International Journal of Soft Computing 10 (2): 137-142, 2015
ISSN: 1816-9503

Invulnerable Colossal Information Storage Based on Dynamic Encryption Algorithm on Cloud

[1]K. Anand and [2]A. Chandra Sekar
[1]Department of CSE, Saveetha Engineering College, Chennai, India
[2]Department of CSE, St. Joseph's College of Engineering, Chennai, India

Abstract: In recent times, cloud computing has become a trend among many organizations to store and retrieve data across the globe. In this data storage devices and data retrieval process, security is the prime concern to the client. This task provides a challenge to the service providers in terms of security and consistency. As shared systems are prone to be attacked, various counter measures have been proposed by experts to secure the stored data. In this research, yet another efficient technique is introduced to the storage and retrieval process, the data is encrypted by the advanced Encryption algorithm with AES-X encryption which is considered to be the most competent in the present security scenario. The main aim of this study is to throw light on how to store massive data in small space. In order to use AEX-X encryption, the number of rounds of AES algorithm should be increased. A symmetric key is generated to the stored file. To further enhance the trust of the service provider, the trust certificate of the company is sent along with the keys to the client. A hash function is also generated to enhance the security of the stored file. Also, the trust of the service provider is provided to the client by sending the trust certificate of the company along with the keys to the client. All the communication process is taken place using the DH key exchange protocol. These techniques are performed to ensure the client that the stored data is secured, integrated and a total control over the route in which the data is communicated. In this research work, a new efficient technique is proposed which indicates the effectiveness, flexibility of the storage and retrieval process by a generic framework. This framework fills the gap between the security needs and challenges.

Key words: Diffie Hellman, advanced encryption standards-X(512 bits), cloud service provider, cloud security alliance group, flexibility

INTRODUCTION

The term "cloud" as used in this study, appears to have its origins in network diagrams that represented the internet or various parts of it as schematic clouds. "Cloud Computing" was coined for what happens when applications and services are moved into the internet "cloud." Cloud Computing is not something that suddenly appeared overnight; in some form, it may trace back to a time when computer systems remotely time-shared computing resources and applications. More currently though, cloud computing refers to the many different types of services and applications being delivered in the internet cloud and the fact that in many cases, the devices used to access these services and applications do not require any special applications. With cloud computing the software programs that we use aren't run from the own pc, it is warehoused on servers retrieved via internet. Anyone with accurate security authorizations can only has the right to use the documents and control in partnership on those documents in real time without the need of any software and the user no longer needs knowledge over the technology infrastructure in the cloud.

The importance of safe computing: Moreover, nearly all IT resources can be distributed as a cloud service: application, power computation, storage capacity, networking, programming tools, communication facilities and collaboration tools. Cryptography is considered to be the science or art of secret codes. In its broadest sense, cryptography addresses a number of practical problems:

- Confidentiality: keeping message secret
- Origin authentication: verifying a message's source
- Integrity: assuring that a message has not been modified
- Key management: distributing the secret "keys" for cryptographic algorithms

Corresponding Author: K. Anand, Department of CSE, Saveetha Engineering College, Chennai, India

Network security is becoming more and more important as people spend more time connected in a network. It involves all the activities that organizations, enterprises and institutions undertake to protect the value and on-going usability of assets and the integrity and continuity of operations. Security attacks include unauthorized reading of a message of file, traffic analysis, modification of messages or files and denial of service. One of the most publicized types of attack on information systems is the computer virus. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them. Security involving communications and networks is not as simple as it might first appear to the novice. The expansion of the connectivity of computers makes way for protecting data and messages from tampering or reading important. Intruders may reveal the information to others, modify it to misrepresent an individual or organization or use it to launch an attack. One of the primary reasons that intruders can be successful is that most of the information they acquire from a system is in a form that they can read and comprehend. One solution to this problem is the use of cryptography. Cryptography ensures that the messages cannot be intercepted or read by anyone other than the authorized (Sekhar and Nanaji, 2013) recipient. It prevents intruders from being able to use the information that they capture.

