International Journal of Innovative Research in Computerand Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488|

||Volume 9, Issue 5, May 2020||

Cryptographically Enforced Dynamic Access Control in Cloud: A Survey

Chethan S V[1], Dhananjaya[2], Harish S[3], Rajeshwari B S[4]

Student, Dept. of CSE., BMS College of Engineering, Bengaluru, India[1]

Student, Dept. of CSE., BMS College of Engineering, Bengaluru, India[2]

Student, Dept. of CSE., BMS College of Engineering, Bengaluru, India[3]

Assistant Professor, Dept. of CSE., BMS College of Engineering, Bengaluru, India[4]

ABSTRACT: Some users find it enticing to allow the untrusted cloud to have cryptographically enforced access controls for data. But a effective cryptographically enforced, dynamic access control system in the cloud is still difficult to design and build.The previous works show high traffic when practically changing access control strategies is required. Earlier the user's access to the system was done by modifying his accession to which the files were previously encoded. This idea is still not secure since before the revocation, the user can take a copy of the keys in his local machine. Documents should be re-encoded with new keys to manage these types of issues. This method has generated contact traffic, as the file owner wants to access the file, Re-encode the file, and update it to whatever it was previously. Due to its huge benefits, people and industries are using the cloud quickly these days to store and manage data. Cloud service vendors including Amazon, IBM, etc. are offering more services to easily reachable consumers like small scale services.But still, the incidents of data breaching happening in recent times such as data loss, release of personal images have created caring about the privacy of cloud information. Generally, cloud service is not always safe due to the bad incidents happening around us. Now, the main challenge is how to make an insecure cloud safe in data management. Therefore, various structures and techniques suggested by the various authors are mentioned in this paper for a cryptographically enforced regulation of dynamic access in the cloud.

KEYWORDS: Cloud Computing, Access control, Revocation.

I. INTRODUCTION

The main purpose of energy efficient algorithm is to maximize the network lifetime. These algorithms are not just related to maximize the total energy consumption of the route but also to maximize the life time of each node in the network to increase the network lifetime. Energy efficient algorithms can be based on the two metrics: i) Minimizing total transmission energy ii) maximizing network lifetime. The first metric focuses on the total transmission energy used to send the packets from source to destination by selecting the large number of hops criteria. Second metric focuses on the residual batter energy level of entire network or individual batt Consumers are increasingly finding it easier to store and exchange data through cloud platforms with the big breakthroughs in cloud services. Cloud service providers such as Amazon, Microsoft, Apple and so on provide numerous cloud-based services, from small-scale personal services to massive-scale industrial services . Nonetheless, latest data breaches such as leaks from private photos have sparked questions about the safety of cloud-managed data. In fact, due to the drawbacks of the software and system design weakness, a cloud service is typically not secure. As such, how to maintain regulation of access to data on the potentially unsecure cloud is a critical issue. In reaction to these security problems, several works have been suggested by utilizing cryptographic primitives to help access control over unsecured cloud services. Advanced cryptographic primitives are used for the implementation of many paradigms for access control.

II. DYNAMIC ACCESS CONTROL

Dynamic access control is a brand new windows technology that enables Windows administrators to modify the authorization to file server resources using conditional logic based on user or device claims. Crypt-DAC, a tool that offers practical cryptographic compliance with the complex access control inside the potentially unsecure cloud provider.Crypt-DAC uses three strategies to accomplish its objectives. In particular we recommend delegating the cloud with a delegation-conscious encryption approach to update policy data in a privacy-conserving manner. Using an adjustable onion encryption strategy, we recommend avoiding costly re-encryption on the administrator side of the file files. Alternatively a delayed de-onion encryption technique is recommended prevent overhead reading of the text.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488|

||Volume 9, Issue 5, May 2020||

III. CLOUD BASED SECURITY TECHNIQUES

YossibShallabi et al., [4] proposed an architecture that supports Role-Based access control for No SQL database systems. The Role-Based Access Control (RBAC) service is being researched using cryptography for the distributed databases No SQL. Cassandra is a complex DBMS that does provide effective support for massive databases but offers simple security initiatives. Within this the author has proposed a model and protocols for cryptographic compliance of an ACP (full form) in a device style cassandra, Which would reduce the load on the Node Coordinator, thereby eliminating the foundation from the existing security framework. It allows any client to read the data of any storage node(s), given that the encryption keys that allow it number of clients to decrypt data would be owned by only the clients that the ACP grants access to a data.

