A Comprehensive Evaluation and Implementation of AES, RSA and Hybrid Cryptographic Algorithms on a Portable Device

Vikrant Shende, Meghana Kulkarni

***Abstract:** In today's internet era, at every moment terabyte of data being generated. It is a challenging task to provide security to such huge data. Cryptography is used as a tool in the modern world to safeguard this data from any attacks. There are many standard cryptographic algorithms available which can be used to protect data. These algorithms vary in cost and performance. Amongst the available standard cryptographic algorithms, we chose AES which is a symmetric encryption algorithm and RSA which is an asymmetric encryption algorithm and a hybrid combination of both for performance analysis. This paper makes elaborate discussions on performance analysis of AES, RSA and AES-RSA Hybrid algorithms and their implementation on a portable device for flexibility and portability.*

Keywords: AES, RSA, Encryption, Decryption, Hybrid.

I. INTRODUCTION

With the widespread use of communication and the internet, it has become imperative to provide security to data that moves on the internet and other media of communication. The art and science of cryptography have contributed in a major way to sections of society related to military, finance and confidential personal communication. Much of the research in the areas of cryptography has been by using or modifying standard algorithms like DES, AES, RSA, Blowfish, CAST and IDEA. Many of these algorithms were once thought of as unbreakable. But with the increase in computing power and globally available resources, these algorithms can be cryptanalyzed [1]. The standard AES, RSA and AES-RSA Hybrid algorithms are implemented in Python programming language and run on portable device raspberry pi 4.

Revised Manuscript Received on October 30, 2019.

* Correspondence Author

Vikrant Shende*, research scholar at RRC, VTU Belagavi.

Meghana Kulkarni, Associate Professor in the Department of PG studies, VTU Belagavi.

II. LITERATURE REVIEW

Ukrit Arom-oon [2], discuss the implementation of the ECB-AES algorithm with 128-bit, 192-bit and 256-bit keys running on Free RTOS. They evaluated the performances of the proposed system based on the communication of UAVs which also includes the control commands and telemetry commands. C. Biswas, U. D. Gupta, and M. M. Haque [3] discuss the hybrid cryptography and steganography. AES encryption is applied to plain text to get cipher text also RSA encryption is used to encrypt the symmetric key used in AES to enhance security. RSA helps in checking the integrity of the received message.

Rajani Devi.T [4], described briefly about working cryptography. Due to widespread public networks, Cryptography may be a notably fascinating field to keep data secret on these networks. Despite the mathematical model behind the best algorithms are widely known and well documented because they are tested and studied my masses. A good encryption algorithm is one which is used over the years. The choice of the keys decides the strength of an algorithm.

I. Hammad, K. E. Sankary and E. E. Masry [5], aims to realize higher field-programmable gate array (FPGA) throughput/area potency compared to the previous loop unrolled pipelined AES encryptor implementations for the ECB cipher mode. They present a high-speed AES encryptor with efficient merging techniques. Whereas previous styles targeted on improving the encoding stage and replicate it to implement the multistage encryptor, this work took advantage of the repeated operations in every stage of the encryptor to realize resources merging and sharing. Comparison between this work and previous works has been performed using identical FPGA devices to ensure a good comparison. The obtained results have indicated real enhancements in terms of potency.

M. Harini ; K. Pushpa Gowri ; C. Pavithra ; M. Pradhiba Selvarani [6], In this paper, a completely unique security protocol suggested for enhancing the safety. The projected hybrid model is more secure against basic attacks that were faced in AES if was used alone. The projected methodology enhances security by adding MD5 encryption and combines the AES encryption into the RSA structure with hashing.

Sonali Mishra, Ananya Dastidar [7], A hybrid encryption technique is applied to the image. This was done to achieve a greater level of Security. At each level, we can opt for the different level of security without corrupting the image.

The calculated MSE value was higher than the non-hybrid technique. They proposed further optimization to achieve stronger PSNR value. They calculated the entropy and encryption time of the Lena image.

