AENSI Journals

Australian Journal of Basic and Applied Sciences

ISSN:1991-8178

Journal home page: www.ajbasweb.com

Multiple Attributes Based Secured Sharing Of Personal Health Records In Cloud Computing Using Blowfish Algorithm

[1]Rinesh.S, and [2]Dr. K. Baskaran

[1]*Research Scholar, Karpagam University, Coimbatore.*
[2]*Associate Professor, Department of CSE, Government college of Technology, Coimbatore.*

ARTICLE INFO

Article history:
Received 2 March 2014
Received in revised form
13 May 2014
Accepted 28 May 2014
Available online 23 June 2014

Keywords:
Multiple Attributes based encryption, coarse grained and fine grained data access control,Blow fish algorithm, security,encryption, decryption.

ABSTRACT

Personal Health Record (PHR) is a rising patient driven model of health data exchange, which is to be stored at a third party provider like cloud providers. So, there have been wide privacy is important for secure personal health information could be bare to those third party servers. Here blowfish algorithm is used for key generation, encryption and decryption, is more securable and fast data transmission is possible. In order to reduce the risks of privacy exposure, scalability in key management, flexible access, and Multiple Attributes Based key management is used. This Multiple Attribute Based encryption used public and secret key to process the operation. This paper, proposed a novel patient-centric framework Multiple Attributes Based encryption is used in PHR, and this mechanism is for data access Control to PHRs stored in semi trusted servers and also in two domains like Public and private domain, by using this key maintainability is reduced. Blowfish algorithm for fast and secure encryption. To attain fine-grained and adaptable data access control for PHRs, Multiple Attributes-Based encryption (MABE) techniques are used to encrypt each patient's PHR file. The coarse grained access control is used to manage the access requests which allow just constrained data from its inputs. This is attained by arranging the assets into units called access blocks and implementing access control at the cloud just at the granularity of blocks.

To Cite This Article: Rinesh. S and Dr. K. Baskaran., Multiple Attributes Based Secured Sharing Of Personal Health Records In Cloud Computing Using Blowfish Algorithm. ***Aust. J. Basic & Appl. Sci.,*** *8(9): 13-21, 2014*

INTRODUCTION

Cloud computing is a methodology, where resources like computing power, storage, network and software are vague and provided as services on the internet. These services are broadly divided into three categories : Infrastructure-as-a-Service (Iaas), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS). Cloud computing gives the self service, by utilizing this distinctive business units are permitted to get the computing assets as they have to experience IT for tackle. It supports a network access, which permits provision to be inherent ways that adjust to how today in portable, multi-apparatus, and so forth. It likewise gives cost productive too, permits asset pooling, for distinctive computing assets to convey their services to numerous clients. Any user can perform the process in their allocating resources, which considers snappy versatility of assets relying upon the interest. These days, Personal Health Record (PHR) is developing as a patient driven model (Shaheen Taj S.A., Prathibha Kiran, 2013) of health data exchange.

A PHR service permits a patient to make, oversee, and to control her individual health record in one place through the cloud supplier and web (L¨ohr, H., A.R. Sadeghi, 2010), has made the storage, recovery, and offering of the medical information more efficiently and securable. Eachpatient has the full control of her/his medical records and can share her/his health data with a wide range of users, including healthcare providers, family members or friends in a secure manner with the help of encryption technology (Bethencourt, J., A. Sahai, 2007).

Because of the high cost of building and maintaining the specialized data centers, any service provider like cloud can provide the service to maintain the data. This helps to reduce the cost, but it is not securable many of this service are provided by third party owner. Like, Microsoft HealthVault.1 Recently, architectures of storing PHRs in cloud computing have been proposed by using Multiple Attributes Based Encryption (MABE) more than one attribute is processed with the help of single key using this approach and blowfish fish algorithm is used to perform the operation fast and secure manner. While it is energizing to have advantageous PHR services

Corresponding Author: Rinesh. S, Research Scholar, Karpagam University, Coimbatore

Australian Journal of Basic and Applied Sciences, 8(9) June 2014, Pages: 13-21

to ease off, numerous security and protection for every single client who utilize this methodology. The fundamental idea is about if the patients could really control the offering of their delicate particular health information (PHI), when they are saved on an outside server. An alternate methodology to secure particular healthcare data is, however, HIPAA, which is as of late changed to join business copartners (Shaik.Musthafa1, M. Tech Student, Dora Babu. Sudarsa), cloud suppliers are typically not secured elements hand, because of the high esteem of the sensitive PHI, Storage servers are regularly the focuses of different malignant practices which may prompt presentation of the PHI.

