MULTILEVEL ACCESS CONTROL USING SYMMETRIC POLYNOMIAL BASED DOMAIN KEYS IN APPLIED CRYPTOGRAPHY

V. Joseph Emmanuvel [1]* , *E.J. Thomson Fredrik*[2]

ABSTRACT

The techniques of Cryptography for Multilevel Access Control have made concentrated research wellbeing's newly. A bulky number of key administration methods are on the basis of single method functions. Furthermore, lots of these proposals are established with dissimilar types of troubles in conditions of arrangement, safekeeping, competency and dynamics. Here, a novel key organization scheme has been suggested which is used to control the access in positive orders. This suggested strategy is on the basis of secret distribution postulate without using a single mode function possessing the subsequent properties of extending support. Before the access control, authentication has to be established regarding the identity of the entity. If a procedure is followed where in the authentication and the access control goes side by side, it will be an efficient one particularly in Large Group communications which are spread across different domains. As data goes through a large insecure media, the use of domain keys to assure that data is from the entity from whom we wish to receive the data is indeed a boon for transmitting highly confidential data. For providing the secure key exchange among the members of a particular service group, a symmetric polynomial based approach is used. It is combined with Domain key to provide confidential Access. The signature of the sender domain is verified by the receiver domain usually by querying the domain name server for getting the public key and in turn establishes the identity of the domain so that the communication becomes secure, fast and reliable. The process has to be extended to make the signer determine the access level by issuing the group key pertaining to a meticulous service group. The fewer amounts of calculations make probable much more dense implementations for a given level of security, i.e., faster cryptographic operations running on smaller chips.

Index Term : Multicast, Domain keys, Access Control, Group Communication, Symmetric Polynomial.

I. INTRODUCTION

The development in the communication networks plays a very important role for developing of wireless and Internet applications that makes people to converse among themselves. In future, group-relevant functions will provide vital services that make easy real-time information swap over in the midst of a large number of users. In all group-relevant functions, primary assurance is information safety. Domain Key verifies the message is sent by the person indicated on "From" address. There are ways to put any "From:" address in an email message. For example, using some tools anybody can send mail from bill.gates@microsoft.com. Now a domain key verifies if the originating mail server is microsoft.com and if the sender is actually bill. Gates. Thus, when we see "Domain key verified", it's a guarantee that the email "From:" address is correct and legitimate.

In this paper, the domain key concept is used for providing secured access control among users of multiple domains subscribing to a particular set of services. A Symmetric Polynomial oriented construction has been proposed here that facilitates well-organized and protected access control by having the domain controller to issue the variables of the polynomial to the users. Key is computed and it is seen that higher level nodes can derive the lower-level keys. When communication extends between different domains, the signature of the domain is attached. The Diffie-Hellman protocol is used here. The domain controller encrypts this group key with the public key which it shares with the other domains to establish that it is indeed an authorized signatory. This procedure demonstrates that the suggested technique achieves protected, Scalable and resourceful access control.

[1]Department of Computer Science,
Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
[2]Department of Computer Application,
Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
* Corresponding Author

The rest of the paper deals with related work, the design of the system for the suggested Domain key based Multilevel Access Control Using Symmetric Polynomial, explains the use of Symmetric Polynomial for key derivation presents experiments results, the analysis and at the nutshell concludes the paper and future work.

II. RELATED WORK

Access control: When two equipments are joined to the identical link, data protocols are necessary to determine which equipment has control over the link at any possible time. It preserves security against unwanted access to information. It is very extensive and can engage reading, writing, modifying and processing. Several methods are utilized by the user to have access right to the data or resources being the owner of a function. When there are no proper security measures for a data at the receiver's end then the data is discarded. While people step into or leave a group, just the keys can be changed. A quantity of solutions for hierarchical access control has previously been proposed [4, 5, 6, 7, 8 and 10].

Correspondingly, a simple efficient scheme is suggested for dealing with this. This paper uses symmetric polynomial approach which is most suitable for busty operation and builds a secure access control model using domain keys.

III. SYSTEM DESIGN

In this section an overview of multilevel access control including the security model has been proposed.

A. Access control using symmetric polynomial based domain key

The above said method should assure the security requirements such as the users in the service group only can access the resources, prevent new members from accessing past data and prevent past members from accessing present and future information. The focal point of this work is to answer the Multi level access control problem professionally using domain keys by making use of symmetric polynomial. The following system setup is used as in figure [1].