Vipul Goyal et al.,[7] proposed a data encryption approach to Role Based access control.When more confidential data is exchanged and stored on the Web by third-party sites, data at such sites may be required to be encrypted.One downside to encoding data is that it can only be transmitted selectively at the coarse-grained level.Here, the authors created a new cryptographic scheme called Key-Policy Attribute-based encryption for storing encrypted messages with fine grains. Cipher-texts are labeled in the presented crypto scheme with sets of attributes and private keys associated with access mechanisms that monitor and maintain which cipher-texts a user can decrypt to. The authors show the construction's applicability to communicating audit-log knowledge and broadcast encryption.Here these innovations support private key assignment which includes encryption based on Hierarchical Identification.

J. Bethencourt et al.,[5] suggested an encoding based on the Cipher Text Policy feature. Only if the user has a set of credentials or attributes, several distributed system users should be able to reach and get data. Recently, the only way to enforce these policies is by using trusted server to store data and try to resolve control of access. But, if any data storage system is compromised, then data privacy would be compromised. Here they present a framework for the realization of complex access control over encrypted data called Cipher Text Protocol Attribute Based Encryption.Through knowing these encrypted data tricks, the authors can be keep confidential even though they can not trust the storage server.In addition, the approaches described are safe against fraud attacks.Earlier Attribute Based Authentication systems used attributes to identify the encrypted data and generated policies into customer keys, but the user's identities are defined in the defined device attributes, and a data handling player decides how a rule can decode them. Finally, by concept this approach is similar to conventional forms of access control, such as Function Based Access Control. They also include the proposed framework to be introduced to provide performance assessments.

Steven Myers et al.,[1] have proposed a functional revocation algorithm as well as a key revocation. They are considering data maintenance issues on unsecure clouds. There are two important use cases in particular: I the use of public-key encryption to implement complex access control, and (ii) the use of successful key rotation. Revocation of permission is key to allowing dynamic access control andpromoting re-encryptionof data and related technologies as tools to enable insecure revocation of the cloud. Unfortunately, the literature believes data is explicitly encrypted with the primitives. Neat hybrid data encryption is therefore used for performance reasons and these schemes are likely to lead to key scraping threats.In main rotation instances, schemes that are currently implemented nowadays with ineffective protection properties are very computationally robust. The proposed systems are either likely to still trigger main breaching attacks or are too inefficient to deploy them.

LIEHUANG ZHU et al.[6] suggested an Efficient Biometric Authentication Defense of Privacy. These days the fingerprint identification is now becoming increasingly frequent.Through expanded use of cloud computing, database holders are encouraged to outsource the enormous size of biometric information and cloud authentication tasks to take care of the high expense of storage and computation, thus carry consumer privacy risks. Here, authors suggested an outsourcing system for fingerprint identification that would be effective and safeguarding privacy. The biometric data is mainly encrypted and is relocated to the cloud. The database holder encrypts query data to perform biometric authentication and sends it to the cloud server. Cloud conducts ID operations on the authenticated database and returns the output to the owner of the database.This security analysis suggests that even if attackers can build requests for verification and collaborate with the cloud this scheme is secure. Compared to previous procedures, experimental results indicate that the new scheme accomplishes improved performance in both phases of planning and detection.

Bharanidharan M, et al.,[3] proposed an Efficient Privacy-Preserving Data De-Duplication (EPD) structure in Cloud. Safe data de-duplication can dramatically reduce overheads in cloud computing systems for communication and computing, and has possible uses in our technology-driven society. Existing data deduplication systems are typically designed to either withstand brute-force attacks or guarantee the availability of productivity and information, but not both. EPD achieves both the availability of data, avoids threats by brute force and protects data security.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488|

||Volume 9, Issue 5, May 2020||

Additionally, documentation is taken into consideration to provide greater privacy guarantees than current systems. The data deduplication implemented outperforms current competing schemes in terms of overhead processing, connectivity, and storage.

Sultan Aldossary et al.,[2] discussed issues and the current solution in cloud services regarding data protection, confidentiality, accessibility and integrity. Now people are using cloud to store the data, as data is getting bigger and they need to be available from any computer. Because of that, now the storage of cloud data becomes normal. But there are many difficulties that counter data placed in the cloud starting from virtual machine, which is the mean of sharing resources in the cloud and ending up on cloud storage. Furthermore, sharing the data stored in the cloud amongst many users remains a problem as the cloud service provider is untrusted in managing authentication and authorizing. Here author addressed cases that discourage people from using the cloud and approaches that are being done to control the risks of these issues. The researchers addressed that data stored in the cloud must be private, safeguarding the dignity of confidentiality and being accessible.

