IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 5 Issue 4, April 2018
ISSN (Online) 2348 – 7968
www.ijiset.com

An Efficient Technique For Cloud Security Using Triple Des Algorithm

M.uma maheswari[1], D.Jayakumar[2]

PG Student, ,Bharath Institute of Higher Education and Research, Chennai-73, India[1]

Assistant professor, Bharath Institute of Higher Education and Research, Chennai-73, India[2]

Abstract:

Cloud computing is an architecture for providing computing service via the internet on demand and Pay per use access to a pool of shared resources without physically acquiring them. So it saves managing cost and time for organize Cloud Computing is an emerging paradigm. Which has become today's hottest research area due to its ability to reduce the costs associated with computing. In today's it is most interesting and enticing technology which is offering the services to its users on demand over the internet. Since Cloud computing stores the data and its dis seminated resources in the environment, security has become the main obstacle which is hampering the deployment of cloud environments[1]. There are number of users used cloud to store their personal data. So that data storage security is required on the storage media[3]. This concept is used by DNS algorithm it is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable used it is an encryption algorithm that can be used as a replacement for the DES or IDEA algorithms. This paper is used to know about the security of the cloud computing using DES algorithm[4].Practical Sweet32 attack on 3DES-based cipher-suites in TLS required blocks (785 GB) for a full attack, but researchers were lucky to get a collision just after around blocks which took only 25 minutes.The security of TDEA is affected by the number of blocks processed with one key bundle[8]. One key bundle shall not be used to apply cryptographic protection (e.g., encrypt) more than 64-bit data blocks.

Key Words : DES, DNS, Encryption, Deniable Encryption

1.INTRODUCTION:

Cloud storage services have rapidly become increasingly popular. Users can store their data on the cloud and access their data anywhere at any time. Because of user privacy, the data stored on the cloud is typically encrypted and protected from access by other users. Considering the collaborative property of the cloud data, attribute-based encryption (ABE) is regarded as one of the most suitable encryption schemes for cloud storage[7]. There are numerous ABE schemes that have been proposed Most of the proposed schemes assume cloud storage service providers or trusted third parties handling key management are trusted and cannot be hacked; however, in practice, some entities may intercept communications between users and cloud storage providers and then compel storage providers to release user secrets by using government power or other means[3]. In this case, encrypted data are assumed to be known and storage providers are requested to release user secrets. Google released user documents to the FBI after receiving a search warrant . In 2013, Edward Snowden disclosed the existence of global surveillance programs that collect such cloud data as emails, texts, and voice messages from some technology companies. Once cloud storage providers are compromised, all encryption schemes lose their effectiveness[4]. Though we hope cloud storage providers can fight against such entities to maintain user privacy through legal avenues, it is seemingly more and more difficult. As one example, Lavabit was an email service company that protected all user emails from outside coercion; unfortunately, it failed and decided to shut down its email service. Since it is difficult to fight against outside coercion, we aimed to build an encryption scheme that could help cloud storage providers avoid this predicament. In our approach, we offer cloud storage providers means to create fake user secrets. Given such fake user secrets, outside coercers can only obtained forged data from a user's stored ciphertext. Once coercers think the received secrets are real, they will be satisfied and more importantly cloud storage providers will not have revealed any real secrets[8]. Therefore, user privacy is still protected. This concept comes from a special kind of encryption scheme called **deniable encryption**, first proposed[1]. Deniable encryption involves senders and receivers creating convincing fake evidence of forged data in ciphertexts such that outside coercers are satisfied. Note that deniability comes from the fact that coercers cannot prove the proposed evidence is wrong and therefore have no reason to reject the given evidence. This approach tries to altogether block coercion efforts since coercers know that their efforts will be useless. We make use of this idea such that cloud storage providers can provide audit-free storage services. In the cloud storage scenario, data owners who store their data on the cloud are just like senders in the deniable encryption scheme[3]. Those who can access the encrypted data play the role of receiver in the deniable encryption scheme, including the cloud storage providers themselves, who have systemwide secrets and must be able to decrypt all encrypted data1. In this work, we describe a deniable ABE scheme for cloud storage services. We make use of ABE characteristics for securing stored data with a fine-grained access control mechanism and deniable encryption to prevent outside auditing. Our scheme is based on Waters ciphertext policy-attribute based encryption (CP-ABE) scheme[4] . We enhance the Waters scheme from prime order bilinear groups to composite order bilinear groups. By the subgroup decision problem assumption, our scheme enables users to be able to provide fake secrets that seem legitimate to outside coercers.

