Verifiable Cryptographic based Data Transformation System

Aishwarya.M, Computer Science and Engineering, SKP Engineering College, Tiruvannamalai, India,9488839024

Kumaresan.A, Computer Science and Engineering, SKP Engineering College, Tiruvannamalai, India.

Manjuparkavi.R.,Computer Science and Engineering, SKP Engineering College, Tiruvannamalai, India.

Maheswaran.R, Computer Science and Engineering, SKP Engineering College, Tiruvannamalai, India.

Kalaignanam.K, Computer Science and Engineering, SKP Engineering College, Tiruvannamalai, India.

***Abstract* - I propose a strategy for checking the uniqueness of attribute based encryption using proxies and outsourced decryption. An Issues related to the information sharing in a distributed system is one of the major practical issue consisting of autonomous entities which needs to be securely transferred in a heterogeneous multi subdivided systems. Hence the concepts of encryption and decryption are formulated to transfer the data from source to destination securely. By using an encryption/Decryption standard our distributed secure computation systems show that our approach seamlessly integrates security enforcement at the user intensity with a certain trust level. A novel method of verifying the correctness of the conversion from encryption to decryption is made. The drawback in the existing system is that there is no proper verification with the proxies. In addition to that, attribute based master secret key is also not unique at their attribute consideration. Finally the Proxy verification method is introduced for the purpose of overcoming the downside.**

***Index Terms*: Proxy, security, Encryption, Decryption**

I. INTRODUCTION

Cloud acts as a mass storage, whereas the cloud server fetches the information from the proxy server and also from the storage, where the proxy server is maintained separately in the cloud and the storage which stores the encrypted data as well the decrypted data[1].cryptographic technique is the process of secret writing. The process of enciphering and deciphering of data are more specifically concerned with the cryptography with the use of secret key K which maintains the information confidential. Developing a mathematical security notion is the main goal of cryptography where it uses the protocols and schemes for designing and analyzing the cryptographic applications by the semantic security of public key encryption schemes [2, 3].

Considering a power plant organization, the nuclear component details must be transformed securely for the security purpose of the nuclear details. Security is a high complicated issue while transferring data from one end to other end, Thus to avoid the security issue we go on to the cryptographic technique [2]. The concept basis the attributes of the particular end users for the security purpose of data transformation system where the attributes used for encryption and decryption keys [4] and are considered in cryptographic techniques for the behavior of its uniqueness which always overcomes the issues of security [5].These approaches are shown in fig[1].The end user must get access authorized for the transformation process and also to pursue. As soon the access permitted for the end user, The Master secret key is generated obligatory based on some of the unique attributes. Now the end user holds back to receive the email from the proxy server regarding the keys for encrypting the data [6]. Where the public key is known in public but private is kept secret according to public-key cryptography technique [7], also solves the problem of key distribution.

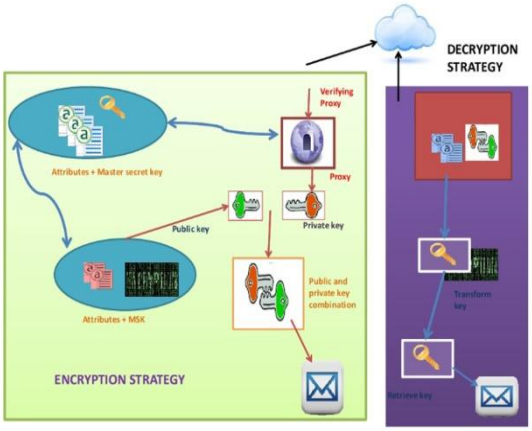

Fig.1 Proposed architecture diagram of cryptographic based data transformation system.

Proxy server acts as a medium [8] as shown in the fig.2. The end user requests Proxy server for keys being used in cryptographic technique. Only Authorities has the access permission to ingress the Proxy server and also maintains the concealment between the transformation systems. Proxy aids as security, against cloud server attacks, reduces upstream bandwidth usage and hardware costs for the large organizations in the distributed systems. Each system connected to the network individually through the proxy server to main server [1].The importation of a Proxy server concerns login requirement where users must log in to attain

ISSN: 2278 – 1323

entree for the authorization discipline. Practically if proxy is trusted fully number of applications would not be in sane [9]. So placing full trustworthy in proxy is off target accordingly.