Mr. Mangesh Nagarkar et al.,[8] explainstiming approach proposed called Public Integrity Auditing for Shared Hybrid Cloud Data with Team User Revocation. Use cloud infrastructure makes storage available everywhere being an growing phenomenon and maintaining open data auditing anywhere is a subject of great significance that has emerged in the literature of science.Some work looks at efficient auditing of public data integrity and safe issue for shared dynamic data. However, these schemes are still not safe in realistic cloud storage network against the revoked community users and cloud storage service collusion during user revoke.Here they find out that the current scheme has collusion attack and offers an effective vector-based public integrity audit scheme with local revocation group verifier signature and stable user group revocation. The author has drawn up a concrete scheme based on description of the author scheme.Ultimately, it is also safe and effective from the security and experimental research with the respective schemes of author's scheme.

Ramalingam Sugumar et al., [9] proposed a Symmetric Encryption Algorithm (SEA) to protectoutsourcedinformation data which is inpubliccloud area. The method of storing data in cloud is awell known popular way for backing up the data, archiving the data anddividing it. Giving the security to the data is one of the major learning of usingcloud.A Symmetric
Encryption algorithm for data protection in the cloud has been proposed here.Traditionally, statistical analysis used cr yptographic techniques to safeguard data. The proposed algorithm executes every value's ASCII code in user's origina l data. Encryption is performed until data is sent to the cloud.Symmetric Encryption Algorithm is implemented in JAVA, and cloud storage performs the encryption and decryption of the SEA. Symmetric Encryption Algorithm reduces the amount of time required to encrypt and decrypt. Data is regularly uploaded to the cloud and the Symmetric Encryption Algorithm suggested for latency when uploading data.The algorithm built can fit easily into cloud storage environment. SEA supports cloud users and service providers in ensuring the protection and privacy of cloud data. Cloud provider will not be allowed to access data stored on cloud servers. Consequently, the SEA offers a stable cloud data storage system. The proposed SEA provides the data stored in the cloud storage with greater protection.This technique is ideal for medical farming and the educational community to store their data safely in cloud storage.

Xiaoguang Wang et al., [10] implemented a SecPod: A Virtualization Platform focused on Security. The OS kernel is detrimental to a computer system's stability. Several schemes for strengthening the defense have been suggested. One fundamental downside of these systems is that page tables are not isolated from the insecure kernel, the data structures that control memory protection, and are therefore subject to interference.Researchers relied on virtualization to solve this problem to secure data protection for the kernel memory. Nevertheless, such memory security includes any change to the page tables of the guest to be reviewed. It actually contrastsalong withfrequentimprovements in virtualization support for the kind of hardware.Here introduced SecPod, an extensible framework for virtualization-based protection and privacy systems that can provide compatibility with new hardware, as well as tight isolationSecPod has two main techniques: paging representatives to a safe location and accounting the kernel's paging activities; execution trapping wiretaps attempts to subvert SecPod by abuse of privileged instructions.SecPod system is implemented based on KVM, and the experimental results demonstrate that SecPod is both powerful and reliable.

Anirudh Mittal et al.,[11] who proposed one attribute algorithm which is based on encryption.Which gives secure data while accessing through cloud, but some other people who knows much about cloud computing We addressed that various property-based encryption proposals for cloud storage were being suggested. Much of the knowledge drug safety research spotlight to get the power.And the author suggested a small unknown name that is an anonymous control in current access control plans to tackle identity safety and as well as customer character security.And all these are in the form of documents to get to the control gain and all these documents are stored in the cloud where it consists of more secure data, displaying the AnonyControl-F along these lines which ultimately holds the liquid-

shaped character spillage. And both AnonyControl-F, AnonyControl are secured under the DiffieHellmanpresumption,and these mechanisms shows the achievement of author plans.

