Hybrid Cryptography in Cloud Computing: AES & RSA

Presented by: Jason Paek, Bryan Nix, Mohammad Umar

Introduction

Cloud computing is the delivery of on-demand computing services.

- Data Storage, servers, databases, networking, software application.

Our goal for this project is a simple implementation of an AES and RSA hybrid algorithm.

Purpose of using the hybrid algorithm is to combine the best of both AES and RSA algorithms without sacrificing too much in terms of performance.

Motivations

Vulnerability in Cloud Computing:

- Necessity of cyber security with **cryptosystems** and **encryptions**

Desire for Hybrid Cryptography:

- **Symmetric** and **asymmetric** cryptosystems
- Symmetric: faster execution, less secure, simpler
- Asymmetric: slower execution, more secure, complex

Hybrid Cryptography: combines benefits from both asymmetric and symmetric

Challenges

Complexity

- Ease of readability, maintenance, writability

Integrity

- Overall functionality, correct implementation without fatal compromise

Security

- Strength in cybersecurity and lack of vulnerabilities

Contributions

Analysis and Implementation of AES and RSA for cloud by Manoj Tyagi, Manish Manoria, Bharat Mishra

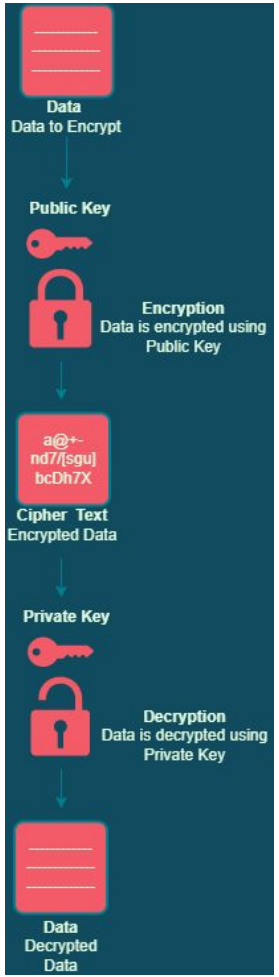
Secure Cloud Computing using AES and RSA Algorithms by K.R.Monisha

These two papers helped us better understand AES and RSA encryption and the need for hybrid solution in cloud computing.

From what we learn from these two papers, we were able to develop our own AES and RSA hybrid solution.

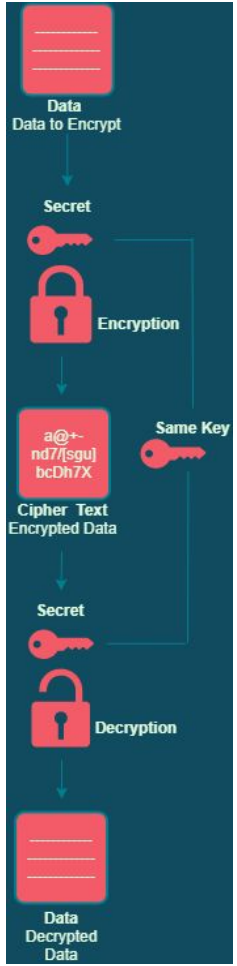
What is RSA?

- RSA (Rivest-Shamir-Adleman) encryption is an asymmetric cryptography algorithm.
- Asymmetric means there are two different key.
- One Public Key and One Private Key.
- Public key can shared with anyone.
- Private key is kept private and is only known to the person decrypting the data.