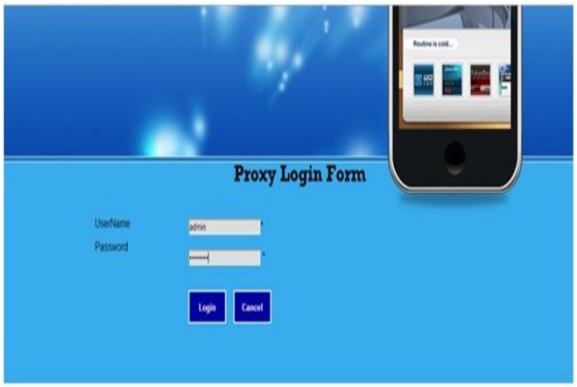

Fig.2 Login design for the medium proxy

II. Related Works

In [10], Amit sahai et al Fuzzy IBE scheme allows private key for the decryption process and after measuring cryptographic technique by the set overlap the scheme are enforced for the permissive of encryption with the help of biometrics input identification where it is specialized in error tolerance and secure. So, it is used in the attribute based encryption. Vipul Goyal et al in [11] considering KP-ABE and are developed in a new cryptosystem for sharing the encrypted data, which supports the trust of private keys containing HIBE (Hierarchical identity based encryption) for the scheme of sharing the verification log information and the performance of encryption. Seeing [12] the private keys are expressed in any access formula in the developed ABE scheme where it provides security of proof based on the BDH (Bilinear Diffie Hellman). In consideration of [13] access control expressed in term of any access formula over the system attributes some systems are developed where PBDHE (Parallel Bilinear Diffie Hellman exponent) proved to be secure and also achieve performance tradeoff under the BDHE and BDH. The concept of [14], confess that cloud increasingly evolved for securing the data. CP-ABE is introduced to overcome the issues of key management and to reduce the overhead of decryption process where the scheme involved in one encryption key and decryption keys ,where the Bilinear map system used to achieve its goal. In [15], Public key encryption is viewed in ABE as the range of allowing user attributes for encrypting and decrypting messages. On pairing operation is done per attribute during decryption in the ABE implementation. Also presents the Decryption process in first key-policy ABE systems with constant static number of pairings. Taking under advisement [16] the fiat and Shamir [FS86] designed and proposed a digital signature scheme which designs the secure interactive identification protocol in the starting observation, where the sender himself selfness to a receiver and also verifies, validates the message to be verified in a way producing a digital signature by the signer. Also, 2-step approach was proposed to design a secure digital signature. Mihir Bellare et al Considering RO model in [17] where a practical protocol is proved for its correctness with the replacement of the oracle access by choosing a hash function. Produces more efficient and favor in provable security.

III. Subsisting Component Transformation Via Proxy Is Unassured

The problem in the existing system is that there is no proper verification for the proxy. Proxy may act as an intruder since a third party server. In [1] Based on the user attributes the encryption and decryption processed. By using the access policies and ascribed attributes the ABE has flexible access control on the stored data in cloud. The defects involved in the complex growth of access policy on the decryption process in particular to the number of pairing operations are too expensive as well complex [18,19]. Green et al reduced the overhead for the users in the decryption side by proposing an ABE system with outsourced decryption. ABE system provides an untrusted server along with the transformation key which translates the ciphertext into simple ciphertext. The transformation correctness was not guaranteed but the verifiability process in the ABE with outsourced decryption are checking whether the transformation is done correctly are not. Chances for the proxy to be an intruder in many ways as selling out the email details (may help the Hacker to trace out the keys and trap the data), Information about the nuclear details (may lead to an big economic problem), It may generate wrong keys (which would collapse the data transformation system), Proxy might act as an intruder for himself or might work for the outside hacker. Touching on [8] which uses the proxy signature function which was proceeded with a function $\pi(s, \pi_{A\to B})$ where the proxy key is specified as $\pi_{A\to B}$ whereas the secret key A signs the signature 's' for the specific particular performing transformation. Suchlike $v(m, \pi(s(m, A), \pi_{A\to B}), B)$ certifies valid where, the signature function $s(m, k)$ with the message m along with the key A. And the verify function $v(m, s, k)$ also points the message m with the signature s by the component key k. Once more in the existing, obviously the proxy function not existed in the digital signature schemes such like RSA [RSA78], DSA [NIS91], (OR) ELGamel [ELG85] etc. and also cannot be said fully such functions do not existed. Where, with the help of proxy signature the asymmetric proxy functions are not all the way considered secure.