Yeongpil Cho et al.,[12] introduced Hardware based Demand hypervisoractivation for Efficient Critical Code Safety Execution in Mobile Devices. Mobile apps must run safety critical codes (SCCs) for secure transaction and sensitive handling of details. The Trusted Execution Environment (TEE) market is that quickly to ensure that SCCs are executed safely.Even though various studies have constructed TEEs usingHypervisors or Trust Zone are faced with major challenges when considering mobile app deployment and have evinced the successful thing in terms of protection. Trust Zone-based approaches block the system's Trusted Computing Base, because they need to increase the most automated code base size.Hypervisorbased solution offers overlay of mobile device performance that has already weakened from asset limitations.To solve these issues, a hybrid solution has been suggested here that uses both the hypervisor and Trust Zone.Presented method effectively operates a TEE using a hypervisor which reduces overhead efficiency by activating only the hypervisor when the SCCs require TEE.It is called on-demand hypervisor activation, which was implemented easily which securely by leveraging the memory protection capabilities of Trust Zone.Presented method, incorporated and experimented with technologies from the real world.The result shows that the device presented can successfully protect SCCs without any significant delay (< 100 μs), while at the same time restricting the overhead increase due to hypervisor near 0 percent during hibernation.

ZhiQiao et al., [13] discussed Attribute Based Encryption (ABE) where an identity set of attributes is used to create secret key and access mechanism that regulates access. It effectively integrates the control of access and encryption into one structure and is perfect for sharing secrets between groups. The ABE scheme can be classified as follow: Based on the location where access structure attached, it can be categorized as Key-Policy ABE (KP-ABE) and Ciphertext-based ABE (CP-ABE). It may be classified as Centralized Authority and Decentralized Authority Schemes based on the type of Trust authority. The authors finally addressed the parameters for the optimal ABE program, followed by a comparison on both functionalities and efficiency.

Rathna D et al., [14] Proposed application Distribute Data Stored in Cloud with Competent Revocation. Access control is done to be handled with main distributed canter on a centralized model. Data are impacted if any of the main gets attacks because of processing on centralized form. To restore the data from the threats, decentralized method provides attributes for the data. A decentralized approach to access control is implemented to safeguard cloud data storage. Access control provides user authentication so that the encrypted data can be decrypted only by authenticated users. The user identification and permission control scheme is implemented in a standardized method of access control, which prevents replication attacks and allows the modification of cloud-saved data.Most information is being processed in the cloud and a lot of this is classified information. Clouds store sensitive patient data and allow medical professionals, hospital personnel, researchers and policy makers access. The decentralized approach provides authorization, without revealing the identity of the user.

ShukunYang et al., [15] proposed DPPG: A dynamic password generation software. Major websites and apps have a password protection tool, a password checker, to preserve the information by creating quick passwords for clients. Authors addressed that important password checker criteria are to be stringently effective in password protection analysis. The author explaining that irrespective of the strictness, these static checkers will reveal information and would potentially help the opponent strengthen the efficiency of their attacks. The Dynamic Password Policy Generator was added here to clear the problem, as it is an simple and practical alternative to the current password strength checker. DPPG aims at forcing distributed password space and creating complex rules for people to construct unique passwords that will contribute to good password database security for the program. DPPG is module-based, and can work on different basic policy creation metrics,In addition, they implement a diversity-based password security metric that tests password database protection in terms of availability and password space. The metric is useful as an anti-measure for well-designed algorithms to crack off-line.

WenjianLuoetal., [16] proposed A mechanism called Encrypted Negative Password Authentication, more efficient password storage is the key feature of a password authentication scheme, which, given some security concerns, is the most commonly used authentication concept.Here authors suggested a mechanism for eliminating a password authentication method designed to secure the safety of passwords which could be easily integrated into current encryption schemes.In this proposed framework, initially, aclient's obtained plain password is hashed by some cryptographic hash function. Then the hashed password is changed to negative password. The negative password will finally be encrypted into an encoded negative password using the traditional symmetric key method.Encryption of several versions may also be used to further enhance privacy security. The cryptographic hashing function and key encryption used to make it impossible to break the Encrypted Negative Password passwords. In fact, a given plain password has a lot of matching Encrypted Negative Password, which makes pre-computation attacks difficult.Analyzes and comparisons of the time complexity of the algorithm would suggest that the ENP rejects lookup table attacks that provides greater parental controls under the form of dictionary attack. ENP does not

incorporate any additional elements and will therefore avoid attacks by precomputation.Mainly, ENP is also the first password security concept that uses all the cryptographic hash, negative password and symmetric key algorithm without any need for more information except for flat password.

Geeta C M et al.,[17] addressed challenges in cloud computing and future development on data monitoring and privacy. Cloud information services needed to store information in the cloud and also to distribute information to different clients. The registry of cloud information includes issues with the confidentiality of information, data security and access to information by prohibited customers. Therefore it is important to have a private analysis and editing facility to ensure that the information is correctly accommodated and used in the cloud. Here the authors addressed state of the art data monitoring and security / security methods.It poses challenging issues in the auditing and protection of the repository content. The directions were presented for future research in data monitoring and privacy.

