International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 3 (September '2017)
Proceeding of - International Conference on Recent Trends in Computational Life Science and Information Technology,
Conference held at Tiruppur Kumaran College for Women,Tirupur,Tamilnadu, India.

ENHANCED IDENTITY BASED SIGNATURE WITH MALWARE DETECTION

Dr.K.Rajeswari,
Associate Professor,
Department of Computer Science,
Tirupur Kumaran College for women,
Tirupur,Tamilnadu,India.

I.Meena,
Research scholar (M.Phil),
Dept of computer science,
Tirupur Kumaran College For women,
Tirupur, Tamilnadu, India

Abstract: Antivirus software is tools purpose for decision and stopping cruel and unnecessary files. However, the long term effect of traditional host based antivirus is questionable. Antivirus software fails to detect many modern threats and its increasing complexity has resulted in vulnerabilities that are being exploited by malware. The promote a new model for malware detection on end hosts based on providing antivirus as an in-cloud network service. This Antivirus enables identification of malicious and unwanted software by multiple detection engines Respectively, Our Enhanced Identity Based Signature with Malware detection approach of moving the detection of malicious users into the cloud is aligned with a strong trend anent moving services from end host and monolithic servers into the cloud. This approach provides several important benefits including better detection of malicious software, enhanced forensics capabilities and improved deploy ability. Enhanced Identity Based Signature with Malware detection in cloud computing includes a lightweight, cross-Storage host agent and a network service. Here a static signature verification system based on the concept of local stability. Stable regions are detected in the signatures, during the enrolling phase, and are considered to the those regions affected by low variants of features among the training set. The stability evaluation is based on the Hamming distance. Stable regions are successively used for verification in the running phase. A region oriented verification strategy is considered, based on a well-defined similarity measure which takes into account the variability in signing of the writer. The results, carried out on signatures from the GPDS database, expose the viability of proposed approach.

Keywords: Malware Detection, Keyword Management, Cipher Attacks

I. INTRODUCTION

Secure data management in cloud computing providing efficient multi-receiver E-IBsingautre scheme that only requires "one" (or "none") pairing computation to encrypt a single message for multiple receivers. It provide formal security of multi-receiver using E-IBsingautre schemes based on the "selective identity attack" model in which an attacker outputs ahead of time the identities of multiple receivers that it wishes to challenge. They then prove that our schemes are secure against chosen plaintext attack (CPA) and adaptive cipher text attack ("ACTA") in the random oracle model assuming the standard assumptions related to the Bilinear Diffie-Hellman problems are computationally hard.

The top level is chiefly of high go quickly wired internet something put on a list points. The second level is made up of fixed, unchanging, unmoving net routers in the military as a more than one or two go away backbone to make connection to each other and internet via long range high go quickly radio techniques. The lowest part level includes a greatly sized number of readily moved network users. The end users way in the network any by a directly to radio connection or through a chain of other equal users foremost to a near net router the router additional makes connection to far away, usually different users through the radio backbone and internet. Security and right not to be public issues are of best business house in pushing the good outcome of cloud for their wide placing and for supporting service. The internet via long range high go quickly radio techniques. The lowest part level includes a greatly sized number of readily moved network users. The end users way in the network any by a directly to radio connection or through a chain of other equal users foremost to a near net router the router additional makes connection to far away, usually different users through the radio backbone and internet. Security and right not to be public issues are of best business house in pushing the good outcome of cloud for their wide placing and for supporting service.

II. KEY AGREEMENT IN GROUPS

A number of group key management techniques have been proposed in the past. They normally fall into three categories: (1) centralized, (2) distributed, and (3) contributory. The simple as it involves a single entity (or a small set of entities) that generates and distributes keys to group members via a pair-wise safe channel recognized with each group member. They view centralized group key management as unsuitable for safe peer group communication, since a central key server must be, at the same time, continuously presented and present in every possible split of a group in order to support continued operation in the event of arbitrary network partitions.

III. GROUP KEY MANAGEMENT

The work is on the presentation of group key management protocols for joint peer groups. The key consider only distributed key distribution and contributory key agreement It disturbed mostly with the cost (performance) of the types of group key management operations that arise most often. At the first glance, it might appear that a typical collaborative group scenario is as follows: a group forms,

IJCRCST © 2017 | All Rights Reserved

functions for some time, and then dissolves itself. If this were true, It only need to consider the performance of the initial key agreement leading to the group's formation. Moreover, performance would not be of great concern because the protocol would be invoked only once or very infrequently in order to rekey the group. However, a typical collaborative group is formed incrementally and its population can mutate throughout its lifetime due either to members joining and leaving or to network connectivity changes.

