IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 5, May 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005098|

Design of 256-bit Data Security Unit with the Analysis of Security Attacks

Paresh Kumar Pasayat, Soumya Ranjan Panigrahi, Manaswini Mishra, Ajay Kumar Manadhata

Assistant Professor, Department of Electronics & Telecommunication Engineering, I.G.I.T., Sarang, India

B.Tech Student, Department of Electronics & Telecommunication Engineering, I.G.I.T., Sarang, India

B.Tech Student, Department of Electronics & Telecommunication Engineering, I.G.I.T., Sarang, India

B.Tech Student, Department of Electronics & Telecommunication Engineering, I.G.I.T., Sarang, India

ABSTRACT: The paper aims to provide a security solution for 256-bits digital data using Cryptography and Steganography techniques during its transmission over the digital network with data integraty test and the analysis of active & passive attacks. The Cryptography technique has been implemented using a newly developed data security algorithm having various operations on the data and the keys and the Steganography technique has been implemented using data cover technique. In order to check the integrity of the data, the data integrity check has been done so as to ensure that the data has not been modified by the attacker during its transmission. The proposed algorithm is found to be resistant towards various types of attacks such as Brute-force attack, timing attack, pattern attack etc. The maximum combinational path delay of proposed project is 14.426ns.

KEYWORDS: Cryptography; Steganography; Combinational Path Delay; Brute-force attack

I. INTRODUCTION

In order to maintain the privacy of the data, different researches are carried out so as to avoid the hacking of the information / data. The privacy can be achieved by using data security techniques. The technique may be A Cryptography Technique or Steganography Technique or the combination of both the techniques. The Cryptography technique uses the concept of encryption process to achieve data security and the the Steganography technique uses the concept of data cover / imge cover / audio cover / video cover to achieve the privacy of the information. In the Proposed algorithm, the data cover has been used to provide privacy to the 256-bits data. In the encryption algorithm, four keys are used to achieve the data security.

II. PROPOSED ALGORITHM

The algorithm used in the proposed work is given as follows:

Step 1: The 256-bits data and four keys having key sizes of 256, 512, 512, 256-bit are given to the 1st block of Cryptography unit which produces 256-bits coded data and the output of the 1st block with eight keys each having 64-bit are given to the input of the 2nd block of Cryptography unit which produces the 256-bit middle encrypted data.

Step 2: The output of the 2nd block of the Cryptography unit and the 256-bits covering data is given to the Steganography unit which produces 512-bits final encrypted data.

Step 3: The reverse operations are performed on the middle encrypted data, final encrypted data and the keys so as to produce the 256-bit data which is the exact repica of the 256-bit original input data.

Step 4: The data integrity test has been done in order to check the integrity of the data (i.e. change in the data (if any)).

Step 5: The analysis of the active and passive attacks has been done with respect to the proposed data security algorithm.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005098|

III. SIMULATION RESULTS

In the simulation result of the encryption unit, the original 256-bits data and four keys are used for the generation of the 512-bits encrypted data.