In this paper, Multiple Attributes Based Encryption (MABE) is used, more than one attribute is processed with the help of a single key, so key maintainability is reduced, this technique is used to display the basic health information about patients in the public domain in order to gather the information in case of Emergency condition. The sensitive information like health condition, personal files and sensitive data, Which are maintained in the private section only particular owner can able to access this file. The semi trust server also maintains the sensitive information of PHR owner. It is used to access the information when the user is in offline, from this semi trust server only the owner can able to access the data in case of security. Blow fish algorithm (Blowfish Brent A)is used to perform the encryption process with fast and secure manner.

One xisting work Attribute Based Encryption methodology is used because of that key maintainability is difficult. In proposed approach is overcome by using Multiple Attributes Based Encryption and Blow fish algorithm , access also easy because of fine grained and coarse grained data access control is used.

The rest of this paper is organized as follows. Section II Related Work, Section III presents Patient Centric Framework for Multiple Attributes Based Encryption and security, Section IV describes our proposed methodology, Section V presents Conclusion and Future Enhancements.

II. Related work:

Multiple Attributes Based Encryption is used to encrypt more than one field by using a single key, besides that challenging key maintainability is reduced. This MABE is used in third party provider. This system contain two types of user public user and private user, Public user can able to see only the selected attribute which undergoes encryption and private user can able to see the complete history of PHR owner file only those who give exact user identification and secret key this is designed mainly for security purpose in order to avoid illegal user ,for encryption Blowfish algorithm is used to encrypt the files .It is faster and securable than comparing with DES algorithm and fine grained access control is used to access the data in row wise manner and also enhance security mechanism for Rows by using this data confidentiality is achieved. The coarse Grained access control is used to manage the access request from inputs by using these two we can perform both read and write operation. When user is in the offline can able to access the data with the help of semi trust server.

Mostly an enormous amount of work based on ABE (Yu, S., C. Wang, 2010) to understand the fine grained access control for secure data (Jana M. McPhersona; Lohr, H., A.R. Sadeghi, 2010). Particularly, there has been an increasing interest in applying ABE to secure Electronic Healthcare Records (EHRs). Recently, Narayan et al. Proposed an attribute based infrastructure for EHR frameworks, where every patient's EHR documents are encoded utilizing a broadcast variant of CP ABE (Suhair Alshehri, Stanisław Radziszowski)that permits immediate denial. Be that as it may, the cipher text length develops straightly with the amount of unrevoked clients, So here this Multiple Attributes Based Encryption is utilized to stay away from this linear developing. In a variant of ABE that permits the assignment of access rights for encoding EHRs. To deal with the offering of PHRs, the idea of open and private dominions is presented. In (Shucheng Yu, Yao Zheng, 2013), Akinyele et al. Examined utilizing ABE to create securing toward oneself EMRs, which can either be saved on cloud servers or cell phones so EMR could be entered when the health supplier is disconnected from the internet. However, there are several common drawbacks are their of the above works. This can be overcome as possible this fine grained access mainly used to access the data row wise this used to prevent collision. It also provides security mechanism for row levels by using this data confidentiality is maintained.

To manage Access request while learning only limited information from its input(Jana M. McPhersona)This is achieved by arranging resource into units of access block with the help of this private and public sensitive information request can be performed properly. With the help of this and blowfish algorithm particular user and PHR owner can able to access the information.

This module is happening at the time of an emergency, the regular access policies may not be possible for longer. To handle this circumstance, break glass access is required to access the PHR records. This idea is based on every PHR holder's access right, the owner can likewise erase it from an emergency department to avoid from ill-use of Break glass alternative, the emergency staff needs to contact the ED to check her/his Identity and the circumstance to get the impermanent read keys. After the Emergency is over; the patient can renounce the emergent access through the ED.

