Global Journal of Computer Science and Technology
Volume 12 Issue 1 Version 1.0 January 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

LH-Cipher: A Linear Hierarchical Cipher approach for Data

By M Sadanandam

Kakatiya University, Warangal

Abstract - Dividing the data into blocks and there by arranging the blocks in hierarchal order is termed as a linear hierarchical cipher approach for data .The encryption code, a access id code for each level based on the propagation code is generated in this technique. However the level propagation code and the access-id code of previous hierarchy level are matching with upper hierarchical level .The access-id code is set based on the time sensing key and a time seed, and the time seed updates with respect to the encryption pulse. By simply modifying and inversing the data security it is possible to decrease the number of key volume.

GJCST Classification: E.4

LH-Cipher: A Linear Hierarchical Cipher approach for Data

M Sadanandam

Abstract - Dividing the data into blocks and there by arranging the blocks in hierarchal order is termed as a linear hierarchical cipher approach for data .The encryption code, a access id code for each level based on the propagation code is generated in this technique. However the level propagation code and the access-id code of previous hierarchy level are matching with upper hierarchical level .The access-id code is set based on the time sensing key and a time seed, and the time seed updates with respect to the encryption pulse. By simply modifying and inversing the data security it is possible to decrease the number of key volume.

I. Introduction

With the growth in communication technology, there have been lot many positives but to counterfeit a lot many techniques to misuse this technology have also been growing. It is important to make data protected from all such malpractice [2]. Of all the methods of protecting the data, encryption is the most effective one. In this technique the data is simply hidden and later it is recovered by de-encryption.[1].to encrypt a data, a specific process or pattern is followed which may include mathematical operations, shifting and substitute techniques .after the data is encrypted it is termed as ciphertext [3].with the help of key based algorithms it is possible to encrypt the data and this key based encryption technique is classified as symmetric and asymmetric. The former uses only a single key for both encryption and de-encryption where as the later uses two different keys each for encryption and de-encryption. There are number of key based Encryption techniques viz. DES, RSA, Elliptic curve, and several other mathematical methods [4, 5]. The wireless communication systems have seen a rapid development in recent times as such Wireless Sensor Network, Bluetooth, zigbee are the most recent ones. The WSN finds its application in monitoring systems especially security concerns.

The WSN constantly sends the information about the state of the object being monitored to the control room that enables collection of related information.

II. Related Work

Multilevel cryptosystems saw a steady growth in recent times. The following are some of the proposed multilevel encryption methods explored in table 1.

The models [1, 2] provide multi level ciphering but the final result so obtained is not generic and databases specific .Linear hierarchical cipher based data encryption and decryption is generic and considers the heterogynous in each level to overcome the drawbacks of the proposed AES and elliptical curve method [3,4,5].

III. Linear Hierarchical Cipher Approach

To ensure data protection in wireless communication encryption is the best technique but today we have lot many users accessing different levels of data. A multi user system has an access to different data levels. For each level we have an encrypted key which is used to de-encrypt and access it. However as the number of levels increases it get difficult to manage with the multiple keys .Hence forth managing the encryption with key technique is termed difficult. It is important to know that the keys are changed every time and hence data security is still ensured .Since the keys used are to be changed each time both level-based keys and time-based keys are to be altered each time.

To resolve the above problem of managing both the time based and level based keys at a time a data encryption technique is explained in detail. As stated earlier the data is initially partitioned into different level. While encrypting the data a specific level we also consider the encryption code of the previous level .Thus the user can de-encrypt the data easily from the already de-encrypted data levels however the data security still holds good. This technique of managing data at various levels is called a linear hierarchical cipher based encryption technique.

