International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 05 | May - 2022 Impact Factor: 7.185 ISSN: 2582-3930

DATA SECURITY IN CLOUD COMPUTING USING HYBRID ENCRYPTION ALGORITHMS

Lovish Awasthi, Dr. Navin Prakash, Mohd. Anas Abbasi, Mohd. Laraib, Palash Ranjan
Dept. of Computer Science & Engineering, Babu Banarsi Das Institute of Technology and Management, Lucknow, India

ABSTRACT

Cloud computing is an ever growing stream in computer science. The use of cloud systems has increased manifold in the last decade including growing number of opportunities and services like Microsoft Azure, Amazon Web Services, Google Cloud etc.

The security of cloud systems is one of the founding pillars of cloud computing as data security issues are rampant on the internet as of late.

Ensuring a high level of security is vital for any cloud service provider to make sure the network is protected, identity of user is secured, data privacy is ensured and the confidentiality of data is intact.

This research paper focuses on these security measures and how they can be improved upon using encryption algorithms. The algorithm, in a virtual environment, encrypts and decrypts the said file using the AES algorithm.

Keywords - Encryption, Data Confidentiality, AES, Security issues, Data Privacy

INTRODUCTION

Cloud Computing introduces a new virtual environment to provide traditional services without the need of expensive hardware or travel costs. Almost every service is available over the internet such as Infrastructure as a service-AWS,IBM Cloud, Platform as a service-Azure, Google App Engine, Software as a service-Dropbox,Salesforce etc.

Cloud computing provides on demand self service for the users. This means that users can make use of any service, from any part of the world at any time without the hassle of scheduling and booking appointments. Google Drive is a cloud storage service provided by Google for end users. Google Drive comes with Google's own security measures and the trust that comes with the brand Google. It is a step ahead of every other cloud storage platform like Dropbox, OneDrive, Mega etc. hence, it has more than 1 billion users worldwide. It provides storage services for any type of file such as documents, videos, photos accessible over multiple platforms such as Mobile phones, Tablets, Desktop etc. It can be accessed over the web and through mobile applications.

Google App Engine (GAE) is a Platform-as-a-Service (PaaS) product that provides web app developers and enterprises with access to

DOI: 10.55041/IJSREM13299

Google's scalable hosting and tier-1 Internet service. Google App Engine provides more infrastructure than other scalable hosting services. The App Engine also eliminates some system administration and developmental tasks to make it easier to write scalable applications. We made the use of GAE in this project to authorize access to the application with software tester privileges. This allows the tester to link their google drive storage account with the application, to encrypt and decrypt the files they choose to upload on cloud.

Security is the most essential part of cloud computing architecture but even after years of development it still remains an area of concern among users when using cloud technologies. Most of these concerns arise from a fear of losing private/personal data, third party service providers gaining access to sensitive information and misusing it. These concerns are also present due to a shared multi-tenant environment, lethargic authentication and identity management and also due to resource pooling which may create a problem of cloning data. Network issues including SQL injection attacks, DDOS attacks, incomplete data deletion pose a security threat not just to the data but also to the users connected to the network. This may lead to users losing access to their own data altogether due to these malicious attacks. DDOS attacks in virtualisation also lock up the resources of the users machine, rendering it unfit and unsafe for future use.

We propose a method for improving security for the cloud using Asymmetric Encryption algorithms. These will be implemented using google drive as the main storage platform representing cloud architecture. The file will be encrypted using our application by generating keys. Once encrypted, no third party will be able to access the file even if they are able to access the cloud storage itself, without a key. To gain access to the file, the user must possess the generated key for decryption of the file. Then this file will be downloaded to the source folder of the application from the google drive using the application. This adds an additional layer of security ensuring the data is more secure.

Our Project is aimed at creating an application which connects to an online cloud storage platform and can upload files while encrypting them and as you download the file it should decrypt the encrypted file. The program was built in such a way that it should be able to handle multiple users to login and download these secured files and also the key should be shared among them.

Encryption and Decryption are the essential features of cloud computing security. The encoding of information is called encryption. It converts human readable text, or plain text into text that is incomprehensible known as cipher text. Encryption is not just limited to text files but to every format in existence ranging from audio,video to documents and other executable files. Digital encryption algorithms manipulate the contents of a file mathematically using a digital key that produces a ciphertext version of the file. Security and privacy of communication between sender and recipient is ensured if they are the only ones with access to the key. Shared key cryptography works on the basis that both the sender and the receiver must have access to the same key, otherwise the file cannot be decrypted. It follows the process of securing a file chosen by the user by first encrypting by generating keys, then uploading it to the cloud. This results in an encrypted file which can only be accessed by the user through the application and not any third parties. To download the file and decrypt it, the user must make use of the application, granted they have access to the application. Each file has its own unique file name and key. A key is generated whenever a user decides to encrypt a file. To decrypt a file, the key must be present on the system so that it can be read by the program, if the key is not present the program will be unable to read and therefore will be unsuccessful in decrypting the file. One of the driving forces behind this project is to ensure privacy which is achieved by making sure the keys are not shared publicly and can only be accessed privately by the user who generated them.