Australian Journal of Basic and Applied Sciences, 8(9) June 2014, Pages: 13-21

III. Patient Centric Frame Work For Multiple Attributes Based Encryption and Security:

The principle objective of this system is to give secure patient centric(Shaik.Musthafa1, M.Tech Student, Dora Babu.Sudarsa), (Ratan Madnani1, Sreedevi) PHR access and efficient key administration at the same time. The key idea is to divide the system into multiple security domains like public domains (PUDs)(Shaheen Taj S.A., Prathibha Kiran, 2013) and private domains (PSDs)) according to the different users, their data access requirements are changed, this will perform according to the user requirements. Using this multiple attributes based encryption[18] only the selected fields will be displayed in this public domain within a single key in order to maintain the key maintainability. The attributes which are displayed on this domain is like name, hospital, insurance, Emergency. If anyone wants to access the public data means they want to login in the PUD domain, only those can know the identity of a particular user can able to access or see the data from that domain.

This PUD might be mapped into an independent part in the society, for example, for instance, medical services, government or insurance division. In a PRIVATE USER domain, personal file, Medical history, Current Medical Examination, Insurance details, and other sensitive details are maintained. In order to maintain this sensitive information blowfish algorithm (Blowfish Brent A) is used only authorized user can able to extract information from here. A domain which administering a disjoint subset of attributes. Role attribute are characterized for PUD are represented as the professional role or some obligations of a PUD user. Users in PUDs got their attribute based secret keys from the attribute authority at the time of absence of the owner or without his/her permission to control the access from PUD and also to provide security in row wise mechanism the role based fine grained access is used it is not necessary to list down the authorized user at the time. This system greatly helpful as to reduce the key administration overhead for both the managers and clients.

Every PHR owner's application will generate its corresponding public/secret keys. The public keys can be published in of some social media like an online healthcare, social-network (HSN) (It is part of the PHR service. There are two ways for conveying secret keys. Initially, when first utilizing the PHR service, a PHR owner can indicate the access privilege of an informed reader in her PSD, and lets her provision create and appropriate relating key to the latter, Second, a reader in PSD could acquire the secret key by sending an appeal (showing which sorts of documents she needs to access), and the owner will give her a subset of requested information sorts. Taking into account that, the policy engine of the requisition immediately infers an access structure, and runs the Blowfish algorithm to create the client secret key that inserts her access structure.

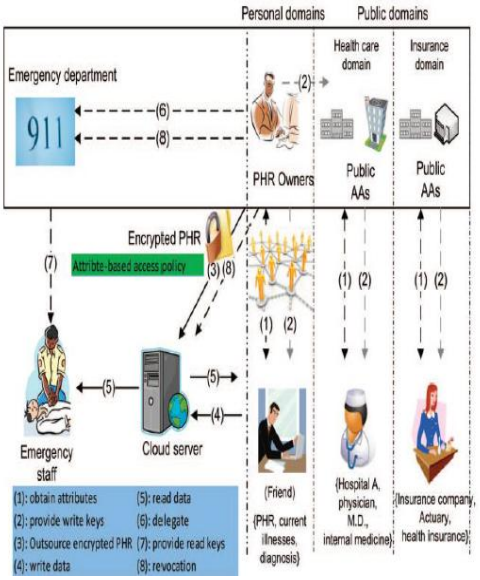


Fig. 1: Proposed framework for secure and scalable sharing of patient health record.

In addition, the data attribute can be organized in a hierarchical manner for efficient policy generation, when the user is granted all the file types under a category, her access privilege will be represented by that category instead. The owners upload MABE-encoded PHR files to the server. Each owner's PHR file is encrypted both under a certain fine grained and role-based access policy for users from the PUD to access, and under a selected set of data attribute that allows access for users in the PSD. Only authorized users can decrypt the PHR files, excluding the server. For improving efficiency, the data attribute will include all the intermediate file types from a leaf node to the root. The data readers download PHR files from the server, and they can decrypt the files only if they have suitable attribute based keys. The data contributors will be granted write access to someone's PHR, if they present proper write keys.

Australian Journal of Basic and Applied Sciences, 8(9) June 2014, Pages: 13-21

IV Multiple Attribute-Based Encryption Technique:

In this proposed system the concept of Multiple Attribute-Based Encryption (MABE), is introduced, i.e., a fully distributed version of CP-ABE (Suhair Alshehri, Stanisław Radziszowski), using this Multiple Attribute-Based Encryption more than one attribute is processed with the help of a single key, so key maintainability is reduced, this technique is used to display the basic health information about patients in the public domain in order to gather the information in case of Emergency condition. The framework is demonstrated in Fig 1.