Cloud computing architecture: When discussing cloud computing, it's supportive to choose it into two segments: the front end and the back end. They join together through a network, usually the internet. The front end is on the side of the user or simply the client. The back end is the cloud section of the structure (Fig. 1).

If the cloud computing corporation has a portion of clients, there is a possibility of high request for storage area. Some firms involve hundreds of digital storage manoeuvres. Cloud computing systems need at least twice the number of storage strategies to keep all its clients' data warehoused. That's because these strategies, like all computers seldom break down. Cloud computing system necessities make a copy of all its clients' data and store it on other devices. The copies allow the central server to contact backup machines to recover the data or else they would be inaccessible. Making copies of data as a backup is called redundancy.

Categories

Public clouds: These are managed by third parties. Works from different customers may be assorted together on the servers, storage structures and other infrastructure in the cloud. End user does not know whose job is executing on the same server, network or disk as their own jobs.

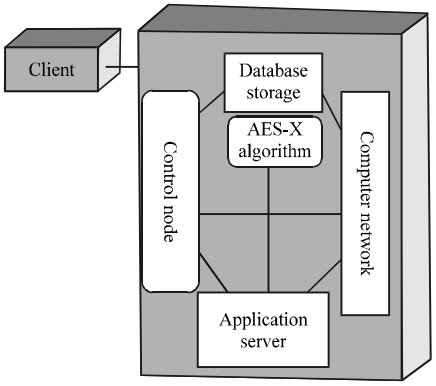

Fig. 1: Cloud computing architecture

Private clouds: This is a good option for corporations involved in data security and SLA. These are on-demand infrastructure operated by a single customer who maintains which application and where to run. They possess the server, network and disk and can choose which users are permitted to use the infrastructure.

Hybrid cloud: This combines the Public and Private Cloud Models. Industries own parts of the cloud and share others in a controlled way. It also offers on demand, externally managed scale but in addition to it the difficulty of defining how to dispense applications diagonally across these different places. While enterprises may be fascinated to these features of a hybrid cloud, these will likely be set aside for simple displaced applications that are not in need of complex databases or synchronization.

Concerns over cloud computing

Influential internet link: Cloud computing will only be conceivable with a strong internet link. Cloud computing might not work in areas where link is feeble. Even though there are presentations that might work with humble dial-up connectivity, the application could easily go down particularly when there is too many data to be handled.

Interoperability: A chief barricade to cloud computing is the interoperability of applications. Though it is conceivable to enclosure an Adobe Acrobat file into a Microsoft Word document, possessions get a little bit tackier when we discourse about web-based applications.

Security and privacy: The leading concern of any initiative or commercial or end users in dealing with cloud computing is security (Chen and Zhao, 2012). Vivacious facts located in cyber space faces meaningfully greater dangers in interior data depositories and software system. The cost of shielding the data can balance the advantages

of the cloud, especially if there is a security break. Hacks on the structure will last to be there as well. The outbreak that users experience today will also progress to adjust to different sorts of security methods. Worries can continue about loss of control over convinced sensitive data and the lack of security for stowed kernels. Privacy is another problem. If a client can log in from any locality to access data and applications, it's likely the client's privacy could be negotiated (Mohammed *et al*., 2012). Cloud computing corporations will need to find methods to defend client privacy. One way is to use verification techniques such as user names and passwords. Another is to employ an authorization format which enables the user to access only the data and applications applicable to his or her job.