DATA SECURITY ISSUES IN THE CLOUD

I. Data Confidentiality

The first aspect when it comes to Data security issues, is the confidentiality of data. Data confidentiality, in layman's terms, means protection of data from unauthorized access. Dealing with the privacy of Data on the cloud, to make sure unauthorized parties are not accessing, editing or sharing said data is known as data confidentiality. This may include encryption or enciphering of certain data, limiting access to data, enabling certain softwares and applications such as firewalls and antivirus softwares and even disposing physical data securely so it can't be misused. Data confidentiality on the cloud is of utmost importance, especially with the rise in the no. of people with access to the internet, it is very difficult to fully secure data. Encryption algorithms such as RSA and AES have slowly but steadily succeeded in providing additional security to data that is stored on the cloud.

II. Data Integrity

Data integrity is very similar to the real world meaning of the word integrity. Ensuring that the

compatibility and the vendor must also regularly update the data that is present on the cloud so that it doesn't become outdated and unfit for use.

standards that have been set for data over the internet, must be met and complied with so that the accuracy and precision of data is ensured. Consistency of data when others have access to it is hugely important for security on the cloud, that is why data confidentiality and data integrity go hand in hand.

Data integrity must not be confused with data security or data quality, as in simple terms, data integrity is making sure that the data is in the same state as it was before different parties had access to it. It doesn't matter whether the data is up to the mark in data quality or not, all that needs to be ensured is that the integrity standards are met and the data isn't manhandled, edited or changed with malicious intentions. This is achieved through rigorous error checking and data validation.

III. Data Availability

Data availability makes up the 3 core aspects of data security on the cloud, alongside integrity and confidentiality. Data availability, as the name suggests, refers to how easily and quickly your data is available and accessible through the cloud. With almost every brand and business dependent on the internet for customer acquisition, retention etc. it is vital for the data and services to be available on the go to ensure the best results.

Having the data available **24x7x365** gives an overall better user experience as well as increased traffic and reach for the business.

It is vital to note that data availability needs capital investment, not just for businesses but for anyone who wishes for their data to be available on the cloud at any given time. Data flow must be ensured alongside data

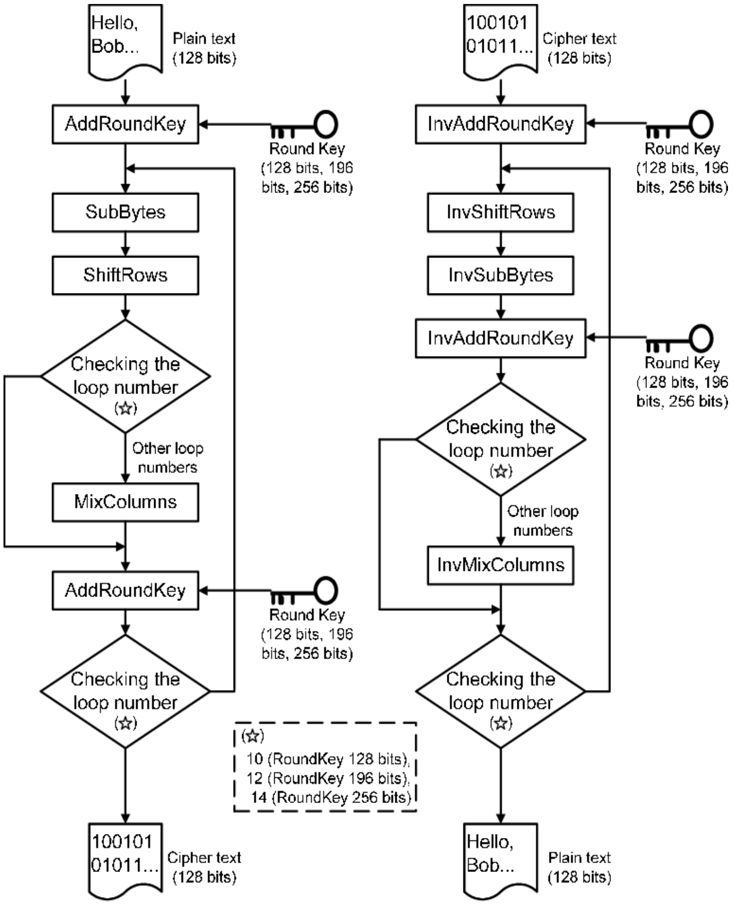
IV. Data Storage (Backup and Recovery)