The sensitive information like health condition, personal files and sensitive data, Which are maintained in the private section only particular owner can able to access this file. The semi trust server also maintains the sensitive information of PHR owner. It is used to access the information when the user is in offline, from this semi trust server only the owner can able to access the data in case of security where different attribute authorities may be available and disseminate secret attribute keys. Moreover, we give the first development of a MABE approach, the cipher text develops linearly with the amount of conjunctive terms in the plan.

The scheme is very simple and efficient, demonstrating the practical viability of MABE. Besides giving a verification of security in the non specific aggregation model; despite the fact that this evidence is weaker than the evidences of some recent CP-ABE (Suhair Alshehri, Stanisław Radziszowski) approaches, the proposed scheme is much more efficient, requiring only (1) pairing operations during encryption and decryption. The diagrams show that the authority for every user. The key concept is to divide the system into multiple security domains like public domains (PUDs) (Shaheen Taj S.A., Prathibha Kiran, 2013) and private domains (PSDs) according to the different users, their data access requirements are changed, this will perform according to the user requirements. Using this multiple attributes based encryption only the selected fields will be displayed in this public domain with inside single key in order to maintain the key maintainability.

The attributes which are displayed on this domain is like name, hospital, insurance, Emergency. If anyone wants to access the public data means they want to login in the PUD domain, only those can know the identity of a particular user can able to access or see the data from that domain. This PUD can be mapped into an self-governing region in the society, such as like health care, government or insurance sector.

In a PRIVATE USER domain, personal file, Medical history, Current Medical Examination, Insurance details, and other sensitive details are maintained. The fundamental thought behind it is to give two levels of access control: coarse-grained and fine-grained the coarse grained level access control will be upheld expressly by the cloud provider and it might additionally represent the granularity at which service provider will take in the access pattern of clients. Despite the fact that the cloud provider will take in the accessible design overall client requests, won't have the capacity to recognize requests from diverse clients, which might come as unknown tokens. The fine-grained access control will be upheld absent to the cloud through encryption and might prevent suppliers from separating demands that bring about the same coarse-grained access control choice however have diverse fine-grained access design.

The mapping between records and access blocks is transparent to the clients as in they can submit record requests without knowing in what blocks the records are present. While most existing results, keep focus on read request, in view of this two access control both read and write access control operation is performed. Picking the granularity for the access blocks in the read and write access control approach influences the privacy ensures for the approach and additionally its effective performance.

Advantages of Proposed System:

1) It provides data confidentiality by implementing a fine-grained and coarse grained cryptographic
2) It supports sensible and adaptable information sharing approach by taking care of both read and write operations in the access control model.
3) It upgrades information and client privacy by securing access control rules and access designs from the storage provider. It gives information confidentiality by actualizing a fine-grained and coarse grained cryptographic access control method.

Security concern:

Data access control is the main challenging issues in cloud computing. It provides the secure data access control by allowing only authorized users to access the data. For the secure data access control the fine-grained data access control is used, which means different types of data can be able to access by different types of users. The fine-grained access control also faces the challenges such as user collusion and key abuse the ABE (one to many encryption) design tool to avoid the collusion resistance and user accountability is proposed.

Key Policy:

To prevent users from sharing the illegal key two key policies such as cipher text policy (Suhair Alshehri, Stanisław Radziszowski) ABE (CP-ABE) and key policy ABE (KP-ABE). These two policies are powerful tools for fine-grained access control. The key distribution is based on the hierarchy access structure associated with a set of attribute. The decryption of data requires satisfy the user access structure. In the existing system,

the message is encrypted with the CP-Y. The sender computes with Y, If the key is in following form the sender can decrypt the data.

K(B,Y) = 1

The sender computes a cipher text with policy Y, such that any user with attribute list K (B,Y)=1 can decrypt, regardless of the identity ID. This four generation of the person user's secret key is for B‖PEK, where K (B, Y)= 1. From this user can only decrypt the cipher text with the private key of B and the secret key of PEK is proposing the key structure using CP-ABE under the set of attribute and id in the following form.
K (B||PEK,Y) = 1

Performance Evaluation:

The following Fig 2 shows the performance of this approach, by using this Blowfish algorithm the encryption speed is faster and scrabble when comparing to other algorithms like DES and IDEA. The number of clock cycles per bit encryption is also lesser when comparing to other two so only it perform the operation very fast when comparing to other two algorithms in order to avoid a collision for user request and to perform proper operation two data control methodology is used by using this collision is somewhat reduced.

