AES and RSA Hybrid Cryptography in Cloud Computing

Jason Paek[1]
College of Computer and Software Engineering
Kennesaw State University
Marietta (GA), United States
jpaek4@students.kennesaw.edu

Mohammad Umar[2]
College of Computing and Software Engineering
Kennesaw State University
Marietta (GA), United States
mumar2@students.kennesaw.edu

Bryan Nix[3]
College of Computer and Software Engineering
Kennesaw State University
Marietta (GA), United States
bnix13@students.kennesaw.edu

Abstract

Cloud computing provides many different services over the internet. Which means cloud computing allows you to use services such as data storage, servers, database, software applications and networking systems. As long as you have access to the internet you can access these cloud services from anywhere. Since cloud computing provides many important services it is crucial to have a security system in place to protect users data. In this paper we will analyze AES symmetric encryption and RSA asymmetric encryption to construct a hybrid encryption which will include the best of both AES and RSA. Additionally, we will implement a simple AES and RSA hybrid algorithm. From the results we will generate graphs and analyze our results to draw conclusions about our AES and RSA hybrid solution.

Keywords: Hybrid Cryptography, RSA, AES, symmetric, asymmetric, encryption, decryption, Cloud Computing

I. Introduction

Cloud Computing is the delivery of different services through the internet. These resources include tools like data storage, servers, databases, networking, and software applications. Rather than keeping files on a proprietary hard drive or local storage, cloud computing makes it possible to store those files remotely. As long as an electronic device has access to the web, it has access to services and data stored in the cloud. As the use of cloud computing services increases the security risks increase with it which is why it is crucial to have sufficient cryptosystems in place to protect cloud computing services. One such cryptosystem can be created using AES or RSA algorithms. RSA is an asymmetric cryptographic algorithm used to encrypt and decrypt messages over the internet. RSA uses two different keys. Public key is used to encrypt the message which is known to anyone and private key is used to decrypt the message which must be kept private. AES is a symmetric key block cipher algorithm. It is a standard algorithm used by banks and governments to encrypt and decrypt sensitive data. The main goal of this project is a simple implementation of an AES and RSA hybrid algorithm which can later be integrated with cloud computing services to construct more secure cloud systems. The purpose of using the hybrid algorithm is to combine the best of both RSA and AES algorithms without sacrificing too much in terms of performance.

II. Motivation

A. Vulnerability in Cloud Computing

While Cloud computing provides an array of benefits including reliability, flexibility, and lower cost, concerns of data security intimidate enterprises from incorporating cloud services. Fears from cloud data breaches and exploitations in cloud infrastructure cripple the potential benefits of utilization; however, cyber security measures in both cryptography and cryptosystems allow cloud computing to reach its full functionality and productivity.

B. Motivations for Hybrid Cryptography

Our main objective is to fuse the benefits of both symmetric and asymmetric cryptosystems to create a flexible cryptosystem that allows for optimizable efficiency in both small data or large data systems. Benefits of asymmetric cryptosystems include security and convenience due to the lack of key distribution, exchange of private keys, and detection of tampering; however, it can be slow, and more complex. Additionally, when a key is compromised, it is

risky for widespread security compromise. On the contrary, symmetric cryptosystems benefit from faster speeds from shorter key lengths and executions, it is algorithms are more simplistic than symmetric, and it is better for larger data pools; however, the use of only one key can compromise security and the threat of interception is high.[7] In offering a flexible cryptosystem, enterprises will be able to adjust their scope, optimize their desired performance in speed, and ultimately be able to move around limitations and risks that result from using only one type of cryptosystem.

III. Challenges

The main challenges that arise from hybrid cryptography resonate in its reliability in security performance and complexity in readability and writability. With pre-existent cryptosystems that have already been established to work, testing experimental hybrid cryptosystems can have risks as faulty implementation can compromise the integrity of the system and create security breaches in the cloud. Complexity is another factor to take into consideration as the combination of both asymmetric and symmetric key encryption principles can complicate readability in the code and writability when incorporating AES with RSA encryption in the cloud.

