An Analysis of Cloud Security Models in Real-Time Distributed Computing

Lakshmi Naga Divya Tamma, Shaik Shakeel Ahamad

Abstract: ***Cloud security plays a vital role in the distributed environment for sharing structured or unstructured data in a secured way. As the size of the cloud data increases, it is difficult to secure the user's data using the traditional cloud security models. Most of the traditional cloud security algorithms such as AES, DES, ECC, RSA etc are used to encrypt the limited structured data to the cloud server. However, these algorithms are independent of cloud user credentials due to high computational time and memory. In this paper, different types of traditional cloud security and encryption models are summarized along with limitations or issues.***

Index Terms: Attribute Based Encryption, Cloud Service Providers, CPABE, KPABE

I. INTRODUCTION

The cloud storage architecture generally consists of four entities. Initially, the data owner stores data and outsources them (the encrypted cipher text) to cloud service providers. Data owners have a major responsibility of specifying and implementing access policy trees over users. The above access control policies are applied in order to encrypt important information efficiently and after the successful completion of encryption, these encrypted cipher text data are uploaded into the cloud servers. Then, these uploaded data are allowed to be shared among different numbers of authenticated and validated users.

All the problems of data security and data confidentiality must be solved before user stores his sensitive private information on cloud server. In order to overcome these security and privacy issues, many cryptographic approaches are developed. This enables secure outsourcing of data to the cloud server. The data confidentiality issue is overcome by implementing an access privilege scheme for all users who wants to access the data stored in cloud servers. The problem related to fine-grained access control mechanism is resolved by applying access rights for data in a hierarchical order. Cryptographic approaches are applied on data of cloud server in order to encrypt them into cipher text. Only the authorized

users are permitted to execute the decryption algorithm and get the values of decryption keys. When an unauthorized user wants to take part in the process of decryption, the decryption algorithm does not allow him because he does not have decryption keys. There exist many issues in the process of encryption which includes costly bilinear pairing and slower processing speed of resource constrained devices.

Cloud Service Providers (CSPs) are responsible for handling cloud infrastructures which may include cloud servers as well as professionals. Data owners are required to store huge amount of sensitive data in cloud servers. Cloud service providers can be defined as service providers which manages the outsourced data. Data owners transmit the encrypted data to cloud servers and make these data available for others. Cloud servers must have large storage capability and huge computational resources. The process of information hiding uses the redundancy of human sense organs on digital signals in order to embed essential information. Different digital media carriers (audio, video, images, etc.) are used for the processing of information hiding. Various algorithms are implemented in order to perform the information hiding procedure smoothly.

Network Access Servers have the responsibility to connect the network with every individual cloud client. These cloud clients are capable of communicating with other nodes as well as with other cloud clients inside a particular cloud network. Apart from this, cloud clients are capable to behave just like cloud routers and they have the responsibility to route traffic for various other clients within a particular cloud network. Almost all previous researches on cloud network directly emphasizes on the cloud networks where all cloud routers and cloud gateways are operated by a particular operator. In order to access cloud network, at first the cloud client is required to register with the operator. All the traffic started by or terminated at cloud clients are safeguarded against external attackers. Many internal attackers just like cloud routers, cloud routers operated by malicious operators, and curious or malicious routing are not at all considered. Again, all previously developed techniques are capable to resolve the authentication issues and traffic protection.

Now-a-days, as the size of the data increases with technology, cloud computing has become popular data storage system and computing services for a large number of applications. As it overcomes all the disadvantages of traditional computing mechanisms of centralized system, it has become widely accepted and distributed computing in various domain fields.

Revised Manuscript Received on April 07, 2019.

Lakshmi Naga Divya Tamma, CSE, KLU, Guntur,India.
Dr.Shaik Shakeel Ahamad, Dept of Information Technology,,CCIS, Majmah University, Al Majmaah,Riyadh, Kingdom of Saudi Arabia and Dept of CSE,KL University,Guntur,,India.