Multiple Attribute Based Encryption (MABE) more than one attribute is processed with the help of a single key, so key maintainability is reduced, this technique is used to display the basic health information about patients in the public domain in order to gather the information in case of Emergency condition. The sensitive information like health condition, personal files and sensitive data, Which are maintained in the private section only particular owner can able to access this file.

The semi trust server is also maintaining the sensitive information of PHR owner. It is used to access the information when the user is in offline, from this semi trust server only the owner can able to access the data in case of security.

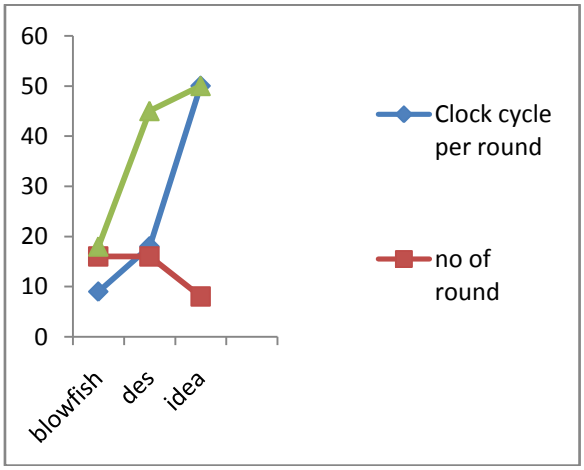


Fig. 2: Comparison graph for algorithm.

Table 1: Comparison of algorithms.

Algorithm	Cycles per Round	No of round	No of clock cycle per byte encryption
blowfish	9	16	18
Des	18	16	45
Idea	50	18	50

Table 1represents a comparison between the numbers of encrypted algorithm. This is based on the number of clock cycles per round, number of round and the number of clock cycles per bit encrypted. This is used to identify the speed of the algorithm on comparing with the previous one, from this graph we can easily judge which algorithm is best to perform the process. Blowfish algorithm, it requires 18 clock cycles for per byte encryption, 9 cycles per round. To complete one operation, it requires 16 rounds. For Des algorithm, it requires 45 clock cycles for per bit encryption, 18 cycles per round. To complete one operation, it requires 16 rounds, for idea algorithm, it requires 50 clock cycles for per byte encryption, 50 cycles per round. To complete one operation, it requires 18 rounds. On seeing this blowfish algorithm is better to perform the process and more securable.

Blow fish algorithm:

Blowfish is a variable key length with 64-bit block of cipher. Fig 3 shows the process of providing input and output to the blowfish algorithm. This algorithm[6] consists of two parts a key Implementations of Blowfish that require the fastest speeds should spread out the loop and ensure that all sub keys are stored in cache.

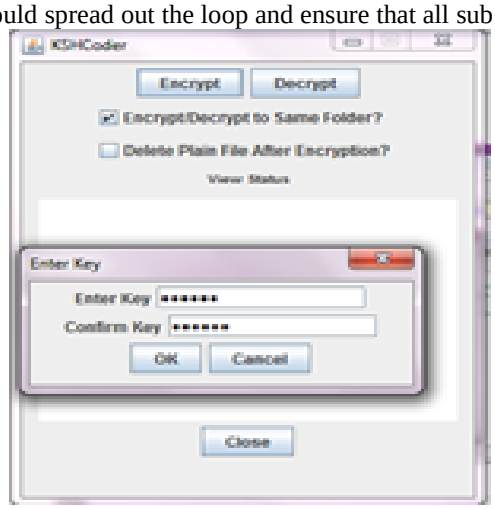


Fig. 3: Process of Encryption and Decryption using Blow fish algorithm.

Sub keys:

Blowfish uses a large number of sub keys. These keys are recomputed before any data encryption or decryption.

Design Decisions On Variable Length-key (64-Bit Block Cipher):

According to the above parameters, we have made these design decisions. The algorithm should support this condition:

Step 1: Operate data in large blocks which preferably 32 bits in size.
Step 2: if block size is 64-bit or a 128 use it.
Step 3: Design key which starts from32 bits to at least 256 bits.
Step 4: Use simple microprocessor to be implementable on an 8-bit processor
Step 5: design and use sub keys
Step 6: Use a design that is simple to understand. This will facilitate analysis and increase the confidence in the algorithm.

