International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

# A Framework for Moving Target Defence with Data Encryption Standard

**G.Lohitha, P L Srinivasa Murthy, N. Shalini**

***Abstract:*** ***Moving Target Defence (MTD) became an important research area in the wake of increased cyber security threats. As the attackers are gaining knowledge on existing methods, it is essential to have more dynamic approach that can defeat plans of attackers. As improving systems with higher level of security is a never ending process, MTD has got significance in military and other applications where critical digital infrastructure needs to be protected from adversaries. When attack surface is dynamically evolving with mutation strategy, it can lead to realization of MTD. As MTD increases complexity and uses dynamic encryption mechanism, the attack surface evolves from time to time confusing attacker. Traditional approaches like AES and DES alone will have their limitations. However, when they are used along with the concept of MTD strategies, it is possible to provide highly secure environment. In this paper, we proposed a framework with an underlying algorithm which ensures MTD with dynamically evolving attack surface and dynamic encryption standards based on DES. The experimental results revealed that the proposed scheme is effective and shows improved performance over its predecessor.***

***Index Terms –Security, cyber security, encryption, DES, moving target defence, network coding***

## I. INTRODUCTION

Networks of different kinds need secure communications. With the emergence of wireless networks like Wireless Sensor Network (WSN) and Mobile Ad Hoc Network (MANET), there is ever growing list of applications of such networks. There are multimedia content distribution systems that work on top of MANET and other such wireless networks [1]. In any application where there is data transfer among nodes in the network, security is very important. There have been many security primitives. Widely used approach is cryptography. It has different methods like symmetric and asymmetric based on key sharing phenomenon. They are shown in Figure 1 and Figure 2. There are different approaches in cryptography. They include Elliptic Curve based solutions [2], homomorphic encryption schemes [3] and AES [5] to mention few. The traditional cryptographic methods like DES and AES are not actually dynamic in nature. To overcome this drawback, dynamic encryption schemes like Synchronous Dynamic Encryption System (SDES) [10] came into existence.

Gradually, the dynamic encryption research led to Moving Target Defence (MTD) which provides evolving and dynamic attack surface which confuses adversaries by making the security system so complex.

Thus MTD can defeat the plans of attackers [17]. In this paper, we proposed a framework that is light weight MTD based on DES to have a dynamic encryption scheme. We proposed an algorithm for achieving this. Different permutations and transformations are used with mutation strategies to achieve better performance. Our contributions are as follows.

- We proposed a framework for realizing a novel light weight framework with MTD based on DES.
- We proposed an algorithm named Lightweight Target Defence Scheme (LTDS) which has different levels of encryption besides multiple iterations followed by DES leading to MTD which gets dynamically evolving attack surface.
- We built an application to show the effectiveness of the proposed scheme when compared with existing MTD approach.

The remainder of the paper is structured as follows. Section 2 provides literature on security and dynamic encryption standards. Section 3 provides preliminaries to understand the proposed scheme. Section 4 presents the proposed scheme in detail. Section 5 presents experimental results. Section 6 concludes the research and gives directions for future work.

## II. RELATED WORK

This section provides review of literature related to secure communications in networks. Sethuraman et al. [2] proposed Diffie Hellman algorithm for security based on Fuzzy Genetic Elliptic Curve (FGEC). With respect to data aggregation and security, Kapusta et al. [3] proposed a homomorphic encryption scheme. It is suitable for data security and secure communications over sensor networks. Split algorithm is proposed by Singh and Sharma [4] for cloud storage security. Musliana et al. [5] enhanced AES based on temporal key generation process. Rajesh et al. [6] on the other hand proposed a lightweight encryption scheme for secure transfer of data in embedded systems.

Manuscript published on 30 September 2019
* Correspondence Author
**G.Lohitha*,** Department of CSE, Institute of Aeronautical Engineering, Dundigal, Hyderabad, India.gudalohithareddy4@gmail.com,
**P L Srinivasa Murthy,** Associate Professor , Department of CSE, Institute of Aeronautical Engineering, Dundigal, Hyderabad, India. pl.srinivasamurthy@iare.ac.in,
**N. Shalini,**Assistant Professor, Department of CSE, Institute of Aeronautical Engineering, Dundigal, Hyderabad, India.
nimma.shalini26@gmail.com

Chaos and secure Hashing concepts are employed by Zhu et al. [7] towards image encryption.

