Secure data sharing for mobile cloud computing using RSA

M Arumugam1, 6, S Deepa2, G Arun3, P Sathishkumar4 and K Jeevanantham5
1, 2 Assistant Professor, Department of Computer Technology - PG, Kongu Engineering College, Perundurai, Erode, India
3 Assistant Professor, Department of Information Technology, M P Nachimuthu M Jaganathan Engineering College, Chennimalai, India
4 Assistant Professor, Department of Computer Science and Engineering, Bannari Amman Institute of Technology, Sathyamangalam, India
5 Currently pursuing Master’s degree programme in Software Systems, Kongu Engineering College, Perundurai, Erode, India
6 Corresponding Author E-Mail: maructpg@gmail.com

Abstract—Mobile cloud computing (MCC) refers to an infrastructure in which data processing and storage can take place far from mobile devices. The convergence of compact registration and network distributed computing has created scalable distributed computing. This technology provides consumers a number of points of interest, similar to storage limits, reliability, scalability and access to real-time information. As a result, it is expanding steadily and is undoubtedly organised into a daily day-to-day life. The Cloud servers can be used for the preparation and storage of information. However, in the current conditions, the secrecy of photos and information is generally important. In this paper, we concentrate mainly on the safe re-appropriation of photographs.

Keywords—MCC, Cloud servers, RSA, ACP, AES, SLR, ABE.

1. Introduction
The utility of portable registration has become a modern breakthrough in diversified distributed computing. As a mixture of portable recording and distributed computing [1-3], The MCC enables flexible customers to have a capacity limit, unequivocal efficiency, adaptability and ongoing access to knowledge. Due to the limited storage and planning of cellular phones, many consumers start spending their information as records, images and music. All who does not have a competent insurance instrument will open up details in the broad daylight cloud. Therefore, legitimate security and confidence inquiry needs to be answered. Regardless of whether encryption is used to guarantee delicate details, the handling of scrambled data involves complex procedure. Other than this, we cannot prevent the important connexion between reports during encryption from being secured by another downside. It is a methodology intended to allow portable terminals to register in the heart of the cloud, which facilitates an ideal application of resources. The protection and information insurance problem has taken an impressive account in the field as an influence of a major concern for cloud customers. Various scientists have clarified that in the concept of "data identifying with perceived or recognisable individuals" obtained by the Economic Co-operation and Development Association[4-5] the defence is, indeed, "any information identification with perceived or recognisable individuals (informational subjects)".

IOP Conf. Series: Materials Science and Engineering 1055 (2021) 012108 doi:10.1088/1757-899X/1055/1/012108
Scientists have shown increased enthusiasm for MCC since the beginning. Currently, several papers on MCC with a growing passion for security and information security have been published. The results of the latest security and information assurance exams are not addressed alongside these innovations in MCC. Similarly, no clear exploration indicates advancing trends, measures for evaluating ebb and flow structures, and opened inspection problems, including potential safety inspection headings for the MCC.

Several mobile cloud apps have been used extensively. These apps can upload images, videos, reports and other files to the cloud and share these data with others (data users), which they want to share. They can also share these data. CSPs can provide data owners with data management capabilities. Due to the sensitivity of personal data files, data owner can choose either to publish their data files or to share it only with specific information users. Clearly for many data owners, the privacy of confidential personal data is of great concern. The main objective is to provide stable, easy, convenient data storage and networking services for all computing resources that are perceived as services and supplied across the Internet.

Cloud Computing emerged as a technological model as well as an architecture distributed. The Public Key algorithm is commonly used by RSA. RSA stands for the first public identification of Ron Rivest, Adi Shamir, and Len Adleman in 1977. We use the RSA algorithm in our work, to encrypt data so that only the user concerned can access it. We do not allow unauthorised access to this data by protecting it. The user information is first encrypted and then saved in the cloud. As requested by the customer, the data for the cloud provider is authenticated and the data is produced by the cloud provider. RSA is a block cipher that matches each message to an integer. The public-key and private-key RSA consists of Public Key is known to everyone in our cloud world, while private key is only known to the person who has the data at first.

The review states that multi-faceted customers around the world will reach $7.3 billion by the end of 2017, and over $8 billion by 2016. Ericsson's Overview further indicates that more than 9 billion of the 2019 portable clients will arrive. Due to increased use of mobile phones and various cell phones, the requirement for the distributed computing in mobile phones is growing and Mobile Cloud Computing has become a result. Mobile phones do not need more storage and incredible computing and handling speed. Since information is placed on the cloud, however, there is a security issue. Mobile phones do not need more storage and incredible computing and handling speed. Since information is placed on the cloud, however, there is a security issue. Most information technology experts do not demonstrate their enthusiasm for mobile cloud computing (MCC) because of their danger about stores of information. We propose a powerful system, with a certain amount of information reliability and information secrecy, to guarantee the correctness of customer information on the cloud. We use the idea of RSA calculation and Hash to work alongside some encrypted devices to give the information better security on a mobile cloud.

