ISSN 2347 - 3983
Volume 8. No. 10, October 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter198102020.pdf
https://doi.org/10.30534/ijeter/2020/198102020

DES Based Dynamic Encryption Scheme for Moving Target Defense in Network

[1]RAJESH KOPPOU, [2]Dr.SEKHAR BABU BODDU
[1]M. Tech Student, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh kr.kr7386@gmail.com
[2]Assoc.Professor, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh sekharbabu@kluniversity.in

ABSTRACT

In today's cyber world the powerful innovations proposed in recent years by Federal Network and Information Technology Research and Development (NITRD) [9] is Moving Target Defense (MTD) [10]. Usually network security designs are static and similar. Now a day's security features are minimizing the problems of searching the network for cyber attackers to specify the unique targets and store valuable information. Then attackers will take the asymmetrical advantages of constructing, initiating and spreading attacks and the users are in a passive role. This condition cannot be changed by the current defensive mechanisms and approaches. In order to change the asymmetrical condition of attacks and defenses, MTD is introduced as a modern innovative technology. It moves the protected target attack surface by dynamic shifting which the administrator can monitor and manage.

Key words: Dynamic Shifting, Moving Target Defense (MTD), Network Security, Passive Role.

1. INTRODUCTION

In cryptography architecture a related dynamic concept can also be adopted. It is well founded in the Data Encryption. Meanwhile DES algorithm laid the foundation for the modern block cipher theory to be developed and applied. At present the DES algorithm is more vulnerable algorithm with the rapid development of computing resources which makes the successful cyber-attack on DES algorithm. So, the triple DES algorithm or Advances Encryption Standard (AES) has been gradually substituted because they have the large key space using while encoding and decoding the plain text. After using the AES and Triple DES algorithm encryption and decryption time is increases gradually so we introduced the new security mechanism called moving Target Defense in network. In this process we have the three layers of security with the less time of encryption and decryption time. In this project we will encode the data in two times so that the security levels will increases. Now we will describe the process i.e. in the first layer we will encode the given data by using encoders. In the second level we encrypt the encoded data with Des algorithm, then we will get chipper text, after getting the chipper text third level will start I.e. we again encode the chipper text with encoders. In this way we provide the security to the user data.

2. LITERATURE SURVEY

While we are travel reading book is our best partner in journey every time. Spending journey time with book we will get the more knowledge. As we now getting knowledge and skill with more money is not possible so that reading pdf file while travelling with moving Target Defense system, we will be safe from the attackers in the cyber world. The MTD system will create an asymmetric key system form cyber-attacks [1]. As we know our cyber security defense system are static and organized by the very lengthy process for examining the crime spot. So, the attackers will get a more time and have a chance to plan the attack and they will be successful in that attack. So, we need a new type of defense technologies to face the attackers and secure our data from attackers that new technologies are Moving Target Defense (MTD) [2]. Today's very difficult task is securing the software's through web applications from cyber-attacks. The attacker always deploys a powerful configuration to attack the system. To secure the software's by web applications users will always change or transfers to different web application configuration for securing the software's. If we transfer the web-stack configuration periodically cost of maintenance will increase. So MTD is proposed to secure the software in the network using network configuration process [3]. As we see in [5] there they used the visual cryptography concept in that author splits the picture in to the three different parts for providing the security, like that we are proposed MTD scheme in this paper. As we see in the [8] website quality based on appearance by authors they said that we can calculated the website quality by seeing the appearance of website. So, we proposed system also has the website so the new users can easily understand that viewed site is genuine or hacked site. It is the best of calculating the quality of website [8].

3. EXISTING SYSTEM

The existing system Configurations of the network security are usually deterministic, static and homogeneous. So, the files or data easily hacked by the attackers. Then the users we are stored their files or data in the network will lose the data integrity and security of the file. The attackers will increase their attack and they will hand over the server very easily. Day by day cyber-attacks are increasing by static and homogeneous security policies. The users are always in the passive position.