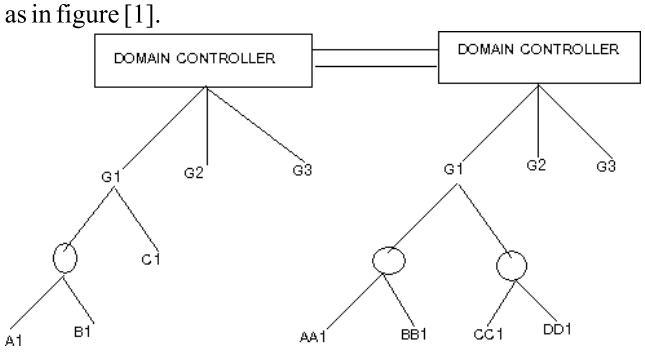

Fig. 1. System Setup

G1, G2 & G3 represents different service groups. These service groups may be under different domains. A1,B1,C1 are the users with similar subscription under Domain 1 and AA1,BB1,CC1 are also having the same subscription in a different domain. The safe access control among various domains is maintained by utilizing domain key signature. The users in a group are maintained by using the symmetric polynomial. The Components of the Domain controller is given below in Figure [2].

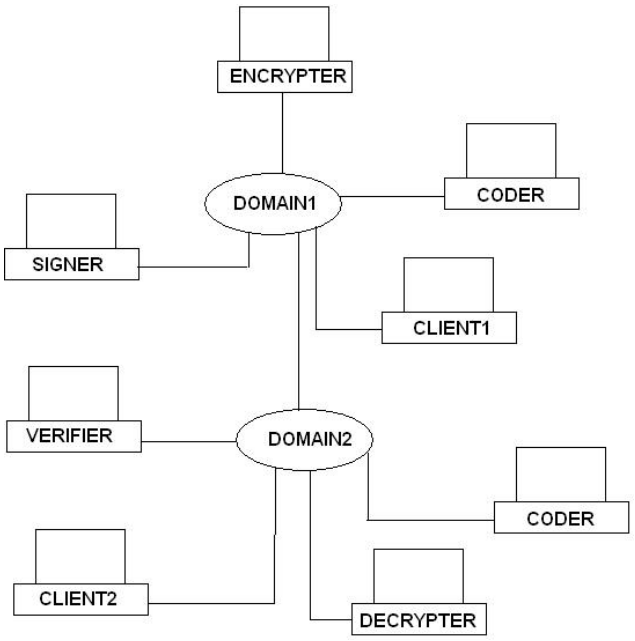

Fig. 2. Domain Controller

components in the Domain Controller Client1
Client1 is software which works as follows

- It accepts users' commands and functions accordingly.
- If the user is a normal user, he will be allowed to compose ordinary messages and the message will be forwarded by this software to the SIGNER.
- In case he is the administrator he will be allowed to compose service message and ordinary message which is forwarded to SIGNER.
- It also allows the new user to sign up.

Client2
Client2 is software which works as follows

- It accepts users' commands and functions accordingly.
- It allows users to request message to the SIGNER.
- If SIGNER. has the message in the inbox, the message is sent and this software allows users to read the message
- It allows the user to report a message to be a spam and this report is received by the SIGNER

Encrypter
This module functions as follows

- It receives the text strings from the SIGNER.
- Then it fetches the key to be used from the database.
- The key fetched is used to encrypt the text. The Key will be generated.
- Then it returns the encrypted text to the SIGNER for further processing

Decrypter
This module functions as follows

- It receives the text strings from the VERIFIER
- Then it fetches the key to be used from the database.
- The key fetched is used to decrypt the text.
- Then it returns the encrypted text to the VERIFIER for further processing.

Signer
This module functions as follows

- It receives the message from the clients.
- It uses this message and passes to the ENCRYPTER, then the returned string is sent to the coder.
- CODER sends the key of RSA and the encrypted hash.
- Then the hash is sent to the destination VERIFIER to verify the message.
- The signer also presents the user with the message whenever they request to view the message.
- Accepts the spam reports and records it as desired.

Verifier
This module functions as follows

- It receives the message from the SIGNER.
- Sends the message to the coder, so that the message's hash value is computed which it compares with the one sent by the SIGNER.
- Then, it decrypts the entire message, with the help of

DECRYPTER.