A dynamic encryption algorithm known as DEA-RTA is proposed by Omari et al. [8] for security in real world applications. Encryption algorithms and their parameters are extensively studied in [9] while the applications related to SDES are investigated in [10].

Dynamic encryption is studied in [11] with hiding techniques based on the notion of corner point. Moving Target Defence for computer networks is investigated in [12] while the same is explored for cloud based solutions in [13]. For MANET a lightweight encryption scheme is proposed in [14] which is coupled with network coding. The network coding approach is also used in [15] for secret key distribution in a secure way.

Network coding approach is evaluated with large scale content distribution systems in [16]. From the review of literature, it is understood that the developments in cryptography led to the creation of MTD system which will have dynamically evolved attack surface that confuses attacker more and defeats any plans of attacks. Existing MTD system presented in [17] is the motivation behind this paper. In this paper we proposed a framework that exploits different mutation strategies based on the attacker's approaches. Thus the proposed system shows comparable performance improvement over the existing.

## III. PRELIMINARIES

This section provides preliminaries that help in understanding the proposed lightweight framework. In the security domain, encryption is the procedure which takes plain text and converts it into some form which cannot be understood by humans. The input text is also known as secret message that needs to be protected from attacks. When secret message is transformed into some format that cannot be interpreted to gain meaning, that text is known as cipher text. When the reverse process is carried out, it is called as decryption. The result of decryption procedure is the original secret message that has been subjected to transformation. The cryptography domain has two important kinds of encryption and decryption. They are known as symmetric and asymmetric encryption standards. The former is shown in Figure 1 while the latter is presented in Figure 2.

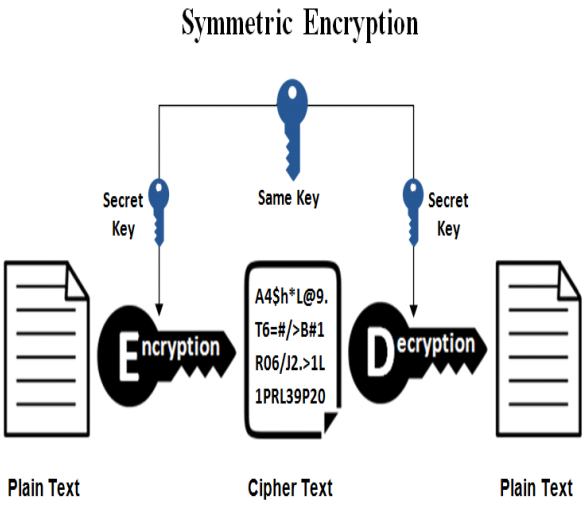


**Figure 1: Symmetric encryption process**

Symmetric cryptography employs a single key for both operations such as encryption and decryption. When sender of secret message encrypts it with certain key, the same key needs to be used by the receiver in order to obtain plain text again. It is evident in the key transfer shown in Figure 1. The issue with this kind of encryption is that key needs to be transferred to the recipient of the message. Therefore, it causes security problems. In order to overcome the problem of key sharing, asymmetric encryption came into existence. This encryption standard does not need key sharing. It follows different phenomenon to avoid key sharing.

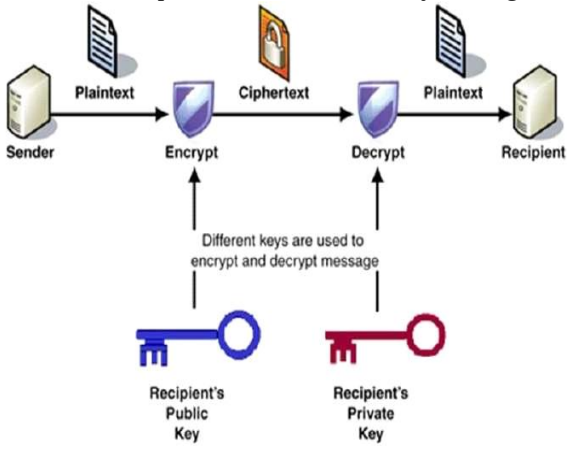


**Figure 2: Asymmetric encryption process**

In order to get rid of key sharing, the asymmetric cryptography involves two keys given to each participant. In other words, both sender and receiver will have two keys pre-distributed. One key is called private key while the other key is known as public key. The former is kept secret while the latter is disclosed to public. Thus the sender is aware of public key of the receiver. Therefore, the data is encrypted with the public key of the receiver. Then such encrypted text can only be decrypted by the receiver. The recipient's privacy is used to decrypt the message. As the users do have key combination and can decrypt data without actually sharing key, it promotes security and avoids key sharing issue. The encryption standard used in the scheme proposed in this paper is DES. The modus operandi of DES in terms of encryption and decryption is as shown in Figure 3.