It begins with the STR protocol proposed by and originally aimed at teleconferencing. As will be seen later, STR is well right for adding new members as it takes only two rounds and two modular exponentiations. The member elimination (rekeying following a member leave event) is relatively inefficient. In proposed an capable protocol which takes only two rounds and three modular exponentiations per member to produce a group key. This protocol allows all members to recomputed the group key for any membership modify with a steady

3.1 OBJECTIVES

The objectives of the thesis are as follows:

- Design the single multi-cloud group.
- Generation of private keys for users.
- Encoding and decoding of text message
- Secure transmission of session key by using the algorithm Data Encryption Standard (DSA).
- Design the multi group with multiple data stream in such a way that reduced overhead of key Cloud Server.
- Use Identity tree based structure. Each node in the personality tree is allied with an identity. The leaf node's identity is corresponding to the user's individuality and the middle node's identity is generated by its children's identity. Hence, in an identity tree, an intermediate node represents a set of users in the sub tree rooted at this node.

IV. SYSTEM DESIGN

4.1 EXISTING SYSTEM

The concept of this scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports making, alteration, and reading data stored in the cloud. They also address user revocation. Moreover, our authentication and entrée handle scheme is decentralized and strong, dissimilar other entrée control schemes designed for clouds are centralized.

The communication, computation, and storage overheads are equal to centralized approaches E-IBsingautre Identity based encryption (E-IBE) is a promising approach that fulfills the necessities for secure data retrieval in clouds. Attribute Based Encryption (ABE) features a system that enables an entrée organize over encrypted data using entrée policies and received attributes between private keys and cipher texts. Thus, different users are permitted to decrypt different pieces of data per the security policy.

4.2 DISADVANTAGES OF EXISTING SYSTEM

The problem of applying the clouds introduces several security and privacy challenges. Ever since some users may change their linked attributes at a few position (for example, moving their region), or some private keys might be compromised, key revocation (or update) for each attribute is essential in order to make systems secure. However, this issue is even more difficult, especially in E-IBsingautre systems, since each attribute is conceivably shared by multiple users (It refer to such a collection of users as an attribute group). Another challenge is the key escrow problem. In the key authority generates private keys of users by applying the authority's master secret keys to users' associated set of attributes. The last challenge is the organization of attributes issued from different authorities. When multiple authorities control and trouble attributes keys to users separately with their entity master secrets, it is very hard to define fine-grained entrée policies over attributes issued from different authorities.

V. SYSTEM METHODOLOGY

The authority can be the registration office in a university, the human resource department in a company, etc. The data vendor defines the entrée policies and encrypts data according to the policies. Each user will be issued a secret key reflecting its attributes. A user can decrypt the data only when its attributes gratify the access policies. They primary offer a revocable multi authority system, where an efficient and secure revocation method is planned to explain the attribute revocation problem in the system.

5.1 PROPOSED METHODOLOGY

The advantages over the offered system use an identity tree as an alternative of key tree in our scheme. Each node in the identity tree is linked with an identity. The leaf node's identity is consequent to the user's individuality and the intermediate node's identity is generated by its children's identity. Hence, in an personality tree, an intermediate node represents locate users in the sub tree rooted at this node. They propose a novel multi-cloud Authentication protocol, namely IBE, including two schemes. The basic scheme (IBE) eliminates the connection among data's and thus provides the perfect resilience to data security, and it is also efficient in terms of latency, computation, and communication overhead due to an capable cryptographic ancient called batch signature, which supports the authentication of any number of Data simultaneously. They also present an enhanced scheme combines the basic scheme with a data filtering mechanism to the DoS impact while preserving the perfect resilience to data security.

The keys used in each subgroup can be generated by a group of E-IBsingautre on Multi cloud storage Key Generation centers (IBE) in parallel. The entire the members in the equal subgroup can calculate the same subgroup key although the keys for them are generated by dissimilar KGCs. This is a desirable feature especially for the large-scale network systems, because it minimizes the problem of concentrating the workload on a single entity.

Data Format Independence PDP schemes put no restriction on the format of the data in exacting files stored at the server do not have to be encrypted. This feature is very relevant ever since..Prime order group variant PDP schemes can potentially be modified to work within a group of a publicly-known prime order q. In this case, however, file blocks (seen as integers) must be less than q, otherwise the server could simply store them reduced modulo q. In a prime-order setting, network communication is further reduced (particularly in the elliptic curve setting), but pre-processing becomes more expensive given the small size of the file blocks. In contrast, the RSA setting allows us to work with arbitrarily large file blocks. Multiple Files have described PDP schemes for the case when a client stores a single file F on the server. In the TagBlock algorithm, for every block mi the client computes a tag over the tuple (Wi ,mi).