Author : Assistant Professor of CSE, KU College Of Engineering, Kakatiya University, Warangal. Telephone: 919440448790, E-mail : sadanb4u@yahoo.co.in

Method	Proposed by	Special features
Multi level encryption	Zhou Yuping et al [1]	Encrypt the data system, table level and field level of objects
Multi level secondary storage	Chaitanya et al[2]	Flexible performance against security trade-offs
Multi level crpto disk(MLCD)		For generic storage devices
Multi level secure architecture	Sathiaseelan et al[3]	Integrated web services especially for academic institutions
Parallel AES algorithm	Deguang Le et al[4]	Fast Data Encryption on GPU to overcome the draw backs of CPU resource consumption.
ElGamal encryption and transmission scheme	Fu Minfeng et al[5]	It is based on elliptical based cryptosystem that aimed to improve ElGamal algorithm, ECC ElGamal encryption algorithm

Table 1 : Current State of the art in multi level encryption model

Firstly the data is divided into different levels and each level is related to at least one user. Then we encrypt each level by using the encryption key of each level based on the level propagation code and a access-id code of each level. However the level propagation code and the access-id code of one level are generated based on the level propagation code and the access-id code of previous level (the access-id code is produced based on the time propagation code and a time seed). The time seed has to be periodically altered. Then the encrypted data is transferred to the user. This method also includes the generation of encryption code for each level and also other authorized levels based on the level propagation and access id codes and then again decrypting the data at respective levels.

In the paper we elicit a new concept of linear hierarchical cipher based encryption considering a data storage and one encryption module. The data storage generates levels based on the different user approaching for the data access. This also produces the time propagation code, a time seed and a level propagation code based on the propagation codes of the previous levels. With the help of encryption key ,the encryption module encrypts the data with the help of time propagation code, the time seed, and the level propagation code of each level, and thus generates the access-id key (based on the accessed code of previous level) according to the time propagation key and the time seed. All the encrypted data is stored by the data storage. The decryption module finds the related encrypted data block in the related authorized level and then produces the encryption codes to access that level data block with the help of level propagation codes and access id codes .It then decrypts the encrypted data blocks with the help of the propagation level and access id codes which could be generated with the help of previous level codes The data storage also considers the variation in the encryption code with the time with the help of time seed and thus generates the access-id code for each level considering the encryption periods .

IV. Encryption Approach

- ➢ Divide data into multitude data blocks
- ➢ Generate access-id key of the highest level of the hierarchy
- ➢ Sequentially generate the access-id keys of the other levels of the hierarchy using FIPS-180-1 hash standard.
- ➢ Generate encryption key of the each hierarchical level based on level propagation and access-id keys of each level
- ➢ Encrypt the data block each level using corresponding encryption key
- ➢ Send encrypted data-block to data storage

V. Decryption Approach

- ➢ Authenticate the user according to user key and find user position in hierarchy
- ➢ if authentication succeed then
    - ▪ generate an access-id key for the hierarchy level of the user
    - ▪ send encrypted data blocks to the authorized levels
    - ▪ Encryption time and access-id key to the

decryption module.

- decryption module generates propagation keys for current level and other authorized levels of the hierarchy
- decryption module generates access-id keys of the authorized levels of the hierarchy by using access-id key of the current level
- Respectively decrypts the corresponding encrypted data-blocks according to the level propagation keys and access-id keys of the authorized levels by decryption module