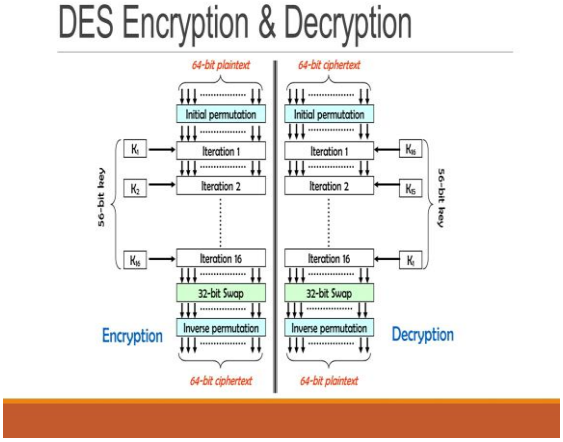


**Figure 3: DES encryption and decryption processes**

The encryption process in DES has many iterations, swapping and inverse permutation to generate 64-bit cipher text by taking 64-bit plain text. The reverse process is then carried out in order to generate the original message. It is one of the symmetric key encryption schemes which makes use of 56-bit key. It played crucial role in the improvement of security of systems earlier.

However, it is preferred in the modern systems selectively. It uses block cipher concept for encryption and decryption. It is very widely used algorithm for secure communications. Many companies developed products based on DES for security. There is an enhanced form of DES known as Triple DES which provides better security than traditional DES. When DES is applied for three times, the security it provides will be higher.

## IV. PROPOSED FRAMEWORK

In this paper, we proposed a framework for Moving Target Defence (MTD) which highly confuses attackers and defeat the efforts of them. Light weight DES standard is employed in order to realize MTD. DES along with MTD is capable of providing dynamic security to systems. Thus critical digital infrastructure can be protected from malicious attacks. The proposed framework which has methodology to deal with MTD is as shown in Figure 4. It has service provider taking care of finding all nodes status, then choosing neighbour nodes, verify network or moving nodes, finding the nodes that behave dynamically in order to confuse attackers and provide highest level of security to the system.

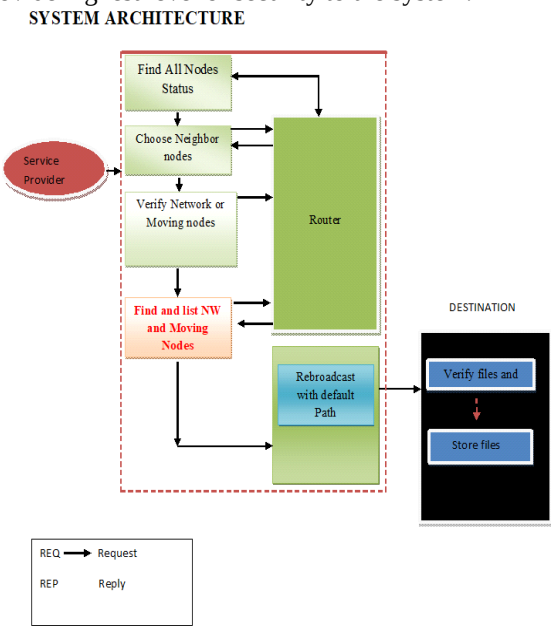


**Figure 4: Proposed framework**

The attacker's strategy if any is analysedand well informed decisions are made. From the given end point, Sibson entropy is computed with respect to the end point considered. The Sibson entropy finds whether the reconnaissance is original or follow-up. Equations (1) and (2) are used to achieve this.

(1)

(2)

In case of non-reconnaissance strategy, attackers exploit half-blind or blind reconnaissance for many purposes. In order to scan entire end-point space, the attacker uses blind reconnaissancestrategy. However, it is not possible for attacker to completely use this approach for some reason. By using Sibson threshold and entropy is it possible to determine whether the attacker is using half-blind or blind approach. Equations (3) and (4) are used to achieve this.