1.1security:

In general, Triple DES with three independent keys has a key length of 168 bits (three 56-bit DES keys), but due to the meet in the middle attack, the effective security it provides is only 112 bits.Keying option 2 reduces the effective key size to 112 bits (because the third key is the same as the first). However, this option is susceptible to certain chosen plain-text or known-text attacks,and thus, it is designated by NIST to have only 80 bits of security.This can be considered broken, as the whole 3des keyspace can be searched thoroughly by affordable consumer hardware today (2017) .

1.1 Previous Work on ABE

Sahai and Waters first introduced the concept of ABE in which data owners can embed how they want to share data in terms of encryption[4] . That is, only those who match the owner's conditions can successfully decrypt stored data. We note here that ABE is encryption for privileges, not for users. This makes ABE a very usefultool for cloud storage services since data sharing is an important feature for such services[2]. There are so many cloud storage users that it is impractical for data owners to encrypt their data by pairwise keys. Moreover, it is also impractical to encrypt data many times for many people. With ABE, data owners decide only which kind of users can access their encrypted data[5]. Users who satisfy the conditions are able to decrypt the encrypted data.

I. There are two types of ABE, CP-ABE and Key-Policy ABE (KP-ABE).

The difference between these two lies in policy checking. KP-ABE is an ABE in which the policy is embedded in the user secret key and the attribute set is embedded in the ciphertext. Conversely, CP-ABE embeds the policy into the ciphertext and the user secret has the attribute set[3]. Goyal et al. proposed the first KPABE in . They constructed an expressive way to relate any monotonic formula as the policy for user secret keys. Bethencourt. proposed the first CP-ABE in[4] . This scheme used a tree access structure to express any monotonic formula over attributes as the policy in the ciphertext. The first fully expressive CP-ABE was proposed by Waters in which used Linear Secret Sharing Schemes (LSSS) to build a ciphertext policy[5]. Lewko et al. enhanced the Waters scheme to a fully secure CP-ABE, though with some efficiency loss.

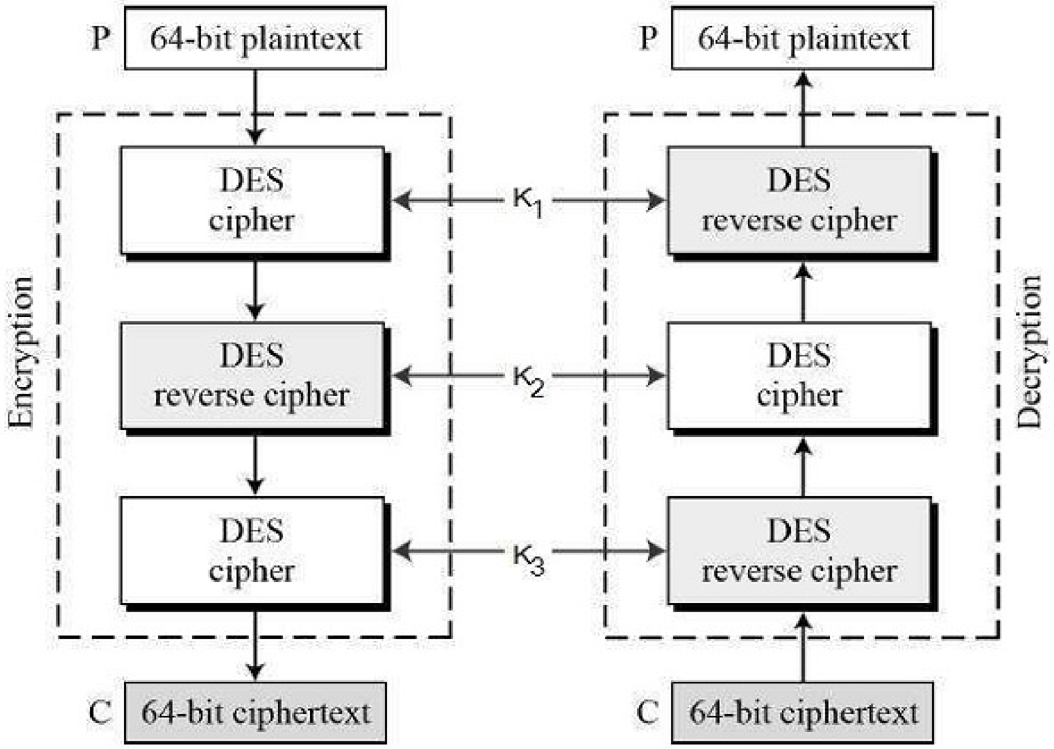


Fig.1 STANDARD OF TRIPLE DES

2. FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.Three key considerations involved in the feasibility analysis are