IV. Prospective New Model Of Proxy Verification Along With ABE

The keys generated by the proxy are been used to submit the details of the nuclear components as well the assigned work for the particular end user (receiver) by the user base (sender). This is the way the component data are encrypted using the keys produced by the proxy server. The proxy server prompt an email to end user (receiver) regarding the allocation of the encrypted data with their identity along

ISSN: 2278 – 1323

with the cipher text verification keys called transformation key and the retrieving key or validating key. The decryption process is started by the end user (receiver) by fetching the encrypted data with the identification and makes a formal application of the transformation key which produces the partial cipher text [1] shown in the fig.3. Now, proposing the secondary step to apply the retrieving key which produces the plain text which is done as a verifiable cryptographic [20] for helping the user overhead in decryption process [7] as shown in the fig.4. So we propose an algorithm called proxy signature verification to verify the proxy server to prevent proxy from being an intruder as shown in the fig.5.

Fig.3 Generation of Transformation key produces the partial text.

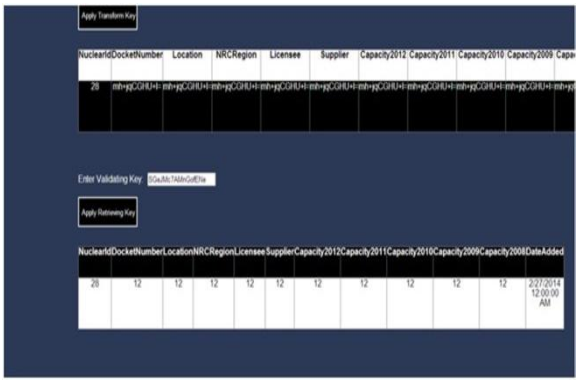

Fig.4 Original text retrieved using the Retrieving key.

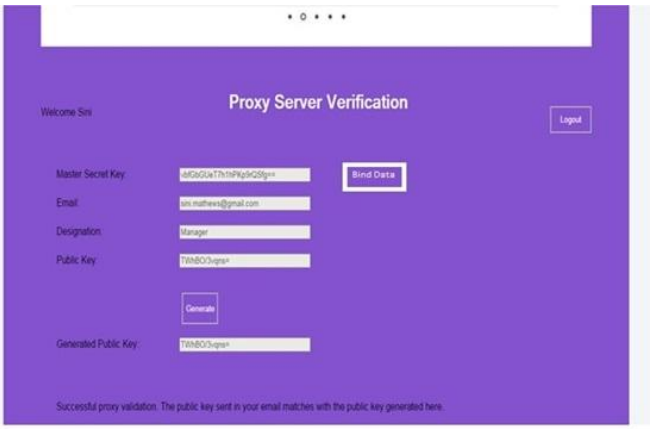

Fig.5 Proxy server verification.

In multi-party system [5], both secret sharing and key distribution schemes are used and further they allow the secret information to get stored in network which also helps only the good user to perform actions in a system. In implementing a proxy signature verification algorithm, we had a goal in mind. Wanted to show the proxy signature verification algorithm incorporated successfully into a basic cryptographic file system. So, the verification process includes similar to the digital signature [8] but where the code is used to verify the proxy. If suppose, for the action of being an intruder as notifying the set of data repeatedly without the users request. SO, verification of proxy may help in security for the data transformation system. So proxy signature verification algorithm is to verify that the proxy itself becomes an intruder or supporting the intruder. The Quantization Algorithm is used for the encryption process where the plaintext message m is encrypted using the master secret key K along with the private key and their encryption function EK(.), resulting in the ciphertext c. Also Message digest algorithm with 128-bit MD5 algorithm used incipiently advanced to verify in correctness to the transmission of data safety measure. From the multiple hash functions the output are concatenated and also provides the private and public key information $c = E_k(m)$. Where, the product is the public key information which given rise to the ciphertext. Along n user, supporting unique attribute based id with $\frac{[n(n-1)]}{2}$ key specification as private key. Therefore,