Cloud security is the process of securing sensitive information those are transmitted through the network by encoding them. The process of encoding original sensitive message is known as encryption in which plain text is converted to cipher text with the help of an encryption key. On the other end, the encrypted cipher text is decoded by using the decryption algorithm with the help of decryption key. A large number of cryptographic approaches are integrated with each other to form hybrid and more secure approaches. Since years vast amount of research works have been carried out in order to develop an efficient and advanced cryptographic scheme. Clients want to make their sensitive information secure, before uploading them into the cloud server. Therefore, these sensitive details are needed to be encrypted before uploading. In this research paper, we thoroughly studied and analyzed several previously developed attribute-based encryption as well as decryption approaches. There has been extensive amount of research works carried out in order to ensure the security of cloud networks. There are numbers of different efficient approaches by implementing which many attacks can be identified. Below are the severe issues those are found in the above-mentioned research works.

1. Excessive packets are eliminated and those are not at all processed. Again, lower priority packets are also eliminated that may result packet loss.
2. The security protocol results huge control overhead because of cryptographic extension and acquisition delay.
3. These systems are not at all efficient and effective for huge numbers of nodes. It also results huge execution time.
4. Initial packet loss can be noticed because of probable selection of wormhole nodes.
5. In each and every case, these approaches results noticeable identification inaccuracy.

Chaotic Quantum Cryptography can be defined as an integration of two separate topics known as quantum cryptography and chaos functions. According to the chaos function and random processes in quantum cryptography, a chaos function and its initial condition is responsible for defining random numbers. Out of all of these random numbers, one is chosen in order to detect the random process of photon Sops at sender or at receiver. The initial key is constructed by applying two separate random processes at sender as well as receiver. In the initial step, both sender and receiver accept the chaos function and all its properties completely.

II. RELATED WORK

G. Akilarasu and S. Mercy Shalinie developed a new and advanced security scheme in order to achieve wormhole-free routing [1]. Again, the above proposed scheme is efficient in order to prevent DoS attacks. With the advancement of technology and its implementation in various applications, cloud networks are considered as the present day's research area. Wormhole attack is considered as the most common and dangerous attack that can affect vast numbers of routing protocols. Hence, an efficient and effective scheme is needed which can obtain wormhole-free routes in the network. The above proposed scheme is basically a monitoring scheme to enhance the traditional security mechanisms of cloud networks. At first, final state model is implemented where the nodes gather information related to the sender and the receiver. After that, wormhole-aware secure routing scheme is applied in order to get wormhole free routes in the network. At last, the priority mechanism is implemented, and the data packets are sent according to their priority. In other words, higher priority packets are sent first, and then lower priority packets. Apart from these, the above presented finite state model has the responsibility to eliminate malicious or wormhole nodes from the network. In this piece of research work, an advanced monitoring approach is introduced in order to make an improved security mechanism. This technique is efficient enough to distinguish among cooperative nodes and selfish nodes. In the subsequent phase, it can eliminate those selfish nodes properly. By analyzing the outcomes of the evaluation phase, we can mention here that, the above approach can decrease the packet drop which can be caused due to certain attacks. Additionally, it enhances the packet delivery ratio remarkably. The above presented technique completely emphasizes on the static cloud network which is counted as a limitation of the technique. In future, further research works can be carried out in order to implement the above proposed scheme on dynamic cloud networks.

Initially in 2005, Attribute-based encryption and decryption model was proposed by Sahai and Waters. They tried to enhance the security and privacy of all existing traditional cryptographic models and hence developed Attribute-Based Encryption model (ABE). The above proposed model is capable of resolving all limitations of traditional cryptographic schemes. This is the prime objective and major concern of this proposed model. Here, users attributes plays an important role in the process of constructing secret key and cipher text. A user-defined threshold value d is set for this algorithm. Both secret key and cipher text are required to satisfy this minimum threshold d. When secret key and cipher text satisfies threshold, the process of decryption is possible for that system. Without satisfying minimum threshold, the process of decryption becomes impossible. This model is collision resistant in nature. There exists only a single issue in this model i.e.: for successful execution of encryption algorithm, users' public keys are mandatory. Because of involvement of monotonic attributes, this technique can't be efficiently implemented in real world applications.

This model requires further modification and extension in future in order to be implemented practically in cloud computing.