3.1 Existing System Disadvantages:

- We Can Upload Single Data at a time.
- Produce Single key for Security of each parameters.

4. PROPOSED SYSTEM:

The outsourced computation data is more secured.
In this paper we are proposed the three-layer encryption scheme. We are providing the 3 ways security i.e. (i) encode,

(ii) encryption, (iii) encoding the encrypted data i.e. done in second stage. So, we can easily secure the data and we can upload multiple data at a time. If we need to open the file which is uploaded by the owner, we need the four keys to open it. If we need keys, we need to request the owner who is uploaded the file and owner will accept the request and send the keys to the user for access the file. In this way we are proving the security to files in the network.

4.1Proposed System Advantage:

- Multi-key scenario allows multiple data sources with different secret keys.
- Keys are modified when user download the file.
- To upload their endless data and give access to the data to all users.

5. DES PROCESSES

The Data Encryption Standard (DES) [7] algorithm is one symmetric key process. It follows the Feistel Structure. The block size of the algorithm is 64bit and it has the 16 rounds encryption process to produce the 64bit cipher text. Size of the key is 64bitand it uses 16 sub keys. Each sub key is used for each round. And the size of each sub key is 48bit. The decryption process of this algorithm is as same as encryption process in reverse direction to gain the plain of 64bit size. In the earlier time it plays a good role to improve the security of the system. The encryption and decryption process shows in the Figure.1.

.

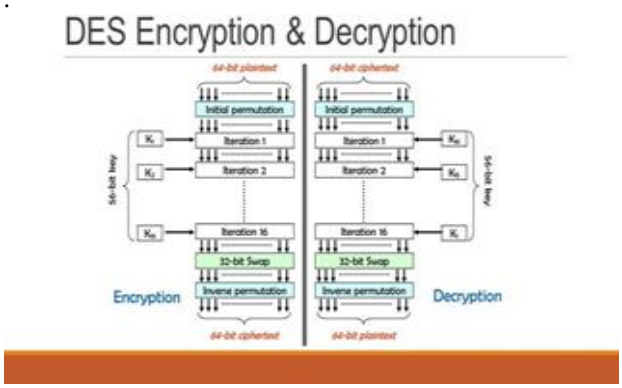

Fig.1:DES Encryption & decryption

6. IMPLEMENTATION

In this paper we are proposed the novel encryption process contains three layers of security i.e. first and third layers are encoding sections and second layer is the encryption process used by the DES algorithm. In this new implementation process both the exhaustive and analysis attacks are safe to resist the cyber-attacks. Comparatively the running time of proposed system is lower than the running time of the triple DES algorithm. Here we are proposing some methodologies for proposed system are given below.

6.1: Methodologies:

(a) User Interface Design.
(b) Admin.
(c) Data Owner.
(d) Moving Target Defense.
(e) User.

A. User Interface Design:

In this user interface design module first, you will see the home page and register and login page. After that the owner and the user need to be register first. All registered users' details are stored in database. If the user connects with the server, they need to be to enter their username and password for secure login into the server. If they already have their login credentials, they can directly login to server otherwise they need to be register with some personal details like username, password and Email id. By using these details server will create an account to the users. When the server creates an account to the entire users, they will maintain their download and upload ratio. The username of the account will be the Email id and password is what you have set at the time of registration process. Both user and owner login pages are different i.e. both have their own login pages in server and database. The user interface design flow chart shows in Figure 2.

