Indian J.Sci.Res. 17(2): 481-488, 2018 ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

AN OPTIMISTIC SECURITY PROTOCOL USING HIERARCHICAL BASED TOKEN SYSTEM FOR CLOUD INFRASTRUCTURE

[1] S.Prabaharan, [2]M.Saravanan, [3] S.Karthik
[1] Department of Computer Science and Engineering, Jyothishmathi Institute of Technology & Science, Karimnagar.
[2] Department of Computer Science and Engineering, Aurora Technological and Research Institute, Hyderabad.
[3] Department of Information Technology, College of Computing & Informatics, Saudi Electronic University, Ar rabi, Riyadh.

Abstract- Cloud computing developers face multiple challenges in adapting systems and applications for increasingly heterogeneous datacentre architectures. Many challenges remain, but ultimately cloud computing will both benefit from and contribute to the improved compute efficiencies and capabilities. Cloud computing has drastically condensed the computational and storage costs of outsourced data. The existing access control techniques or users access provisions centered on the common user attributes like Roles, which reduces the engrained access measure. A Hierarchical System and Access Stipulation (HSAS) scheme that provides the user an exclusive access through the use of a hierarchical structure which is a combination of user's unique and common attributes. Also, we deploy the concept of Token Provision that allows the users to verify the correctness of outsourced data without the retrieval of the respective less. The tokens are derived from the metadata containing location that helps in the process of storage correctness verification and improvises the storage efficiency.

keywords- Access Control, Access Structure, Barrier Limits, Storage Efficiency, Token Provision

I. Introduction

Cloud computing is one of the widely used emerging technique that offers various methods to acquire and manage IT resources on a large-scale [19, 22]. Cloud computing, in turn, provides different types of services such as Infrastructure-as-a-service (IaaS) also sometimes called as hardware as a service (HaaS) [1, 7], Platform-as-a-service (PaaS) and Software-as-a-service (SaaS). Cloud computing planning promotes the resource sharing in a pure plug and provides a model that dramatically implies its infrastructure. The major advantage of cloud computing includes ease-of-use and cost-effectiveness in accessing the resources over the Internet. Employing the resources in the cloud provides greater expediency to the user because of its systematic manner. Cloud helps us to make use of the existing technologies such as virtualization, service-orientation and grid computing in large-scale distributed environment [4, 5]. To assure the cloud data integrity and availability, efficient approaches that enable storage correctness assurance on behalf of cloud users have to be premeditated. Hence, cloud operations should also imperatively support the dynamic features that make the system design even more challenging. As Cloud computing is a new emergent technology despite having many beneficial factors, it faces many threats in various ways. It has spread very fast due to its flexibility over ease of access as it eliminates the need for extra hard drives and memory space allocation.

As the cloud is a distributed system, the data stored in it is widespread in distinct locations, and it is accessed anywhere. The distributed nature of the data creates the requirement for high security over outsourced data as there exists a probability that anyone can exploit the outsourced data. The hackers [1, 2, 16], can also access the outsourced data by hacking any server virtually, and the statistical results. Showed that one-third of the breaches happened from stolen or lost laptops exposing the data unintentionally from the users or the employee of the organization over the Internet. Further, nearly 16 percent of this data exposure is due to the insider theft.

The cloud security providers were even trying to provide a solution to security problems such as security, privacy, reliability, legal issues, open standards, compliance, freedom and long-term viability.

Cloud has three major types of deployment models, which comprises of Public, Private, and Hybrid Cloud. Most-common level people and some organizations make use of the public cloud model in a majority for data storage purposes because it consumes less cost and correspondingly provides utmost security over the outsourced data, but there is also a probability of data leakage in a public cloud environment. The private cloud model [9, 13], depends upon a particular but found to be comparatively costlier than the public cloud. The combination of either private-public or public-public or private-private infrastructure forms the Hybrid cloud environment [12, 15], providing the combined advantage of both the private and the public

[1]Corresponding Author

cloud. The significant benefit of the use of the hybrid cloud involves improvised security with lesser management costs.

