IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 33-37
www.iosrjournals.org

Traceable Cipher Text-Policy Attribute-Based Encryption Using White-Box

R.vidhya
M.E. Computer science and Engineering
M.A.R College of Engineering and Technology

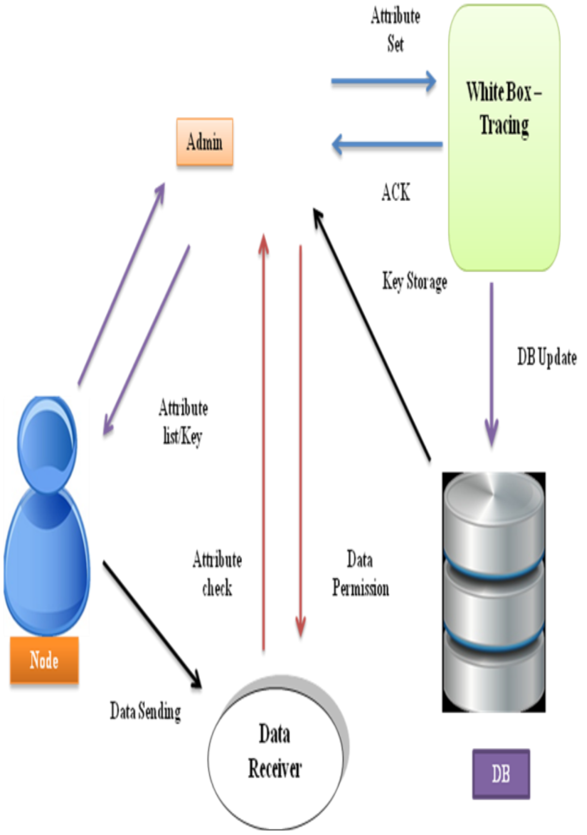
Abstract: The escalation of network security, day-by-day there are many encryption schemes has been come. Belongs to one of them is Attribute-Based Encryption (ABE) system, it is used for more sensitive data is stored by third party websites on the internet,(such as e-mail stored on website in yahoo,google,etc.,)there will be need to encrypt data and gave private key to the individual users for decrypt the data.Secondly,there is another policy has been came it is Cipher text-Attribute-Based Encryption(CP-ABE)technique, encrypted data can be kept confidential even if the storage server is untrusted.It is act against the collusion attacks. But in this (ABE) and (CP-ABE) there will be a drawback of giving private key to other users with the same set of attributes other than the original users persuade to seep out the data and decrypt the data. So the secret was not maintained efficiently, it may not be always possible to mark out the original key users. So this problem rigorously limits the applications of (CP-ABE).[1] I proposed a policy of Traceable Cipher text- Policy Attribute-Based Encryption (T-CP-ABE) systems have been proposed to tackle this problem, but the articulateness of policies in those systems, where only AND gate with wildcard is now supported, and accessed in any monotone access structures. Before that non-monotonic access structure was handled. So the number of intrusion, worms attacks has being caught, so the security was now maintained efficiently. But currently available, that is, this work adds traceability to an existing expressive, efficient, and secure CP-ABE scheme, without declining its security.

Key terms: Cipher text, Traceability, Monotone access, Attribute-Based Encryption.