Storing data on the cloud comes at a cost and can also lead to data security issues. Cloud services are hosted by third party vendors who provide storage space, accessibility and a very basic level of security. These vendors also back up the data on backup servers in case of an outage. This can lead to security issues as the backup servers must also be provided with the right level of security. Data loss is another issue that comes with cloud computing. Storing data with third parties may lead to loss of data, resulting in confidential information getting destroyed, potentially costing the users a lot of money in damages and security.

METHODOLOGY

Advanced Encryption Standard or AES is an encryption algorithm created in 2001. It is a symmetric block cipher chosen by the US government to protect classified information. The key size can vary from 128 to 256 bits, while the block size is 128 bits. It converts these blocks using keys of 128/192/256 bits, once it encrypts these blocks, it joins them together to form the cipher text.

Steps involved in the encryption process of the AES algorithm are - Plain text is taken as input, of size 128 bits. From the plaintext, derive the round key (size can be 128/192/256 bits). Add the round key to the state array which is passed onto the next step as input. Each byte of the state array is converted into hexadecimal form and divided into two equal halves which helps in generation of values for the final array. Then the rows created in the previous step are swapped among each other after skipping the first row. The columns are mixed in the next step and multiple. In the final step, the round key is XOR'd from the array from the previous step.


Hello, Bob...
Plain text (128 bits)
AddRoundKey
Round Key (128 bits, 196 bits, 256 bits)
SubBytes
ShiftRows
Checking the loop number (☆)
Other loop numbers
MixColumns
AddRoundKey
Round Key (128 bits, 196 bits, 256 bits)
Checking the loop number (☆)
(☆) 10 (RoundKey 128 bits), 12 (RoundKey 196 bits), 14 (RoundKey 256 bits)
100101 01011...
Cipher text (128 bits)
100101 01011...
Cipher text (128 bits)
InvAddRoundKey
Round Key (128 bits, 196 bits, 256 bits)
InvShiftRows
InvSubBytes
InvAddRoundKey
Round Key (128 bits, 196 bits, 256 bits)
Checking the loop number (☆)
Other loop numbers
InvMixColumns
Checking the loop number (☆)
Hello, Bob...
Plain text (128 bits)

(a) Encryption flow (b) Decryption flow

FIG 1.

After encryption, the files are uploaded to the user's Google drive, with the account they used to log in the application. To accomplish this task we need to open the API library on Google cloud platform and enable the Google drive API from the admin's end. The 'clientsecret.json' file was generated once the user's ID was approved by the admin as 'tester', to be able to make use of the application and sync it to their personal google drive.

To download the files in usable form, they need to be decrypted first.

To decrypt the ciphertext, all the steps performed during the encryption phase are performed inversely. This includes, InvAddRoundKey, InvShiftRows, InvMixColums and finally InvAddRoundKey again.

If the user downloads the encrypted file manually through the google drive onto their system, without using the application, the file will be downloaded in encrypted form and rendered inaccessible. To access the file with all its original functionalities intact, the user must use the application to decrypt their file and then download it onto their system.

PROPOSED WORK

As displayed in Fig 2. the encryption algorithm we proposed makes the use of two existing algorithms, i.e. RSA Algorithm and AES algorithm. These algorithms have been in use individually on their own for a long time, but the results have been less than optimal as of late. Mainly due to the huge increase in the amount of users making use of cloud services, which makes it difficult for these algorithms to keep up with, considering they were developed quite a while ago.

In this project, we combine these two to develop a hybrid RSA-AES Algorithm, which is better suited for today’s user heavy cloud platforms.

This takes the least possible computing time in the encryption and decryption process while also ensuring a high level of security. We also prepared a brand new Graphical User Interface, which would give the users a better overall experience. While the whole encryption and decryption process can be completed by writing simple statements using menu driven programming, it is better for any product to have a more attractive interface. The use of HTML, CSS and Javascript to develop the GUI was paramount for the success of the project, especially for user acquisition and retention.