- *ECONOMICAL FEASIBILITY*
- TECHNICAL FEASIBILITY
- SOCIAL FEASIBILITY

2.1 ECONOMICAL FEASIBILITY:

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

2.2 TECHNICAL FEASIBILITY:

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resoursces. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

FIG.2 WORKING OF TRIPLE DES ALGORITHM

2.3 SOCIAL *FEASIBILITY:*

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

3 INPUT AND OUTPUT DESIGN OF DES ALGORITHM:

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy.

- Input Design is the process of converting a user-oriented description of the input

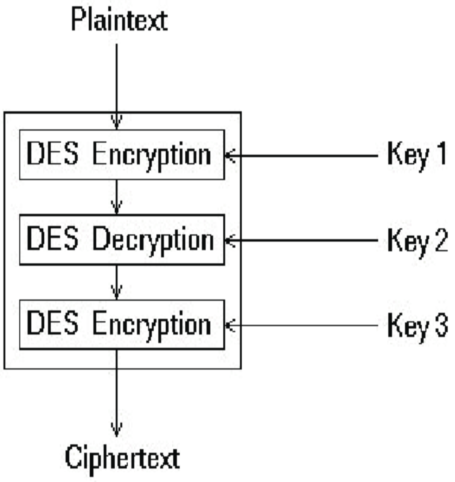


FIG.2 WORKING OF TRIPLE DES ALGORITHM

- into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

- It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

- When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the userwill not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

4. Output Design:

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

- Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
- Select methods for presenting information.
- Create document, report, or other formats that contain information produced by the system.

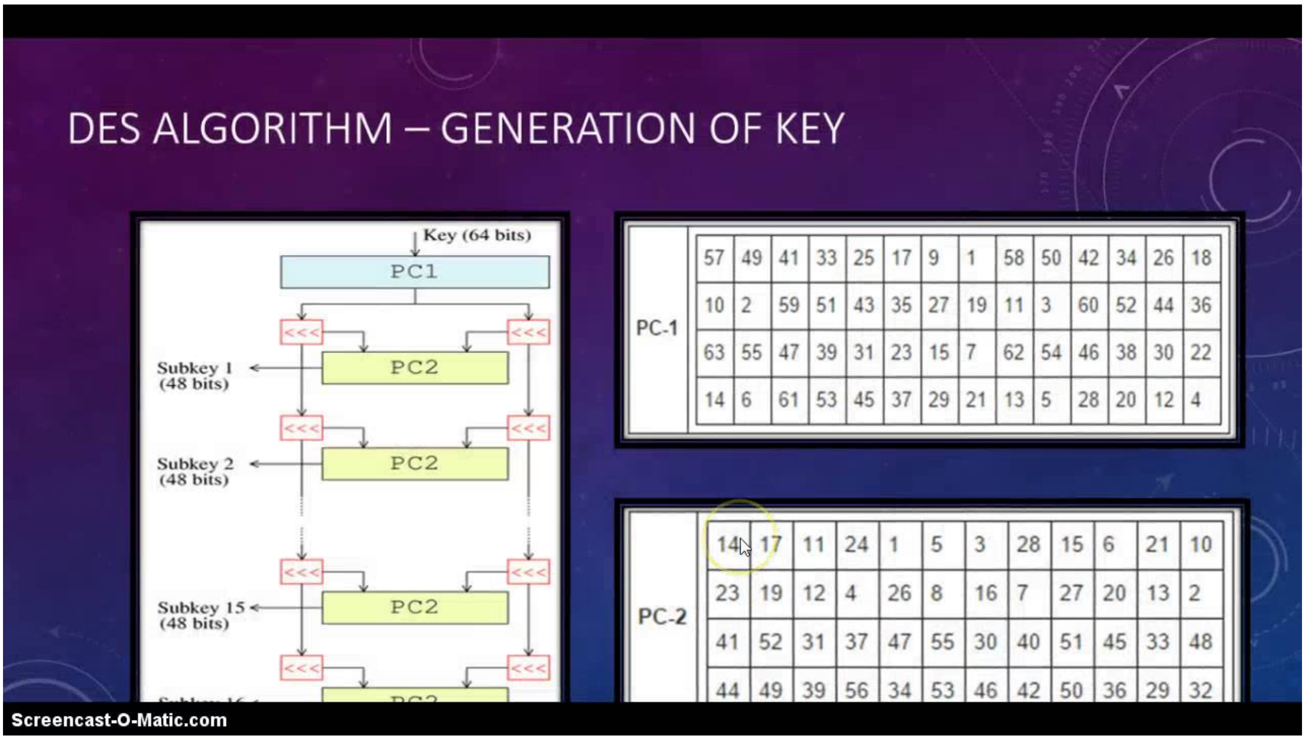
The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.