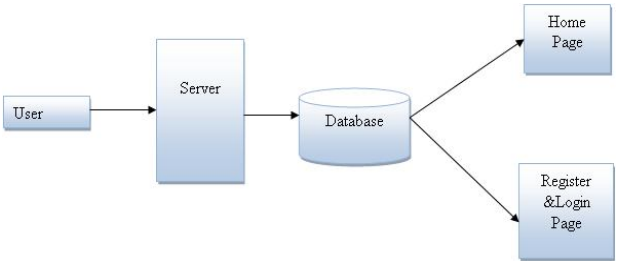

Figure.2: User Interface Design Flow Chart

B. Admin:

This is the first module of this project. In this module admin can login. Admin will see the details of data owners and users. Admin has information about files, and he need to protect the keys from attacker by updating the file keys regularly. Admin need to approve the file request from user and send to data owner to give permission to access the files. Admin will see the attacker details, users who will access the files without data owner permission. The Admin Flow chart shows in the Figure 3.

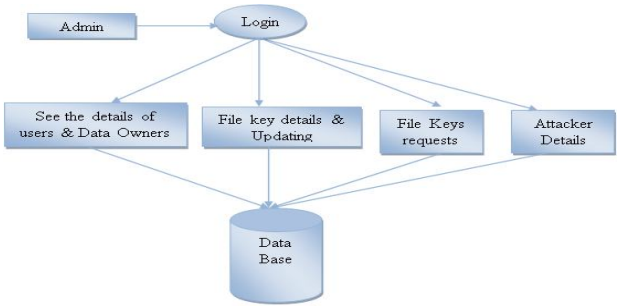

Figure.3: Admin Flow Chart

C. Data Owner:

This is the second module of this project.
In this module data owner should login. Data owner will upload the files. Those files are split into multiple parts and then triple encrypted and stored into the database. If any user wants to access that files, then data owner needs to provide the keys for that file. If admin accept the users request to access the file, then data owner will provide the keys for that file. The Data Owner Flow Chart shows in Figure 4.

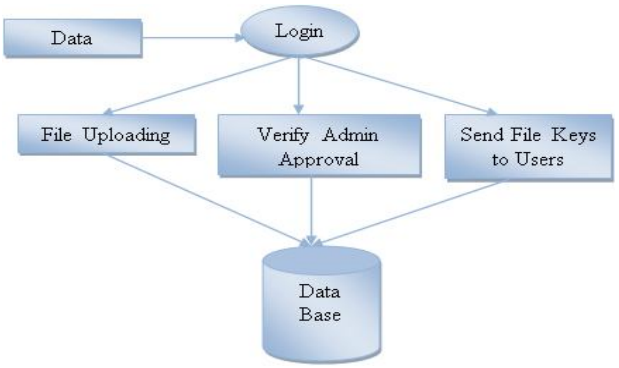

Figure.4: Data Owner Flow Chart

D. Moving Target Defense:

This is the third module of the project.
In this module file uploaded by the data owner will split into multiple parts, then first the content will encoded in the network, then it will undergo DES encryption, then again that encrypted data is encoded, and then store in the database. And admin need to modify the keys to protect the data from the attackers. He will alter the key size also. And the Moving Target Defense Flow Chart shows in the Figure 5.

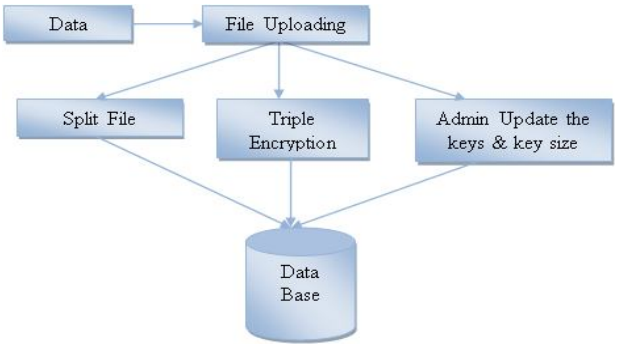

Figure.5: Moving Target Defense Flow Chart

E. User:

This is the fifth module of this project.
In this module user need to register and then login. Then user can search the files based on the file name. If the file exist it will display, else it shows the message that file not exist. The file available, then user will download the file, which is triple encrypted format. So, then user required the keys to decrypt the file. So, user will send the request to provide the keys. Then admin will accept his request. Some updated keys will display to the user, at the time user try to download original file multiple times then user treated as attacker. Data owner will provide the keys for file then user can download the original file. The User Flow Chart shows in Figure 6.