Anane Nadjia, Anane Mohamed [8], The AES architectures are implemented on Virtex-5 FPGA. The VHDL is used in ISE 12.2 Design suit to design the model. The ISim is used for functional verification of the architectures.

The Proposed implementations optimize SubBytes and MixColumns stages at the lowest level. High-frequency operation with a small occupied area is achieved with this optimisation.

Vatchara Saicheur, Krerk Piromsopa [9], Here iPhone7 is used to implement the AES algorithm. The 128-bit AES with 512-bit block size is used to develop the algorithm. Increase in performance was achieved with an expanded block. This implementation is useful when running on mobile devices. The data can be made secure with a longer size key.

Fenghua Zhang ,Yaming Chen ,Weiming Meng and Qingtao Wu [10], Authours proposed P-AES algorithm to suit medical data. Here higher efficiency than standard AES algorithm is achieved. RSA is used in hybrid combination with modified AES in the medical information system. This model can give extra security for patients' data and provide protection on the cloud. At present this algorithm can only be used on text data. Also, it can only use a 128-bit key.

Madhumita Panda [11], this paper presents the performance analysis of some chosen symmetrical and asymmetric algorithms. From the obtained results, it was concluded that AES has higher performance than other algorithms in terms of throughput and encryption-decryption time.

III. ALGORITHMS IN OUR EXPERIMENT

Advanced Encryption Standard (AES): The AES encryption algorithm shows the sequence of transformations in every round. The exactly reverse process of encryption gives plaintext by decryption procedure by the same set of keys. AES processes the entire data block as a single matrix during every round using substitutions and permutation.

RSA: Is one of the most successful, asymmetric encryption algorithms. It is discovered in 1973 by cryptologists Rivest, Shamir and Adleman, It is discovered as an attempt to break another cryptographic predicament. Unlike symmetric encryption, RSA uses two different keys: A "public" key, and a "private". Both works opposite to each other, a message encrypted with one of the keys can only be decrypted by its complement. Since the private key can't be calculated from the public key, it is generally made available to the public. A message that is to be encrypted is treated as one large number because the security of RSA is mainly based on the mathematical problem of integer factorization.

IV. IMPLEMENTATION

We have implemented and compared AES, RSA and Hybrid encryption algorithms. These algorithms are implemented in python-3 using Pycrypto package. We used different file sizes consisting of text, image, audio and video as input for encryption. The encrypted output is saved as a different file, which in turn acts as an input for decryption. The same input files are used for all algorithms throughout the experiment. We have run the said algorithms on raspberry pi 4 which provides extra flexibility and portability.

V. RESULT AND DISCUSSION

The performance analysis of the AES, RSA and Hybrid algorithms was conducted with different types of files (Text, Image, Audio, Video). The performance matrices considered are encryption time, decryption time and avalanche effect. The values for each criterion was recorded.

Table-I, shows different size of input text files and the corresponding time taken by each algorithm. From the table, it is clear that the AES takes the least time for encryption and RSA takes the highest time. AES-RSA Hybrid algorithm takes slightly more time than AES but far less than RSA. Table-II, shows different size input text files and the corresponding time taken by each algorithm. From the table, it is clear that the Hybrid algorithm takes the least time for decryption and RSA takes the highest time. AES algorithm takes a bit more time than the Hybrid algorithm.

Table- I: Encryption Time in ms

File size	AES	RSA	Hybrid
500 KB	68.38	3706.39	69.55
1 MB	94.07	7430.80	81.80
5 MB	290.58	48385.91	292.81
10 MB	562.69	119657.89	539.34
50 MB	2540.73	1797074.09	2523.74

Table- II: Decryption Time in ms

File size	AES	RSA	Hybrid
500 KB	65.51	41395.98	57.73
1 MB	129.15	84135.05	81.90
5 MB	308.42	423158.67	304.60
10 MB	557.21	868019.96	594.60
50 MB	2622.68	5142942.76	2648.45.