Design Decisions:

In des algorithm a 64 bit block size gives a 32 bit word size, and also it was maintained by the block size compatibility .Blowfish(Blowfish Brent A)is easy to scale up to a 128 bit block, and down to smaller block sizes. The Feistel network is used to design the body of Blowfish. Blowfish is designed to be as simple as possible, while still retain the desirable cryptographic properties of the structure. Round i of a general Feistel network Sn, i and Ni are reversible, non-reversible functions of text and key. For speed and simplicity, XOR is chosen as reversible function. Because of that there is a chance to occur collision. So the four XOR function forms into a single XOR function.

$RP_{1,i+1} = R_{1,i+1} \text{ XOR } R_{2,i-1} \text{ XOR } R_{3,i} \text{ XOR } R_{4,i}$

This is the R-array substitution in Blowfish. The XOR can also be considered to be part of the non-reversible function, Ni, occurring at the end of the function. The Function F, the non-reversible function, gives Blow fish and the best possible avalanche effect for a Feistel network so every text bit on the left half of the round affects every text bit on the right half. Besides that, every sub key bit is affected by every key bit, After every round the value of key and right half of the text has a perfect match of avalanche effect the so, this algorithm exhibits a perfect avalanche effect after three rounds and again every two rounds totally Five rounds.

The non reversible function is mainly used to design for strength, speed, and simplicity. Four different types of S-boxes are used instead of one S-box in order to avoid the similarities between the values and key chosen at the time of processing. The output of four S-box design is faster, easier to program, and seems more secure. The function that combines the four S-box outputs should be as fast as possible. Then the final simpler function isto combine the four values of XOR. The alternation of addition and XOR ends with an addition operation because an XOR combines the final result with xR. If the four indexes chose values outside of the same S-box, this require more complex combining function to eliminate symmetries.

Australian Journal of Basic and Applied Sciences, 8(9) June 2014, Pages: 13-21

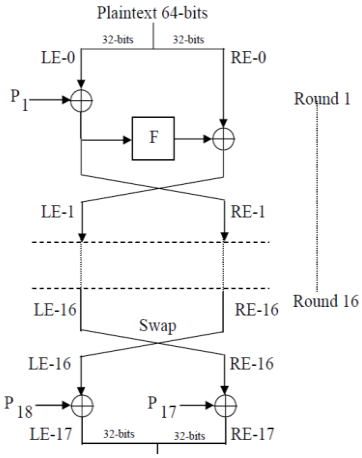
As the structure of the S-boxes are completely hidden from the cryptanalyst because the differential and linear cryptanalysis attacks will easily attack the structure of s _box and it is a little bit difficult to redesign the structure. There is a chance to replace some affected S_box by new designed S_box. The key dependent S-boxes are easier to implement and less liable to arguments of unknown properties. This S_box are mainly designed to reduce the large storage requirements in the database.

The input to the s_box is the bit which belongs to xL is used. In DES algorithm large number of bits are used as inputs to two S-boxes, but this faced lot of complication is not necessary and it does not affect the key dependent S-boxes. The P array substitution also be considered to be as a part of the F function, and is already iteration dependent. When the number of rounds is set to 16 the size of the P array and the generation process, 16 iterations which makes to generate key lengths up to 448 bits. This number of bits required for generation is reduced in blowfish and also speed is increased.

There are two basic ideas behind that key design, it helps to increase the security level one is carefully design of key it will maintain the complete structure of the process, so this is more secure and another approach is based on brute force a design approach is used to design the key with so many key bits this helps to reduce the key length by several bits.

Blowfish Encryption:

Blowfishhas 16 rounds.
The input is a 64-bit data element, x.
Divide x into two 32 bit : xS,xM.
Then, for i = 1 to 16:
xS = xM XOR Q_i
xM = F(xS) XOR xM
Swap xM and xS
After the sixteenth round, swap xS and xM again to undo the last swap.
Then, xM = xM XOR P17 and xS = xP XOR Q18.
Finally, recombine xS and xM to get the ciphertext.



