A Comprehensive Cloud Security Model with Enhanced Key Management, Access Control and Data Anonymization Features

G.Venifa Mini [1], K. S. Angel Viji [2]

[1]Department of Computer Science and Engineering, Noorul Islam University, Kumaracoil, India.
[2]Department of Computer Science and Engineering, College of Engineering, Kidangoor, India.

Abstract**:** A disgusting problem in public cloud is to securely share data based on fine grained access control policies and unauthorized key management. Existing approaches to encrypt policies and data with different keys based on public key cryptosystem are Attribute Based Encryption and proxy re-encryption. The weakness behind approaches is: It cannot efficiently handle policy changes and also problem in user revocation and attribute identification. Even though it is so popular, when employed in cloud it generate high computational and storage cost. More importantly, image encryption is some out complex in case of public key cryptosystem. On the publication of sensitive dataset, it does not preserve privacy of an individual. A direct application of a symmetric key cryptosystem, where users are served based on the policies they satisfy and unique keys are generated by Data Owner (DO). Based on this idea, we formalize a new key management scheme, called Symmetric Chaos Based key Management (SCBKM), and then give a secure construction of a SCBKM scheme. The idea is to give some secrets to Key Manager (KM) based on the identity attributes they have and later allow them to derive actual symmetric keys based on their secrets. Using our SCBKM construct, we propose an efficient approach for fine-grained encryption-based access control for data stored in untrusted cloud storage.

Keywords**:** Key Management, Access Control, Anonymization, policy, cloud**.**

1. Introduction

Cloud computing is rapidly evolving as a 21st century computing paradigm cutting across physical boundaries and resource limitations [1]. It became a vital part of day to day business operations [2]. Cloud computing is offering access to computing facilities such as storage and processing capabilities to its users at predominately lower cost [3]. Software as a service, Platform as a service and Infrastructure as a service are some of the services offered by cloud computing. Cloud computing dynamically supplies on demand basis computing resources to users [4]. Remote storage is one of the widely availed cloud service, in which user will be able to store their data in remote cloud servers maintained by cloud service providers [5]. Unlike local storage server remote servers are mainly located at various countries where cost of installation and maintenance is very low [6]. This offers the cloud users a cost based advantage freeing them from any capital expenditure and maintenance costs [6].

The cloud services are provided by third party service providers who are independent of geographical locations. However these service providers are often non-trustable and unaccountable since they are independent of geographical locations. This gives rise to serious security, privacy and trust issues in the cloud computing environment [7]. Although cloud services proved to be economically benefit, large number of users are not willing to avail cloud services mainly due to security and privacy concerns [8]. Cloud services encounter serious security threats and vulnerabilities due to lack of adequate safety mechanisms [9]. Security problems in cloud can be attributed as data breaching, data loss, traffic hijacking, insecure application programme interfaces, denial of service, malicious insiders, data abuse and shared technology based issues [10].

Storage as a service application in cloud make the user, data owner to share his data to other users through pay-per-use service. The user may be an individual or an enterprise. They are attracted by unpredictable storage with long-term archive. Moreover, this will greatly reduce the maintenance cost. But a problem occurs due to the unauthorized accessibility of sensitive data. That is data security, existing in other applications. Data security is closely embedded with data confidentiality. Protecting the confidentiality of data from cloud server is not an option, but a requirement for service oriented environment like healthcare application. Healthcare application works under the principle of Health Information Portability and Accountability Act (HIPAA). Furthermore, the data users are content providers. They publish data to cloud server for sharing it with fine grained access control. Content providers generate access structure and permission for which data accessed by which user. For example, Electronic Medical Record (EMR) stores millions of sensitive information in the cloud. It allows data consumers such as doctors, patients, researchers to access various types of healthcare records under policies admitted by HIPAA. The cloud servers are present outside the trusted boundary of user. Data owner has to solve this problem. To enforce access policies, Data owner has to create proper access control policies to allow authorized users to access the data. On the other hand, the originality of data can be hidden from cloud server.