- It takes care of saving the message in the inbox.
- It subscribes and unsubscribes services on behalf of users getting information about access level.

Coder

- It receives the message from the SIGNER and codes it to the required hash.
- It receives the message from the VERIFIER and codes it to the required hash.

The symmetric polynomial is secret information to identify all members belonging to a particular service group or particular hierarchy. Whenever there is a movement of a member from one service group to another, it will be taken care by the Domain Controller and new values will be generated and sent to various signer modules thereby providing secrecy. Users of a service group will be able to view only the messages intended for them and their descendents.

B. Suggested Signature Content

Because to maximize compatibility with more verifiers, it is suggested that signers follow the outlined here when signing a message. Anyway, these are generic recommendations which can be applied to general case; precise senders may desire to adjust these guidelines as required by their exclusive states of affairs. Verifiers should verify signatures even if one or more of the recommended header fields is not signed or if one or more of the not

recommended header fields is signed.

The below mentioned fields must be included in the signature [1, 2], if they are present in the communication being signed:

- From
- Sender & Reply To
- Theme
- Date & Message ID
- To & CC
- Return-Path
- Received
- Comments, Keywords

IV. SYMMETRIC POLYNOMIAL BASED SCHEME

A. Symmetric Polynomial

Polynomial F(x; y; z) is symmetric if F(x; y; z) = F(x; z; y) = F(y; x; z) = F(y; z; x) = F(z; x; y) = F(z; y; x):A polynomial in variables x1,…. xn is called symmetric which never changes when permuting the variables. It has excellent properties where using some variables the keys held by the descendents can be found out as explained below.

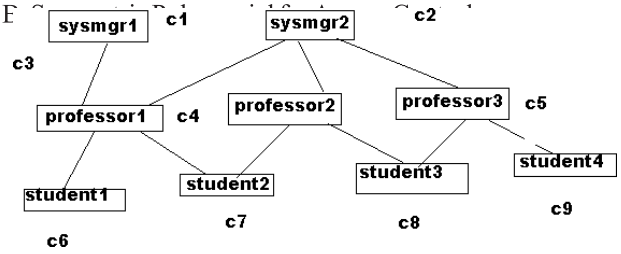

Fig. 3. An example Hierarchy

x3, x4, x5, x6, x7) with 7 parameters, then CA can compute nine polynomial functions for class Ci from the symmetric polynomial function P(x1, x2, x3, x4, x5, x6, x7). Once polynomial functions are got they are transmitted securely to every class Ci. For example, class C3 will have a polynomial function g3 (x4, x5, x6, x7) as

g3 (x4, x5, x6, x7) = P(s3, s1, s2, x4, x5, x6, x7).

since S3 = {C1,C2} and their associated numbers are s1 and s2. Also, another form of the polynomial function is

g3 (x4, x5, x6, x7) = P(s1, s2, s3, x4, x5, x6, x7).

as the symmetric polynomial function gives the same result no matter what order of si is used.

Key k3 is computed as

k3 = g3(s1′, s2′, s3′, s4′,) = P(s1,s2,s3, s1′, s2′, s3′, s4′,)

Also, another polynomial function for class C7 can be computed as,

g7(x6, x7) = P(s1, s2,s3,s4 ,s7 ,x6,x7)

because S7 = {C1,C2,C3,C4) and their associated numbers are s1, s2,s3,s4 .Key k7 is computed as

k7 =g7(s1′, s2′) = P(s1, s2,s3,s4 ,s7, s1′, s2′).

Class C7 cannot decide its parent C3's key, but class C3 can calculate its descendant C7's key. As we know that S 7/3 = {C4} since classes C1 and C2 are common ancestors needed to be excluded from set S 7/3 class C3 can compute key k7 as k7 = g7(s7, s4, s1′, s2 ′) = P(s1,s2,s3,s4, s7, s1′, s2′,) = g7(s1′, s2 ′) Class Ci performs key computation and key derivation in the same way. No matter where Ci's descendant is, the key derivation process is computed by using the same polynomial function gi with different si and si′, values substituted.

V. EXPERIMENTAL RESULTS AND DISCUSSION

Hence the experiments for computing the keys are implemented on a LENOVA laptop with the latest configuration and 2GB RAM under Windows XP using JAVA.