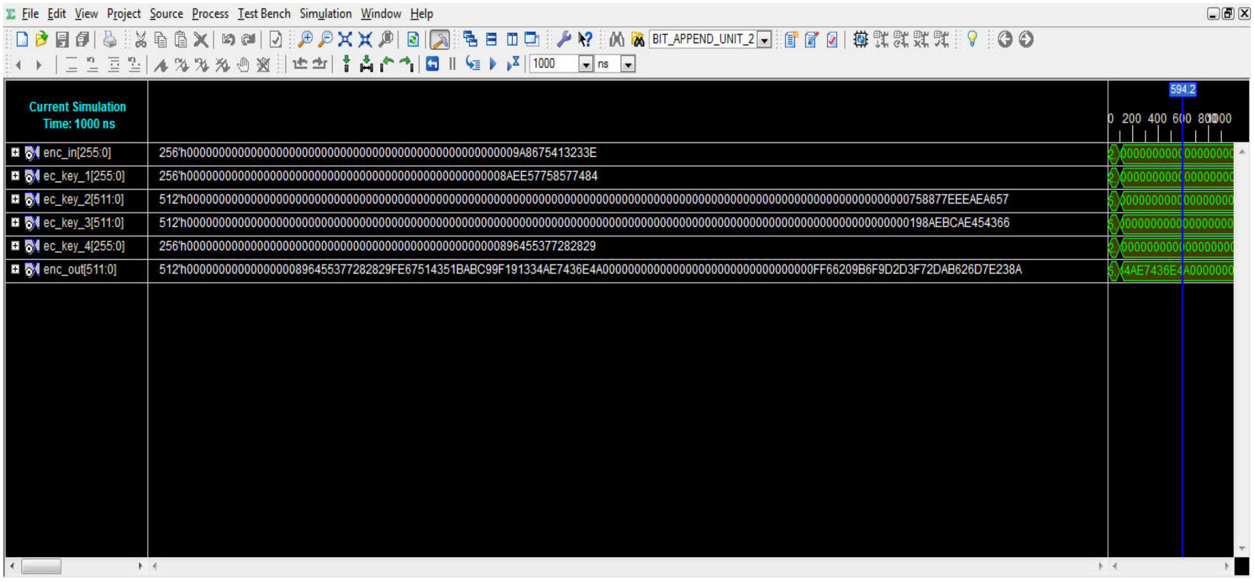

Fig.1. Simulation Result of the Encryption Unit

In the simulation result of the decryption unit, the 512-bits encrypted data and four keys are used for the generation of the 256-bits original / decrypted data.

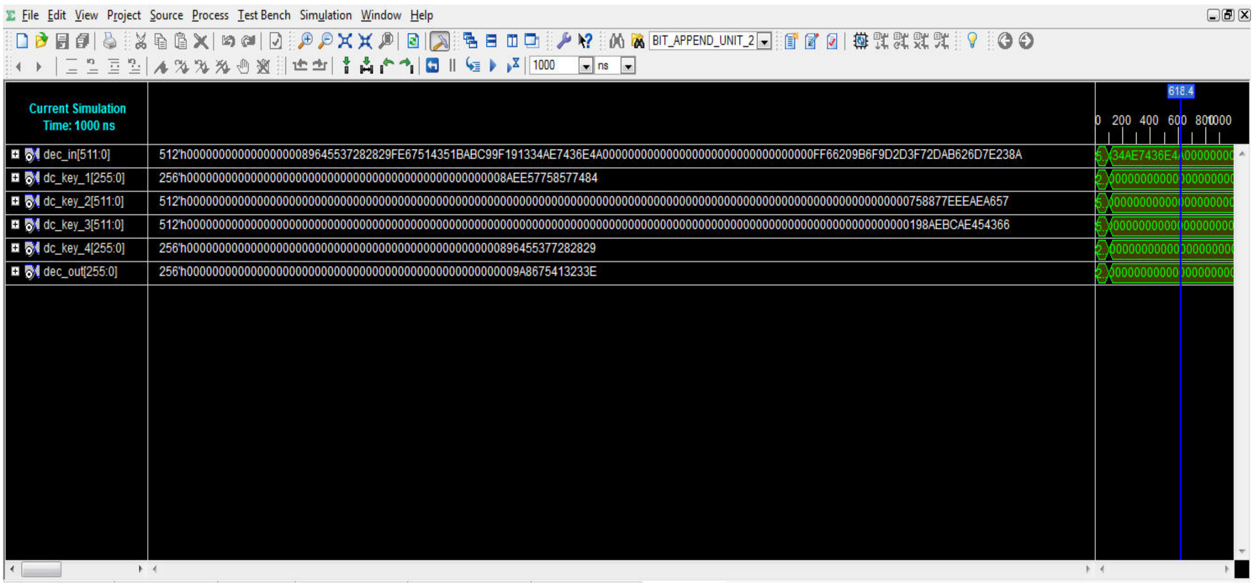

Fig.2. Simulation Result of the Decryption Unit

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005098|

In the simulation result of the Proposed Project with Analysis of Passive Attack, the analysis has been done to know the effect of the passive attack on the various data set with data integrity test.