1.1. Cloud based secure data sharing

Cloud computing provides a flexible and convenient way for data sharing, offering broad social advantages as well as individuals. However, there is a natural reluctance for consumers, since data often provide valuable information, to outsource the shared data directly to the cloud server. Cryptographically improved control of access on the shared data should also be enforced. This involves a mechanism that could remove the user from the software until the permission to any user expires.

The enhancement of administration, for example, portable learning, human resources control and web-based business, have improved multi-faceted processing in ebb and flow science. Millions of people consistently provide the knowledge and accomplishment that builds their customers. For multipath communication and the transmission of information, the preferred use of distributed computing for the simple multipath correspondence is feasible. Due to the increased number of customers and the strain, the innovation increases more security breaks. Only if penetrations are minimised must the system be considered as steady and secure. Since applications need increased reliability, less pressures and heart-feltness, the correspondence must start to end much better.
Cloud Storage is a digital technology that frees enterprises from in-house data storage systems. However, data storage does give rise to security problems. In case of group-shared data, the data face both cloud-specific and classical insider threats. A major research concern is the secure sharing of data in a group that counteracts the challenges raised by legitimate but malicious users [6]. The stable data sharing approach in the clouds:

1. Privacy and honesty of data
2. Regulation of access
3. Data sharing without computational re-encryption (forwarding).
4. Protection of the insider threat
5. Control of forward and reverse entry.

Open data sharing with others is possible with Cloud. Moving data to a third party (cloud service provider) off-site storage network where data owners have little control presents various challenges to privacy – threats of unauthorised disclosure of sensitive data by service providers, data integrity authenticity of out-of-service data, etc. Since the cloud enables the exchange of data, careful attention must be paid to the comprehensive access control of the stored data.

This sensitive information confidentiality is normal approach to encrypting it until it is moved to the cloud. The user encrypts his file and stores it in a traditional public key infrastructure on the server, and only the actual approved user is told about the decryption key. With regard to confidentiality, this method is secure, but reliable, tested and complex management and distribution is necessary for this solution. Even this solution wouldn’t succeed, as the number of programme users is growing. These limitations and the need to track fine-grained access to data sharing, implement new access control systems based on attribute-based encryption (ABE).

2. Literature review

Eltayieb et al combine the blockchain concept with attribute-based signing to secure cloud data sharing. The proposed scheme meets the cloud computing security criteria, such as confidentiality and impoverishment. In addition, the intelligent contract fixes cloud storage issue, such as returning incorrect results in the conventional cloud server. Finally, our proposed scheme is more effective than others in terms of performance comparison and simulation results and is practical [7].

Sinha et al. provide a cloud-based platform that enables safe data sharing between many hierarchical groups of people. The system promotes restrictive scenarios of communication where one can identify a communication policy in order to comply with the hierarchical structure by defining "who can speak to whom". We are developing the tree-based group-significant management scheme that reduces time and space complications, and expanding it to healthy connectivity within and across groups. There is no semi-trustworthy third party involved in the main distribution process and the intensity therefore increases. In comparison to current approaches, our idea is very similar to the actual situations where there are several classes in a hierarchy, such as any association or institution [8]. This is true of our approach.

Hu et al proposed Ghostor, a framework for data sharing that [1] masks user identities from the server utilising only a decentralised trust, and [2] enables users to detect server integrities violations. To do that, Ghostor does not hold any user-specific state on the server, forcing us to reinvent the framework to avoid standard paradigms, such as user-specific mailboxes and authentication. Ghostor develops a methodology known as verifiable antonymic past in order to achieve [2]. Ghostor rarely uses a blockchain and once per epoch publishes only one haze to the blockchain. In comparison with an unsecure baseline, we measures Ghostor with a 4–5 times performance overhead. Although significant, the overhead of Ghostor can be worthwhile for applications that are secure and privacy sensitive [9].

The policy on connectivity and data sharing in the cloud setting was discussed by Gutte et al. The easiest and easiest way to manage our important data remotely in the 21st century is cloud computing. Confidentiality of one day is now one of the primary and most critical issues. Also of interest during data sharing with others is the protection weakness. A significant function is played
when we use a cloud-like confidence factor. A significant number of unauthorised user groups are attempting to access sensitive information and steal them. Encryption technology is used for data security in the 21st century. Exchanging cloud data at the best level in groups of users remains a key issue, in particular with the diverse user community. In this paper, we proposed a revoking and privacy mechanism that addresses the complex user community issue with the Access Control Policy (ACP) [11].

