Encryption Algorithms in Cloud Computing

Ameer M Shariff, Ph.D.

Abstract — Cloud computing has become fragile the information is mostly concentrated in the cloud. For data privacy protection, sensitive data should be encrypted. Prior to our outsourcing, it makes efficient data use a very challenging task. Although traditional searchable encryption plans allow users to securely search encrypted data. By keywords, these methods only support Boolean search, without capturing any v image of the data files. This approach when applied directly, one suffers from two major drawbacks, On the one hand, customers who do no prior knowledge of encrypted cloud data, each recovered file must be post processed to find people most people are interested in their mail; On the other hand, forever retrieve all files with query keywords. Unnecessary network traffic, which is undesirable Today's pay-as-you-use cloud model.

In this article, we first define and solve the problem of encrypted effective yet Secure rank Keyword Search Cloud data. Greatly increases the use of a ranked search system returning files that match the order of certain relevant criteria (e.g., keyword frequency), thus creating one step towards the practical expansion of privacy-protection data hosting services in cloud computing. We will give one first straightforward and yet ideal creation of sorted keyword search under State-of-the-art Symmetric Encryption (SSE) demonstrates the definition of security and its inefficiency. To obtain more practical work, then we propose a definition rank able Symmetric Encryption, and Give Effectively design using existing cryptographic primitive, sequence-protection symmetric encryption (OPSE). The analysis shows that our proposed solution guarantees “stronger than expected” security compared to previous SSE schemes. Perceiving the rank keyword search target correctly. Demonstrates the potential of comprehensive experimental results the proposed solution.

Index Terms — Encryption, Cloud, Cloud Computing, Algorithms.

1 Introduction

Cloud computing is the ability to access computing resources that are owned and operated by third parties over the Internet.. This is not a new technology, but a way to distribute computing resources based on long-term technology such as server virtualization. "Cloud" is made up of hardware, storage, networks, interfaces, and services, enabling users to independently seek infrastructure, computing power, applications and services. Cloud computing typically involves the transfer, storage and processing of information on the infrastructure of infrastructure providers. Customer control is not included in the policy. Cloud computing is a service (IaaS), platform is a service (PaaS), software is a service (SaaS) (SaaS), all of which relate to information as a data-driven architecture.

The first benefit of cloud computing is that it reduces the cost of hardware the user can use at the end. Since the user does not need to store the data at the end

Elsewhere. So, to buy the entire infrastructure needed to run the processes and save the bulk data that you are renting the property to meet your needs. The same idea lags all cloud networks. It uses remote services over the network using various resources. This is basically a maximum delivery with minimal resources, meaning that the user needs minimal hardware at the end but is using maximum efficiency.

This is only possible through this technology and using its resources in the best possible way. The advantages of cloud computing over traditional computing are: agility, low access cost, device independence, location independence and scalability. To address the data integrity check problem, several schemes have been proposed under different systems and security models [2], [3], [4], [5], [6]. In all of these tasks, great efforts are made to create solutions that meet diverse needs: high project efficiency, stateless validation, continuous use of queries, and data retrieval, and more. Considering the role of the verifier in the model, all schemes are performed before collapse. Give

Categories: Private Audit and Public Audit. Although private audibility schemes can achieve high scheme efficiency, public audibility does not allow anyone (clients) to challenge cloud servers for the accuracy of data storage without keeping private information.

Additionally, in cloud computing, data owners can share their outsourced data with multiple users, who only want to recover the data files they are interested in. One of the most popular ways to do this is through keyword-based retrieval. Keyword-based retrieval is a specialized data service and is widely implemented in plain cases where users retrieve context

Files in a file set based on keywords. However, it is a difficult task in ciphertext scenarios due to limited operation on encrypted data. In addition, in order to improve the feasibility and save the cost in the cloud instance, it is preferred recovery results with the most relevant files that are of interest to the user above all the files, which indicates that the files should be ranked. Only the interest of the users and the stance of the files

A series of cipher symmetric encryption schemes is proposed to enable search on the cipher. Traditional SSE schemes allow users to retrieve the cipher securely, but these schemes only support Boolean keyword search, that is, if a file contains a keyword, it queries keywords in these files.

To improve security without sacrificing efficiency, the submitted schemes show that the top-k single keyword retrieval is supported under different conditions.

