Journal of Engineering Sciences

Vol 10, Issue 9, Sept /2019
ISSN NO:0377-9254

A Moving Target Defense For Data Communication Over Networks Using AES Based Dynamic Encryption Scheme

[1]Nelofar Khusboo, [2]Nasira Mahjabeen
[1]PG Scholar, MTech, Dept of CSE, Shadan Women's College of Engineering and Technology HYD, T.S.
nelofarkhushboo123@gmail.com
[2]Asst Professor, Dept of CSE, Shadan Women's College of Engineering and Technology HYD, T.S.

Abstract - Moving target defense (MTD) is one of the internet game-changing progressive advances proposed by Federal Networking, IT Research and Development (NITRD) as of late. These days, organize security arrangements are normally deterministic, static and homogeneous. These highlights lessen the troubles for digital aggressors checking the web to distinguish explicit targets and assemble basic data. In this way, the assailants accept the uneven facts of interest of structure up, propelling and spreading assaults, protectors stand upon latent position. The present-day barrier instruments besides procedures can't switch this circumstance. MTD is planned additional progressive innovation to variation the awry circumstance of assaults and barriers. It continues affecting the assault apparent about affecting the guaranteed focus through powerful moving, that cloud be controlled and overseen finished by the director. Alongside of appearances, the assault surface presented to assailants seems confused in addition changes constantly. End to end these outlines work as exertion, i.e., the expenditure and unpredictability for assailants to statement a fruitful assault, determination remain enormously expanded. Therefore, fruitful assaults succeed to diminished, with intensive about effective versatility aside from protection to ensured target always be improved adequately. The upheavals of MTD cloud be abridged from the associated three perspectives: (I) Dynamic guard: the modification from static to dynamic in framework engineering. (ii)Active barrier: the variation from inactive observation into effectively setting squares to shortcoming and infection privacy component. (iii)Flexible safeguard: the transformation from ordinary into an adaptable activity mode. The important determination of MTD be about through prefect the dynamic resistance toward, outside assaults, obscure vulnerabilities and indirect accesses. Until this point in time, MTD considered in distinguish settings, including distributed computing also web applications.

Index Terms—Moving target defense, dynamic defense theory, cyber security, linear network coding, AES.

I. INTRODUCTION

The comparable powerful thought can similarly embrace in cryptography plan. It's notable that Advanced Encryption Standard (AES), generally utilized as a standard symmetrical encryption. Cutting-edge effective interim, AES has build-up a structure on the adjacent of impressive improvement and consumption of current time square figure hypothesis. At present, beside the quick improvement of figuring power, the countless iterated square figure AES has revolved obtainable towards continue delicate, which causes the effective acknowledgment of AES split, thorough assault. Hence, it's fastest than by triple-DES calculation also encoder has a huge enough key space compare triple-DES.The comparable powerful thought can likewise be received in cryptography design. The fundamental goal of MTD [1],[2] is to accomplish the dynamic defense to the outside attacks dependent on obscure vulnerabilities and secondary passages. Until this point, MTD has been examined in different settings, including distributed computing and web applications [6], [7]. It is outstanding that Advanced Encryption Standard (AES) has been generally utilized as a standard symmetrical encryption. In the meantime, AES has established a framework for the development and utilization of present-day square figure hypothesis. At present, with the quick development of computing power, the great iterated square figure AES has a strong encryption, which causes the compelling acknowledgment of AES split by the thorough attack. Thus, it has gradually been supplanted by the triple-DES algorithm or Advanced Encryption Standard (AES) so that the encoder has a large enough key space. Besides, reference [9] concluded that AES can oppose the Timing Attack effectively too. Likewise, so as to streamline AES, many improved algorithms have been proposed, for

Journal of Engineering Sciences

example, various AES, changeable Sub-byte, shift row, add round keys and so on Although the previously mentioned algorithms, for example, the triple DES and DES have gradually supplanted the established AES, despite everything they can't meet the dynamic security necessities of the intelligent information network because of their static expansion to the key space. In this paper, we present an encryption plan to improve AES under the concept of MTD, by methods for (direct) network coding (NC), which advocates straightly combining coding along with data propagation [10]. The following two reasons rouse us to pick NC. To start with, NC, which has been utilized in and for encryption conspire design, changes the static idea of network information transmission, so it is a good match to accomplish the dynamic, dynamic and random highlights of MTD as characterized [3]. Second, the utilization of NC as an encryption plot can possibly oppose the thorough attack, as a L-bit plaintext may relate to conceivable cipher texts. We make the following principle commitments in this paper:

We propose a novel encryption plot consisting of 3 layers. The internal and external layers basically perform NC and the center layer executes AES. In consequence, the new plan has good conduct to oppose both thorough and investigation attacks. We additionally approve that the running proportion of the proposed plan is generally lower than or practically identical to the triple DES.