VI. Emblematic Model of LH-Cipher

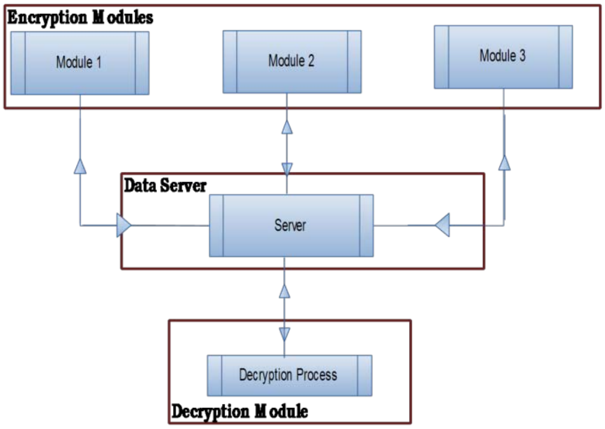

Figure 1 : schematic representation of LH-Cipher

Let us consider an Emblematic Model represented as fig 1, the linear hierarchical cipher system that includes three encryption modules, and data storage. In the selected emblematic model, the LH-Cipher implemented based on an ad hoc network. The considered Emblematic Model consist three nodes with encryption modules those serves as data collectors, and a control device that serves as data storage. In the Ad hoc network, the three nodes collect related data such as images around where they are disposed, and respectively encrypt the data through the first second and the third encryption modules and transmit the encrypted data to the control device that acts as data storage. Whenever required an eligible user can connect to the data storage through the network to read the data recorded therein. The operation of the Ad hoc Network is not in the context of proposal and therefore will not be discussed here. However, it should be understood that the LH-Cipher is not limited only to an ad hoc network; rather it may also be deployed in other constrained device communication environments, such as IEEE802.11 family standard device based networks.

The control device accepts the egress data of the encrypted modules as input and stores in data storage. A generic data access device with a database can be data storage.

As a part of its functionality the data storage controller groups the authorized users into multiple levels so as to manage these users and the data to be accessed by these users based on the users level. It is precise that a user of a level can access more data than a user of its lower levels. In other words, the users in upper level groups will have high end rights when compared to users in lower level groups. An upper level user can decrypt and access the data assigned to his group level and all lower group levels but it is not true in vice versa.

In order to manage the rights of preceding users of diverse levels, the data storage generates a level propagation key for each of the levels to encrypt the data. In particular, the level propagation key of a level is generated according to the level propagation key of its upper level so that the data can be managed based on the user levels.

Let consider that in the selected emblematic model, the data storage groups three different users u1, u2 and u3 into three levels, wherein the u1 belongs to the first level which has the highest right, the u2 belongs to a second level which has the second highest right, and the u3 belongs to a third level which has the lowest right.

The data storage randomly generate a group key $K_{(g)1}$ for the users of the first level that also considered as top level and then sequentially generates group keys $K_{(g)2}$, $K_{(g)3}$ for the other two levels through a fips-180-1 standard hashing technique, as shown below:

$$K_{(g)i} = F(h)^{l-1}(K_{(g)1}),$$

Where in $F(h)$ is a hash function and l represents the level (i.e. l=1..3). The Eq1 represents the FIPS-180-1 standard hashing function that is using to generate the group keys $K_{(g)2}$ and $K_{(g)3}$ of the other two level.

Next, the data storage respectively generates a level propagation key {$PK_{(m,l)}$, 'm' is node identification code and 'l' is level id.} for each level according to the group keys {$K_{(g)1}, K_{(g)2}, K_{(g)3} \ldots K_{(g)n}$} of the levels and an identification code of the encryption module through the fallowing function.

$$PK_{(m,l)} = f_{(e)}(K_l, m),$$

Wherein $f_{(e)}$ is the encryption function, and l represents the level id.

In the selected emblematic model, the encryption function is any standard encryption function of choice, as a part experimental results we opt to the advanced encryption standard (AES).

It should be mentioned that in the selected emblematic model, the node identification codes are used as one of the factors for generating the level propagation keys because a different level propagation key is provided to each of the node in selected network. However, if the situation of multiple nodes is not considered or every node uses the same level propagation then as an alternative the group key can be used as the level propagation key.

The data storage also generates a access-id key(A_k) and a time seed besides the level propagation keys. The access-id key(A_k) and the access time as seed are used for generating an access identification key(AI_k) for each encryption period. In the selected emblematic model, a different access identification key(AI_k) is used during each encryption period so that the data to be encrypted can have forward and backward data security. Therefore, a user with expired authorization unable to use his original key to access the data, and can avoid a new authoritative user from accessing data that encrypted in past.