IV. CONCLUSION AND FUTURE WORK

Dynamic access control is a spanking new technology in windows that enables Windows Administrators to configure the permission to use conditional logic based on user or device claims to file server resources. In this paper various cloud security techniques proposed by different authors in satisfying the agreed dynamic access control is discussed. Different architecture that takes care of dynamic access control in cloud is discussed. Various security techniques for the data in cloud and its approach are discussed.

REFERENCES

[1] Steven Myers and Adam Shull Practical Revocation and Key Rotation,Springer International Publishing AG,part of Springer Nature 2018,LNCS 10808,pp 157-178.

[2] Sultan Aldossary ,PrinceSattam Bin Abdulaziz,Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4.

[3] Bharanidharan M, Karunakaran E An Efficient Privacy-Preserving Data De-Duplication in Cloud International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 8 .

[4] YossifShalabi and Ehud Gudes,Cryptographically Enforced Role-Based Access Control for NoSQL Distributed Databases,IFIP International Federation for Information Processing 2017 Published by Springer International Publishing AG 2017. All Rights Reserved G. Livraga and S. Zhu (Eds.): DBSec 2017, LNCS 10359, pp. 3–19.

[5] J. Bethencourt, A. Sahai, and B. Waters, Ciphertext-policy*attribute based encryption*,2007 IEEE Symposium on security and privac.

[6] LIEHUANG ZHU, CHUAN ZHANG , CHANG XU , XIMENG LIU, AND CHENG HUANG, Efficient privacy-preserving biometric identification,IEEE ,Volume 4,pp(99):1-1.

[7] Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters ,Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,Proceedings of the ACM Conference on Computer and Communications Securtiy,Article number 1180418,pp 89-98.

[8] Mr. Mangesh Nagarkar , Prof. Patole R.G2 ,Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation,JARIIE-ISSN(O)-2395-4396,Vol-3 Issue-3 2017.

[9] Ramalingam Sugumar and Sharmila Banu Sheik Imam,Symmetric Encryption Algorithm to Secure Outsourced Data in Public Cloud Storage,Indian Journal of Science and Technology, Vol 8(23), DOI: 10.17485/ijst/2015/v8i23/79210.

[10] Xiaoguang Wang ,Yue Chen, ZhiWang,Yong Qi, YajinZhou,SecPod: a Framework for Virtualization-based Security Systems,Open access to the Proceedings of the 2015 USENIX Annual Technical Conference (USENIX ATC '15) is sponsored by USENIX.

[11] Anirudh Mittal, Attribute Based Encryption for Secure Data Access in Cloud,

[12] Yeongpil Cho, Seoul National University; JunbumShin,Donghyun Kwon, Seoul National University; MyungJoo Ham and YunaKim,YunheungPaek, Hardware-Assisted On-Demand Hypervisor Activation for Efficient Security Critical Code Execution on Mobile Devices,2016 USENIX Annual Technical Conference.

[13] ZhiQiao, Shuwen Liang∗, Spencer Davisand Hai Jiang,Survey of Attribute Based Encryption,15th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence,Networking and Parallel/Distributed Computing.

[14] Rathna D, Sankaragomathi R, Thulasika S and ThiruselvanP,Distribute with Proficient Revocation of Data Stored in Clouds,J Inform Tech SoftwEng ISSN: 2165-7866 JITSE, an open access journal,Volume 5 • Issue 2 • 1000146.

[15] ShukunYang,Shouling Ji and Raheem Beyah DPPG: A Dynamic Password Policy Generation System,IEEE Transactions on Information Forensics and Security 2018, volume 13,Issue: 3,

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488|

||Volume 9, Issue 5, May 2020||

[16] WenjianLuo,Yamin Hu, Hao Jiang, and Junteng Wang, Authentication by Encrypted Negative Password, IEEE Transactions on Information Forensics and Security ,volume: 14 , Issue: 1.

[17] Geeta C Ma , Raghavendra Sb , Rajkumar Buyyac , Venugopal K Rd , S SIyengare , L M Patnaikf, Data Auditing and Security in Cloud Computing: Issues, Challenges and Future Directions, International Journal of Computer (IJC) (2018) Volume 28, No 1 , pp 8-57.