The possession of fine-grained data access control and storage correctness verification remains to be a mandatory feature in any system, which shares the data contents among multiple users with different level of trust. To ensure the property of cloud data security, highly trusted cloud users might be allowed with full access rights while the other users were assigned partial access rights over the outsourced data. Efficient management of the fine-grained access provision in a system with users having different access privileges remains to be a challenging issue in cloud computing. Showed that one-third of the breaches happened from stolen or lost laptops exposing the data unintentionally from the users or the employee of the organization over the Internet. Further, nearly 16 percent of this data exposure is due to the insider theft. The cloud security providers were even trying to provide a solution to security problems such as security, privacy, reliability, legal issues, open standards, compliance, freedom and long-term viability.

Cloud three major types of deployment models, which comprises of Public, Private, and Hybrid Cloud. Most-common level people and some organizations make use of the public cloud model in a majority for data storage purposes because it consumes less cost and correspondingly provides utmost security over the outsourced data, but there is also a probability of data leakage in a public cloud environment. The private cloud model [9, 13], depends upon a particular but found to be comparatively costlier than the public cloud. The combination of either private-public or public-public or private-private infrastructure forms the Hybrid cloud environment [12, 15], providing the combined advantage of both the private and the public cloud. The significant benefit of the use of the hybrid cloud involves improvised security with lesser management costs.

The possession of fine-grained data access control and storage correctness verification remains to be a mandatory feature in any system, which shares the data contents among multiple users with different level of trust. To ensure the property of cloud data security, highly trusted cloud users might be allowed with full access rights while the other users were assigned partial access rights over the outsourced data. Efficient management of the fine-grained access provision in a system with users having different access privileges remains to be a challenging issue in cloud computing.

To provide better security features in cloud computing environment, a novel Hierarchical System and Access Stipulation Scheme (HSAS) is given. It comprises of two parts, where the first part designates the access structures to the users and the second presents a storage correctness scheme through the use of the access structure defined at the preliminaries. A combination of public key, private key, and access structures is assigned to all the users of the system that is derived from the appropriate user attributes. Through the distributed keys and access structures, every single user of the system establishes the secure cloud connection and performs accesses to the cloud data. For every successful cloud data upload, the user is provided with a token, which is used to verify and validate the storage correctness associated with the outsourced data thereby improving the storage efficiency.

The paper is organized in the following manner. The section next to introduction details the literature survey, the next part, deals with the summary of limitations followed by preliminary concepts and algorithms, system design, the proposed HSAS scheme, case study, Implementation Details, Results, and Discussion. Conclusion.

II. Related Work

This section describes and analyses other approaches towards facing the challenge of fine-grained access provision to cloud users. Multiple solutions are examined, after which an overview of their works was given. This section also describes the comparison of two major approaches that is related to the fine-grained access provision techniques.

Overview

This section presents an overview of the works, which is related to the proposed HSAS scheme.

Cloud-based Access Control Techniques

This presents a data access control scheme called DAC-MAC for the multi-authority cloud storage system. It provides a multi-authority CP-ABE scheme with efficient data decryption and user revocation functions. This work further offers an Extensive Data Access Control Scheme (EDAC-MACS) that provides secured user data access even at weaker security assumptions. The security analysis results of this scheme prove that this scheme is collision resistance but lacks at the property of fine-grained access provision to the individual users of the system. In work done by [25, 10], integration of cryptographic techniques with RBAC techniques was made, and it uses role keys for data decryption. Further, this work presents a hybrid cloud architecture, where the public cloud contains the basic level details and most sensitive information over the private cloud. This work separates the property of user delegation to active and passive types and establishes effective role management through the use of delegation servers and protocols. The Ciphertext-Policy Attribute-Based Encryption was given by; it realizes the complex access control mechanisms over the encrypted data [23, 14]. Here the attributes expressed the user credentials solitarily and the person who encrypts the data could x the access limit to the users for data decryption. Through the use of this scheme, the data stored could be kept confidential even

though it resides on the untrusted server. The ID-based cryptographic scheme [8], makes use of the user attributes such as user id for encryption and decryption process of the outsourced data. The development of ID-based cryptographic scheme provides the secured data storage over the public cloud and improved client authorization for other users to access the data content.