K. Ren, S. Yu, W. Lou and Y. Zhang introduced a new privacy-enhanced yet accountable security framework for metropolitan cloud networks [2]. The multi-hop cloud networks have become more popular now-a-days. This technique is actually a low-cost technique which can be implemented in order to provide broadband internet access within metropolitan areas. Both security and privacy are considered as the major factor behind the efficiency of cloud networks. Presently, there are numbers of service-oriented applications which can be supported by deploying cloud networks. There is no significant amount of research works have been carried out during the process of privacy preservation in case of cloud networks. This approach is known as PEACE (privacy enhanced yet accountable security framework). This method enforces sophisticated user access control in order to manage the gap between free riders send malicious users. Apart from this, this technique provides an advanced user privacy protection scheme that is beneficial for all of the network entities. This technique is a perfect combination of strong authentication and key agreement protocols in order to carry out the complete process of short group signature variation.

U. C. Yadav and S. T. Ali studied and analyzed all approaches of cloud data security based on CP-ABE techniques [3]. They identified privacy issue of traditional CP-ABE techniques and proposed an extended approach which is known as Cipher text Policy-Hiding Attribute-Based Encryption. They presented a highly secure CP-ABE technique through composite-order bilinear groups that is responsible for hiding access structure. In case of all classical CP-ABE techniques, the data owner is required to send the access structure with cipher text. Hence, everyone will be able to learn the access policy. There exist chances of access structure violation. In other words, it discloses secret information cipher text has and also discloses the partial anonymity of the decryptor. Access structure merged with cipher text in case of biomedical database and cloud server applications, it is required to hide access structure.

L. Touati, et.al analyzed the drawbacks of traditional CP-ABE techniques [4] and introduced a new scheme known as Cooperative Cipher text Policy Attribute-Based Encryption approach [5]. The proposed research work is a collaborative technique which is based on CP-ABE approach in resource-constrained nodes. Cooperative Cipher text Policy Attribute-Based Encryption approach follows the basic concepts of heterogeneity of the network in order to distribute the encryption overhead. Verification of security is performed automatically with the help of an advanced validation tool AVISPA.

L. Warren and H. Chi introduced a new approach to include extended security to the EHRs through the implementation of CPMA-ABE approach [6]. In the above presented approach, a framework is built in order to efficiently share biomedical documents of patients more securely. The above framework overcomes the problems of multiple EHR owners and also the issues related to users. The above scheme can result better data privacy and complexity of key management is decreased remarkably as compared to other previously developed approaches. The encryption technique is implemented to carry out the process of encryption by encrypting the EHR data. Only authorized users can access or modify these sensitive details, but all unauthorized users are unable to access and edit these confidential data. These users can be either individual users or multi-dimensional users. One of the significant advantages of this technique is, handling several user revocation and accesses.

In order to overcome the issues of single cloud storage schemes, multiple cloud storage schemes are developed. This scheme is developed to add security to multi-cloud data. DepSky is a multi-cloud storage scheme which is presented to support availability, confidentiality and integrity. RACS [7] is commonly used multi-cloud storage technique that supports availability. It eliminates vendor lock–in, economic failure and outages failure. RACS stands for Redundant Array of Cloud Storage [8]. It is a proxy approach that involves RAID in order to split and store data in multiple clouds. RACS is integrated with Zookeeper to manage the clients' action with cloud database. It uses erasure code for replication of data over multiple clouds. Another technique HAIL (High Availability and Integrity Layer) is proposed for multi-cloud systems to support availability and integrity. This also utilizes RAID for replication of a single file in multiple clouds. The redundancy of same file ensures integrity and availability. All the downloaded files are similar. Inter-cloud is another multi-cloud storage scheme that uses RAID for data replication. In the following section we have analyzed the pros and cons of both single cloud storage and multi cloud storage.