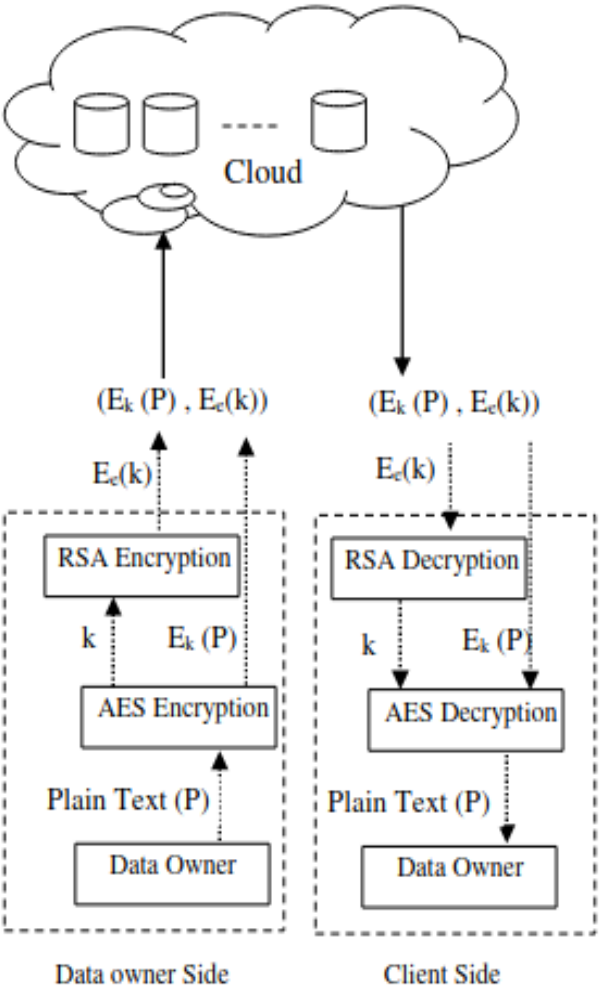
IV. Contributions

We reviewed many different sources for our project, but our primary source was a paper titled "Analysis and Implementation of AES and RSA for cloud" [1]. Cloud computing is an emerging technology and it has many advantages. One of the biggest advantages is that cloud computing services are available at all times at a very low cost. In cloud computing, Cloud Services Provider is a third-party company offering a cloud-based platform. Cloud services use a pay-per-use model for their businesses. Which means that you only pay for what you use and it's much better in ragrets to scalability and reliability than physical computing services.

There are four different access types in cloud computing. Public cloud is a computing service offered by third-party providers over the internet, making them available to anyone who wants to use it. Private cloud is a computing service offered either over the internet or over a private internal network and it is only available to select customers. A hybrid cloud is the combination of both public and private cloud. Community cloud is a multi-tenant platform which allows different organizations to work in the same platform.

Advanced Encryption Standard (AES) is a fast and secure form of symmetric encryption. It uses only one key to encrypt and decrypt data and has three different key sizes. Rivest-Shamir-Adleman (RSA) is an asymmetric encryption that uses two large prime numbers to encrypt and decrypt data. RSA uses the public key to encrypt data and private key to decrypt data.

The following figure is the hybrid model we study [1] in order to better understand the functions of AES and RSA hybrid cryptosystems. This model was instrumental in helping us with our proposed solution.