(3)

(4)

It is important to ensure dynamic and randomness towards different strategies of attackers in order to defeat their efforts to compromise systems. Dynamic encryption approach is thus recommended for MTD. This procedure which uses encryption adaptively is conceptually similar to the one illustrated in Figure 5.

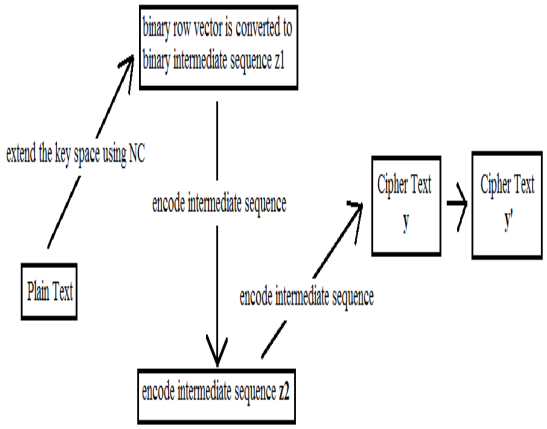


**Figure 5: Shows the encryption process involved in MTD**

As the encryption process is very dynamic and involves network coding, it will be difficult to attackers to succeed in making attacks. Due to its dynamism, the concept of MTD has attracted researchers and academia. Digital infrastructure which needs high level of security can be protected well with MTD proposed. Moreover, it can be employed in the National Cyber Safety and Security (NCSS) activities. As part of the MTD, the probing of forwarding paths is computed as in Eq. 5.

(5)

In the same fashion, the malicious reconnaissance probability is computed with respect to net-flow passes using Eq. (6) and (7).

(6)

(7)

With respect to mutation period, smoothing coefficient alpha is set to 0.75 and the magnitude of $T_{emp}$ is as shown in Eq. (8). In order to increase the magnitude of $T_{emp}$, Eq. (9) is used.

(8)

(9)

Based on the attacker's strategy, the proposed scheme uses corresponding mutation strategy in order to have MTD in an appropriate way. The algorithm proposed to this effect is as in Section 4.2.

### 4.2 Proposed Algorithm

An algorithm named Lightweight Target Defence Scheme (LTDS) is proposed for implementation of the MTD. The algorithm takes secret message and generated encrypted message. However, unlike traditional approaches, it uses number of iterations, permutations and combinations to have dynamic encryption process which will confuse attacker and defeat any sort of attacks made.

**Algorithm**: Lightweight Target Defence Scheme (LTDS)
**Input:** Secret message (plain text) denoted as ***s***
**Output:** Encrypted message ***s'***

- Start
- Initialize binary row vector ***V***
- Initialize low dimension binary matrix ***M***
- ***V***=ConvertIntoBinaryRowVector(***s***)
- ***V'***=DESEncryption(***V***) //intermediate step 1
- ***M***=OuterLayerEncryption(***V'***) //intermediate 2)
- ***C***=GenerateFinalCipherText(***M***)
- ***C'***=DynamicUpdate(***C***)
- Return ***C'***
- End

**Algorithm 1: Lightweight target defence scheme**

As presented in Algorithm 1, there are two intermediate steps in which encryption is taking place. Moreover, DES has many iterations internally for better combinations and permutations. The final cipher text will provide strong protection against different kinds of attacks. The rationale behind this is that the proposed scheme is dynamic and encryption process is dynamic in tune with the MTD mechanism.

## V. EXPERIMENTAL RESULTS

Experiments are made with a prototype application built to show the effectiveness of the proposed scheme. Various cryptographic operations involved are considered for comparison. The performance of the proposed MTD scheme is compared with that of [17]. Different permutation matrices like L, $D_a$, $L_c$and $D_c$ are used with different values for performance comparison.

**Table 1: Execution time of cryptographic operations**

| Cryptographic Operations | Existing Time (sec) | Proposed Time (sec) |
|---|---|---|
| Encryption for the whole scheme | 115.24 | 100 |
| Des in step(b) | 78.14 | 70 |
| Nc encoding in step (a) and (c) | 37.1 | 30 |
| Triple DES encryption scheme | 234.42 | 230 |
| Decryption for the whole scheme | 91.24 | 87 |
| DES decryption for step (b) | 78.14 | 70 |
| NC decoding | 13.1 | 10 |
| Partial Update | 0.004 | 0 |

($L_a$=64, $D_a$=1, $L_c$=16, $D_c$=1)

As presented in Table 1, the proposed scheme is compared with that of existing. Different cryptographic operations are observed in terms of time taken with parameter settings such as La=64, $D_a$=1, $L_c$=16, $D_c$=1.