The ABE approaches are developed for privacy preservation of users through hiding some query information about the owner and user. The updated version of traditional attribute-based encryption technique includes a searching strategy for encrypted data. Hence, it is implemented in privacy preservation applications in the fields like finance, biomedicine and military database. Achieving the same level of security and performance along with other conventional techniques are more costly in terms of computational cost, storage cost and communication overheads. As compared to both KP-ABE and CP-ABE, the performance of CP-ABE-WP is much better. This approach includes the idea of Secure File Sharing System (SFSS) which is executed over cloud. The above system enables the authenticated users to perform some file related operations such as create, read, write, delete and modify the files stored in chunk format. All the traditional CP-ABE models can't satisfy the needs of scalable media sharing. In order to overcome this problem MCP-ABE approach is introduced which is able to support scalable media.

Multiple messages are encoded by applying encryption algorithm and form a cipher text message. The most widely implemented application of this algorithm is the content delivery systems.

III. PROPOSED MODEL

In our new model we are introducing a Novel Client Integrity Verification of Quantum Key distribution with Cipher text Policy based Attribute Based model was done on storage of cloud data. This model was shown in three phases as shown in Figure 1. In the Phase 1, Unique Identification Key(UIK) is generated to authorized cloud user for integrity verification. In the Phase 2, control access mechanism and the encryption operations will be performed on the authorized user's cloud data. In the Phase 3, user control access verification, decryption operations will be done on encrypted cloud data. Here, a Quantum key distribution based CPABE encryption and decryption model was used for data encryption and decryption process. Quantum cryptography is a technique used to secure information exchange between legitimate users along communication lines. Chaotic Quantum Cryptography can be defined as an integration of two separate topics known as quantum cryptography and chaos functions. According to the chaos function and random processes in quantum cryptography, a chaos function and its initial condition is responsible for defining random numbers. Also, a novel chaotic hash algorithm is used for integrity verification.

Trusted Authority Agent (TAA) is a server program used to verification and validation of cloud user's integrity as access control mechanism. TAA takes cloud parameters, attribute list and policies as input to generate unique identification key (UIK) as client integrity value.

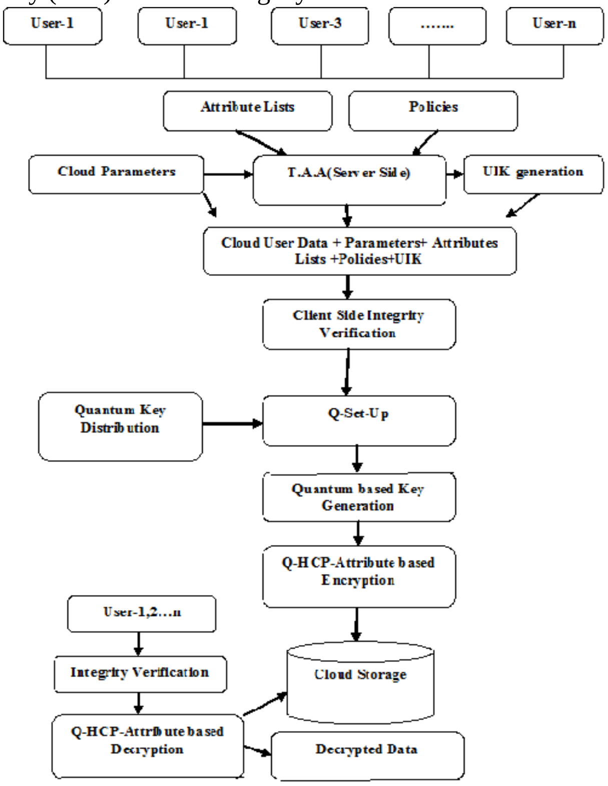

Figure1: Proposed Model

IV. EXPERIMENTAL RESULTS

Experimental results are performed on the real time cloud computing environment such as Amazon EC2 servers. Proposed client integrity verification-based Quantum –CPABE model is executed on Amazon EC2 cloud services. Here, Amazon S3 is used for client data storage and access control mechanism.