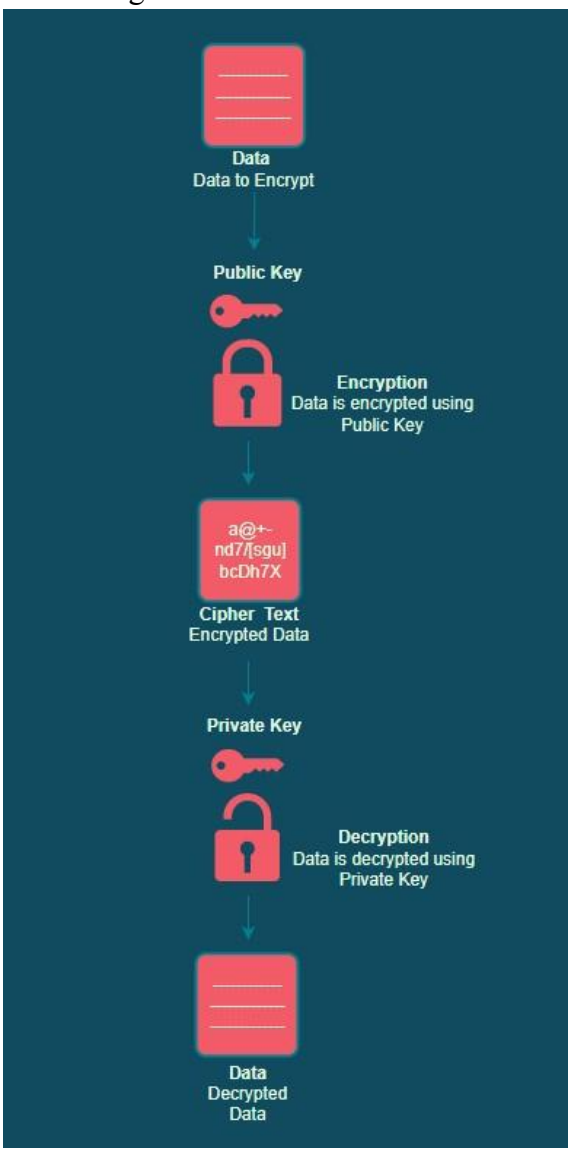


V. Proposed Solution

A. Rivest-Shamir-Adleman (RSA)

RSA (Rivest-Shamir-Adleman) algorithm is an asymmetric cryptography algorithm which means that it uses two different keys. A public key that is shared publicly and a private key that is kept secret. The keys are generated by taking two prime numbers. The prime numbers need to be large so that they will be difficult for someone to figure out. RSA is much better at securing data as the sender does not need to know the recipient's private key to encrypt the data.

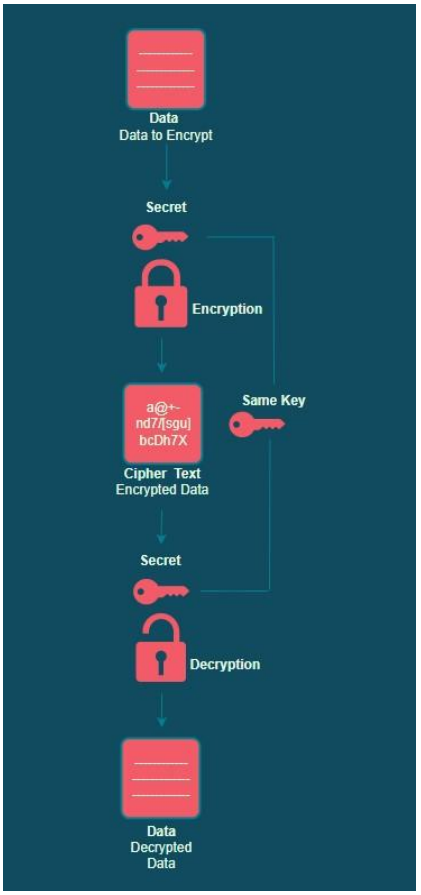
The following illustration shows how RSA asymmetric cryptography works. It takes the data the user needs to encrypt and uses a public key to encrypt that data. A ciphertext is generated which can be decrypt using the private key to return the data in its original form.