Hierarchical Based Access Control Schemes

In HASBE [17, 21], the user access rights were provided by the hierarchical access structure framed for each user of the system. This scheme ensures the property of scalability through the extension of ASBE (Attribute-Set Based Encryption) technique [6]. It defines a hierarchical structure that delegates the operation of trusted authority and private key generation to the domain authorities of the lower level. Here the user attributes were converted into the stable structure of the recursive type that permits the users to define constraints dynamically by representing a different combination of attributes, which satisfies the user access policy. That ensures the property of flexibility and fine-grained access control over HASBE systems. The concept of Hierarchical Based Access Structure is extended to form the Hierarchical Structure used in this paper.

Token-Based Access Verification Systems

Here they proposed distributed storage integrity auditing mechanism that consists of tokens and erasure-coded data. Tokens are provided to the users from randomly chosen block indices from each data vector space analogous to the memory location of the user requested le in the cloud. The use of erasure coded data technique protects the user data and eliminates the system errors such as data redundancy, fault tolerance, and server crashes. In Privacy-Preserving Public Auditing for Secure Cloud Storage by [18, 11] comprises a third-party auditor (TPA) for auditing the integrity of outsourced data; this eradicates the new threats and realizes the data privacy. This scheme uses random masking technique integrated with a homomorphic authenticator that ensures the privacy of public auditing. Flexible distributed storage integrity checking mechanism is proposed by [3] using homomorphic tokens, and it avoids security problems like identifying unknown users. Through the use of homomorphic tokens and distributed erasure coded data, users were permitted to audit the outsourced data. This auditing allows the users to identify both the improper data access and cloud server misbehaviors. This scheme even ensures the cloud data security, which allows the users to perform dynamic operations efficiently over the outsourced data. Experimental analysis of their proposed scheme proves that it provides high efficiency against Byzantine failure, unknown user attacks and attacks on cloud data modification. Access control schemes based on the token system were developed to provide greater security over the cloud storage systems.

Comparison of Related Works

This section presents a summary about two major approaches relating to the proposed HSAS scheme. The HASBE scheme given by [17], and the flexible integrity auditing mechanism provided by Wang Cong et al., were taken into comparison, and it is described as follows:

To ensure the property of scalability and flexibility over outsourced data, a solution is presented in work done by [17]. This work shows a Hierarchical Attribute-Set-Based Encryption (HASBE) scheme to cloud users, which extends the property of Cipher-text attribute-set-based encryption technique. This scheme not only aims in the achievement of scalability, it even inherits the property of flexibility and fine-grained access provision through the management of compound attributes. The HASBE scheme makes use of multiple value access expiration time to deal with user revocation problems. The first part of this work describes the extension of HASBE from ASBE technique using the hierarchical structure. Whereas the second part provides a clear demonstration of the implementation of access control scheme based on HASBE for cloud computing.

The cloud computing system considered in this work consists of major entities. The cloud service provider provides services to users. The data owners share their data contents through the cloud in an encrypted manner. Data consumers decrypt the shared contents to perform their respective access operations. Each data owner and data consumer was assigned with a domain authority, where each domain authorities could be managed through parent domain authorities or trusted domain authorities. The major responsibility of every domain authority is to administer the domain authorities at next level or the data owner or consumer in its domain. In HASBE scheme the data users were only assumed to possess read access. All the entities associated with this scheme were organized hierarchically to accomplish their tasks.

A recursive set based key structure is formed for every user, where each element of the set is either a set or an element corresponding to a user attribute. The depth of the key structure is found using the level of recursions in the recursive set, which is similar to the definition of depth tree. For a key structure of depth 2, members of the set can either be sets or attribute elements at depth1. At depth two it is mandatory that all the members of the set should be of attribute elements. A unique label for the user attributes was formed using key structure. The access structure to the users in HASBE was formed in a similar way to the ASBE scheme given by [3]. In access tree structures, the leaf nodes were considered to be the attributes, and non-leaf nodes represent the threshold gates. The non-leaf nodes were defined using its children and threshold values.