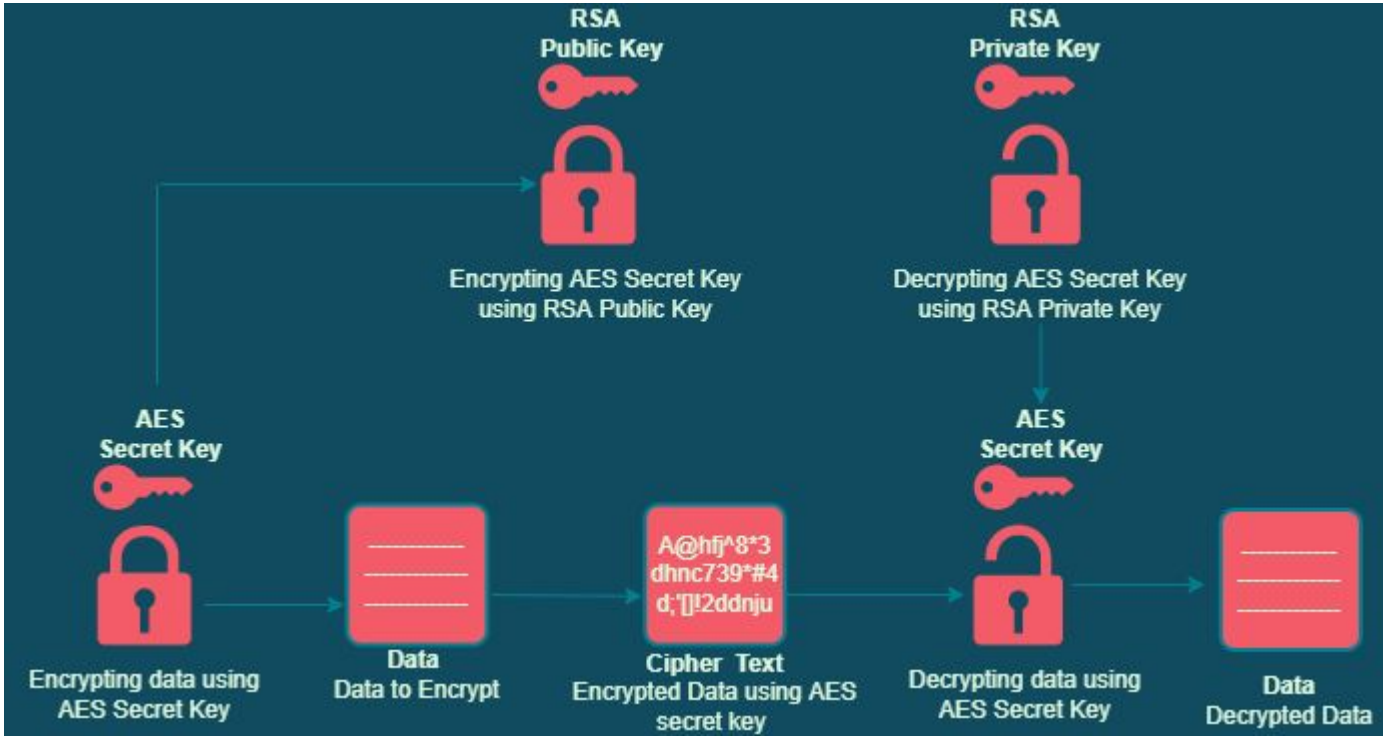


What is AES?

- AES (Advanced Encryption Standard) encryption is an symmetric cryptography algorithm.
- Symmetric cipher use the same key for both encryption and decrypting the data.
- AES is NIST (National Institute of Standards and Technology) certified and is used by the US government, banks, etc.
- AES encryption encrypts and decrypts data in blocks of 128 bits.
- AES can do this using 128-bit, 192-bit, or 256-bit keys.
  - 128-bit AES encryption key will have 10 rounds.
  - 192-bit AES encryption key will have 12 rounds.
  - 256-bit AES encryption key will have 14 rounds.

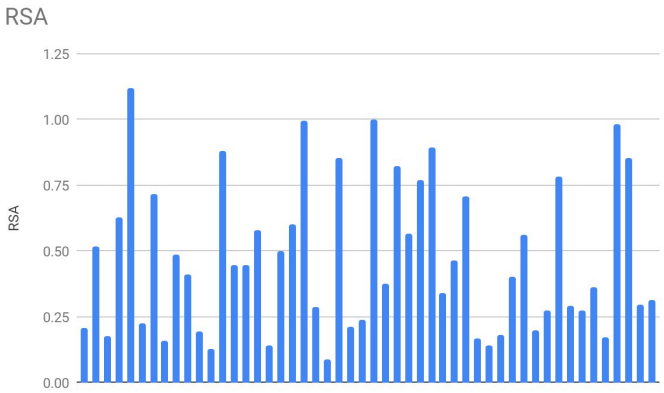


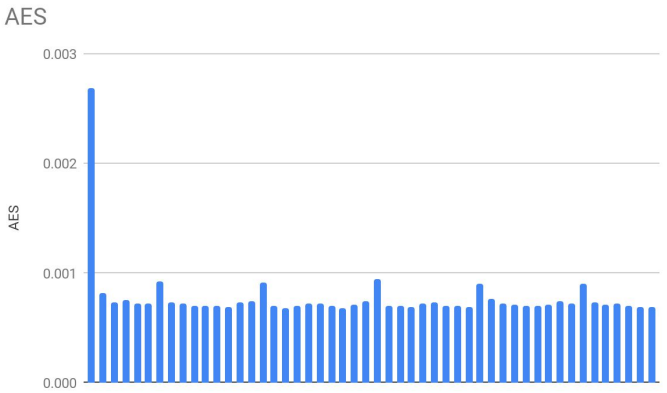
What is our Proposed Solution?

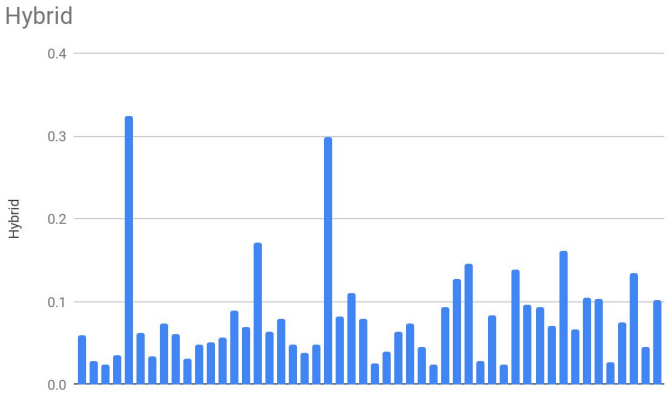


Implementation

Evaluation Results







Conclusion

Hybrid Cryptography

- Tested and proven Improvements in security and time efficiency
  - Longer key length → bit security
  - Optimal time improvement (still not as fast as symmetric)
- Concluded that Hybrid Cryptography with AES and RSA encryptions can be:

  A flexible and optimal solution that allows for a fusion between

  Symmetric and asymmetric encryptions which provides

  Benefits from both into one.

Future Works Blueprint

Cloud implementation

- Integrate to a cloud server

Memory measurement

- File size to time ratio/ Memory RAM utilization

Security testing

- Stress testing the cloud security with the hybrid cryptosystem.
- Hacking vulnerabilities: different with symmetric and asymmetric

References

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.

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

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.

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

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.

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

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.