For example, the data storage generates the access-id key{$A_{(k)m}$, m is device id} by using a primary key $K_{(p)}$ and an identification code of the wireless sensor through a sixth function. In the selected emblematic model, the encryption function used as shown below:

$$A_{(k)m} = f_{(e)}(K_{(p)}, m),$$

Wherein $f_{(e)}$ is the encryption function. In the selected emblematic model, the encryption function is an standard model of our choice.

Similarly, in the selected emblematic model, the identification codes of the nodes involved are used as one of the factors for generating the access-id key(A_k) because a different access-id key(A_k) is provided to each node involved. However, if the situation of multiple nodes is not considered or each of the nodes uses the same access-id key(A_k), the primary key $K_{(p)}$ can be directly used as the access-id key.

The data storage generates a user key for each of the users and assigns the user key $K_{(u)m}$ to the user while assigning the group key to the user. This user key will be generated with the help of fallowing equation represents an encryption function.

$K_{(u)m} = f_{(e)}(K_{(p)}, m)$, wherein m is user identification.

$K_{(u)m}$ is user key for user identified by m.

$f_{(e)}$ is any encryption function of choice

$K_{(p)}$ is primary key

m is user identification

The primary key $K_{(p)}$ of the data storage is generated randomly. Besides, the data storage generates a different access identification seed S_T corresponding to different encryption periods T. In the selected emblematic model, the S_T corresponding to the current encryption period is generated according to the $K_{(p)}$ and the other parameter of choice such as current date or timestamp.

As described above, all encryption modules are used for encrypting the data to be transmitted by corresponding nodes. The process of encryption fallows.

The first encryption module receives the access-id key(A_k), the time seed S_T, and the level propagation key {$K_{(L)l}$, l is level identifier} of each level from the data storage, wherein l represents the level. In the selected emblematic model, the data storage broadcasts a new time seed S_T at certain intervals to the all encryption modules to allow them to generate the access identification keys of the current encryption period T according to the new time seed and the access-id key. Access Identification Key can be generated using the fallowing function.

$AI_{k(m,T)} = f_{(h)} (A_{K(m)} , S_T)$, wherein $f_{(h)}$ is the hash function.

The process of AI_k generation is sequential, that is the first encryption module generates the access identification key of the second level according to the access identification key of the first level and finally generates the access identification key of the third level according to the access identification key(AI_k) of the second level.

The first encryption module divides a data to be transmitted into multitude of sub-data blocks corresponding to different user levels. In addition, the first encryption module generates an encryption key for each level according to the received level propagation key of the level and the access identification key(AIk) generated based on a new seed. Encryption key will be generated by using the fallowing function.

$$K_{(E)\ (m,l,t)} = f_{(h)} (K_{L(m,l)} , f_{(h)}^{\ l-1} (AI_{k\ (m,t)})),$$

Wherein $f_{(h)}$ is the hash function, and l represents the level and m represents the node id.

The first encryption module uses the encryption key $K_{(E)(1,L,T)}$ (wherein 1 is first node id and L=1..3) of each level for respectively encrypting the sub-data blocks.

If the first encryption module does not receive the new time seed but generates the access identification key(AI_k) by using the old time seed and encrypts the sub- data blocks by using the encryption key generated by using the old access identification key, the data storage determines the time seed after it receives the encrypted sub-data blocks and records the sub-data blocks which are encrypted by using the incorrect time seed as reference for subsequent data decryption. In addition, the data storage broadcasts the current time seed to the first encryption module again if the first encryption module does not use the correct time seed to encrypt the data.

After the encryption modules encrypt the sub-data blocks and the encrypted data is sent to the data storage, the respective users can read the encrypted sub-data blocks stored in the data storage through the decryption module allotted to respective end user device. In the selected emblematic model, the end-user device is connected to the control device with the choice of network model; here we consider a wired connectivity.

The decryption module reads the encrypted sub-data blocks corresponding to the level of a user and other authorized levels of the user and corresponding to the encryption period from the data storage. To be specific, in the selected emblematic model, a user having higher right can read the data assigned to users having lower rights but a user having lower right cannot read the data assigned to users having higher rights. Thus, the data storage provides the corresponding authorized data to a user according to the level of the user after it authenticates the user according to a user key of the user.