B. Advanced Encryption Standard (AES)

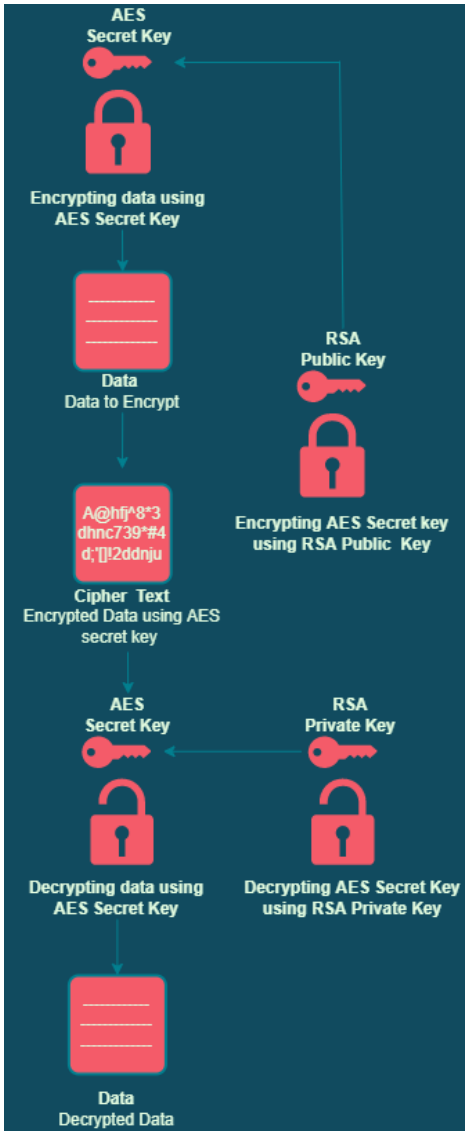
AES (Advanced Encryption Standard) is a symmetric encryption cipher. It means that the same key is used to encrypt and decrypt the data. AES encryption itself has proven to be very effective and efficient. AES is a fast and highly secure form of encryption that is a favorite of businesses and governments worldwide. However, AES encryption is only secure as its key and the key is secure using passwords. If the password securing the key is weak then it would not be very difficult for someone to get the key. AES encryption uses a substitution-permutation network, with multiple rounds to produce ciphertext. The number of rounds depends on the key size being used. A 128-bit key size dicates ten rounds, a 192-bit key size dictates 12 rounds, and 256-bit key size dictates 14 rounds. The larger the key size the more secure the encryption.

The following illustration shows how AES symmetric cryptography works. It takes the data the user wishes to encrypt and encrypt it using the secret key that has been chosen. A ciphertext is generated which can be decrypted using the same key it was used to encrypt to get the original data.