I. INTRODUCTION

Traditionally, access-control mechanisms have been enforced by a server that acts as a trusted reference monitor; the monitor will allow a user to view data only if his access policy allows it. While the use of trusted servers allows for a relatively straightforward solution, there is a large downside to this approach both the servers and their storage must be trusted and remain uncompromised. With the increasing number of worm attacks and other forms of intrusion, maintaining the security of any particular host is becoming increasingly difficult. This problem is exacerbated in larger systems where sensitive data must be replicated across several servers because of scalability and survivability concerns.[4] A natural solution to this problem is to encrypt stored data in order to reduce data vulnerability in the event that a storage server is compromised. However, traditional public-key encryption methods require that data be encrypted to one particular user's public key and are unsuitable for expressing more complex access control policies. Recently, addressed this issue by introducing the concept of Attribute-Based Encryption (ABE). In Attribute-Based Encryption an encryption will associate encrypted data with a set of attributes.[3] An authority will issue users different private keys, where a user's private key is associated with an access structure over attributes and reflects the access policy ascribed to the user. The original ABE construction is somewhat limited in that it only permits an authority to issue private keys that express threshold access policies, in which a certain number of specified attributes need to be present in the cipher text in order for a user to decrypt., greatly increased the impressibility of Attribute-Based Encryption systems by creating a new ABE scheme in which users' private keys can express any monotone access formula consisting of AND, OR, or threshold gates. While the work is a large step forward in the capability of Attribute-Based Encryption systems, one fundamental limitation of their techniques is that there is no satisfactory method to represent negative constraints in a key's access formula. This is particularly a problem in scenarios where conflicts of interest naturally arise. Consider the following example. A university is conducting a peer-review evaluation, where each department will be critiqued by a panel of professors from other departments. Bob, who is a member of the panel this year from the Biology department, will need to read (possibly sensitive) comments about other departments and assimilate them for his written review. In an Attribute-Based Encryption system the comments will be labeled with descriptive attributes. Distributed Attribute-Based Encryption (DABE) to mitigate this problem. DABE allows an arbitrary number of authorities to independently maintain attributes. There are three different types of entities in a DABE scheme: a master, attribute authorities and users. The master is responsible for the distribution of secret user keys. However, in contrast to standard CP-ABE schemes, this party is not involved in the creation of secret attribute keys; the latter task can independently be performed by the attribute authorities. Attribute authorities are responsible to verify whether a user is eligible of a specific attribute; in this case they distribute a secret attribute key to the user. In distributed attribute based encryption every attribute is associated with a single attribute authority, but each attribute authority can be responsible for an arbitrary number of attributes. Every attribute authority has full control over the structure and semantics of its attributes. An attribute authority generates a public attribute key for each attribute it maintains; this public key is available to every participant. Eligible users receive a personalized secret attribute key over an authenticated and trusted channel[6]. This secret key, which is personalized to prevent collusion attacks, is required to decrypt a cipher text. Users can encrypt and decrypt messages. To encrypt a message, a user first formulates his access policy in the form of a Boolean formula over some attributes, which in our construction is assumed to be in Disjunctive Normal Form (DNF). The party finally uses the public keys corresponding to the attributes occurring in the policy to encrypt. In DNF, all negations are atomic, so attribute authorities should be able to issue negative attributes as well in order to make use of the full expressive power of DNF formulas. Here, (T-CP-ABE) two authorities, one for generating tracing information and the other one for issuing decryption keys to users, while no single authority is able to independently generate decryption keys.

I. System Architecture



I Node Endorsement and Connected Phase

This module contains the nodes and the administrator authentications. The admin will have permission to view the entire processes done by the user. The nodes can enter only the authenticated process after getting registered to the approach. Nodes can view their personal information and the data which sent by him. In the receiver's module have the static and secure login to enter and starts the receiving of data. The network has divided by workgroups. This module will help us to get the connected and the active systems in the network.

After getting login to our process, this module will get the connected systems and shows to the users.The user can select the system to deliver their data by file transfer. The disconnected and the shutdown systems are not visible in the list. All the data transactions and intruder information are forward to the administrator. The administrator can view all the reports and monitor the network paths. The whole histories of data are maintained by the administrator. So that, the administrator can able to make the denial of service of the intruder from the reports module. This proposed work contains two step authorities. There are two authorities, one for generating tracing information, and the other one for issuing decryption keys to users, while no single authority is able to independently generate decryption keys.

II. CONVERSION AND DATA FORWARDING PHASE

After the successful chosen of attribute selection, node has to transfer the data which is to be forward to destinations based on the attributes. The data will encrypt before it transmit. The encryptions will takes strategies belong to plain text conversion.