Cloud computing is one IT revolution that enables users to share resources, services and data through a network. Data are vulnerable to unauthorised attacks because users have the same network rights to data transfer. In recent times, data security in a system focuses only on data storage in the cloud through internet security, although there is a slight concentration during data transfer. When security is considered a serious concern, a suggested encryption scheme is presented for security during data transfer. Hidayat et al suggest an approach to improve data transfer device protection to deter unlicensed data theft. To prevent an attack by unauthorized person, Advanced Encryption Standard (AES) will be proposed to secure data transfer and storage in cloud computing. For better future, authors will propose Systematic Literature Review (SLR) to generate suggestions and opportunities in AES cloud computing [11].

Cloud computing security has continuously been an essential part of enhancing the efficiency of cloud service providers’ services. Cloud data storage has a data protection issue. Cloud computing does, however, create several fresh and not well-examined security problems. Kumar et al. has suggested an efficient framework with a specific characteristic of data security and privacy to ensure that the user's data are protected in the cloud. His team works on cloud data management and virtual environment security concerns. A public Cryptosystem method of storing and preserving data in the Cloud uses a modified RSA algorithm to enhance the protection of data stored in the Cloud [12].

Today, technology has improved that the tremendous amount of data transmitted to the network is increased. Security is one of the biggest issues. Encryption algorithms have been developed and act a significant function in data securing. Many strategies tried to safeguard the shared data. Boomathi et al suggest encryption to protect information during network transmission. Any data transfer from source to target in the network should be encrypted by cryptography using the encryption algorithm. In addition, the destination will access the plaintext using the decryption algorithm. In this work focus Boomathi et al analysis three encryption algorithms such as AES, DES, RSA and also demonstrate in terms of performances, weakness, strengths to given each algorithm.

In the Mean processing time and combination MD5+ECC+AES algorithm is better than others, Parsi Kalpana et al., describe the findings that the AES algorithm is better than other algorithms in the Speed-Up Ratio [14]. Li et al introduced a mobile cloud computing lightweight data sharing (LDSS) framework. It uses CP-ABE, a cloud-based access control technology but changes the access control tree structure to make them appropriate for mobile cloud environments. LDSS transfers from mobile devices to external proxy servers a significant proportion of computer intensive access control tree Transition within CP-ABE. In addition it introduces lazy-revocation definition fields of attributes which are a thorny problem in the software based CP-ABE systems in order to reduce the user revocation expense. Experimental results show that when users share data in a mobile cloud environment, LDSS can effectively reduce the overhead on the mobile device side [15].

3. Methods and Techniques

3.1. LDSS-RSA algorithm

It is now the only algorithm used for secret and secret key formation and for encryption it is a fast encryption. RSA is the most widely used encryption. The Public Key cryptography production is the biggest and probably gives a radical start. The asymmetric algorithm is also recognised since two keys and the hidden key are used. The plain text and the cypher text in that scheme are integers for any n between 0 and n-1. The encrypted user data is processed in the cloud first and then. When
appropriate, the user places a cloud provider database request, the cloud provider authenticates the user and supplies the data. RSA is a block cypher that matches each message to an integer. The public-key and private-key RSA consists of. Public keys are known to everyone in the cloud world, while private key is only known to the user who has the data. The cloud service provider is then encrypted and the cloud user or client decrypts them. The data can be decrypted with the private-key only once the Public-Key has been encrypted.

**RSA algorithm**

1. **SELECT** two large prime number a and b.
2. Compute n=a*b the computed n is made public.
3. Now compute f(n)=(a-1)*(b-1). **SELECT** two large prime number a and b.
4. Choose a random number ‘e’ as the public in the range 1<e<f (n) such that GCD (e,f(n)=1.
5. Find private key d such that d = e-1 mod f(n), where d and f (n) are mutually prime.

3.2. **RSA algorithm involves three processing:**

1. Key Generation
2. Encryption
3. Decryption

3.2.1. **Key Generation:**

Key generation should be performed before the data is encrypted. This procedure is carried out between the cloud service provider and the customer.

3.2.1.1 **Key generation algorithm**

a. **SELECT** two large prime number a and b.
b. **SELECT** two big number one and two large numbers a and b.
c. Measure n = a*b that is made public by the measured n.
i. (a-1)*(b-1)
d. Measure now.
e. Pick the public random ‘e’ in the set 1 < e < f(n) GCD (e,f(n)=1) is the product of this.
f. Find private keys d such that d = e-1 mod f(n) is mutually primitive for d and f(n).

3.2.2 **Encryption**

Take the user to securely send a message to b using rsa algorithm. E is the public key of b now. A e is permitted because e is public. The message m of a set o < m < n has been converted to cypher for encryption. Where the text C = Me mod n cypher.