2 Challenges of Cloud Encryption

Security is considered one of the most important aspects of everyday computing and is not unique to cloud computing due to the sensitivity and importance of data stored in the

cloud. Cloud computing infrastructure is also using new technologies
Services, many of which have not yet been fully tested in terms of security. There are many major and major problems in cloud computing, such as data security, trust, assumptions, rules, and synthetic issues. Another problem with cloud computing is that data management may not be completely reliable; The low access to the cloud and the risk of cloud services failing have attracted strong attention from companies. Whenever we talk about cloud security, there are various security issues when it comes to cloud. Below are some security issues and fixes:
SECURITY CONCERN 1
In the cloud physical security is lost due to sharing computer resources with other companies. There is no information or control over where the sources operate.
ENSURE: Secure data transfer
SECURITY CONCERN 2
Ensuring the integrity of the data (transfer, storage and retrieval) is in fact only a response to authorized transactions. A common criterion for ensuring data integrity does not yet exist.
ENSURE: Secure Software Interface

SECURITY CONCERN 3
Users can sue cloud service providers if privacy services are violated, and cloud service providers can in any case jeopardize their reputation. When it is not clear why individuals' personal information is requested or how it is used or transmitted to other parties.
ENSURE: Data Segmentation

SECURITY CONCERN 4
Who controls the encryption / decryption key? Logically it must be the customer.
ENSURE: Secure storage data

SECURITY CONCERN 5
In the case of the Payment Card Industry Data Security Standard (PCI DSS), managers and regulators must provide data log protection.
ENSURE: User Access Control

3 Problem Formulation

Cloud computing technology have a variety of policy issues and threats, including privacy, loneliness, storage, reliability, security, efficiency and more. The main concern of these, however, is the security and service provider
Ensuring it is maintained. Cloud computing usually involves many customers, such as general users, academics, and organizations, who have different motivations for moving to the cloud. If cloud clients are academia, then the security impact on computing performance and the cloud providers need to find a way to combine security and performance. The most important issue for companies is security but with a different perspective. Therefore, we focus primarily on the USER_CLOUD security of cloud computing using the encryption algorithm using a special proposed scheme.

4 Proposed Work Plan

We have proposed various security algorithms to eliminate concerns about data loss, isolation and privacy when accessing web applications in the cloud. Algorithms: RSA, DES, AES, Blowfish are used, and comparative studies are presented between them to ensure data security in the cloud. DES, AES, Blowfish Symmetric Key Algorithms, in which a single key is used for both encryption / encryption of messages, while the DES (Data Encryption Standard) was developed by IBM in the 1970s. In 1993, Blowfish was created by Bruce Schnier for use in a performance-constrained environment such as embedded systems. The AES (Advanced Encryption Standard) was created in 2001 by NIST. RSA is a public key algorithm invented by Reverend, Shamir and Edelman in 1978 and is also called asymmetric key algorithm, an algorithm that uses different keys for encryption and decryption purposes. The main shapes of all the algorithms are different from each other. The main length of the DES algorithm is 56 bits. The main size of the AES algorithm is 128, 192, 256 bits. The main size of the blowfish algorithm is 128–448 bits. The main size of the RSA algorithm is 1024 bits. Using Net beans IDE 7.3, and the Java Run Time Environment, we implemented our idea as the encryption and decryption algorithms discussed above, and we compared them between them.

5 Security Alogrithms used in Cloud Encryption

RSA ALGORITHM
The most common public key algorithm is the RSA, named after its inventors Rivest, Shamir and Edelman (RSA). RSA is basically an asymmetric encryption / decryption algorithm. This is unparalleled in the sense that the public key is being distributed to all
Through this the message can be encrypted and the private key used for decryption is kept secret and not shared to all. A description of how RSA works in a cloud environment is described as follows: The RSA algorithm is used to ensure the security of data in cloud computing. We encrypt our data to provide security in the RSA algorithm. The purpose of obtaining data is that only relevant and authorized users can access it. The next encryption data is stored in the cloud. So, you can request it from a cloud provider when needed. The cloud provider authenticates the user and distributes the data to the user. Since RSA is a block cipher, each message is mapped to an int. In the proposed cloud environment, the public key is known to all, but the private key is only known to the user who first holds the data. Encryption is done by the cloud service provider and the decryption is done by the cloud user or the user. Once the data is encrypted with a public key, this can only be decrypted using Private Key.