The proposed plan can accomplish the MTD includes by the following methodology. Initial, a re-encryption procedure can be actualized on the external NC layer of the plan, with the goal that the key and cipher texts can be progressively changed. Second, the key length can be effectively expanded, with the goal that the plan is versatile to the fast development of the computing power. Third, the parameters in the plan can be adapt ably picked, so that there is a change among efficiency and security.

II. PRELIMINARIES

A. AES Features against Analysis and Exhaustive Attack

In the investigation of Cryptanalysis, the efficiency of the examination assault to split a figure relies upon the seasons of encryption emphasis. References [20] demonstrated that the principle of picking legitimate occasions of cycle pursues that creation the efficiency of examination assault is lower than that of thorough assault: if the seasons of emphasis in AES is under 10, investigation assault (like DC or LC) will have the higher efficiency contrasted with the comprehensive assault. The motivation behind why this principle is alluring is that it makes making a decision about the quality and the upsides of a calculation quite basic: if there is no achievement in Cryptanalysis, the quality of any encryption calculation fulfilling the principle just relies upon the key space.

At present, AES can keep the computational security with the fast improvement of processing power. The comprehensive assault makes the compelling break AES with a much lower cost. Be that as it may, AES still has kindhearted incalculability to examination assault and timing assault. In existing AES varieties, encryption is delicate before the man-in-the-center assault and it can accomplish the objective of utilizing numerous encryptions to increase the key length. The triple encryptions increase the key length which is computationally secure and broadly utilized for the present. Be that as it may, the encryption/unscrambling multifaceted nature of the triple DES is multiple times the single AES, and each time the dynamic re-encryption procedure of the triple DES requires decoding the first message first and after that encrypting it again dependent on another key. Along these lines, the triple DES isn't appropriate for effective dynamic digital security assurance as required in clever networks. In the meantime, the previous examination is additionally meaningful to AES. So it is critical to locate another approach to accomplish dynamic digital security with proficient activities and low multifaceted nature.

B. Network Coding (NC) and Matrix Representation of Finite Fields

In the hypothesis of NC [19][20], information images transmitted along the edges in a network have a place with a limited field GF(q), where q can be either a prime or a prime power. Each cordial edge of a hub v transmits an information image that is a GF(q)- straight blend of the incoming information images to v. Such a coding instrument is alluded to as NC. In particular, expect the data on the incoming edges to be a double sequence and after

Journal of Engineering Sciences

that partition the sequence into L squares (vectors) m1, m2… mL of a fixed length d. The fixed length equals the component of the augmentation field GF(2d) and each mi can be viewed as either a parallel vector over GF(2) or a component over GF(2d). At that point, each cordial edge likewise transmits a GF(2d)- direct mix of data on every single incoming edge.

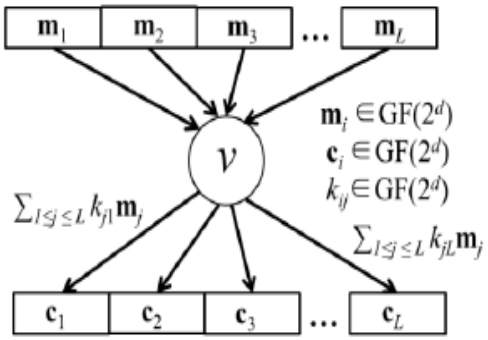

Fig. 1. NC Operations

The previously mentioned instrument of NC has been examined for the utilization in expansive scale conveyed capacity frameworks. For the situation that the component of the expansion field GF(2d) is exceptionally huge and progressively changed, rather than putting away a few query tables, it is important to locate an advantageous method to acknowledge both increase and expansion math over GF(2d).