**Figure 6:**Performancecomparison($L_a$=64, $D_a$=1, $L_c$=16, $D_c$=1)

As presented in Figure 6, the horizontal axis provides different cryptographic operations. The vertical axis shows the execution time taken in seconds. The results revealed that the proposed light weight scheme exhibits better performance over the state of the art when parameter setting is $L_a$=64, $D_a$=1, $L_c$=16, $D_c$=1.

**Table 2: Execution time of cryptographic operations**

| Cryptographic Operations | Existing Time (sec) | Proposed Time (sec) |
|---|---|---|
| Encryption for the whole scheme | 116.91 | 110 |
| Des in step(b) | 79.12 | 70 |
| Nc encoding in step (a) and (c) | 37.79 | 30 |
| Triple DES encryption scheme | 237.36 | 230 |
| Decryption for the whole scheme | 92.8 | 85 |
| DES decryption for step (b) | 79.12 | 73 |
| NC decoding | 13.68 | 10 |
| Partial Update | 0.002 | 0 |

($L_a$=64, $D_a$=1, $L_c$=8, $D_c$=1)

As presented in Table 2, the proposed scheme is compared with that of existing. Different cryptographic operations are observed in terms of time taken with parameter settings such as La=64, $D_a$=1, $L_c$=8, $D_c$=1.

**Figure 7:** Performance comparison ($L_a$=64, $D_a$=1, $L_c$=8, $D_c$=1)

As presented in Figure 7, the horizontal axis provides different cryptographic operations. The vertical axis shows the execution time taken in seconds. The results revealed that the proposed light weight scheme exhibits better performance over the state of the art when parameter setting is $L_a$=64, $D_a$=1, $L_c$=8, $D_c$=1.

**Table 3: Execution time of cryptographic operations**

| Cryptographic Operations | Existing Time (sec) | Proposed Time (sec) |
|---|---|---|
| Encryption for the whole scheme | 112.55 | 105 |
| Des in step(b) | 75.71 | 70 |
| Nc encoding in step (a) and (c) | 36.84 | 30 |
| Triple DES encryption scheme | 227.13 | 220 |
| Decryption for the whole scheme | 88.67 | 80 |
| DES decryption for step (b) | 75.71 | 70 |
| NC decoding | 12.96 | 8 |
| Partial Update | 0.001 | 0 |

($L_a$=64, $D_a$=1, $L_c$=4, $D_c$=1)

As presented in Table 3, the proposed scheme is compared with that of existing. Different cryptographic operations are observed in terms of time taken with parameter settings such as La=64, $D_a$=1, $L_c$=4, $D_c$=1.

**Figure 8:** Performance comparison ($L_a$=64, $D_a$=1, $L_c$=4, $D_c$=1)

As presented in Figure 8, the horizontal axis provides different cryptographic operations. The vertical axis shows the execution time taken in seconds. The results revealed that the proposed light weight scheme exhibits better performance over the state of the art when parameter setting is $L_a$=64, $D_a$=1, $L_c$=4, $D_c$=1.

**Table 4: Execution time of cryptographic operations**

| Cryptographic Operations | Existing Time (sec) | Proposed Time (sec) |
|---|---|---|
| Encryption for the whole scheme | 453.48 | 445 |
| Des in step(b) | 80.35 | 70 |
| Nc encoding in step (a) and (c) | 373.13 | 365 |
| Triple DES encryption scheme | 241.05 | 230 |
| Decryption for the whole scheme | 93.67 | 84 |
| DES decryption for step (b) | 80.35 | 71 |
| NC decoding | 13.32 | 10.2 |
| Partial Update | 0.004 | 0 |

($L_a$=256, $D_a$=1, $L_c$=16, $D_c$=1)

As presented in Table 4, the proposed scheme is compared with that of existing. Different cryptographic operations are observed in terms of time taken with parameter settings such as La=256, $D_a$=1, $L_c$=16, $D_c$=1.

**Figure 9:** Performance comparison ($L_a$=256, $D_a$=1, $L_c$=16, $D_c$=1)

As presented in Figure 9, the horizontal axis provides different cryptographic operations. The vertical axis shows the execution time taken in seconds. The results revealed that the proposed light weight scheme exhibits better performance over the state of the art when parameter setting is $L_a$=256, $D_a$=1, $L_c$=16, $D_c$=1.