C. AES and RSA Hybrid Solution

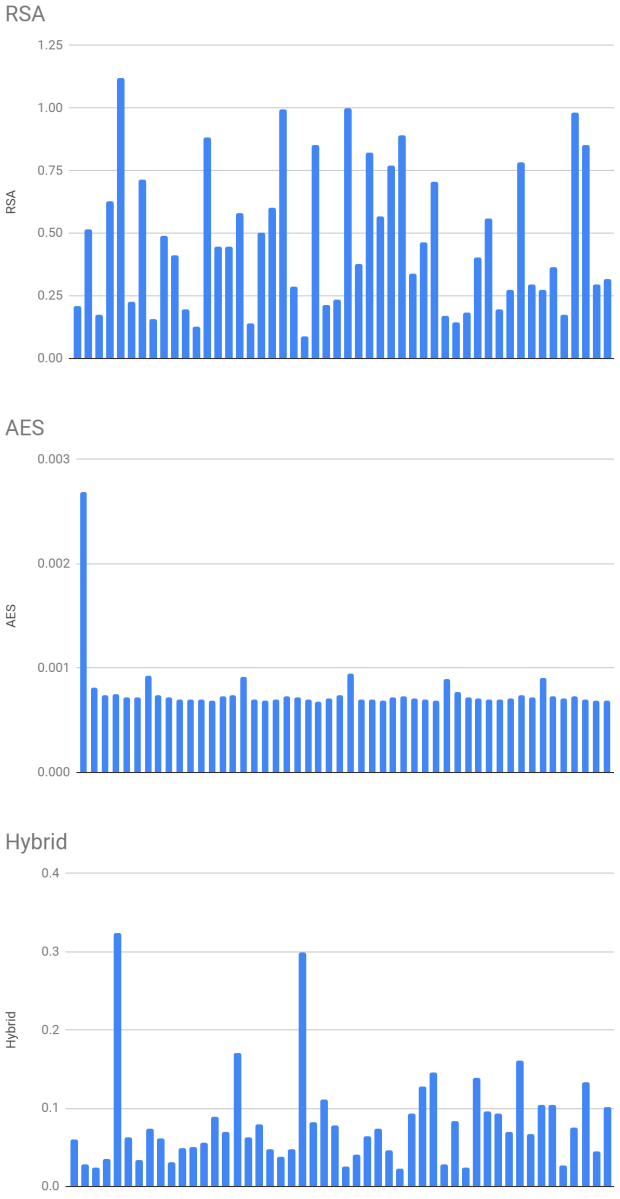
The following illustration shows our AES and RSA hybrid cryptography solution. It takes the data the user needs to encrypt and encrypt it using AES secret key. A ciphertext is generated by the AES encryption program. AES secret key is then encrypted using RSA public key in order to protect the AES secret key. In order to decrypt the data, you need to first decrypt the AES secret key using the RSA private key. Then, you can use the AES secret key to decrypt the ciphertext and get the original data. This is an optimal solution as it includes the best of both AES and RSA to construct an even more secure encryption.



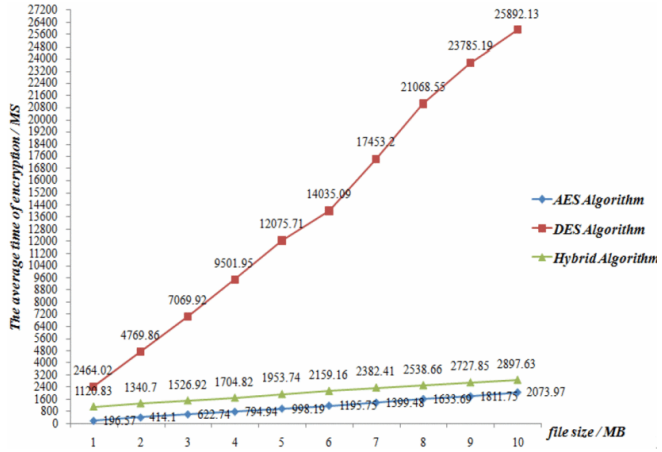
VI. Implementation

In this implementation, a simple string was used for the encryption process on all algorithms used. This is because of the limitations of RSA algorithms which are limited to encrypting data of a size that does not exceed the maximum key size. Since RSA is not designed for encrypting files, our test results need to use the same size data for consistent results. Each encryption algorithm was set to its maximum key size which means our RSA algorithm encrypts data with a 2048-bit key, the AES algorithm utilizes 256-bit encryption, and the hybrid algorithm also uses a 2048-bit private key size to be consistent with the RSA key size. Multiple iterations of the encryption and decryption process were executed, averaged, and then collected into a pool of data. The hybrid RSA-AES encryption algorithm was implemented from .

VII. Evaluation Results



In comparison to another hybrid encryption algorithm by Liang [8], the trend in our results is identical:



Both our hybrid RSA-AES algorithm and their hybrid DES-AES algorithm demonstrate a balance in performance that improves on their asymmetric component while retaining the benefits of the symmetric component.