III. DESIGN OF THE ADVANCED ENCRYPTION SCHEME

In this section, we present a novel encryption scheme with an efficient dynamic encryption process, which has a good behavior to resist both exhaustive and analysis attacks, and the potential to be compatible with existing secure NC schemes. The proposed encryption scheme, consists of 5 steps

1. User Interface Design
2. Admin
3. Data Owner
4. Moving Target Defense
5. User

DESCRIPTION

1. User Interface Design

We plan the windows for the venture. These windows are functional aimed at secure login clients. To associate with server user must give their info & secret word then no hacker can access accept user ready to plug-in to server. User got a tiny chance to consumer exits straight forwardly can login else client must enroll their details, client name, confidential key & email id. Host determination create the register up transfer & download rate. Name will be fixed as client id. Signing in take to enter a requested page.

2. Admin

Admin login. Administrator outlook the restraints of records owners and clients. Administrator has data about records, and direction of shield the keys from assailant by refreshing the text keys consistently. Administrator favor the article demand from client and send to information proprietor to proposal authorization to acquire to the records. Admin will get the aggressor subtleties, clients who will get the files without document owner authorization.

3. Data Owner

Information proprietor will transmission of the documents. Those documents are part into various slices end to end with triple scrambled in database. Fortuitous a certain any client need to access that records, all in once information proprietor essential to give the keys to that document. Continuously the rotten opportunity that administrator acknowledge the user's solicitation a document, point information proprietor will deliver the keys to that record.

4. Moving Target Defense

Document transferred by the records manager will part into numerous parts, formerly the substance will encoded in system, experience AES encryption, that scrambled statistics is encoded, and after that stored in, database. Also, administrator duty to alter the keys to protection the manuscript away the aggressors. He will adjust key size too.

5. User

Completely as soon as client can look over,

Journal of Engineering Sciences

documents focus on initial heading name. Else it show that document not exist. The text accessible, a reader will download the record, triple encoded design. It's a way, at that moment client required the keys to unscramble the document. Client will send the solicitation to give the keys. Instant admin will acknowledge his solicitation. Some refreshed keys will show to client, client effort to download unique text on numerous occasions then client treated as aggressor. Information proprietor will provide keys to document then user can download the foremost record.

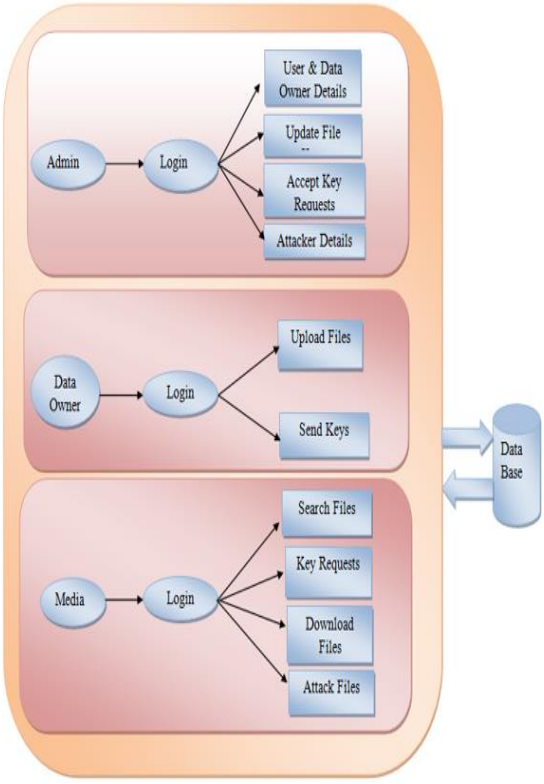

Fig 2 System Architecture For Encryption

1. Upload the file by data owner.
2. File will split into four parts like (file size/4)
3. Then by using Base64 class in Java 8. There are methods for encoding.
   a. static Base64.Encoder getEncoder();
   b. Base64.Encoder base64Encoder= Base64.getEncoder();
4. Then Encoder class object will created above. Then the method in that Encoder class and which will take content and that is converted into UTF-8 form. (Unicode Transformation Format)
   a. byteArray = base64Encoder.encode(text.getBytes("UTF-8"));
   b. There text means content, and that will converted into UTF-8, then that content will converted into byte array data.
5. Then that byte array data and encrypted key which is generated randomly to Cipher which will convert into cipher text.
   a. Key desKey = new SecretKeySpec(key.getBytes(), "AES");
   b. Cipher cipher = Cipher.getInstance("AES");
   c. cipher.init(Cipher.ENCRYPT_MODE, desKey);
   d. byte[] encrypted = cipher.doFinal(byteArray);
   e. There first key will generated, then Cipher class object is created and that is used for AES encryption, and then byte array content will encrypted in doFinal() which will take the byte array content.
6. Then we will get cipher text in the form of byte array, then it will give as input to Base64 Encoder class, then it will convert into byte array by using base64Encoder.encode() method.
7. Then that byte array is converted into string form and stored in database.
   a. String ekey = new String(encrypted);
8. By above mentioned manner whatever the data uploaded by the data owner will undergo network coding, AES encryption, and network coding.