Security issues in cloud computing: The importance of cloud computing is increasing and receiving a growing attention in the scientific and industrial communities. Cloud computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned over the internet and released with minimal management effort or service provider interaction. It combines a number of computing concepts and technologies such as Service Oriented Architecture (SOA), Web 2.0, virtualization and other technologies with reliance on the internet, providing common business applications online through web browsers to satisfy the computing needs of users while their software and data are stored on the servers. Although, there are many benefits to adopting cloud computing, there are also some significant barriers to adoption. One of the most significant barriers to adoption is security followed by issues regarding compliance, privacy and legal matters (Inan *et al*., 2012). Because cloud computing represents a relatively new computing model, there is a great deal of uncertainty about how security is at all levels (e.g., network, host, application and data levels) can be achieved and how applications security is moved to cloud computing. That uncertainty has consistently led information executives to state that security is their number one concern with cloud computing.

Security concerns (Bisong and Rahman, 2011) relate to risk areas such as external data storage, dependency on the "public" internet, lack of control, multi-tenancy and integration with internal security. Compared to traditional technologies, the cloud has many specific features such as its large scale and the fact that resources belonging to cloud providers are completely distributed, heterogeneous and totally virtualized. Traditional security mechanisms such as identity, authentication and authorization are no longer enough for clouds in their current form security controls in cloud computing are for the most part, no different than security controls in any IT environment. However, because of the cloud service models employed, the operational models and the technologies used to enable cloud services, cloud computing may present different risks to an organization than traditional IT solutions (Hashizume *et al*., 2013). Unfortunately, integrating security into these solutions is often perceived as making them more rigid. Moving critical applications and sensitive data to public cloud environments is of great concern for those corporations that are moving beyond their data centre's network under their control. Here, researchers present countermeasures related to these threats and other security issues which try to solve these problems.

LITERATURE REVIEW

Nalinipriya and Kumar (2013) proposed that system an advanced cryptographic encryption standards is being used to prevent the attack on the data. This method is necessary for the hour as the vulnerability of the data in the remote server is high. The privacy of the sensitive data that is being stored in the server is done using the most advanced algorithm; the AES-NI. Before encrypting the sensitive data a hash number along with a time stamp is being generated using MD5 such that the integrity of the stored data is confirmed. Singh *et al*. (2011) proposed about a secured cost effective multi-cloud storage in cloud computing which seeks to provide each customer with a better cloud data storage decision taking into consideration the user budget as well as providing him the best quality of service offered by available CSP.

Kumar and Sexena (2011) proposed to facilitate the client in getting a proof of integrity of the data which he wishes to store in the cloud storage server also minimizes the size of the proof of data integrity so as to reduce the network bandwidth consumption. This scheme proves advantageous to thin clients like PA's and mobile phone. The encrypting process is very much limited to only a fraction of the whole data thereby saving the computation of the client. This scheme applies only to the static storage if the data.

Bisong and Rahman (2011) proposed that deploying cloud computing in an enterprise infrastructure bring significant security concerns. Successful implementation of cloud computing in an enterprise requires proper planning and understanding of emerging risks, threats, vulnerabilities and possible countermeasures. Researchers believe enterprise should analyse the company/organization security risks, threats and available

countermeasures before adopting this technology. Nalinipriya and Kumar (2013) proposed an overview of different types of vulnerabilities on the cloud. They also discuss about the state of art cloud offerings such as SQL Injection, Command Injection and Cross-Site Scripting. In this research, researchers have discussed security risks and concerns in cloud computing and enlightened steps that an enterprise can take to reduce security risks and protect their resources. Researchers have also explained cloud computing strengths/benefits, weaknesses and applicable areas in information risk management.

In the allied system, researchers have described the various techniques which have been followed to ensure the privacy of the data and they have concluded that AES is the most recent, widely used and the best known algorithm. Even though AES can be used in the cloud, it has a common drawback; the time consumption. This can lead to various attacks during the encrypting process. This has to be reduced at the hour and a still more efficient algorithm is needed. Further, researchers have extended their concern about more efficient algorithms are needed to have an efficient access and retrieval of the data. This needs to be done because most of the attacks on the data are only in the channel or the medium on which it is being propagated. Since, the proposed mechanism are too old and DES has been broken long back; researchers could not rely on that as it might be too harmful. Despite the abundance of standards and products dealing with the protection of cloud computing systems, many aspects such as the third party auditing and resource allocation are still being investigated. Privacy protection issues are also a greater concern where the data are prone to the third parties.