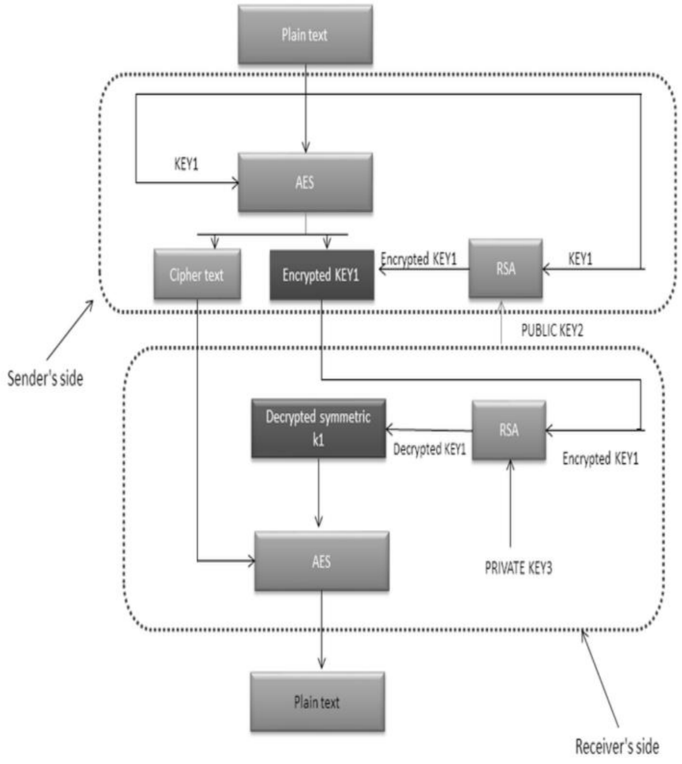


FIG 2.

SCOPE FOR FUTURE WORK

Use of hybrid cryptography algorithms is still fairly new in cloud computing, and there is still a lot of room for progress in their development.

Although our work focuses on the use of only 2 hybrid algorithms, it is a step in the right direction considering the state of data security on the cloud. More and more technology companies and startups are pushing towards a more secure space on the internet and cryptography has a bigger role to play in that.

Hybrid algorithms are limited to just AES and RSA, other cryptography algorithms such as DES, TDEA, DSA, ECDSA etc. are still widely used but individually. The use of these algorithms in hybrid form will also aid the development of cloud system security, and protect users data, ensuring confidentiality, availability and integrity.

REFERENCES

1. Malgari, V., Dugyala, R and Kumar. A. (2020). A novel data security framework in distributed cloud computing. In: IEEE Fifth International Conference on Image Information Processing , Shimla, India, India, 15-17 /11/ 2019. DOI: 10.1109/ICIIP47207.2019.8985941
2. Tabrizchi, H. and Rafsanjani, M. K. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The Journal of Supercomputing, 76(n/a), 9493– 9532
3. Zou, L., Ni, M., Huang, Y., Shi, W. and Li, X. (2020). Hybrid encryption algorithm based on AES and RSA in file encryption. Springer Nature Singapore Pte Ltd, n/a(n/a),541–551. DOI:10.1007/978-981-15-3250- 4_6
4. Marqas, R. B., Almufti. S. M. and Ihsan, R.R. (2020). Comparing symmetric and asymmetric cryptography in message encryption and decryption by using AES and RSA algorithms. Journal of Xi'an University of Architecture & Technology, 12(3), 3110-3116
5. Sarwar, A., & Khan, M. N. (2013). A Review of Trust Aspects in Cloud Computing Security. International Journal of Cloud Computing and Services Science (IJ-CLOSER), 2(2), 116-122
6. Sakharkar, N. (2019). Survey of cryptographic techniques to certify sharing of information in cloud computing. International Research Journal of Engineering and Technology, 6(8), 397-400
7. .N. Saravanan, A. Mahendiran, N. Venkata Subramanian and N. Sairam”An Implementation of RSA Algorithm in Google Cloud using Cloud SQL” Research Journal of Applied Sciences, Engineering and Technology 4(19): 3574- 3579, 2012.
8. Khan, S. and Sharma, S. (2019). Analysis of cloud computing for security issues and approaches. International Journal on Emerging Technologies, 10(1), 68-73
9. Mohan, D. N., Kumar, V. H. and Shashank, N. (2020). Enhancement of cloud computing security with secure data storage using AES. International Journal of Research in Engineering, Science and Management, 3(1), 586–587
10. Khaing, K. K. and Naung, Y. (2019). Encryption data measurement and data security of hybrid AES and RSA algorithms. International Journal of Trend in Scientific Research and Development, 3(6), 834-838
11. Singh, B. and Sharma, S. (2019). Enhancing data security using encryption and splitting technique over multi cloud environment. International Journal of Scientific Research & Engineering Trends, 5(3),1041-1047.