1) Consider the user who must send the message to b using the rsa algorithm in a safe way.
2) Now e's public key for b. Since e is public, e access is permitted.
3) In encryption, the message m is translated to cypher within the range 0 < M < N < IS.
4) Where C = Memod n cypher text.

3.2.3 **Decryption**

The cypher text c is now sent from a useb. The message is determined with its private key ß in which the RSA message uses a two keys, and an authentication scheme that uses an algorithm. One is a secret recipient only known to the message and the other is a public key known to everyone and can be distributed freely. You can use either key to encrypt and decrypt a document. However, if only a key is used to encrypt a message, then only b key can be used to decrypt if converse, if b key is used to encrypt a message, then only a key can be used to decrypt it. RSA is the most popular algorithm for asymmetric cryptography. The suggested minimum key length is 1024 bits.
Steps:

1. The customer of the cloud demands the data from the cloud service provider.
2. The cloud service provider tests the user legitimacy and gives encrypted details.
3. Afterwards, the consumer in the cloud decrypts the data, $c = me \pmod{n}$.
4. Once $m$ is collected, the user extracts the original $m$ message data.

4. Conclusion
The highly secure Data Encryption technique is given by the RSA Algorithm. It is really safe from any other encryption technology. Cloud Computing is still a modern and developing model for on-demand computing. So only the approved user can access the data in our proposed work. Since a certain attacker (unauthorised user) inadvertently or deliberately extracts the data, it cannot decrypt it and retrieve the original data from it. The data cannot be retrieved. The implementation of the RSA algorithm therefore provides data protection. The cloud loses power when the company decides to move to the cloud. The amount of security provided for data protection is therefore directly proportional to the data value. Cloud protection depends on efficient computing and encryption.

References

[1] Ibtihal, Mouhib, and Hassan Naanani, 2020, Homomorphic encryption as a service for outsourced images in a mobile cloud computing environment, In Cryptography: Breakthroughs in Science and Practice, pp. 316-330. Global IGI.
[2] Buyyya, R., Yeo, C.S., Venugopal, S., Broberg, J. And Brandic, I, 2009, Cloud computing and emerging IT platforms: vision, hype, and fact to offer computing as the 5th utility, Future Generation of Computer Systems, 25(6), pp. 599-616.
[3] Aljawarneh, S., 2011, Web innovation safety approach for e-learning applications, Network Security, p. 12-15.
[4] Organisation for Economic Co-operation and Development, 2002, OECD guidelines on the protection of privacy and transborder flows of personal data, OECD Publishing.
[5] Alnajrani, H.M., Norman, A.A. and Ahmed, B.H., 2020, Privacy and data protection in mobile cloud computing: A systematic mapping study, Plos one, 15(6), p.e0234312.
[6] M. Ali et al., June 2017, SeDaSC: Secure Data Sharing in Clouds, in IEEE Systems Journal, vol. 11, no. 2, pp. 395-404, doi: 10.1109/JSYST.2014.2379646.
[7] Eltayieb, N., Elhabob, R., Hassan, A. and Li, F., 2020, A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud, Journal of Systems Architecture, 102, p.101653.
[8] Sinha, D., Datta, S. and Das, A.K., 2020, Secure Data Sharing for Cloud-Based Services in Hierarchical Multi-group Scenario, in Advances in Computational Intelligence, pp. 229-244, Springer, Singapore.
[9] Hu, Y., Kumar, S. and Popa, R.A., 2020, Ghostor: Toward a secure data-sharing system from decentralized trust, in 17th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 20), pp. 851-877.
[10] Gutte, P., Wankhade, J.V. and Mote, S., 2020, Key Generation & Access Control Policy in Cloud Data Sharing, (No. 2562). EasyChair.
[11] Hidayat, T. and Mahardiko, R., 2020, A Systematic Literature Review Method On AES Algorithm for Data Sharing Encryption On Cloud Computing. International Journal of Artificial Intelligence Research, 4(1).
[12] Kumar, Y.K. and Shafi, R.M., 2020, An efficient and secure data storage in cloud computing using modified RSA public key cryptosystem, International Journal of Electrical and Computer Engineering, 10(1), p.530.
[13] Boomathi, V. and Banumathi, A., 2020, Efficient analysis of encryption algorithms RSA, DES and AES for sensitive data, Purakala with ISSN 0971-2143 is an UGC CARE Journal, 31(4), pp.1937-1945.

[14] Parsi Kalpana, et al, September 2012, International Journal of Research in Computer and Communication technology, IJR.CCT, ISSN 2278-5841, Vol 1, Issue 4.

[15] Li, R., Shen, C., He, H., Gu, X., Xu, Z. and Xu, C.Z., 2017, A lightweight secure data sharing scheme for mobile cloud computing, IEEE Transactions on Cloud Computing, 6(2), pp.344-357.