For Decryption

1. Initially user will get the original keys, then user will uploaded the keys.
2. Then based on the public key which is FILEID, all the four parts will get according to their keys.
3. Then each part of file and key related to that part will given decryption(String text, String key).
4. Then initially by Base64 class we will create Decoder class object.
   a. Base64.Decoder base64Decoder= Base64.getDecoder();
5. Then the content (text) is converted into byte array form using text.getBytes().
6. Then content will decode by using base64Decoder.decode(byteArray);
7. Then we will get the cipher text and key, those will given Cipher class object

a. Key desKey = new SecretKeySpec(key.getBytes(), "AES");
b. Cipher cipher = Cipher.getInstance("AES");
c. cipher.init(Cipher.DECRYPT_MODE, desKey);
d. String decrypted = new String(cipher.doFinal(encrypted));
e. At last we will get the encoded data by decrypting the cipher text with that key.

8. Then that decrypted content is passed through Decoder class object
   a. byte [] byteArray = decrypted.getBytes();
   b. byte[] strdec=base64Decoder.decode(byteArray);
   c. String ekey = strdec.toString();
   d. By that the original content is retrieved.
9. Then all the four parts content will added to a string and stored into one file and that will given to User.

IV. RESULT

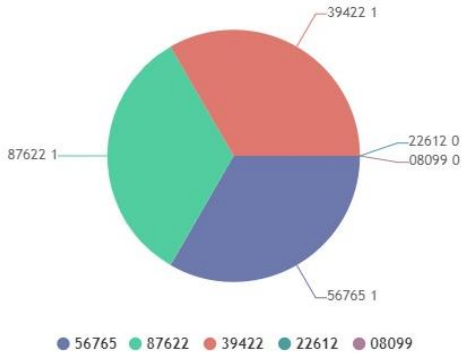

Fig 3 Request Files

- The above fig 3 shows requested files from the users. Green color indicates files are mostly requested.

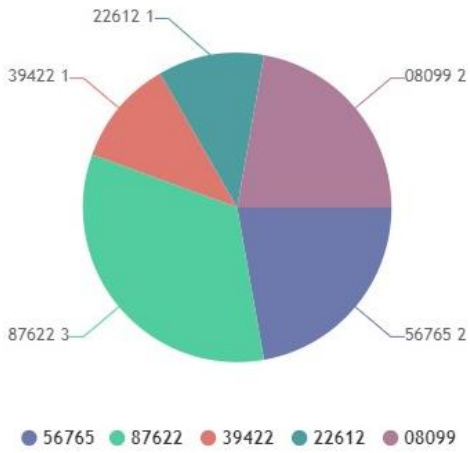

Fig 4 Attacked Files

- The different colors indicates different files which are attacked by the intruders and depicts the percentage of mostly attacked files.

V. CONCLUSION

Overall it's a proposition of a novel encryption conspire which consolidates both the AES, effective system coding trademark and has great conduct to oppose both comprehensive and examination assaults. The reproduction results demonstrate the running proportion of proposed plan is commonly fastest and greater at that time as well the triplex DES. The NC idea of the current plan causes it to enrich the dynamic, dynamic and arbitrary attributes are the thought of Moving Target Defense (MTD).

REFERENCES

[1] S. Jajodia, A. K. Ghosh, V. Swarup, C. Wang, X. S. Wang, Moving Target Defense—Creating Asymmetric Uncertainty for Cyber Threats, Germany: Springer, 2011..

[2] S. Jajodia, A. K. Ghosh, V. Subrah manian, V. Swarup, C. Wang, and X. S. Wang, Moving target defense II, Application of Game Theory and Adversarial Modeling. Series: Advances in Information Security, Springer Science & Business Media, New York, 2013.

[3] M. Carvalho and R. Ford, ―Moving-target defenses for computer networks. ‖ IEEE Security & Privacy, vol. 2, no.12, pp. 73-76, 2014.