In the selected emblematic model, the data storage generates a access identification key(AI_k) corresponding to the level of the user and sends AI_k together with the encrypted sub-data blocks to the decryption module of the end-user device.

The decryption module generates the encryption cipher keys for the authorized levels (i.e., the second level and the third level) of the user according to the level propagation keys and the access identification keys of the authorized levels and decrypts the encrypted sub-data blocks by using the encryption keys. In particular, the decryption module generates the level propagation key and AI_k of a lower level according to the level propagation key and the access identification key(AIk) of an upper level.

VII. Conclusion and Future Work

The proposed linear hierarchical ciphering model is robust and scalable where data is encrypted corresponding to multiple levels so that a user having higher right can access the data assigned to users having lower rights but a user having lower right cannot access data assigned to users having higher rights. In addition, in the present invention, an access identification key updated by using a access seeds generated based on access time is adopted to ensure the encrypted data to have forward and backward security and that no synchronous process is required. Thus, the encryption process relaxed from computational complexity. Moreover, the level propagation key and the access identification key(AI_k) of a lower level are generated according to the level propagation key and the access identification key(AI_k) of one level up in hierarchy. Thereby, the number of keys to be managed by an end-user device is reduced and accordingly the calculation load of the end-user device is also reduced. In future this solution can be extended to achieve the key generations without considering the sequence in levels of hierarchy.

References Références Referencias

1. Freeman J., Neely R., and Megalo L. “Developing Secure Systems: Issues and Solutions”. IEEE Journal of Computer and Communication, Vol. 89, PP. 36-45. 1998.
2. Agnew G. B., Mullin R. C., Onyszchuk I. M., and Vqanstone S. A. “An Implementation for a Fast Public-Key Cryptosystems”. Journal of Cryptology, Vol.3, No 2, PP. 63-79. 1995.
3. Beth T. and Gollmann D. “Algorithm Engineering for Public Key Algorithms”. IEEE Journal on Selected Areas in Communications; Vol. 7, No 4, PP. 458-466. 1989.
4. IBM. “The Data Encryption Standard (DES) and its strength against attacks”. IBM Journal of Research and Development, Vol. 38, PP. 243-250. 1994.
5. IBM. “The Data Encryption Standard (DES) and its strength against attacks”. IBM Journal of Research and Development, Vol. 38, PP. 243-250. 1994
6. Zhou Yuping; Wu Xinghui; , "Research and realization of multi-level encryption method for database," Advanced Computer Control (ICACC), 2010 2nd International Conference on , vol.3, no., pp.1-4, 27-29 March 2010.
7. Chaitanya, S.; Urgaonkar, B.; Sivasubramaniam, A.; , "Multi-level Crypto Disk: Secondary Storage with Flexible Performance Versus Security Trade-offs," Modeling, Analysis & Simulation of Computer and Telecommunication Systems (MASCOTS), 2010 IEEE International Symposium on , vol., no., pp.434-436, 17-19 Aug. 2010.
8. Sathiaseelan, J.G.R.; Rabara, S.A.; Martin, J.R.; , "Multi-Level Secure Architecture for distributed integrated Web services," Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on , vol.8, no., pp.180-184, 9-11 July 2010.
9. Deguang Le; Jinyi Chang; Xingdou Gou; Ankang Zhang; Conglan Lu; , "Parallel AES algorithm for fast Data Encryption on GPU," Computer Engineering and Technology (ICCET), 2010 2nd International Conference on , vol.6, no., pp.V6-1-V6-6, 16-18 April 2010.
10. Fu Minfeng; Chen Wei; , "Elliptic curve cryptosystem ElGamal encryption and transmission scheme," Computer Application and System Modeling (ICCASM), 2010 International Conference on , vol.6, no., pp.V6-51-V6-53, 22-24 Oct. 2010.