Ciphertext 64 bits

Fig. 4: The encryption routine for Blowfish uses a 16 round Feistel network, a swap operation and two exclusive-or operations. Each round consists of exclusive-or operations and the F function.

Generating the Subkeys:

The subkeys are calculated using the Blowfish algorithm:

Step.1). Initialize Q-array and then the four S-boxes, with a fixed string. This string consists of the hexadecimal digits of pi (less the initial 3): Q1 = 0x243f6a88, Q2 = 0x85a308d3, Q3 = 0x13198a2e, Q4 = 0x03707344, etc.

Step.2). XOR Q1 with the first 32 bits of the key, XOR Q2 with the second 32-bits of the key, and so on for all bits of the repeatedly cycle through the key bits until the entire Q-array has been XOR ed with key bits

Step.3). Encrypt the all zero string with the Blowfish algorithm, using the subkeys described in steps (1) and (2).

Step.4). Replace Q1 and Q2 with the output of step (3).

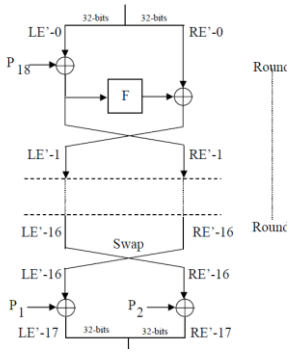
Step.5). Encrypt the output of step (3) using the Blowfish algorithm with the modified

With the help of a large number of microprocessors and with large amounts of memory Blowfish is designed the sub key generation process is designed to secure the entire structure of the key and to distribute that

Australian Journal of Basic and Applied Sciences, 8(9) June 2014, Pages: 13-21

structure uniformly throughout the sub keys. Fig 4 shows the process of encryption. The values of pi are chosen as the initial sub key table because of two reasons: it is a random sequence not related to the algorithm, and it could either be stored as part of the algorithm or derived when needed. Any Number of strings for random bits RAND tables, output of a random number generator will be enough for pi. The value of sub key was changed at the time of sub key generation process, there are simple changes in sub keys with every pair of generating sub keys. This is to look after against any attacks of the sub key generation process. It also reduces storage requirements. The 448 bits limit on the key size conforms that every bit of every sub key depends on every bit of the key.

The key bits which repeatedly perform the XOR operation by using the digits of pi in the initial P array to prevent the potential attack .Consider if that's the key bits are not repeated, but they had padded with zeros to increase it the length of the P array. An attacker can easily find the two keys, but that are different only in the 64-bit value XOR with P1 and P2 that produce the same encrypted value. If so, he can easily find the two keys and also sub keys which are produced by the two keys.



Ciphertext 64 bits
Plain text 64 bits

Fig. 5: The decryption routine for Blowfish is identical to the encryption routine except the P-array key values are applied in the reverse order.

This is a highly attractive attack for a malicious key generator. To avoid this same type of attack, the value of initial plain text is fixed in sub key generation process. The interrelated key bits, such as an alphanumeric ASCII the bit 0 was set to every byte of operation, will produce random sub keys. The time overwhelming for sub key generation process includes some amount of complexity of a brute-force attack. A total of 522 iterations of the algorithm are required to test a single key.

Fig 5 describes the decryption process. For decryption process, the same approach as encryption is applied, except that the p array is applied in reverse order.

V. Conclusion and Future Enhancement:

In this paper, Multiple Attribute Based Encryption is used to reduce the maintainability of keys, with the help of Coarse grained and Fine grained data access control, data are accessed in case of row wise and security for the data is provided, Access request from input is also managed. With the help of this blowfish algorithm security at the time of encryption is increased. Performance is also increased on comparing to other encryption algorithms like DES. The future enhancement is concentrated on reduction of collision in the system with tight security at the time of sending and receiving the request from PHR owner.

REFERENCES

A Novel Method for Patient Centric Secure and Scalable sharing of PHR in Cloud Computing using Encryption Shaheen Taj S.A., Prathibha Kiran, 2013. Elavarasi International Journal of SoftComputing and Engineering (IJSCE) ISSN: 2231-2307, 3-4.

Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption Ming Li, Member, IEEE, Shucheng Yu, Member, IEEE, Yao Zheng, Student Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, ieee transactions on parallel and distributed systems, 24(1), january 2013.