This work provides user access provision with the help of the hierarchical access structure, and it is formed using

appropriate user key structure and access structures. It means that the user with private key corresponding to attributes in key structure would be able to access the data, only when their attributes satisfies the access policies defined by the access structure. System Setup, Top-Level Domain Authority Grant, New Domain Authority/User Grant, New File Creation associated with integrity auditing scheme to be a probabilistic feature. The proposed HSAS scheme solves this issue by granting tokens to the users in a deterministic manner. In HSAS scheme tokens were derived from Metadata containing le locations and distributed to all the users of the system during appropriate phases. Here the major advantage is that as a result of the write operation done by the authorized system an updated token would be provided to all the users of the system, through which the property of storage correctness is achieved. The Cloud Service Provider (CSP) provides services to the users of the system and performs the validation of the user given inputs and outputs during the process of encryption and decryption. Service Consumers (Users): A Service consumer is also called as the user of the system, consumes the services provided by the cloud computing environment. Data Owner: Shares valid data contents over cloud computing environment and data access limits across data users.

III. Construction of Storage Correctness and fine-grained access Provision Technique

System Design

This section presents a conceptual design of the novel scheme called Storage Correctness and fine-grained Access Provision (HSAS) scheme, which was described in Figure 1. The proposed HSAS scheme consists of two parts. The first part deals with the construction of hierarchical based user access structures and the second part depicts the algorithmic phases associated with SC-FAP scheme that helps in the achievement of fine-grained data access and improved storage efficiency across the out-sourced cloud data storage. A set of appropriate cryptographic keys and access structures derived from the exact user attributes were distributed to all the users of the system. Through the use of the access structures and cryptographic keys, every user of the system performs the cloud data access securely. As a result of the encryption process, both the data owners and users were provided with a token, which assists in the process of integrity and security verification over the outsourced data.

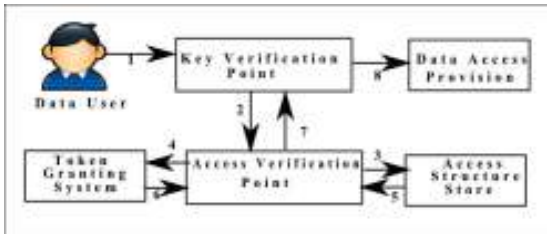

Figure 1: System design of HSAS

The proposed system consists of major entities and the description to the entities was given as follows, Attribute Authority (AA): The major responsibility of the Attribute Authority (AA) is to manage all the attribute related activities in specialization with the activities to the management of user roles. This includes maintenance of role revocation, delegation, key allocation to users and authentication of the user given credentials like the public key, private key, etc. Cloud server (CS): Cloud server performs all the computation related activities. This includes the computation of user given inputs and producing corresponding computational results and acknowledgments to the users. Cloud Service Provider (CSP): The Cloud Service Provider (CSP) provides services to the users of the system and performs the validation of the user given inputs and outputs during the process of encryption and decryption. Service Consumers (Users): A Service consumer is also called as the user of the system, consumes the services provided by the cloud computing environment. Data Owner: Shares valid data contents over cloud computing environment and fixes data access limits across data users.

Cloud server performs all the computation related activities. This includes the computation of user given inputs and producing corresponding computational results and acknowledgments to the users. Cloud Service Provider (CSP): The Cloud Service Provider (CSP) provides services to the users of the system and performs the validation of the user given inputs and outputs during the process of encryption and decryption. Service Consumers (Users): A Service consumer is also called as the user of the system, consumes the services provided by the cloud computing environment. Data Owner: Shares valid data contents over cloud computing environment and data access limits across data users.