AES ALGORITHM
Advanced Encryption Standard (AES), also known as Rezindel, is used to capture information. AES is a symmetric block cipher that has been extensively analysed and is now widely used. How does AES work in a cloud environment? AES, Symmetric key encryption algorithm is used for this purpose

with a key length of 128-bits. AES is widely used these days to protect the cloud. According to the implementation proposal, first, the user decides to use the cloud services and migrate to them Data in the cloud. The user then presents their service needs with the Cloud Service Provider (CSP) and selects the best services the provider has to offer. Migration of data to the selected CSP occurs, and when an application uploads data to the cloud in the future, the data is first encrypted using the AES algorithm and then sent to the provider. Once encrypted, the data is uploaded into the cloud, and any request to read data occurs when the user decrypts it at the end, and then the user can read plain text data. Plain text data is never written to the cloud. It contains all kinds of data. This encryption solution is transparent to the application and can be integrated quickly and easily with no changes to the app. The key is not always stored next to encrypted data, as it also compromises the key. To store the keys, the user can set up a physical key management server on campus. This encryption protects data and keys and assures that they are user controlled and will never be stored or transported. AES For all-category applications, DES has been converted to an accepted standard.

DES ALGORITHM

Data Encryption Standard (DES) is a block cipher. It encrypts data in blocks of 64 bits size. This 64-bit plane text passes as input to DES, generating 64 bits of ciphertext. The same algorithm and key are used for encryption and decryption with minor variations. The main length of this algorithm is 56 bits; However, the 64-bit key is input. DES is so symmetric key algorithm.

BLOWFISH ALGORITHM

Blowfish is a symmetric key cryptographic algorithm. Blowfish encrypts 64-bit blocks with a variable length key of 128-448 bits. According to Schneier, Blowfish is designed with the following objectives:

The fast-blowfish encryption rate is 26 bytes per 32-bit. Microprocessors.

Compact-blowfish can run in less than 5kb of memory.

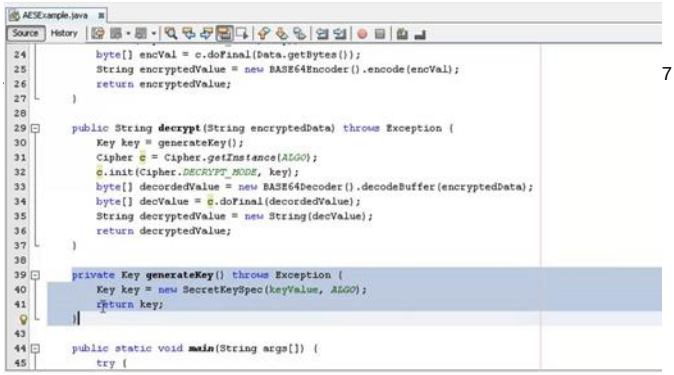
Simple-blowfish uses only primitive operations. Additionally, XOR and Table Lookup simplify its design and implementation.

Safe - Blowfish has a variable length of up to 448-bits, making it safe and comfortable.

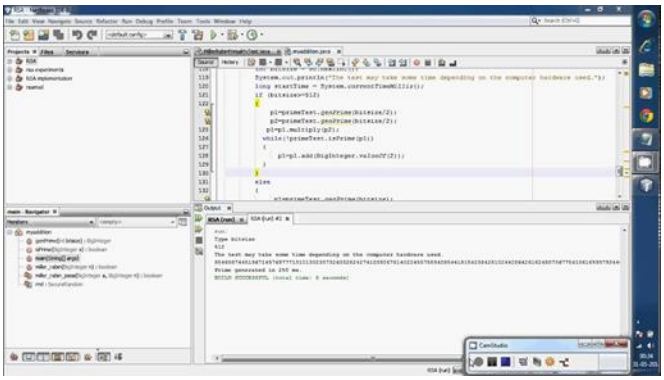
Keys are suitable for blowfish applications that are stable for a long time (such as communication link encryption), but not where keys change frequently (e.g. packet swapping).

6 Implementation and Results

Implementation of algorithms has been done using NetBeans IDE with Java.