- Trigger an action.
- Confirm an action.

5. Security:

In general, Triple DES with three independent keys has a key length of 168 bits (three 56-bit DES keys), but due to the meet-in-the-middle attack, the effective security it provides is only 112 bits. Keying option 2 reduces the effective key size to 112 bits (because the third key is the same as the first). However, this option is susceptible to certain chosen-plaintext or plaintext attacks, and thus, it is designated by NIST to have only 80 bits of security[3].This can be considered broken, as the whole 3des keyspace can be searched thoroughly by affordable consumer hardware today attack on 3DES-based cipher-suites in TLS required blocks (785 GB) for a full attack, but researchers were lucky to get a collision just after around blocks which took only 25 minutes[4].The security of TDEA is affected by the number of blocks processed with one key bundle.



DES ALGORITHM – GENERATION OF KEY

PC-1														
	57	49	41	33	25	17	9	1	58	50	42	34	26	18
	10	2	59	51	43	35	27	19	11	3	60	52	44	36
	63	55	47	39	31	23	15	7	62	54	46	38	30	22
	14	6	61	53	45	37	29	21	13	5	28	20	12	4

PC-2												
	14	17	11	24	1	5	3	28	15	6	21	10
	23	19	12	4	26	8	16	7	27	20	13	2
	41	52	31	37	47	55	30	40	51	45	33	48
	44	49	39	56	34	53	46	42	50	36	29	32

FIG.3 TRIPLE DES ALGORITHM GENERATION KEYS

6. CONCLUSION

Furthermore, we provide this authenticator can be efficiently generated by the data owner simultaneously with the encoding procedure. Extensive analysis shows that our scheme is provable secure and the performance evaluation shows that our scheme is highly efficient and can be feasibly integrated into a regenerating-code-based cloud storage system.

7.REFERENCES

[1] M. Armbrust *et al.*, “Above the clouds: A Berkeley view of cloud computing,” Dept.

Elect. Eng. Comput. Sci., Univ. California, Berkeley, CA, USA, Tech. Rep. UCB/EECS-2009-28, 2009.

[2] G. Ateniese *et al.*, “Provable data possession at untrusted stores,” in *Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS),* New York, NY, USA, 2007, pp. 598–609.

[3] D.jayakumar,”A Resourceful allocation of data storage in cloud computing”,”international jornel of advances in engineering and emerging technology, vol. 1, pp 45-50,2013.

[4] D.jayakumar,N.monisha,V.deepika,a.ishwarya., ”An efficient technique for data compression and convergent encryption in the hybrid cloud”,International journal of computerscience and mobile computing,vol. 5, pp 330-336,2016

[5] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, “MR-PDP: Multiple-replica provable data possession,” in *Proc. 28th Int. Conf. Distrib. Comput. Syst. (ICDCS),* Jun. 2008, pp. 411–420.

[6] K. D. Bowers, A. Juels, and A. Oprea, “HAIL: A high-availability and integrity layer for cloud storage,” in *Proc. 16th ACM Conf. Comput. Commun. Secur.*, 2009, pp. 187–198.

[7] J. He, Y. Zhang, G. Huang, Y. Shi, and J. Cao, “Distributed data possession checking for securing multiple replicas in geographically dispersed clouds,” *J. Comput. Syst. Sci.*, vol. 78, no. 5, pp. 1345–1358, 2012.

[8] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, “Remote data checking for network coding-based distributed storage systems,” in *Proc. ACM Workshop Cloud Comput. Secur. Workshop*, 2010, pp. 31–42.