$$\left(c_{<g^*>}^{(\alpha^{-1})}, (\alpha^{-1})i\right) = inverse\left(n, t, \hat{g}, \hat{h}, \left(c_{<g>}^{(\alpha)}, \alpha_i\right)\right)$$

The decryption process uses the co-ercion algorithm to recover the plaintext m, the ciphertext c is decrypted using the retrieving key k and the decryption function DK (.). Considering, two inputs as H and K where an invertible function with attributes and session key with exclusive OR operator. Taking, $R = R \oplus H(L)$

$$then \quad L = L \oplus H(R \oplus K)$$

$$and \quad R = R \oplus H(L \oplus K).$$

ISSN: 2278 – 1323

Let (Lplain,Rplain) be the plaintext, correspondingly (Lcipher,Rcipher) be the cipher text. Where, the inverted product with Lcipher gives the fully retrieved message and without Lcipher provides transformed partial message

$$K = H^{-1}(R_{cipher} H(L_{plain} \oplus R_{plain}) \oplus L_{cipher}$$

$$K = H^{-1}(R_{cipher} \oplus H(L_{plain}) \oplus R_{Plain})$$

To verify the proxy we are proposing a proxy signature verification algorithm which would make asymmetric proxy function to be secured all the way. The scheme of verification which allows the verifier to examine

$$v' = g^{\sigma}.(y_0.y_p)^{h(w,r_0)} r_0)^{-v} \; mod \; q$$

And also checks whether $v = h(v', m)$.

Sign(S_{dlp}): The signer has to choose a random $t \in z_l$ and should compute $r = g^t mod\, q$ for signing a message M. formerly compute $c = h(m, r)$ and $\sigma = (t - x_c) mod\, l$ on message m, the signature is (σ, c) and also in other words,

$$\sigma \leftarrow S_{dlp}(Params - dlp, (t, r), x, m)$$

Verify(V_{dlp}): verifier compute $r' = g^{\sigma} y^{c} (mod\, q)$ and $c' = h(m, r')$. The validation is checked as, if $c' = c$ then the signature is valid else invalid.

Outcome:

$Result \leftarrow V_{dlp}(Params - dlp, y, \sigma, m)$,

where $Result \in \{Valid, Invalid\}$.

V. Discussion

The experiment is done in a win out environment which upsurge the performance in a asymmetric bounds. The exactitude in verification of data transformation are done in a complete stainless wrap. The achievement of verifying proxy (The untrusted server) had undergone the renovation enforcement in security. The applications get in touch based on the code layout where the c# coding language is used for the layout. Then the Microsoft visual studio 2010 is a IDE specially for the .NET framework which acts a front end and SQL Server 2008 R2 as the back end.

VI. Conclusion

In this paper, we proposed the concept of future enhancement over the Distributed Attribute-Based Encryption (DABE) as an extension of Cipher text-Policy Attribute-Based Encryption (CP-ABE) that supports an arbitrary number of attribute authorities and allows to dynamically add new users and authorities at any time, which will provide an efficient construction of DABE that uses only two pairing operations in the decryption algorithm and no pairing operation in any other algorithm. A limitation of the construction is that access policies need to be in DNF form. We leave it as an open question to design a more expressive DABE scheme, while preferably maintaining the O (1) number of pairings that our construction offers.