PROPOSED ENCRYPTION ALGORITHM

In the proposed system, an advanced cryptographic encryption standard is used to prevent the attack on the data. This method is necessary for the hour as the vulnerability of the data in the remote server is high. The privacy of the sensitive data that is stored in the server is done using the most advanced algorithm; the AES-X. Before encrypting the sensitive data, a hash number along with a time stamp is generated using MD5 such that the integrity of the stored data is confirmed. The hash number thus generated is encrypted along with the data and stored in the database. To further enhance the trust of the CSP, a trust certificate of the CSP along with the hash number and the time stamp is sent to the client either through text message or to e-mail id. This hash code is retained by the client so that during the retrieval process, the integrity of the data can be measured only by this. During the retrieval process the client can decrypt the data by giving the hash value that is obtained during the encrypted process. This should match the hash value stored along with the data in the database. Once it matches the data is decrypted and is shown to the client. This process is used to restrict the access of the data by others.

IMPLEMENTATION

Java implementation of AES 512 encryption and decryption (Sekar *et al*., 2011) is done. Here, AES operates on a 16×32 array of bytes, termed the state. The input key for encryption is 512 bits. To represent the 512 values 9 bits are required:

Step 1: Single round of encryption. Instruction combines the four steps of the AES algorithm-Shift Rows, SubBytes, MixColumns and AddRoundKey into a single instruction.

Step 2: Here, instruction for the last round of encryption. Combines the ShiftRows, SubBytes and AddRoundKey steps into one instruction.

Step 3: Instruction for a single round of decryption. This combines the four steps of AES-InvShiftRows, InvSubBytes, InvMixColumns, AddRoundKey into a single instruction.

Step 4: It performs last round of decryption. It combines invShiftRows, InvSubBytes, AddRoundKey into one instruction.

Step 5: It is used for generating the round keys used for encryption.

Step 6: Here, it is used for converting the encryption round keys to form a usable for decryption using the equivalent inverse cipher.

Hash functions: A public function that maps a message of any length into a fixed length hash value which serves as the authenticator. Researchers will mainly be concerned with the last class of function, however, it must be noted that hash functions and MACs are very similar except that a hash code doesn't require a secret key. With regard to the first class, this can be seen to provide authentication by virtue of the fact that only the sender and receiver know the key. Therefore, the message could only have come from the sender. However, there is also

Table 1: Data security (encryption) in cloud computing

Storage	Processing	Transmission
Symmetric encryption	Homomorphic encryption	Secret socket layer, SSL encryption
AES-DES-3DES-Blowfish-MARS	Unpadded RSA-ElGamal	SSL1.0-SSL3.0-SSL3.1-SSL3.2