**Table 5: Execution time of cryptographic operations**

| Encryption Operations | Existing Time (sec) | Proposed Time (sec) |
|---|---|---|
| Encryption for the whole scheme | 434.78 | 420 |
| Des in step(b) | 76.73 | 70 |
| Nc encoding in step (a) and (c) | 358.05 | 340 |
| Triple DES encryption scheme | 230.19 | 210 |
| Decryption for the whole scheme | 89.76 | 80 |
| DES decryption for step (b) | 76.73 | 71 |
| NC decoding | 13.03 | 10.2 |
| Partial Update | 0.002 | 0 |

($L_a$=256, $D_a$=1, $L_c$=8, $D_c$=1)

As presented in Table 5, the proposed scheme is compared with that of existing. Different cryptographic operations are observed in terms of time taken with parameter settings such as La=256, $D_a$=1, $L_c$=8, $D_c$=1.

**Figure 10:** Performance comparison ($L_a$=256, $D_a$=1, $L_c$=8, $D_c$=1)

As presented in Figure 10, the horizontal axis provides different cryptographic operations. The vertical axis shows the execution time taken in seconds. The results revealed that the proposed light weight scheme exhibits better performance over the state of the art when parameter setting is $L_a$=256, $D_a$=1, $L_c$=8, $D_c$=1.

**Table 6: Execution time of cryptographic operations**

| Cryptographic Operations | Existing Time (sec) | Proposed Time (sec) |
|---|---|---|
| Encryption for the whole scheme | 441.04 | 400 |
| Des in step(b) | 77.37 | 60 |
| Nc encoding in step (a) and (c) | 363.67 | 300 |
| Triple DES encryption scheme | 232.11 | 180 |
| Decryption for the whole scheme | 90.49 | 60 |
| DES decryption for step (b) | 77.37 | 50 |
| NC decoding | 13.12 | 10.2 |
| Partial Update | 0.001 | 0 |

($L_a$=256, $D_a$=1, $L_c$=4, $D_c$=1)

As presented in Table 6, the proposed scheme is compared with that of existing. Different cryptographic operations are observed in terms of time taken with parameter settings such as La=256, $D_a$=1, $L_c$=4, $D_c$=1.

**Figure 11:** Performance comparison ($L_a$=256, $D_a$=1, $L_c$=4, $D_c$=1)

As presented in Figure 11, the horizontal axis provides different cryptographic operations. The vertical axis shows the execution time taken in seconds. The results revealed that the proposed light weight scheme exhibits better performance over the state of the art when parameter setting is $L_a$=256, $D_a$=1, $L_c$=4, $D_c$=1.

## VI. CONCLUSION AND FUTURE WORK

In this paper, we proposed a novel framework for implementation of MTD which is an emerging technique for higher level of security. Unlike traditional DES and AES, it has mechanisms for dynamically evolving attack surface which confuses attacker more to defeat attacks launched by adversaries. With its mechanisms and dynamically changing permutations and combinations while transforming plain text, MTD is superior in providing very confusing outcomes. It leads to dynamic encryption and

decryption schemes. The proposed MTD scheme is based on DES. An algorithm is proposed and implemented. It is known as Lightweight Target Defence Scheme (LTDS). Different permutation parameters are used for mutation strategies. The experimental results showed the performance improvement of the proposed framework over an existing method. In future, we improve the MTD with more mutation strategies possible for better security to systems.

## REFERENCES

1. M. Anandaraj, P. Ganesh Kumar, K. P. Vijayakumar, and K. Selvaraj. (2015). An Efficient Framework for Large Scale Multimedia Content Distribution in P2P Network: I2NC. Hindawi Publishing Corporation Scientific World Journal, p1-12.
2. PriyaSethuraman · P. S. Tamizharasan and Kannan Arputharaj. (2019). Fuzzy Genetic Elliptic Curve Diffie Hellman Algorithm for Secured Communication in Networks. Springer, p1-15.
3. KatarzynaKapusta · Gerard Memmi and Hassan Noura. (2019). Additively homomorphic encryption and fragmentation scheme for data aggregation inside unattended wireless sensor networks. Springer, p1-9.