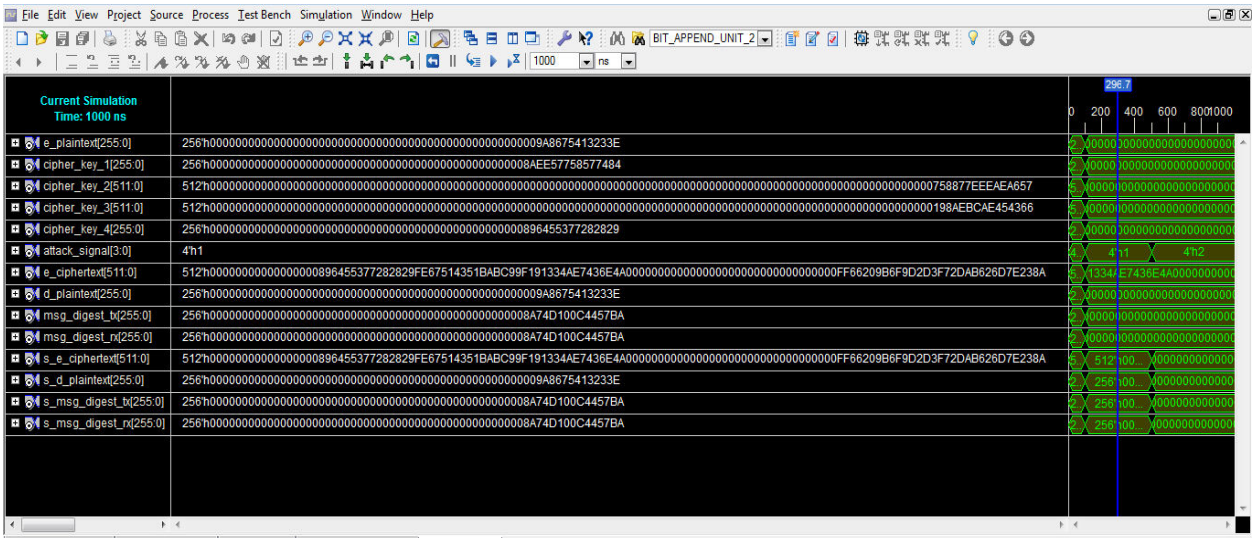

Fig.3. Simulation Result of the Proposed Project with Analysis of Passive Attack

In the simulation result of the Proposed Project with Analysis of Passive Attack, the analysis has been done to know the effect of the active attack on the various data set with data integrity test.