Table- III: Encryption time for different file types in ms

File Type	File size	AES	RSA	Hybrid
Text	500 KB	68.38	3706.39	69.55
Image	1 MB	89.08	21518.59	123.52
Audio	5 MB	310.66	154334.57	284.64
Video	11 MB	622.25	597716.29	602.62

Table- IV: Decryption time for different file types in ms

File Type	File size	AES	RSA	Hybrid
Text	500 KB	65.51	41395.98	57.73
Image	1 MB	126.39	218908.43	133.20
Audio	5 MB	292.13	154384.57	315.91
Video	11 MB	626.23	597786.29	644.09

Table- V: Hamming Distance

AES	RSA	Hybrid
87.5%	98.25%	95.45%

Table- III, shows different type (image, audio, video) of input files and the corresponding time taken by each algorithm. From the table, it is clear that AES algorithm takes the least time for encryption and RSA takes the highest time. From Table- IV we can conclude that AES takes less time for decryption as well.

Cryptographic algorithms should possess avalanche effect property, wherein a small change (single bit change) in input produces large change in output. In standard algorithms a small change in input or a key produce huge change in the cipher. Hamming distance is one of the methods to calculate avalanche effect. the above discussion, we can conclude that an AES-RSA Hybrid algorithm has a less encryption and decryption time and also got good avalanche effect property which is near RSA. Thus Hybrid algorithm is fast and at the same time more secure than the other two algorithms.

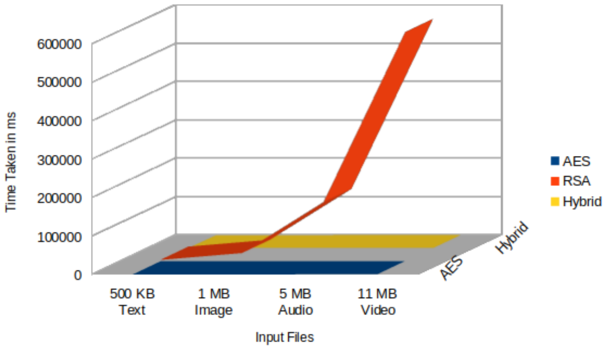

Fig. 1.Encryption Time of AES, RSA and Hybrid.

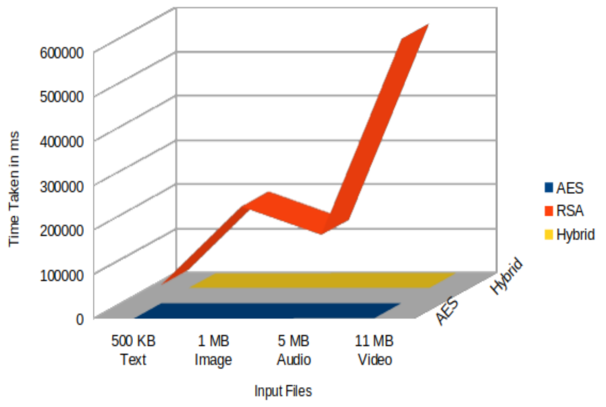

Fig. 2.Decryption Time of AES, RSA and Hybrid.

From the Fig. 1 and Fig. 2, we can conclude that an AES-RSA Hybrid algorithm has a less encryption and decryption time which is near AES time and got good avalanche effect property which is close to RSA algorithm. Thus, Hybrid algorithm is fast and at the same time more secure than the other two algorithms.

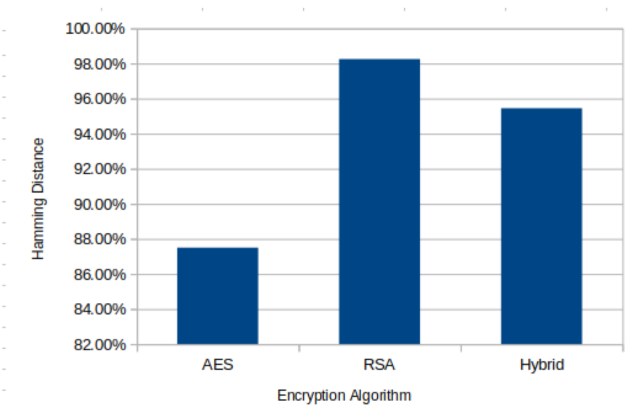

Fig. 3.Fig. 3. Hamming Distance of AES, RSA and Hybrid

We can measure the difference between two strings using Hamming Distance. The hamming distance of cipher-text is considered to be very important concerning the strength of the algorithm. A hamming distance of more than 50% is considered good for any cryptographic algorithm. Table- V shows percentage hamming distance for AES, RSA and Hybrid algorithm. RSA has better hamming distance percentage when compared to the other two.