The encryption algorithm takes as input the public parameter, an access policy over, and a message. It will output a cipher text such that only the users whose decryption keys satisfy should be able to extract. The node has to select the attributes of receiver's to transfer the data and the file to be transferred. The selected file will be encrypted for secured transfer. When the data received by the desired path of destinations, the key automatically enabled and decrypted. When the node starts the process, the proposed work will initiate automatically to find distance and the malicious nodes. In our process, we have to monitor the client data, which are sent to the receiver's with a certain path. After the intruder affects the current data, there is no use of reports. So here, we trace back the path of every data information. Tracing the path of the data from one end to another end. The trace backing schema will Report to the sender side, when the data information path getting differ from the desired paths

III. DETECTION AND PREVENTION PHASE

A novel **Hidden Markov Model** (HMM) for computing behavioral distance, and present the design, implementation, and evaluation of a novel architecture using HMM-based behavioral distance to detect attacks. An HMM models a doubly stochastic process; there is an underlying stochastic process that is not observable (it is "hidden") but that influences another that produces a sequence of observable symbols. When applied to our problem of computing behavioral distance, the observed symbols are process behaviors, and the hidden states correspond to aggregate tasks performed by the processes (e.g., read from a file). An interesting and important observation is that since these hidden tasks should be the same, it should be possible to reliably correlate the simultaneous observable behaviors of the two processes when no attack is occurring, and to notice an increased behavioral distance when an attack succeeds on one of them. Perhaps surprisingly, our technique uses a single HMM to model both processes simultaneously, in contrast to traditional uses of HMMs for anomaly detection, where an HMM models a single process.

Detection

Identify the normal packet and attack packet. For the purpose of identification, we calculate attribute based encryption.

Prevention

To prevent attack if NE value is less then threshold, then simply drops all packets containing the same path for particular time interval. In order to detect malicious attacks, we should continuously monitor attributes values sequentially per every monitoring interval, called window size. Thus, each attributes value should be calculated with respect to each fixed moving average window. There are variants of the simple moving average method. We will use the simple moving average, since we assume the traffic packet arriving is identically and independently distributed, memory less, and a stationary process. The Figure 2.2.1 shows the concept of attack monitoring with simple moving average with size k. Assume we monitor the attributes values for m intervals (i.e., window size of k). If we have a monitoring interval of t seconds, we monitor the attributes value for m×t seconds. In every monitoring interval t, an attributes value is computed.

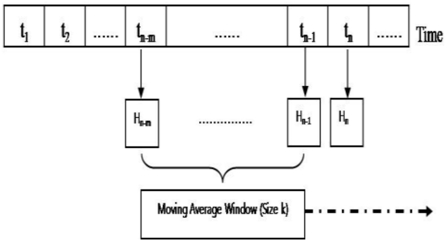


FIG 2.2.1 Attack Monitoring of Window Size

Once a comparison is done, the Moving Average Window will be moving forward along with time evolution (μi will start at tn-m+1).

IV. COMPUTING TRACEABILITY PHASE

The trace back requests to the routers in set A respectively and deliver the confirmed zombies information, set A, to the victim. Whenever the attack strength is less than seven times of the normal flow, low rate detection algorithm is used to detect the attack. There are two algorithms in the proposed trace back suite, the local flow monitoring algorithm and the trace back algorithm. The local flow monitoring algorithm (hypothesis) is running at the no attack period, accumulating information from normal network flows, and progressing the mean and the standard variation of flows. The progressing suspends when a attack is ongoing, Once a attack has been confirmed by any of the existing detection algorithms, then the victim starts the trace back algorithm. The trace back algorithm is installed at routers. It is initiated by the victim, and at the upstream routers, it is triggered by the user's trace back requests from the victim or the downstream routers which are on the attack path. The proposed algorithms are independent from the current routing software; they can work as independent modules at routers. As a result, I do not need to change the current routing software.

A. Our Techniques Detection Procedure:

Calculate attributes on receiver proxy server:
H (X) = -P (xi) log P (xi) Where P (xi) = (Number of attack or normal packet)/ Total No of Packet. Normalized attributes NE = H/log n0 Where n0 = no of source node in particular Time Interval. IF NE < threshold (Δ) identify suspected attack.
Let's define as follows:μi: i-th average of Moving Average Window σ: Standard Deviation of Hn-m ~ Hn-1 with μi Di: absolute value of difference between μi and Hn (i.e., Di = | μi - Hn |) β: threshold multiplication factor, positive integer value (default μ = 3) ω: threshold (ω = β * σ)Once μi is computed, it will be compared with Hn. To detect a traffic pattern change, if Di ≥ ω, we decide that we have an attack (under an attack) in the current monitoring interval n.