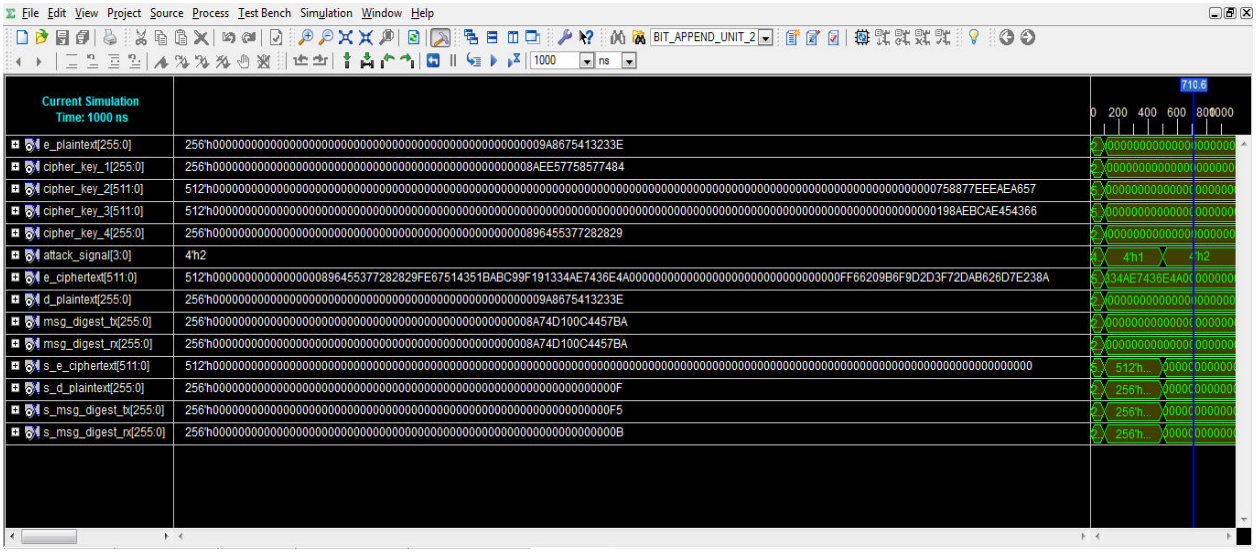

Fig.4. Simulation Result of the Proposed Project with Analysis of Active Attack

IV. CONCLUSION AND FUTURE WORK

The proposed paper shows the analysis of the active and passive attacks with respect to the proposed data security algorithm. The data integrity test has been so as to check the integrity of the data. The proposed algorithm is found to be resistant towards Brute-force attack, timing attack and pattern attack. The maximum combinational path delay is found to be 14.426ns. The proposed security solution can be used in the field of Telecommunication sector, Banking sector and Military sector to provide security to the data.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005098|

REFERENCES

1. Chandrashekhar B, and Dr. Mohamed Abdul Waheed, "Analysis of Possible Attacks on Data and Possible Solutions with Comparative Analysis of Various Encryption Algorithms and Evaluation", International Journal of Innovative Research in Engineering & Management, 2022.
2. Randa Mohamed Abdel Haleem, Eltyeb Elsamani Abd Elgabar, "Enhancing the Integrity of Cloud Computing by Comparison between Blowfish and RSA Cryptography Algorithms", International Journal of Engineering Research & Technology, 2022.
3. Nidhi Kumari, Prof. Vimmi Malhotra, "Secure Cloud Data Storage Using Hybrid Cryptography", International Journal for Research in Applied Science & Engineering Technology, 2022.
4. P. Chinnasamy, S. Padmavathi, R. Swathy, and S. Rakesh,'Efficient Data Security Using Hybrid Cryptography on Cloud Computing', Inventive Communication and Computational Technologies', 2021.
5. W.Xiaoyu, G.Zhengming,'Research and development of data security multi dimensional protection system in cloud computing environment', ICAACI, 2020.
6. S.Riaz, A.H. Khan, M.Haroon, S.Latif, S.Bhatti,'Big data security and privacy', ICIMTECH, 2020.
7. Chunli Su,'Big Data Security & Privacy Protection', International Conference on Virtual Reality & Intelligent Systems', 2019.
8. K.G. Kharade, S.K.Kharade, S.V.Katkar,'Cyber Security - A Method of Generic Authentication of Data with Ip Security', International Journal of Information Systems, 2019.
9. Dr. Prerna Mahajan, Abhishek Sachdeva, 'A study of Encryption AES, DES & RSA for Security', Global journal of computer science & technology, 2015.
10. Rachna Arora, AnshuParashar,'Secure User Data in Cloud Computing Using Encryption Algorithms', International Journal of Engineering Research and Applications, 2013.
11. W. Stallings, 'Cryptography and Network Security ', Prentice hall, 2011.
12. Douglas L. Perry,'VHDL Programming by Examples', TMH, 2010.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details