VI. CONCLUSION

Every algorithm has its own strong and weak points. The best suitable encryption algorithm can be chosen to suit an application knowing its strong points. From the results, it is clear that AES takes less time for encryption than the other two algorithms. The RSA takes more time for encryption and decryption but has better strength than the other two algorithms. Results clearly show that the Hybrid algorithm combines advantages of AES and RSA in one, it is fast and more secure, which makes it suitable for applications where speed and confidentiality are of the highest priority.

REFERENCES

1. Stallings William, Cryptography and Network Security, New Delhi, India:Prentice Hall of India, 2007.
2. Aromoon, U.: An AES cryptosystem for small scale network. In: Third Asian Conference on Defence Technology (3rd ACDT). IEEE (2017)
3. C. Biswas, U. D. Gupta, and M. M. Haque, “An efficient algorithm forconfidentiality, integrity and authentication using hybrid cryptography andsteganography,” in2019 International Conference on Electrical, Computerand Communication Engineering (ECCE), IEEE, 2019, pp. 1–5.
4. Rajani Devi.T, “Importance of Cryptography in Network Security”,International Conference on Communication Systems and Network Technologies, 2013
5. I. Hammad, K. E. Sankary and E. E. Masry, "High-Speed AES Encryptor With Efficient Merging Techniques," IEEE Embedded Systems Letters, Vol. 2 (3), pp. 67-71, Sept. 2010.
6. M. Harini , K. Pushpa Gowri , C. Pavithra , M. Pradhiba Selvarani, “A novel security mechanism using hybrid cryptography algorithms” 2017 IEEE International Conference on Electrical, Instrumentation and Communication Engineering (ICEICE)
7. Sonali Mishra, Ananya Dastidar, “Hybrid Image Encryption and Decryption using Cryptography and Watermarking Technique for High Security Applications”, Proceeding of 2018 IEEE International Conference on Current Trends toward Converging Technologies, Coimbatore, India
8. Anane Nadjia, Anane Mohamed, “AES IP for Hybrid Cryptosystem RSA-AES”, 2015 12th International Multi-Conference on Systems, Signals & Devices.
9. Vatchara Saicheur, Krerk Piromsopa, “An implementation of AES-128 and AES-512 on
10. Apple mobile processor”, 2017 14th International Conference on Electrical Engineering / Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)
11. Fenghua Zhang ,Yaming Chen ,Weiming Meng and Qingtao Wu “hybrid encryption algorithms for medical data storage security in cloud database” International Journal of Database Management Systems (IJDMS) Vol.11, No.1, February 2019

12. Madhumita Panda "Performance Analysis of Encryption Algorithms for Security", International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016.

AUTHORS PROFILE

Vikrant Shende,
Vikrant_shende@git.edu

Vikrant Shende is a research scholar at RRC, VTU Belagavi. He is B.E. in Electronics and Communication Engineering and M.Tech. in Computer Science and Engineering. His area of interests are Network Security, Machine Learning, cryptography etc. He has published more than six research papers in national and international journals.

Meghana Kulkarni
meghanak@vtu.ac.in

Meghana Kulkarni is working as a Associate Professor in the Department of PG studies, VTU Belagavi. She is M.Tech. in VLSI Design and Embedded Systems and done her Ph.D. on TIQ Technique Based Low Power Flash Analog to Digital Converter. Her area of interests are Low Power devices, Network Security, Coding Techniques, VLSI design etc. She has many publications in national and international journals.