Assumptions

This work assumes an existing data access control model to build upon, and the proposed design makes use of the access control properties defined previously at related works. The hierarchical structure described in this paper is assumed to provide many-to-many data sharing in a secure manner through which the property of fine-grained access control, confidentiality, and non-repudiation of the outsourced data is achieved.

Key Terminologies

Access Assignment Structure

A summary on Access assignment structure is depicted in Figure 2.

Hierarchical Structure

The hierarchical structure defines the access policy associated with the individual users of the system. A hierarchy is framed from the combination of the user unique and common attributes. Each hierarchy represents the one to one relationship between the user and their access policies. The access policy defines the set of operations (read or write access) the user could perform over the outsourced data.

.Key Structure

Key structures were designed to preserve the security of the outsourced data. Key structures are derivatives from the common user attributes like roles. The formation of key structure assigns the access privileges to the set of the common users over the outsourced data. This states that users beneath a particular role were assigned with a key structure such that they could gain access to a particular set of less.

Access Structure

Access structures were designed to achieve the property of fine-grained user access, and it is derived from the user unique attributes like user id. It defines the extent to which an individual user could access the data.

Formation of Hierarchical Access Structure

The proposed HSAS scheme makes use of the hierarchical access structure to define the user access rights. The basic concept behind the hierarchical access structure was described in the previous section of the paper. In HSAS scheme each user is assigned with a hierarchical structure, which is derived from their respective key and access structures.

Key structure is premeditated to preserve the security of the outsourced data and it represents the access rights to the group of users with a common identity. The basic concepts behind the formation of the key structure were given in the previous section. It is formed using the common user attributes like dep id. In an organization the most important or most secured less could be accessed only by the personals at the top-most designation order, least important les by the low-level personals and ordinary les could be accessed by the mid-level individuals. In correspondence to the user designation order grades for a group of members with common identity (users under a particular role) is calculated from \grade1.grade n". For every user with a role, grades were allocated concerning their access privilege that defines the level of extent to which the users could access the data.

Access Structure

The access structure represents the access rights to the individual user of the system. Even though a particular user is assigned with a grade representing the key structure, it is not mandatory that the user could access all the lies that come under a particular grade. The access structures associated with the HSAS scheme were designed in such a way that solves the problem of issue mentioned above. The access structure was framed from the user barrier limits, which are derived from the user unique attributes like user id. Barriers are restrictions that were imposed over the user access grades to achieve the fine-grained access control. The assignment of the access structure defines the individual access limits over the set of les. In addition to this, phase 3 of the storage correctness scheme provides a summary about the algorithmic implementation of the user access structure assignment.

Through the use of the key and access structure discussed above, a hierarchical access structure is formed in the proposed HSAS scheme, and it is illustrated in Figure 2.

Token provision

As it is described at the previous section tokens were derived from the Metadata containing the le location that assist in both ways, through which the process of storage correctness, as well as the easier retrieval of the outsourced les, could be made. Correctness is achieved. As it is described at the previous section tokens were derived from the Meta data containing the le location that assist in both ways, through which the process of storage correctness as well as the easier retrieval of the outsourced less could be made.

The prime idea behind the use of Token Provision in HSAS scheme is that at the end of every successful data encryption process the data users were provided with the tokens, through which the data users verifies the existence of the outsourced data. The users could also be able to perform the decryption process only when the Metadata of the user given token points to the user requested le.

HSAS Phases

The storage correctness phases and fine-grained access provision scheme consists of nine phases through which the property of fine-grained access provision and storage correctness verification is achieved. The HSAS phases apply the concept of hierarchical access structure and to-ken granting system described in preliminaries part.

Phase 1: SetUp()

It takes the user security parameter as an input and generates master key mk as an output. This step is done by the cloud server through automatically invoking the KeyGen algorithm.

$$K : m_k \lambda \otimes K_n \qquad Eq\,No(1)$$

Eq No 1 joins the user security parameter with the unique key generated by KeyGen() algorithm and dis-tributes the master key to the corresponding users of the system.