VII. Future Enhancement

In this work we proposed CP-ASBE a form of CP-ABE that organizes user attributes into a recursive family of sets and allows users to impose dynamic constraints on how attributes may be combined. We demonstrated how CP-ASBE can naturally support compound attributes, and numerical attributes with multiple value assignments. We showed that it achieves this versatility with very little overhead through efficiency analysis and performance evaluation of a specific prototype implementation. An interesting direction for future research is to study the potential of CP-ASBE schemes and ABE schemes in general in supporting constructs similar to “OR roles” and constraints like “dynamic mutually exclusive roles” that are common in traditional mediated RBAC settings. Other directions for future work are the design of efficient CP-ASBE schemes that are secure in the standard model and extending CP-ASBE to a multi-authority setting.

References

[1] M. Green, S. Hohenberger, and B.Waters. “Outsourcing the decryption of ABE ciphertexts,” *Proc. USENIX Security Symp.*, San Francisco,CA, USA. 2011.

[2] R. Canetti, H. Krawczyk, and J. B. Nielsen.“Relaxing chosen-ciphertext security,”.*Proc. CRYPTO*, pp. 565–582, 2003.

[3] S. Goldwasser and S. Micali. Probabilistic encryption. *JCSS*. Vol. 28,(No 2),1984.

[4] T. Okamoto and K. Takashima.“Fully secure unbounded inner-product and attribute-based encryption,”.*Proc. ASIACRYPT*, pp.349–366, 2012.

[5] A. Beimel.“Secure Schemes for Secret Sharing and Key Distribution,”.Ph.D. dissertation,Israel Inst. of Technology, Technion City, Haifa, Israel,1996.

[6] C. Gentry and S. Halevi.“Implementing gentry’s fully-homomorphic encryption scheme,” *Proc. EUROCRYPT*. pp. 129–148, 2011.

[7] C. Gentry.“Fully homomorphic encryption using ideal lattices,”.*Proc. STOC*, pp. 169– 178, 2009.

[8] M. Blaze, G. Bleumer, and M.Strauss. “Divertible protocols and atomic proxy cryptography,” .*Proc. EUROCRYPT*, pp.127–144, 1998.

[9] G. Ateniese, K. Fu, M. Green, and S. Hohenberger.“Improved proxy re-encryption schemes with applications to secure distributed storage,”.*Proc. NDSS*, San Diego, CA, USA.2005.

[10] A. Sahai and B. Waters.“Fuzzy identity-based encryption,”.*Proc.EUROCRYPT*, 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,”.*Proc. ACM Conf. Computer and Communications Security*, pp. 89–98, 2006.

[12] R. Ostrovsky, A. Sahai, and B. Waters. “Attribute-based encryption with non-monotonic access

ISSN: 2278 – 1323

structures,".*Proc. ACM Conf. Computer and Communications Security*, pp.195–203, 2007.

[13] B. Waters."Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,".*Proc. Public Key Cryptography*, pp. 53–70, 2011.

[14] J. Bethencourt, A. Sahai, and B. Waters."Ciphertext-policy attributebased encryption,"*Proc. IEEE Symp. Security and Privacy*,pp. 321–334, 2007.

[15] S. Hohenberger and B. Waters. "Attribute-based encryption with fast decryption," .*Proc.*
Public Key Cryptography,pp. 162–179, 2013.

[16] S. Goldwasser and Y. T. Kalai."On the (in) security of the fiat-shamir paradigm," .*Proc.FOCS*. pp. 102–113, 2003.

[17] M. Bellare and P. Rogaway."Random oracles are practical: A paradigm for designing efficient protocols,". *Proc. ACM Conf. Computer and Communications Security*, pp.62–73, 1993.

[18] P. P. Tsang, S. S. M. Chow, and S. W. Smith."Batch pairing delegation,".*Proc. IWSEC*, pp. 74–90, 2007.

[19] S. D. Galbraith, K.G. Paterson, and N. P. Smart."Pairings for cryptographers, ".*Discrete Appl. Math.* vol. 156, (no.16) pp. 3113–3121, 2008.

[20] B.Parno, M.Raykova, and V. Vaikuntanathan."How to delegate and verify in public:Verifiable computation from attribute-based encryption, ".*Proc. TCC*, pp. 422–439, 2012.

ISSN: 2278 – 1323