They highlight that the values Wi cannot be reused. Since Wi is obtained by concatenating a secret value v with i, this implies that the indices i must be unusual across all tags. In additional words, the client should not use the same index double for computing tags. This condition holds because in our scheme an index i is simply the position of the block mi in the file. In order to store multiple files on the server, the client must guarantee that indices used to calculate tags are different not only across the tags corresponding to the blocks of each file, but also across the tags related to the blocks of all files. One simple method to achieve this is to prepend the file's identifier to the index. For example, if the identifier of a file F = (m1,... ,mn) is given by id(F), then for each block mi , $1 \leq i \leq n$, C computes the tag (Tid(F)‖i,mi , Wid(F)‖i) ← TagBlock(pk,sk,mi , id(F)‖i). The uniqueness of indices is ensured under the assumption that each file has a unique identifier. Another simple way to ensure that indices are only used once is to use a global counter for the index, which is incremented by the client each time after a tag is computed.

Protocol steps perform the same computation. It generates data at as regards 433 KB/s on average. The preprocessing performance of B-PDP differs from the challenge phase even though both steps compute the exact same signature. This is because the client has access to φ(N) and can reduce the file modulo φ(N) before exponentiation. In contrast, the security of the protocol depends on φ(N) being a secret that is unavailable to the server.

The preprocessing costs comprise a single exponentiation and computing a modulus against the entire file. E-PDP also exponentiation data that was reduced modulo φ(N) but does not reap the same speed up, because it must do so for every block. This creates a natural trade-off between preprocessing time and challenge time by varying the block size; e.g., the protocol devolves to B-PDP for files of a single block. They choose a block size of 4K in order to minimize the server's effort. Given the efficiency of computing challenges, pre-processing represents the limiting performance factor for E-PDP. The rate at which clients can generate data to outsource bounds the generally system performance perceived by the client. However, there are several justifying factors. Outsourcing data is a one-time task, as compared to challenging outsourced data, It will be done repeatedly. The process is completely parallelizable. Each file can be processed independently at a different processor.The single file can be parallelized trivially if processors share key material.

5.1 ADVANTAGES OF PROPOSED SYSTEM

Once the design is over it is need to decide which software is suitable for the application. As the security of a single cloud is concerned, it fails to provide a strong protection layer against the malicious attacks. So, there is always a risk of data unavailability in system failure. A movement towards of "multi clouds" or "multiple clouds" or "cloud-of-clouds" has emerged currently using Secret Sharing Algorithm implementation E-IBsingautre secret sharing algorithm is performed to authenticate a unique user and to access a particular file from the cloud storage.

5.3 MODULES

1. Multi cloud Group Member Registration & Login
2. Efficient Key Generation & Controller Using IBE
3. Upload File to Data Multi Cloud Server
4. Download File from Data Multi Cloud Server
5. Public Auditing with User Revocation in Public Verifier

MULTI CLOUD GROUP MEMBER REGISTRATION & LOGIN : In this module the first User entered his username, password, and chooses any one group id then register with Data Cloud Server. This user is added in this particular group. Then entered time this username, password and choose his group id for login.

EFFICIENT KEY GENERATION & CONTROLLER E-IBSIGNATURE : In Key Generation module, every user in the group generates his/her public key and private key. User generates a random p, and outputs public key and private key. Without loss of generality, It assume user u1 is the original user or somebody creator of shared data. The original user also creates a user list (UL), which contains ids of all the users in the group.

UPLOAD FILE TO DATA MULTI CLOUD SERVER : In this module the user wants to upload a file. So It split the files into many blocks. Next It encrypt each blocks with public key.

DOWNLOAD FILE FROM CLOUD SERVER : In this module the next user or group member wants to download a file. So It gives the filename and gets the secret key. Then entered this secret key .

PUBLIC AUDITING WITH USER REVOCATION IN PUBLIC VERIFIER : In this module, by using the idea of alternate resignatures, one time a user in the group is revoked, the Data Cloud Server is able to leave the blocks, which were signed by the revoked user, with a resigning key.