Phase 2: GradeGen(mk; Rid)

This phase is performed by the Attribute Authority and it takes the master key mk and Role id Rid as an input, produces public key pk and grade g as an output. Public key is derived from the master key mk by manually invoking the KeyGen() algorithm. Let us consider two sets, R= fR1; R2; R3; ; Rng and G = fg1; g2; g3; ; gng be the set of roles and grades. Such that R G (means that the role R is isomorphic to grade G).

$$Z : \forall R_{id} \in R_{id} \subseteq R \qquad Eq\,No(2)$$

Any R_{id} that belongs to R is the subset of R.

$$Z : \forall R_{id} : P(R_{id}) R_{id} < \bullet R \; Eq\,No(3)$$

At least for one value of Rid the value of Rid in R is true. Such that Rid is covered by r where r 2 R.

$$\therefore Z : \exists R_{id} \rightarrow r \,|\, r \Leftrightarrow G \qquad Eq\,No(4)$$

Through the use of the barrier limits in user hierarchical access structure helps in the achievement of fine-grained access rights to the users of the system.

The algorithmic deployment of the Token Provision helps in the achievement of the storage correctness verification of the outsourced data with improved storage efficiency.

TABLE I. Summary of HSAS phases

Phase No	Phase Name	Input	Output	Done by
1	SetUP()		Mk	CS
2	GradeGen()	Mk; Rid	Pk; G	AA
3	BarrierGen()	Uid; Rk; Pk	B; Prk	RA
4	Encrypt()	F; Rk; Pk	Ct	CSP
5	TokGen)	F; Rk; Pk	Ti	CS,CSP
6	TokenComp()	F; Ti	Ct	CS,CSP
7	TokenUpdate()	Ti	newTi	CS,CSP
8	TokenCorrectness()	Ti; Ct	FileValidity	CS,CSP
9	Decrypt()	Ti; Ct; Rk; B; Prk	Plaintext	CSP

Advantages of Proposed HSAS Scheme

Through the use of the barrier limits in user hierarchical access structure helps in the achievement of fine-grained access rights to the users of the system.

The algorithmic deployment of the Token Provision helps in the achievement of the storage correctness verification of the outsourced data with improved storage efficiency.

The tokens were derived from the Metadata containing the le location. This reduces the le retrieval time associated with the user data access request.

IV.Results and Discussions

The major objective of the experimental implementation is to validate the level of an extent to which the proposed HSAS scheme provides the property of fine-grained data access to the cloud users. To validate this objective prototypes using traditional access control, techniques like ABE and RBAC were implemented, and it is compared with the proposed HSAS scheme. From the results of the implementation, a comparison is made regarding both system performance and fine-grained access provision, which is described in Figure 7 and 8. First, a comparison is made between the amount of data to be retrieved and le retrieval time to find the system performance. At client side, n numbers of client nodes were created, and a large number of less from different client node was uploaded to the cloud storage. Client le access requests were given from various nodes and the number of client requests per minute was calculated regarding size of the data les accompanying the client requests and it is kept as X limits. The time taken by the cloud server to respond to user le access requests was calculated in seconds, and this forms the Y limits. It has been observed that the time taken for le retrieval on the size of the data le for our HSAS scheme remains constant up to a particular threshold.

Even though there is a tremendous increase in le size that happens after a particular threshold, the time taken for le retrieval increases in a consistent manner. But the observation of traditional access control schemes like ABE and RBAC deviates highly and takes more time for le retrieval after a particular threshold. This is due to the inconsistent nature of their underlying access policies. The comparison between HSAS with traditional ABE and RBAC techniques regarding le retrieval time proves that the proposed HSAS scheme takes reduced le retrieval time than the existing schemes. This is due to the use of the token provisions. Since the tokens were derived from the Metadata containing the le location, the time taken for le retrieval and storage correct-ness verification has been comparatively improved. The overall simulation results depict that the le retrieval has been reduced by 0.5 seconds in comparative to the existing access control techniques. This improves the overall performance measure of the system.