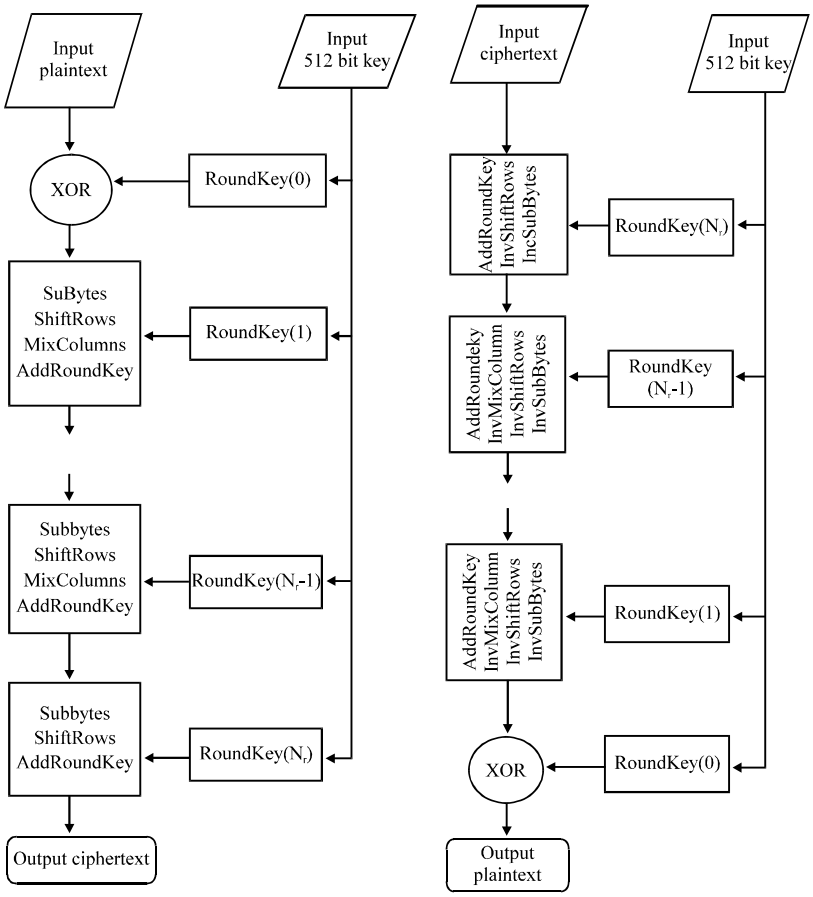

Fig. 2: a) Encryption procedure using AES X and b) decryption procedure using AES X

the problem that the plaintext message should be recognizable as plaintext message. The hash value is appended to the message at the source at the time when the message is assumed or known to be correct. The receiver authenticates that message by computing the hash value. Because the hash function itself is not considered to be secret, some means is required to protect the hash value.

Architecture diagram: The clients register their credentials upon accessing the cloud to upload their data. Once their login is successful, the data upload form is displayed to upload their data. After this process, a hash function is generated to provide a key to the user to access his AES-X algorithm and is being stored in the data. Here, the client data is sent to the cloud server where a hash key and a time stamp are generated. This file along with the key details is encrypted using AES-X algorithm which is the most advanced cryptographic algorithm now. The keys that are generated are sent through the D-H key exchange protocol and hence the route is secured. After the encryption process, the file is stored in the database (Fig. 2a and b).

Comparison: Table 1 indicates that every cloud provider encrypts the data in three types and still there is a threat in the intrusion of the stored data. Hence, a more advanced encryption standard is needed to store the client's data safe.

Figure 3 indicates the complexity that is being computed by the D-H key exchange protocol and other public ciphers. Usage of D-H decreases the computational time and complexity of the process. Figure 4 shows the performance comparison of Encryption algorithms. The results shows that AES-X algorithm is outperformed other