A. Results of Symmetric Polynomial based Access Control

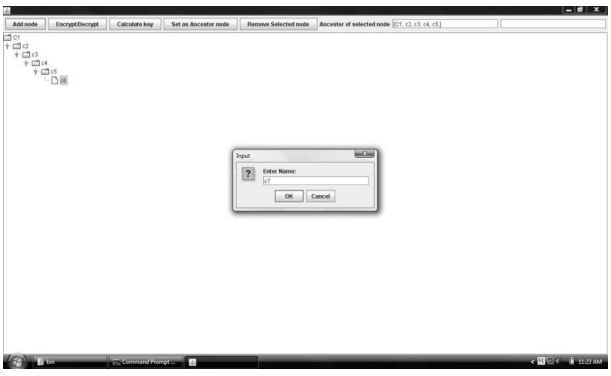

Fig. 4. Adding a Node

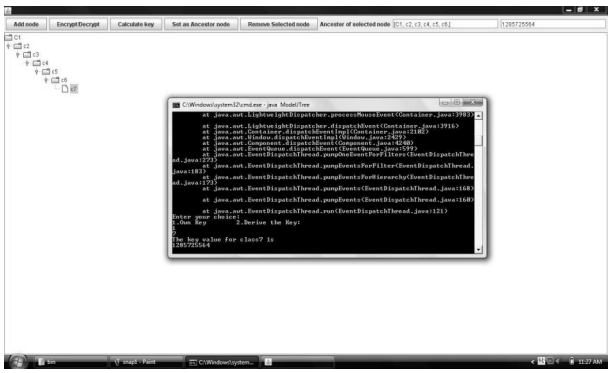

Fig. 5. Key Calculation

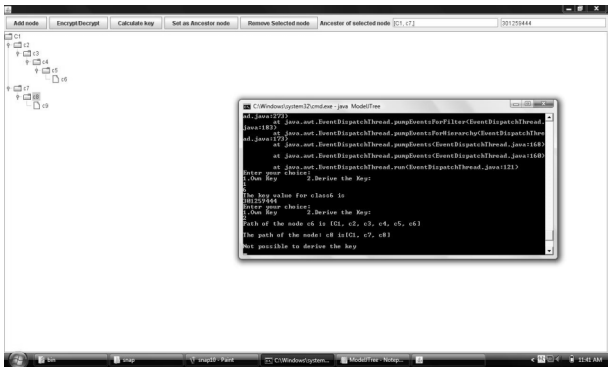

Fig. 6. Key Derivation

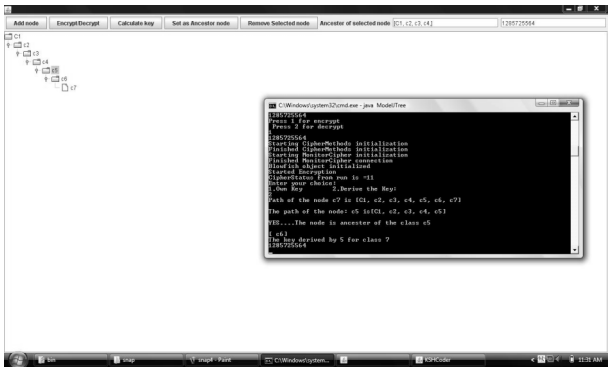

Fig. 7. Key Derivation not possible for low node

B. Results of Domain Key signing and verifying

1) Signer Process Window

The window below shows how the signer signs the message. The message is sent as split parts and hence the entire message is integrated into a single text and the hash is found which is then sent along with hash after encrypting it with the AES.

Fig. 8. Signer Process Window

2) Verifier Process Window

The verifier on receiving the message separates the message, computes the hash value and compares the hash with the hash sent and finally arrives whether the message has arrived with the integrity

VI. COMPLEXITY ANALYSIS

Each user ui will receive

$$g_i = f(s_i, x_2, \cdots, x_n) = g_i(x_2, \cdots, x_n) = \sum_{i_2=0}^{i_2=w} \cdots \sum_{i_n=0}^{i_n=w} a_{i_2,\ldots,i_n} x_2^{i_2} \cdots x_n^{i_n}.$$

Since f is symmetric and so is gi. The number of coefficients in gi is

$$\binom{n+w-1}{n-1}$$

The space requirement of each user is

$$\binom{n+w-1}{n-1}$$

A. Memory Costs

Using Symmetric Polynomial Based method takes very less memory, even when the members get increased.