A measure to the level of fine-graininess associated with the HSAS scheme in comparison to the traditional access control methods like ABE and RBAC were made, which is depicted in Figure 2.

The level of fine-grained access control is measured by the extent to which the appropriate access rights were provided to the users of the system. User access policies based upon HSAS, ABE and RBAC models were de-signed for each client nodes associated with the system.

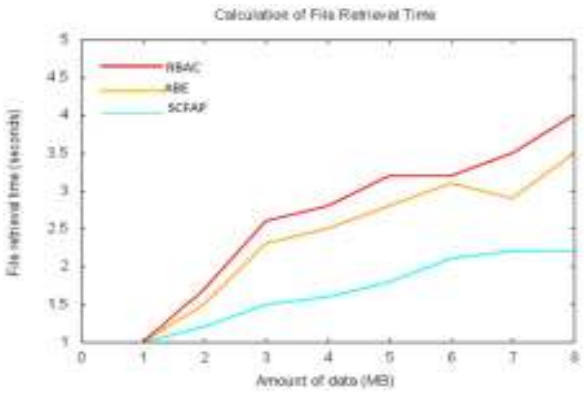

Figure 2: Comparison to fine-grained access provision measure in ABE and RBAC

Through the implementation of HSAS scheme over the eucalyptus-cloud and the use of a vast number of the client nodes, a hierarchy is formed for every user accompanying the client node. A comparative measure of fine-grained access level has been made in association with the depth of access structure. The depth of the access structures was kept in X limits and fine-grained access level in percentage were fixed at Y limits. It has been found that our proposed HSAS scheme provides better fine-grained access level to the data users even at lesser access structure depth. The other access control techniques taken into comparison were found to be lagging inefficiency at the lower level of access structure depth. Achieved through the derivation of appropriate hierarchical structures associated with HSAS scheme, which provides better access provision even at the lower access structure depth. The existing technique lags at fine-grained access provided through the complex access structure formation. The tests were conducted using banking research dataset of the Federal Bank of New York.

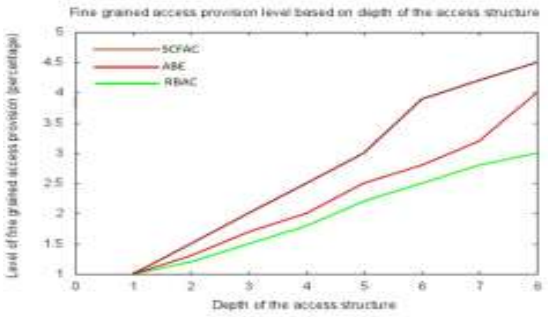

Figure 3: Comparison to fine-grained access provision measure in HSAS scheme

V.Conclusion

The paper defines an HSAS scheme that solves the problem of fine-grained access provision and storage correctness associated with the existing access control techniques. The first part of the HSAS scheme involves the formation of hierarchical structures that fixes the appropriate access policies to the users; this improves the fine-grained less associated with the access policy. The next part deals with the achievement of storage correctness related to the les, and it is made through the usage of the token provider. In addition to this, the use of Token Provision improves the storage efficiency, security, and performance of the proposed system. As this paper explains only on the key structure and Access Structure associated with the plain text but not about the Cipher Text Access Structure.

References

[1] M. H. Au and A. Kapadia, “PERM: Practical reputation-based blacklisting without TTPS,” in Proc. ACM Conf. Comput. Commun.Secure. (CCS), Raleigh, NC, USA, Oct. 2012, pp. 929–940.

[2] M. H. Au, A. Kapadia, and W. Susilo, “BLACR: TTP-free blacklistable anonymous credentials with reputation,” in Proc. 19th NDSS, 2012,1–17.

[3] M. H. Au, W. Susilo, and Y. Mu, “Constant-size dynamic k-TAA,” in Proc. 5th Int. Conf. SCN, 2006, pp. 111–125.

[4] J. Baek, Q. H. Vu, J. K. Liu, X. Huang, and Y. Xiang, “A secure cloud computing based framework for big data information management of smart grid,” IEEE Trans. Cloud Comput., vol. 3, no. 2, pp. 233–244, Apr./Jun. 2015.