Trace Back Algorithm

Initialize set A=ϕ, and obtain local parameter of C and ζ;Let U={ui}, i _ I be a set of upstream routers, D={di}, i _ I be a set of destinations of the packets and V be the victim. Define attack flows fi=<uj,v>, i=1,2,…n,uj _ U, and sort the attack flow in the descent order and we have f1,f2,…fn For i = 1 to n where calculate H(F\fi) if (|H(F)-C|> □) then append the responding upstream router of fi to set A. Submit trace back requests to the routers in set A respectively and deliver the confirmed zombies information, set A, to the victim. Whenever the attack strength is less than seven times of the normal flow, low rate detection algorithm is used to detect the attack.

V. RELATED WORKS

A new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE).[1] Fine-grained access control systems facilitate granting differential access rights to a set of users and allow flexibility in specifying the access rights of individual users. Several techniques are known for implementing fine grained access control. Common to the existing techniques and the references there in is the fact that they employ a trusted server that stores the data in clear. The effectively eliminates the need to rely on the storage server for preventing unauthorized data access. Some techniques create user hierarchies and require the users to share a common secret key (SSS) if they are in a common set in the hierarchy. . We also propose an extended version for our Traceable CP-ABE system. In this extension, there are two authorities, one for generating tracing information, and the other one for issuing decryption keys to users, while no single authority is able to independently generate decryption keys. This extended system can therefore, reduce the trust on each individual authority, and this technique can viewed to be orthogonal to that of using threshold policy between multiple authorities.

VI. CONCLUSION AND FUTURE WORK

In this work, a Traceable CP-ABE system is that achieves a similar degree of high quality, potency and security level mutually of the simplest existing (non-traceable) CP-ABE systems. Specifically, given a decipherment key, the tracing algorithmic program is ready to seek out the key owner, and also determine a malicious key owner who leaks his decipherment key for no matter motivation. This method is the first traceable CP-ABE system that supports any monotone access structures and achieving security within the commonplace model. The cost of achieving traceability in our system is additionally terribly low and more secure to data travel in network. And to trace out the route of the users.

REFERENCES

[1]. V.Goyal,O.Pandey,A.Sahai,and B.Waters,”Attribute-based encryption for fine-grained access control of encrypted data “in Proc.ACM conf. Computer and Communication Security, A.Juels, R.N.Wright, and S.D.C. di Vimercati,Eds., 2006,pp,89-98,ACM

[2]. R.Ostrovsky,A.Sahai,andB.Waters,”Attribute-based encryption with non-monotonic access structures “in Proc.ACM conf. Computer and Communication Security, P.Ning, S.D.C. di Vimercati,Eds.,and P.F.Syverson,Eds.,2007,pp.195-203,ACM.

[3]. A.Sahai and B.Waters,”Fuzzy identity-based encryption,” in proc.EUROCRYPT, R.Cramers, Ed., 2005, vol.3494, pp.457-473, ser.Lecture Notes in Computer Science, Springer.

[4]. D.Boneh and M.K.Franklin,”Identity-based encryption from the weil pairing “in Proc.CRYPTO, J.Kilian, Ed., 2001, vol.2139, pp.213-229, ser.Lecture Notes in Computer Science, Springer.

[5]. A.Shamir,”Identity-based cryptosystems and signature schemes, “in Proc.CRYPTO, 1984, pp.47-53.

[6]. J.Bethencourt, A.Sahai, and B.Waters,”Cipher text-policy attribute –based encryption “, in Proc.IEEE Symp.Security and Privacy, 2007, pp.321-334.

Vidhya.R received the MCA degree in computer science and its applications from Anna university tiruchirapalli in 2011...She is currently doing the M.E. degree under the Anna university Chennai. Her primary research interest is cryptography, in particular, encryption and signature schemes, and anonymous systems. she is also interested in other topics in information security, such as network security, wireless security, database security, and security in cloud computing.