[4] W. Peng, F. Li, C.-T. Huang, and X. Zou, ―A moving-target defense strategy for cloud-based

services with heterogeneous and dynamic attack surfaces,‖ IEEE International Conference on Communications (ICC), Sydney, Jun., 2014.

[5] A. D. Keromytis, R. Geambasu, and S. Sethuma dhavan, ―The meerkats cloud security architecture,‖ IEEE International Conference on Distributed Computing Systems Workshops, Macau, June, 2012.

[6] S. G. Vadlamudi, S. Sengupta, and S. Kambhampati, ―Moving target defense for web applications using bayesian stackelberg games,‖ International Conference on Autonomous Agents & Multiagent Systems, Singapore, May, 2016.

[7] M. Taguinod, A. Doupé, Z. Zhao, and G.-J. Ahn, ―Toward a moving target defense for web applications,‖ in Information Reuse and Integration (IRI), IEEE International Conference, San Francisco, Aug, 2015.

[8] L. Z. Gu, Z. H. Zheng, Y. X. Yang, Modern Cryptography. China: Publishing House of Beijing University of Posts and Telecommunications, 2015.

[9] W. Stallings. Cryptography and Network Security Principles and Practice. 5th ed, NJ, USA: Prentice Hall Press Upper Saddle River, 2010

[10] S. R. Li, Q. T. Sun, Z. Shao, ―Linear network coding: theory and algorithms,‖ Proceedings of the IEEE, vol. 99, pp. 372-387, Mar. 2011

[11] X. Wang, R. Zeng, "The analysis and improvement of DES algorithm," Journal of Shiyan Technical Institute, vol. 19, No.5, pp.84-86, Oct. 2006.

[12] B. Jiang, "Analysis of DES Algorithm Implementation and Improvement Process," Journal of Langfang Teachers College, vol. 10, No.5, pp.46-47, Oct. 2010.

[13] J. X. Gao, "Implementation and improvement of DES algorithm," Network Security Technology & Application, vol. 1, pp.61-62, 2014.

[14] A. Hevia, M. Kiwi, "Strength of two data encryption standard implementations under timing attacks," ACM Transaction Information and System Security, vol. 2, pp. 416-437, Nov. 1999.

[15] P. F. Oliveira, J. Barros, "A network coding approach to secret key distribution," IEEE Transactions on Information Forensics and Security, vol. 3, pp. 414-423, Sep. 2008.

[16] P. Zhang, C. Lin, Y. X. Jiang, "A lightweight encryption scheme for network-coded mobile Ad Hoc networks," IEEE Transactions on Parallel and Distributed Systems, vol. 25, pp. 2211-2221, Sep. 2014.

[17] B. Schneier. Applied Cryptography. New York: Wiley John Sons, pp. 873- 874, 1996.

[18] C. Paar, J. Pelzl. Understanding Cryptography: A Textbook for Students and Practitioners. Germany: Springer, 2009.

[19] S.-Y. R. Li, R. W. Yeung, N. Cai, "Linear network coding," IEEE Transaction of Information Theory, vol. 49, pp. 371-381, Feb. 2003.

[20] R. Koetter, M. Medard, "An algebraic approach to network Coding," IEEE/ACM Transactions on Networking, vol. 11, pp. 782-795, Oct. 2003.

[21] A. G. Dimakis, K. Ramchandran, Y. Wu, C. Suh, "A survey on network codes for distributed storage," Proceedings of the IEEE, vol. 99, pp. 476-489, Mar. 2011.

[22] C. Gkantsidis, R. P. Rodriguez, "Network coding for large scale content distribution," IEEE Infocom, Miami, Mar, 2005.

AUTHOR'S PROFILE

Ms. NELOFAR KHUSBOO has completed her B.Tech from Asifia College of Engineering and Technology, JNTUH University, Hyderabad. Presently, she is pursuing her Masters in Computer Science from Shadan Women's College of Engineering and Technology, JNTUH University, Khairtabad, Hyderabad, TS. India.

Ms. NASIRA MAHJABEEN has completed B.Tech (CSE) from Dr.V.R.K College of Engineering and Technology, JNTUH University, Hyderabad. M.Tech (CSE) from Shadan Women's College of Engineering and Technology, JNTUH University, Khairtabad, Hyderabad. Currently she is working as an Assistant Professor of CSE Department in Shadan Women's College of Engineering and Technology, Khairtabad, Hyderabad, TS. India.

Journal of Engineering Sciences