AES ALGORITHM ENCRYPTION IN JAVA



MAKING CLOUD DATA SOURCE

RESULTS CHARACTERISTICS AND COMPARISON OF ALGORITHMS

Characteristics	AES	RSA	BLOW FISH	DES
Platform	Cloud Computing	Cloud Computing	Cloud Computing	Cloud Computing
Key Size	128,192,256 bits	1024 bits	32-448 bits	56bits
Key Used	Same key is used to encrypt and decrypt the data	Public key is used for encryption and private for decryption	Same key is used to encrypt and decrypt the data	Same key is used to encrypt and decrypt the data
Scalability	Scalable	Not Scalable	Scalable	Scalable
Initial Vector Size	128bits	1024 bits	64 bits	64 bits
Security	Secure for both provider and User	Secure for only user	Secure for both provider and User	Secure for both provider and User
Data encryption capacity	Used for encryption of large amount of data	Used for small amount of data	Less than AES	Less than AES

Authentication Type	Best authenticity provider	Robust authentic implementation	Comparable to AES	Less authentic than AES
Memory Usage	Low RAM needed	Highest memory usage algorithm	Can execute in less than 5 KB	Less than AES
Execution Time	Faster than others	Requires max time	Lesser time to execute	Equals to AES

7 Conclusions

In this article, encryption algorithms are proposed to make cloud data safe and smooth, and to compare security issues, challenges and concerns to find the best security algorithm between AES, DES, Blowfish and RSA algorithms. Compared, it must be in cloud computing to secure cloud data and not be hacked by attackers. The encryption algorithm plays an important role in data security in the cloud, and by comparing different parameters used in the algorithm, it is found that the AES algorithm uses less time to execute the cloud data. The blowfish algorithm requires minimal memory. The DES algorithm takes the least encryption time. RSA consumes the longest memory size and encryption time. By implementing the IDE tools and for all the algorithms in JDK 1.7, the desired output for data on cloud computing has been achieved. In today's era, cloud and user security is a major concern as demand for the cloud is growing. So, the proposed algorithms can help meet today's need. Multiple comparisons can be made with different approaches and results to show the effectiveness of the proposed framework in the future.

7.2 Acknowledgments

I am extremely thankful to Nick Abdelilah, Director of IT Risk and Compliance and Oliver Phippen Managing Director of State Street Global Advisor for supporting in creating this internal refernce architecture article. Their guidelines have been extremely helpful and helped in formulating this formal article on security concerns within cloud infrastructure.

7.3 Authors

Ameer M Shariff achieved his Bachelor of Engineering from University of Mumbai, Masters in Systems Engineering from Madurai Kamaraj University and Doctorate in Computer Engineering from University of Southampton, UK. He has been working as Sr. Infrastructure Architect for General Electric/State Street for past 15 years and has total experience of 20 years in the field of Network and Security Infrastructure. He has been using his expertise in establishing strong network and security controls in our internal infrastructure.

8 References

[1] Journal Papers:

[2] [1] Zhidong Shen, Li Li, Fei Yan, Xiaoping Wu, Cloud Computing System Based on Trusted Computing Platform, International Conference on Intelligent Computation Technology and Automation, Volume 1, May 2010, On page(s): 942-945.

[3] [2] Pearson, S., Benameur, A., Privacy, Security and Trust Issues Arises from Cloud Computing, Cloud Computing Technology and Science (CloudCom), IEEE Second International Conference 2010, On page(s): 693-702.

[4] [3] Rohit Bhadauria and Sugata Sanyal, A Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques. International Journal of Computer Applications, Volume 47- Number 18, June 2012, On page(s): 47-66.

[5] [4] Mohammed, E.M, Ambelkadar, H.S, Enhanced Data Security Model on Cloud Computing, 8 th International Conference on IEEE publication 2012, On page(s): cc-12- cc-17

[6] [5] Sang Ho. Na, Jun-Young Park, Eui- Nam Huh, Personal Cloud Computing Security Framework, Service Computing Conference (APSSC), Dec 2010 IEEE, On page(s): 671- 675.

[7] [6] Wang, J.K.; Xinpei Jia, Data Security and Authentication in hybrid cloud computing model, Global HighTech Congress on Electronics (GHTCE), 2012 IEEE, On page(s): 117-120.

[8] [7] Peter Mell, Timothy Grance, The NIST Definition of Cloud Computing, January 2011. http://docs.ismgcorp.com/files/external/Draft-SP-800-145_cloud-definition.pdf