Attribute Based Encryption for Scalable andSecure Sharing of Medical Records in CloudComputing Design and ImplementationBharti Ratan Madnani1, Sreedevi N2 M.Tech Scholar, Dept. Of CS, MVJ College of Engineering, Banglore, India1HOD & Assistant Professor, Dept. Of Computer science, MVJ College of Engineering, Banglore, India2.

Australian Journal of Basic and Applied Sciences, 8(9) June 2014, Pages: 13-21

Patient–Centric Secure Data Sharing Frame Work for Cloud-Based PHR Systems Shaik.Musthafa1, M.Tech Student, Dora Babu.Sudarsa 2, M. Tech., (Ph.D), Associate ProfessorInternational Journal of Engineering Science Invention ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726 www.ijesi.org, 2(5): 17-26.

Blowfish Brent A. CottomCS 6520 Cryptography8/18/200.

Superiority of Blowfish Algorithm Pratap Chnadra Mandal Asst. Prof, Dept of Computer Application B.P. Poddar Institute of Management & technology, West Bengal, India, 2(9).

Maintaining and Secure Sharing of Personal Health Records in Cloud Environment R.K.Saranya1, Research Scholar, Sathyabama University, Chennai. Assistant Professor / CSE, Jeppiaar Engineering College, Chennai.Dr.V.L.Jyothi2, Professor & Head, Department of CSE, Jeppiaar Engineering College, National Conference on Architecture, Software systems and Green computing-2013(NCASG2013).

Li, M., S. Yu, K. Ren and W. Lou, 2010. Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings, in SecureComm'10: 89-106.

Lohr, H., A.R. Sadeghi and M. Winandy, 2010. Securing the e-health cloud, in Proceedings of the 1st ACM International Health Informatics Symposium, ser. IHI, 10: 220-229.

An Efficient Sharing of Personal Health Records Using DABE in Secure Cloud Environment Parameswaran, T., S. Vanitha, K.S. Arvind 2013. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2-3.

Designing a Secure Cloud-Based EHR System using Cipher text Policy Attribute-Based Encryption Suhair Alshehri, Stanisław Radziszowski and K. Rajendra Raj Golisano College of Computing & Information Sciences Rochester Institute of Technology Rochester, New York 14623, USAsxa3788@rit.edu, spr@cs.rit.edu, rkr@cs.rit.edu

Secured Personal Health Records Transactions Using Homomorphic Encryption In Cloud Computing S. Vidya1 Assistant Professor, Computer Science and Engineering, SNS College of Technology, India. K. Vani2 Assistant Professor, Computer Science and Engineering, SNS College of Technology, India D. Kavin Priya3 Assistant Professor, Computer Science and Engineering, SNS College of Technology, India.

Attribute-Based Encryption forFine-Grained Access Control of Encrypted DataVipul Goyal Omkant Pandeyy Amit SahaizBrent Waters.

Using coarse-grained occurrence data to predict species distributions at finer spatial resolutions possibilities and limitations Jana M. McPhersona, Walter Jetza,b,c,d , David J. Rogers aReceived 12 October 2004; received in revised form 17 July 2005; accepted 3 August 2005 Available online 26 September 2005.

On Demand Security for Personal Health Record in Cloud Computing Using Encryption and Decryption Cryptography M. ijayapriya* M. Phil. Research Scholar PG & Research Department of Computer Science Government Arts College (Autonomous) Coimbatore-18, India Dr. A. Malathi Assistant Professor PG & Research Department of Computer Science Government Arts College (Autonomous) Coimbatore-18, India Volume 3, Issue 9, September 2013.

Yu, S., C. Wang, K. Ren and W. Lou, 2010. "Attribute based data sharing with attribute revocation," in ASSIACCS"10.

L¨ohr, H., A.R. Sadeghi and M. Winandy, 2010. "Securing the e-health cloud," in Proceedings of the 1st ACM International Health Informatics Symposium, ser. IHI, 10: 220–229.

Chase, M. and S.S. Chow, 2009. "Improving privacy and security in multi-authority attribute-based encryption," in *CCS*, 121–130.

Melissa Chase "Multi-authority Attribute based Encryption," Computer Science Department BrownUniversity Providence, RI 02912.

Bethencourt, J., A. Sahai and B. Waters, 2007. "Ciphertext-policy attribute-based encryption," in *IEEE S& P*, 321–334.