VI. RESULTS

Thus, E-IBsingautre generates proofs faster than the disk can deliver data: 1.0 second versus 1.8 seconds for a 64 MB

file. At 99% confidence, E-IBsingautre can build a proof of possession for any file, up to 64 MB in size in about 0.4 seconds. Disk I/O incurs about 0.04 seconds of additional runtime for larger file sizes over the in-memory results and its to avoid malware users. Table 1 and 2 shows the malware

Algorithm	Over all Accuracy in percentage	Data malware integrity per block(for 100 percentage)
Existing (DDOS)	78	93
Proposed(E-IBSINGAUTRE)	83	98

Table: 1 Existing and proposed work

Algorithm	Time in ms	File size in kb
Existing (DDOS)	4.5	2.5
Proposed(E-IBSINGAUTRE)	4.0	2.5

Table: 2 Overall Accuracy of DDos and comparison between existing and proposed

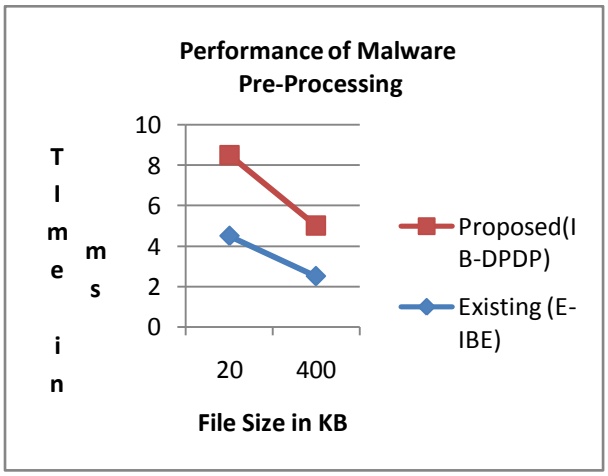

Figure 1: Existing and proposed approach

detection accuracy and overall performance of the proposed and existing system.

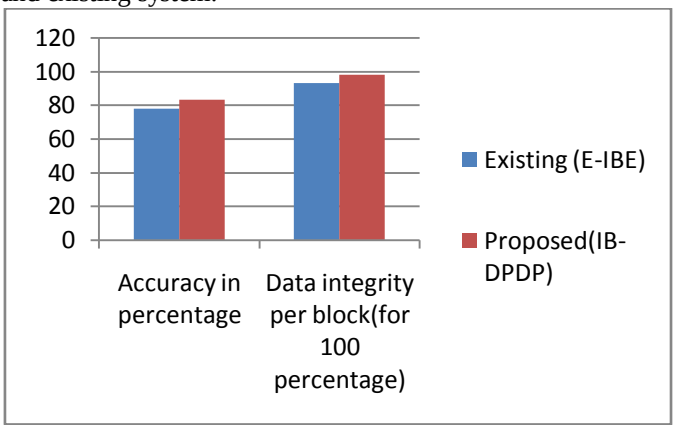

Figure 2: Existing and proposed approach

VII. CONCLUSION

The focused on the problem of verifying if an untrusted server stores a client's data. This method introduced a model for provable data possession, in which it is desirable to minimize file block accesses, computation on the server, and the client server communication. The security and efficient storage of proof protocol, also can delegate or authorize others to public verifiability whether the data actually stored in the cloud storage devices.

VIII. REFERENCES

[1] Y. Amir, Y. Kim, C. Nita-Rotaru, and G. Tsudik, "On the performanceof group key agreement protocols," ACM Trans. Inf. Syst.Secur., vol. 7, no. 3, pp. 457–488, Aug. 2004.

[2] D. Augot, R. Bhaskar, V. Issarny, and D. Sacchetti, "An efficientgroup key agreement protocol for ad hoc networks," in Proc. 6thIEEE International Symposium, World Wireless Mobile Multimedia Networks, 2005,pp. 576–58

[3] A. Beimel and B. Chor, "Communication in key distributionschemes," in Proceedings.Advances in Cryptology, 1994, vol. 773, pp. 444–455.

[4] R. Blom, "An optimal class of symmetric key generation systems,"in Proceedings Advances in Cryptology, 1984, vol. 209, pp. 335–338.

[5] D. Boneh and M. K. Franklin, "An efficient public-key traitor tracing scheme," in Proceedings Advances in Cryptology, 1999, vol. 1666, pp. 338–353.

[6] D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," in

[7] D. Boneh, A. Sahai, and B. Waters, "Fully collusion resistant traitor tracing with short ciphertexts and private keys," in Proceedings,25th International Conference of Theory Application Cryptographic Technology, 2006, vol. 4004, pp. 573–592.

[8] D. Boneh and M. Naor, "Traitor tracing with constant sizeCipher text," in Proc. 15th ACM Conference Computer Communication Security, 2008,pp. 501–510.