4. Abhishek Singh and Shilpi Sharma. (2018). Enhancing Data Security in Cloud Using Split Algorithm, Caesar Cipher, and Vigenere Cipher, Homomorphism Encryption Scheme. Springer, p157-166.
5. ZuharMusliyana, TeukuYuliarArif and Rizal Munadi. (2015). SECURITY ENHANCEMENT OF ADVANCED ENCRYPTION STANDARD (AES) USING TIME-BASED DYNAMIC KEY GENERATION. ARPN Journal of Engineering and Applied Sciences. 10, p8347-8350.
6. Sreeja Rajesh, Varghese Paul, Varun G. Menon, and Mohammad R. Khosravi. (2019). A Secure and Efficient Lightweight Symmetric Encryption Scheme for Transfer of Text Files between Embedded IoT Devices. Symmetry, p1-21.
7. Shuqin Zhu, Congxu Zhu, and Wenhong Wang. (2018). A New Image Encryption Algorithm Based on Chaos and Secure Hash SHA-256. Mdpi Entropy, p1-18.
8. Ahmad H. Omari, Basil M. Al-Kasasbeh, Rafa E. Al-Qutaish and Mohammad I. Muhairat. (2009). DEA-RTA: A Dynamic Encryption Algorithm for the Real-Time Applications. INTERNATIONAL JOURNAL OF COMPUTERS. 3, p191-199.
9. Md Asif Mushtaque. (2014). Comparative Analysis on Different parameters of Encryption Algorithms for Information Security. International Journal of Computer Sciences and Engineering. 2, p76-82
10. Hamdy S. Soliman and Mohammed Omari. (2006). Application of Synchronous Dynamic Encryption System (SDES) in Wireless Sensor Networks. International Journal of Network Security. 13, p160-171.
11. Firas A. Abdullatif, Alaa A. Abdullatif and Amna al-Saffar. (2017). Hiding Techniques for Dynamic Encryption Text based on Corner Point. IOP Publishing, p1-10.
12. Marco Carvalho and Richard Ford. (2014). Moving-Target Defences for Computer Networks. IEEE., p73-76.
13. Wei Peng, Feng Li, Chin-Tser Huang and Xukai Zou. (2014). A Moving-target Defence Strategy for Cloud-based Services with Heterogeneous and Dynamic Attack Surfaces. IEEE ICC 2014 - Communication and Information Systems Security Symposium, p804-809.
14. Peng Zhang, Chuang Lin, Senior Member, IEEE, Yixin Jiang, Yanfei Fan, and Xuemin (Sherman) Shen. (2013). A Lightweight Encryption Scheme for Network-Coded Mobile Ad Hoc Networks. IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, p1-11.
15. Paulo F. Oliveira, and João Barros. (2008). A Network Coding Approach to Secret Key Distribution. IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. 3, p414-423.
16. Christos Gkantsidis and PabIo Rodriguez. (2005). Network Coding for Large Scale Content Distribution. IEEE, p2235-2245.
17. Hanqi Tang, Qifu Tyler Sun, Xiaolong Yang and Keping Long. (2018). A Network Coding and DES Based Dynamic Encryption Scheme for Moving Target Defense. IEEE, p1-9.


## AUTHOR'S PROFILE

**Lohitha Guda**, currently pursuing M.Tech in Computer Science & Engineering from Institute of Aeronautical Engineering, Hyderabad, India. She completed her B.Tech in Computer Science from Vivekanda Institute of Technology & Science. She is a final year student doing research on Moving Target Defence with Data Encryption Standard. Her research areas include MTD also known as LightWeight Target Defence System.

**Dr. P L Srinivasa Murthy**,is a Professor in the department of Computer Science & Engineering. He has 23 years of teaching and research experience. He did B.E. in Instrumentation Technology from Gulbarga University, Gulbarga and M.Tech in Computer Science & Engineering from JNT University, Anantapuram. He was awarded Ph.D. in Information Security from JNT University, Kakinada. He has presented 02 papers in International conferences and published 5 papers in various International journals.

**Mrs. N. Shalini**, is an Assistant professor in Department of Computer Science & Engineering at Institute of Aeronautical Engineering, Hyderabad, India. She obtained her M.Tech in Information Technology and B.Tech degree in Computer Science and Engineering. She has 5 years of teaching experience in Computer Organization and Java programming. Her areas of research include " Friend book A Semantic-Based Recoomender System for Social Networks" and " Providing Behavior Preditction with Guarantee solution for Mobile App from Frauds".