B. Communication Costs

Using other schemes guzzle more bandwidth. The Communication of Symmetric polynomial is easy compared to other scheme as the same method can be used for key computation and derivation.

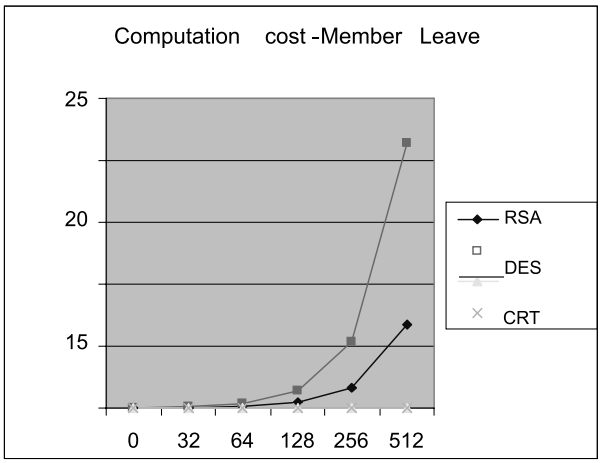

Fig. 10. Communication cost for Member Leave

The amount spend on communication is very much less when compared to ECDH and RSA based scheme. For member leave operation also, our approach takes less time as the variables are locally calculated compared to other approaches.

VII. CONCLUSION AND FUTURE SCOPE

A. Conclusion

Unlike a lot of available schemes based on single mode functions, the proposed method is on the basis of a secret sharing technique which creates the method secure. Key computation and derivation are the most used types of key operations. In the majority available techniques, derivation of the key is dissimilar from computation. The safeguarding check assures that a communiqué is bona fide. When single information is processed like alarm, then it is clearly pictured that t the same is from a single foundation. Hence efficiency to derive a key may be improved. In the event of a continuing communication, like joining of a node to a hub, two features are implicated. The first is at initiating the connection and the second ensures that the association is not obstructed by all means. Here confidentiality plays a major role. As far as data transmission is taken into consideration, plenty of levels of security are implemented here.

This paper successfully uses the Domain key concept and makes a convenient tool for access control across groups that are spread across multiple domains. The paper aims at availing the three important properties of any information such as Confidentiality., Availability and Integrity.

B. Future Scope

"Nothing is invented and perfected at once". There is always a room for improvement. In the future, a better key sharing mechanism may be created so that the distribution of the key will be easy. The certificate authority which delegates the key by itself, if developed makes the paper even better.

REFERENCES

[1] Barry Leiba, Jim Fenton "DKIM: Using Digital Signatures for Domain Verification" CEAS 2007- Fourth conference on Email and Anti-spam,, pp 530-538 August 2007.

[2] J.Fenton,M.Thomas ," Identified Internet Mail", Internet Engineering Task Force , 2005

[3] W. Stallings, editor. Network and Internetworking Security. Prentice Hall,Upper Saddle River, NJ, 1995.

[4] S. G. Akl and P. D. Taylor. Cryptographic solution to a problem of access control in a hierarchy. ACM Transactions on Computer Systems, 1(3):239{247, March 1983.

[5] G. C. Chick and S. E. Tavares. Flexible access control with master keys. Advances in Cryptology: CRYPTO '89 LNCS, 435:316{322, 1990.

[6] S. J. Greenwald. A new policy for distributed resource management and access control. Proceedings of the UCLA conference on New security paradigms workshops, pages 74{86, 1996.

[7] C. H. Lin. Dynamic key management schemes for access control in a hierarchy. Computer Communications, 20:1381{1385, 1997.

[8] S. T. Mackinnon, P. D. Taylor, H. Meijer, and S. G. Akl. An optimal algorithm for assigning cryptographic keys to control access in a hierarchy. IEEE Transactions on

Computers, 34(9):797{802, September 1985.

[9] G. Noubir. Multicast security. European Space Agency, Project: Performance Optimization of Internet Protocol Via Satellite, April 1998.

[10] R. S. Sandhu. Cryptographic implementation of a tree hierarchy for access control. Information Processing Letters,