[5] M. Bellare and O. Goldreich, “On defining proofs of knowledge,” in Proc. 12th Annu. Int. CRYPTO, 1992, pp. 390–420.

[6] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in Proc. IEEE Symp. Secure. Privacy, May 2007, 321–334.

[7] D. Boneh, X. Boyen, and H. Shacham, “Short group signatures,” in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2004, 41–55.

[8] D. Boneh, X. Ding, and G. Tsudik, “Fifine-grained control of security capabilities,” ACM Trans. Internet Technol., vol. 4, no. 1, pp. 60–82, 2004.

[9] J. Camenisch, “Group signature schemes and payment systems based on the discrete logarithm problem,” Ph.D. dissertation, ETH Zurich, Zürich, Switzerland, 1998.

[10] J. Camenisch, M. Dubovitskaya, and G. Neven, “Oblivious transfer with access control,” in Proc. 16th ACM Conf. Comput. Commun.Secure. (CCS), Chicago, IL, USA, Nov. 2009, pp. 131–140.

[11] J. Camenisch and A. Lysyanskaya, “A signature scheme with efficient protocols,” in Proc. 3rd Int.

Conf. Secure. Commun. Netw. (SCN), Amalfi, Italy, Sep. 2002, pp. 268–289.

[12] J. Camenisch and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2004, pp. 56–72.

[13] Y. Chen, Z. L. Jiang, S. M. Yiu, J. K. Liu, M. H. Au, and X. Wang, "Fully secure ciphertext-policy attribute-based encryption with security mediator," in Proc. ICICS, 2014, pp. 274–289.

[14] S. S. M. Chow, C. Boyd, and J. M. G. Nieto, "Security-mediated certificate less cryptography," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 3958. Berlin, Germany: Springer-Verlag, 2006, pp. 508–524.

[15] C.-K. Chu, W.-T. Zhu, J. Han, J.-K. Liu, J. Xu, and J. Zhou, "Security concerns in popular cloud storage services," IEEE Pervasive Comput., vol. 12, no. 4, pp. 50–57, Oct./Dec. 2013.

[16] R. Cramer, I. Damgård, and P. D. MacKenzie, "Efficient zero-knowledge proofs of knowledge without intractability assumptions," in PublicKey Cryptography (Lecture Notes in Computer Science), vol. 1751,H. Imai and Y. Zheng, Eds. Berlin, Germany: Springer-Verlag, 2000, pp. 354–373.

[17] Y. Dodis, J. Katz, S. Xu, and M. Yung, "Key-insulated public key cryptosystems," in Proc. EUROCRYPT, 2002, pp. 65–82.

[18] Y. Dodis and A. Yampolskiy, "A verifiable random function with short proofs and keys," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 3386, S. Vaudenay, Ed. Berlin, Germany: Springer-Verlag, 2005, pp. 416–431.

[19] M. K. Franklin, in Proc. 24th Annu. Int. Cryptol. Conf., Santa Barbara, CA, USA, Aug. 2004.

[20] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fifine-grained access control of encrypted data," in Proc. 13thACM Conf. Comput. Commun. Secur., 2006, pp. 89–98.\

[21] J. Han, W. Susilo, Y. Mu, and J. Yan, "Privacy-preserving decentralized key-policy attribute-based encryption," IEEE Trans. Parallel Distrib.Syst., vol. 23, no. 11, pp. 2150–2162, Nov. 2012.

[22] X. Huang et al., "Cost-effective authentic and anonymous data sharing with forward security," IEEE Trans. Comput., vol. 64, no. 4, pp. 971–983, Apr. 2015.

[23] J. Hur, "Attribute-based secure data sharing with hidden policies in smart grid," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 11, pp. 2171–2180, Nov. 2013.

[24] J. Hur, "Improving security and efficiency in attribute-based data sharing," IEEE Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2271–2282, Oct. 2013.