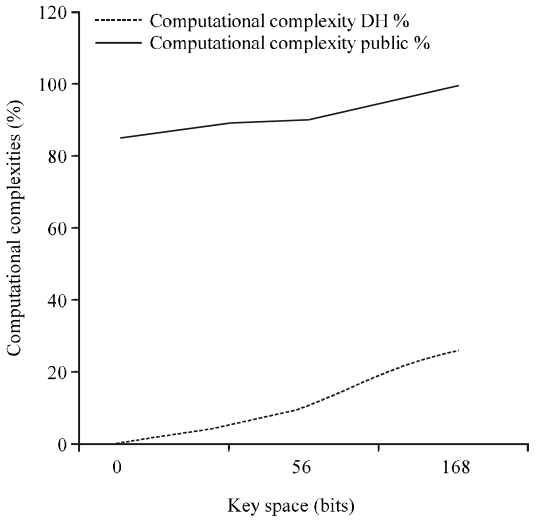

Fig. 3: Computational complexities

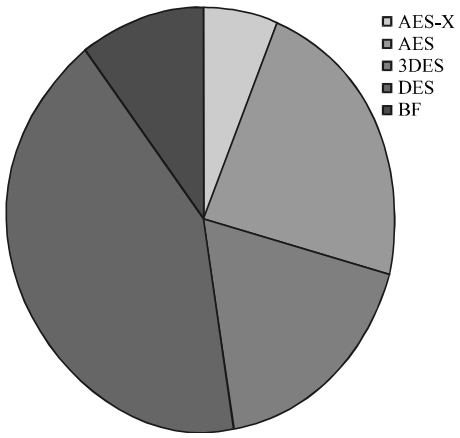

Fig. 4: Cipher encryption performance comparison of various algorithms

algorithms in both the number of requests processes per second in different user loads and in the response time in different user-load situations.

CONCLUSION

As there has been a rapid advancement in the storage and the retrieval of the data from the database the concentration has to be laid on the security issues. Here, the data is being uploaded by the client in a way such that they can be confirmed of the place and the storage details of their file. By this way, the client can be sure that his data is in a secured way and that it has the key that is equal to the key that is being generated during the upload of the data. In this phase, a security protocol is being presented to secure the data files of the client in the cloud infrastructure. Here, the hash key acts as a capability based model to ensure the secure access of the file only by the client. This provides further enhancement to the security concerns of the cloud. This feature also helps in providing a two-step authentication and hence the client is assured with more security for his data. The future research is to focus on the encryption and decryption of the data using AES-X algorithm which will ensure the client, his data being safe and secure using D-H key exchange protocol. It will be practically difficult for the third party to access the data that is stored in the cloud. It also ensures that only the person who uploads the data on the cloud will be able to access the file and the consistency of the data can be maintained during auditing.

REFERENCES

Bisong, A. and S.S.M. Rahman, 2011. An overview of the security concerns in enterprise cloud computing. Int. J. Network Secur. Appl., 3: 30-45.

Chen, D. and H. Zhao, 2012. Data secuity and privacy protection issues in cloud computing. Proceedings of the IEEE International Conference of Computer Science and Electronics Engineering, March 23-25, 2012, Hangzhou, pp: 647-651.

Hashizume, K., D.G. Rosado, E. Fernandez-Medina and E.B. Fernandez, 2013. An analysis of security issues for cloud computing. J. Internet Services Appli. (In Press). 10.1186/1869-0238-4-5.

Inan, A., M. Kantarcioglu, G. Ghinita and E. Bertino, 2012. A hybrid approach to private record matching. IEEE Trans. Dependable Secure Comput., 9: 684-698.

Kumar, R.S. and A. Sexena, 2011. Data integrity proofs in cloud storage. Proceedings of the 3rd IEEE International Conference on Communication Systems and Networks, January 4-8, 2011, Bangalore, pp: 1-4.

Mohammed, E.M., Abdelkader, H.S. and S. El-Etriby, 2012. Enhanced data security model for cloud computing. Proceedings of the IEEE International Conference on Informatics and Systems, May 14-16, 2012, Cairo, pp: 12-17.

Nalinipriya, G., R.A. Kumar, 2013. Secure massive data storage with consistency and route control on the cloud. IOSR J. Comput. Eng., 9: 18-25.

Sekar, A.C., S. Radhika and K. Anand, 2011. Secure communication using 512 bit key. Eur. J. Sci. Res., Vol. 51.

Sekhar, C. and U. Nanaji, 2013. Secure cloud by it auditing. Int. J. Modern Eng. Res., 1: 332-337.

Singh, Y., F. Kandal and W. Zhang, 2011. A secured cost-effective multi-cloud storage in cloud computing. Proceedings of the IEEE Computer Communications Workshop, April 10-15, 2011, Shanghai, pp: 619-624.