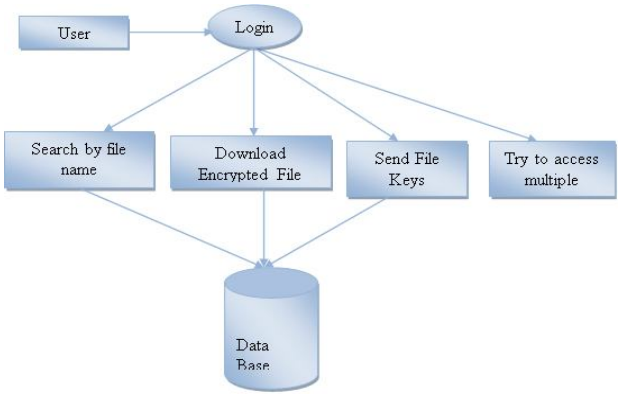

Figure.6: User Flow Chart

7. ALGORITHM USED

7.1 k-NN Secure Schemes with Key-sharing:

By using the k-NN key-sharing schemes,[6] we can assume that the query of the users is secured from attackers and the keys are known to the data owner. And keys are approved by the admin to the data owner.

7.2 Trapdoors Public-Key Cryptosystem:

By using Trapdoors Public-Key Cryptosystem (TPKC) we can easily encrypt and decrypt the data. It is very secure to attack and crack the data that using this algorithm. To know the (TPKC) and its application and so on see [4].

8. CONCLUSION

We suggest a new encryption method that incorporates both the characteristics of DES and network coding which has good behavior to avoid both exhaustive and analytical attacks. The result of the simulation shows that the proposed schemes running ration is comparatively lower than or equivalent to triple Des. In this concept of moving Target Defense (MTD) the NC Design of the proposed system endows it with complex active and random characteristics.

REFERENCES

[1] Moving Target Defense
Creating Asymmetric Uncertainty for Cyber Threats
Editors: Jajodia, S., Ghosh, A.K., Swarup, V., Wang, C., Wang, X.S. (Eds.)--
https://www.springer.com/gp/book/9781461409762
[2] Moving Target Defense II
Application of Game Theory and Adversarial Modeling--
Jajodia,S., Ghosh, A.K., Subrahmanian, V.S., Swarup, V., Wang, C., Wang, X.S. (Eds.)--
https://www.springer.com/gp/book/9781461454151.
[3]Moving Target Defense for Web Applications using Bayesian Stackelberg Games Satya Gautam Vadlamudi,

Sailik Sengupta, Marthony Taguinod, Ziming Zhao, Adam Doupé, Gail-Joon Ahn, Subbarao Kambhampati. http://rakaposhi.eas.asu.edu/aamas16-mtd.pdf.
[4]Emmanuel Bresson,Dario Catalano David Pointcheval- A Simple Public-Key Cryptosystem with a Double Trapdoor Decryption Mechanism and Its Applications.
[5]Attestation Using Visual Cryptography (3,3) Scheme. Dodda Pratap Roy, Dr. M Jaya Bhaskar. http://www.warse.org/IJETER/static/pdf/file/ijeter06832020.pdf
[6] https://en.wikipedia.org/wiki/K-nearest_ neighbors _algorithm.
[7]https://en.wikipedia.org/wiki/Data_Encryption_Standard.
[8] Assessment of Website Quality based on Appearance. B. Vishnu Priya, Dr. JKR Sastry .http://www.warse.org/IJETER/static/pdf/file/ijeter017102019.pdf
[9]https://en.wikipedia.org/wiki/Networking_and_Information_Technology_Research_and_Development.
[10] Moving-Target Defenses for Computer Networks-2014.Marco Carvalho, Richard Ford