justify the performance of our proposed schemes through claim carry catch method.

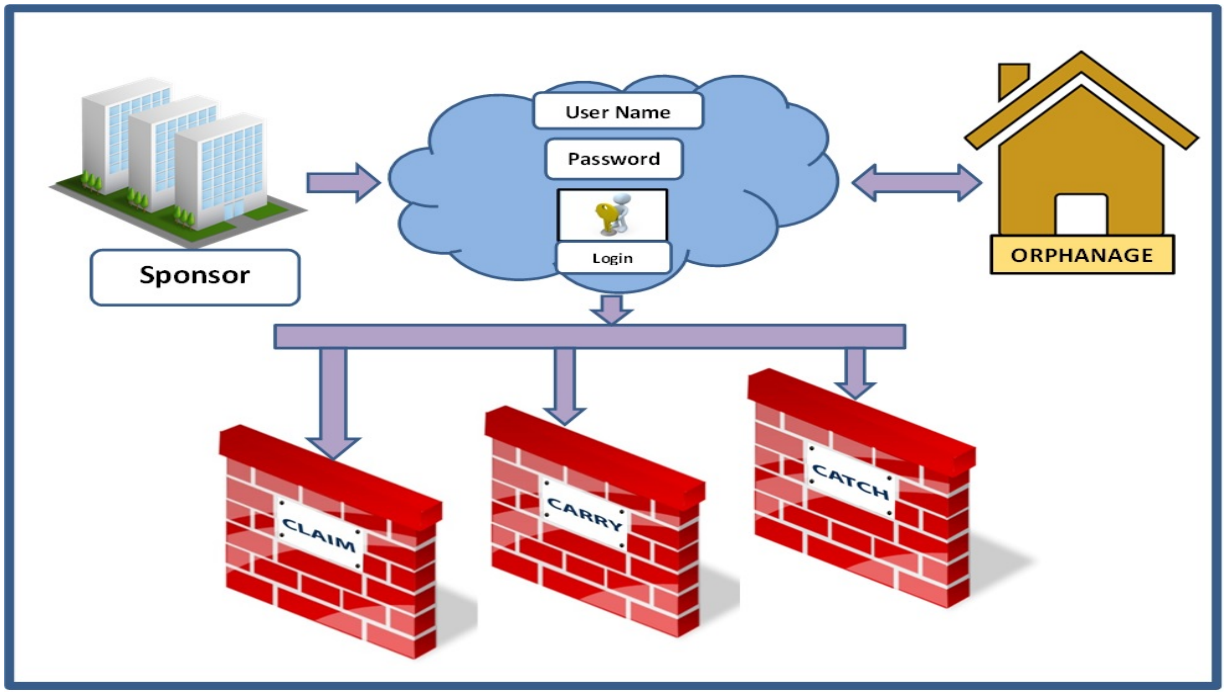

Figure-3. Claim-carry-catch method.

6. CONCLUSIONS AND FUTURE WORK

Our Proposed system provides Security assurance for both orphans' data and sponsors data using claim-carry-catch method along with anonymous authentication and cryptographic techniques. The proposed scheme in the system uses strong authentication mechanism, where the users claim is validated at two levels. Well-defined security methods always hope the best for all the cloud applications. Thus the sensitive data can be securely shared and stored with the authorized users by adopting the cryptographic techniques. Cryptographic methods has been effectively lead by the development of cloud computing and also due to vast increment in the range of users of the cloud. None of these techniques are quite feasible solutions for providing authentication for cloud users as the number of users is typically very large as anonymous authentication. Our claim-carry-catch method generates private key that cannot be attacked by the attackers. It provides trust worthy and secured access to the customer.

REFERENCES

[1] S. Ruj, M. Stojmenovic and A. Nayak. 2013. "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 2, pp. 556-563.

[2] V. K. Saxena and Dr. Shashank Pushkar. 2013. Anonymization Approach for privacy preserving in cloud computing", International Conference on cloud, Big Data And Trust Nov. pp. 13-15.

[3] Tore Kasper Frederiksen, Thomas P. Jakobsen and Jesper Buus Nielsen. 2014. "Fast and Maliciously Secure Two-Party Computation Using the GPU," Applied Cryptography and Network Security, Lecture Notes in Computer Science Vol. 7954, 2013, pp. 339-356. Springer.

[4] Shamir. Identity-Based Cryptosystems and Signature Schemes. In Proceedings. Of Cryptography 1984, LNCS 196, pages 47–53. Springer-Verlag, 1985.

[5] D. Boneh and M. Franklin. 2001. Identity-Based Encryption from the Weil Pairing, Proceedings of Cryptography 2001, LNCS 2139, pp. 213–229, Springer-Verlag.

[6] C. Fontaine and F. Galand. 2007. A survey of homomorphic encryption for nonspecialists, EURASIP Journal on Information Security, 2007, pp.1-15, January.

[7] Sahai A and Waters B. 2007. Attribute-based encryption with non-monotonic access structures. In Proceedings of the 14th ACM conference on Computer and communications security, page 203. ACM.

[8] V. Goyal, O. Pandey, A. Sahai and B. Waters. "Attribute-based encryption for fine-grained access control of encrypted data," in CCS '06, 2006, pp. 89–98.

[9] Bethencourt J., Sahai A. and Waters B. 2007. "Ciphertext- Policy Attribute-Based Encryption", Proceedings of IEEE Symposium Security and Privacy, pp. 321-334.

[10] M. Chase. 2007. "Multi-authority attribute based encryption," in Proceedings of the Theory of Cryptography Conference, pp. 515-534.

[11] Brent Waters. 2011. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In Public Key Cryptography, pp 53-70.

[12] Shucheng Yu., Cong Wan, Kui Ren and Wenjing Lou. 2010. "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", in in Proceedings of IEEE Communications Society for publication, pp. 534–542.

[13] Chase M and Chow S. 2009. "Improving privacy and security in multi-authority attribute-based encryption", in Cloud Computing Security, pp. 121–130.

[14] Ming Li, Shucheng Yu, Yao Zheng, KuiRen and Wenjing Lou. 2013. "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", IEEE Transactions on Parallel And Distributed Systems, Vol. 24, No. 1, January.

[15] Ronald L. Rivest, Leonard Adleman and Michael L. Dertouzos. 1978. On Data Banks and Privacy Homomorphisms, chapter On Data Banks and Privacy Homomorphisms, pp. 169-180. Academic Press.

[16] B. Raja Sekhar, Sunil Kumar, L.S wathi Reddy and V. Poorna Chandar. 2012. "CP-ABE Based Encryption for Secured Cloud Storage Acces," International Journal of Scientific & Engineering Research, Vol. 3, Issue No. 9.