Statistical Integrity Randomness:

Shannon proposed two measures namely confusion and diffusion as essential features for strong integrity verification process. For an efficient diffusion property, there should be 50 percent bit change in the hash value. Let the initial message and its bit values are taken as original data. The changed bits of the computed hash value are

Table 1: Comparative results of new model with previous models

Algorithms	Encryption Time(ms)	Data size
MD5+CPABE	7434	1M
SHA512+KPABE	7845	1M
MD5+FHEncryption	6395	1M
Whirlpool+KPABE	6594	1M
QCP-ABE+ProposedEGCM	5474	1M

Table 1 explains our new model has low encryption time of data during the data security when it is compared with previous existing models.

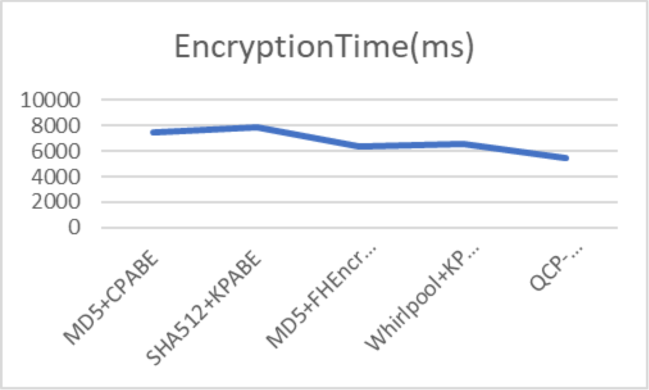

Figure 2:Comparison of Proposed Model to Existing models in terms of average runtime

V.CONCLUSION

With more and more cloud-based applications are being available and stored on various cloud servers, a novel multi-user-based privacy protection mechanism need to design and develop to improve the privacy protection on high dimensional data. As the size of the cloud data increases, it is difficult to secure the user's data using the traditional cloud security models. Most of the traditional cloud security algorithms such as AES, DES, ECC, RSA etc are used to encrypt the limited structured data to the cloud server. However, these algorithms are independent of cloud user credentials due to high computational time and memory. In this paper, different types of traditional cloud security and encryption models are summarized along with limitations or issues.

REFERENCES

1. Abbadi, I.M. and Martin, A. (2011). Trust in the Cloud. Information Security Technical Report, 16, 108-114. doi:10.1016/j.istr.2011.08.006
2. Agarwal, A. and Agarwal, A. (2011). The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences, 1 (Special Issue on CNS), 257-259.
3. Arshad, J, Townsend, P. and Xu, J. (2013).A novel intrusion severity analysis approach for Clouds. Future Generation Computer Systems, 29, 416–428. doi:10.1016/j.future.2011.08.009
4. Atayero, A.A. and Feyisetan, O. (2011). Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption. Journal of Emerging Trends in Computing and Information Sciences, 2(10), 546-552.
5. Bisong, A. and Rahman, S.S.M. (2011). An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications, 3(1), 30-45. doi:10.5121/ijnsa.2011.3103
6. Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J. and Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25, 599–616.
7. Casola, V., Cuomo, A., Rak, M. and Villano, U. (2013). The CloudGrid approach: Security analysis and performance evaluation. Future Generation Computer Systems, 29, 387–401. doi:10.1016/j.future.2011.08.008
8. Che, J. Duan, Y, Zhang, T. and Fan, J. ().Study on the security models and strategies of cloud computing. Procedia Engineering, 23, 586 – 593. doi:10.1016/j.proeng.2011.11.2551

AUTHORS PROFILE

Lakshmi Naga Divya Tamma received her B. Tech in Computer Science and Engineering from JNTUKakinada, Andhra Pradesh and received M. Tech in Computer Science and Engineering from JNTUKakinada, Andhra Pradesh India. Currently she is working as an Assistant Professor in Saraswati College of Engineering, Kharghar, NaviMumbai, India. Her research includes Network Security.

.

Dr. Shaik Shakeel Ahamad is currently working as an Assistant Professor in Department of Information Technology, CCIS, Majmaah University, Kingdom of Saudi Arabia. He was a Professor in the Department of CSE, KL University, Guntur, India (now on lien). He holds a PhD in Computer Science from the University of Hyderabad, India in the realm of secure mobile payments protocols and formal verification. His research interests include cloud-based mobile commerce, secure mobile healthcare frameworks and protocols, wireless public key infrastructure and digital forensics.