VIII. Conclusion

With our findings and evaluation, we have come to the reasoning that hybrid encryptions have been generally faster in speed in comparison to asymmetric encryptions but more secure compared to symmetric encryptions. With our execution time testing, we have found that symmetric was the fastest to process while asymmetric was the slowest. After testing our hybrid encryption, it was concluded that while it was not as fast as the symmetric AES encryption, it was an improvement from the RSA encryption. Additionally, the increase in key size can indirectly show an exponential increase of security strength with a relationship of log(n) or 2^n where n is the amount of keys. As the relative time increase and inferred security improvement is apparent, we can conclude that hybrid cryptography, particularly with AES and RSA, is a flexible and optimal solution that allows for a fusion between symmetric and asymmetric encryptions which provides benefits from both into one with some sacrifices that can be overlooked in comparison to the many improvements.

IX. Future Work

A. Cloud Integration

In the future, we can implement our hybrid solution into a real-time cloud environment with clients and servers to test and see whether or not it would be truly effective in a real world situation. We could integrate this hybrid encryption to communicate plaintext messages, data packets, or other artifacts and see if it is as fast or as secure as our local testing environment.

B. Memory/Hardware Testing

We could also incorporate more testing that involves measuring the amount of memory or RAM that it consumes when executing our solution to test the load it takes on the hardware of any computer. It could measure further the effectiveness of encryption along with understanding more in depth how the increase in running time can affect the hardware. With stronger computers or connecting multiple computers, we could also drastically increase the data pool size and truly stress the amount of data that our solution could handle to see the effectiveness of the encryption beyond the relatively moderate data size we could test.

C. Security Stress Testing

Security is the most important aspect of encryption effectiveness that we can measure, and the only way to truly test the effectiveness of it would be a strongly studied stress test that could truly see the strength of our code without just implicitly stating that it is stronger in relation to key strength. In a future work, we can solidify our claim by trying cypher-text attacks on symmetric encryptions, applying brute force techniques, or even attempting to intercept data. The main goal of stress testing is to simulate a real world data breach or infrastructure weakness in the communication links of a cloud, and attempting to do so and studying the weaknesses could help us modify our code to increase the effectiveness of our solution.

References

[1] Tyagi, Manoj & Manoria, Manish & Mishra, Bharat. (2019). Analysis and Implementation of AES and RSA for cloud. International Journal of Applied Engineering Research. 14. 3918. 10.37622/IJAER/14.20.2019.3918-3923.

[2] K.R.Monisha. (2015). "Secure Cloud Computing Using Aes And Rsa Algorithms" , *International Journal of Advances in Computer Science and Cloud Computing (IJACSCC)* , pp. 77-82, Volume-3,Issue-1

[3] D. P. Timothy and A. K. Santra, "A hybrid cryptography algorithm for cloud computing security," 2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS), 2017, pp. 1-5, doi: 10.1109/ICMDCS.2017.8211728.

[4] Mahalle, Vishwanath & Shahade, Aniket. (2014). Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm. 10.1109/INPAC.2014.6981152.

[5] Kurose, J. F. (2021). Computer Networking: A Top-Down Approach Featuring the Internet by Kurose, James F., Ross, Keith W.(May 23, 2004) Hardcover. Addison Wesley.

[6] Lake, Josh. “What Is Rsa Encryption and How Does It Work?” Comparitech, 22 Mar. 2021

[7] *Top 5 security risks of cloud computing*. SecurityScorecard. (n.d.). Retrieved November 11, 2021, from https://securityscorecard.com/blog/top-security-risks-of-cloud-computing.

[8] Chengliang Liang, Ning Ye, R. Malekian and Ruchuan Wang, "The hybrid encryption algorithm of lightweight data in cloud storage," 2016 2nd International Symposium on Agent, Multi-Agent Systems and Robotics (ISAMSR), 2016, pp. 160-166, doi: 10.1109/ISAMSR.2016.7810021.

[9] Liashkov, Pavel. “BIGBAG/Hybrid-RSA-AES: Helper for Hybrid AES-RSA Encryption.” *GitHub*, https://github.com/bigbag/hybrid-rsa-aes.