Role Based Access Control (RBAC) provides a better security solution for accessing data on the cloud. Further, the confidentiality of the data should be preserved by encrypting the data before uploading to the cloud [11]. In the existing Attribute based Encryption Methods[12] [13], attributes play a main role to generate public key for encrypting data and create access policies to monitor user's access. The access policy can be categorized into Key Policy (KP-ABE) and Cipher text Policy Attribute Based Encryption (CP-ABE) [14] was presented in the literature for understanding

complex access control on encrypted data. Conventional cryptographic methods can be adopted for the encryption process. Due to the computational and storage complexity, existing methods are inefficient for cloud. Hybrid RBAC and Chaos Access (HRCA) control mechanism is a key management access control works on the basis of role hierarchy. The proposed approach enhanced confidentiality of encrypted data by hiding access permissions and privileges of roles from key manager. In our approach user credentials are considered as key and a party encrypting data determines access structure. Based on the access structure, CSP transmit data to receiver.Some of the basic concerns around cloud security are restricting cloud server from learning data stored in it, providing the data owner complete control over their data, allowing only the intended users to access data, avoiding any attacks during data transmission from cloud to user or owner to cloud, ensuring proper access control during data publication and ensuring trust during data sharing [15-17]. This work aims at providing a comprehensive fool proof protocol for providing data security, key management, optimized access control and data privacy.

2. Related Work

Varadharajan et al detailed the vulnerabilities and challenges in cloud computing environment. Security challenges are hindering the growth of cloud computing sector. A flexible security model which can be offered as an additional service to the cloud users was proposed. This service can be extended to the users to safeguard them from basic attacks such as denial of service attacks, insider attacks originating from cloud server and insider attack originating from user end. This scheme provides for providing security as a service that too for some basic kind of attacks [18]. Major security and privacy problems such as cloud learning, uncontrolled access were untouched in this architecture.Data sharing is a great convenience provided by cloud [19] [20]. Cloud is a static repository of combining data and resources. Data users are the active participants. Data is not only shared to an individual but it is shared to others, which bring greater benefits to the society [21].To empower privacy of sensitive information, the collected information should be encrypted before transmission. Noticeably an encryption algorithm must be simple and efficient for time sensitive health care applications. Key generation is the main part in an encryption algorithm. Among conventional methods, Chaos based encryption depends on the sensitivity of their parameters and initial conditions [22]. The experimental analysis shows that chaos based encryption has good cryptography strength and high reliability. Also it is simple to implement. The strength of chaos lies in its symmetric key series. Even though the encryption key is derived by malicious user, he may not generate the original message. Conventional DES, Triple-DES and IDES are not suitable for image encryption due to its abundant storage characteristics of images.

Access control in cloud computing is employed to provide data access to the eligible users. An efficient access control mechanism allows the user to access the data assigned to his/her role. It should also control unauthorized users from accessing data. Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC) are the common types of access control techniques in use. Khan proposed a flexible Attribute based access control mechanism to meet the complex requirements involved in implementing access control to large set of data. This scheme involves encapsulating each data set with attributes with reference to permissions. The permission attribute looks after implementing a role based access control by validating the data user's requirement attribute with the attribute of specific data stored in the server. It is a hierarchical based scheme lacking security [23]. Thus a low hierarchical user may able to access the data assigned for a higher level user by breaking the access mechanism. Also emergency time data access is not provided which is one of the key requirements to achieve flexibility.

Ferraiolo et. al. [24] understood the importance of standardization of Role based access control technique. RBAC is widely used due to its applicability, efficiency and user management provisions. Sessions are important section in the RBAC architecture; each session represents a entirely different set of user permissions. Session can be efficiently used to revoke or grant user permissions dynamically based on need basis. It is suggested to incorporate the session's module separately along with RBAC. Single role activation is presently used in RBAC which can be scaled to a group of users for efficient permission management. Apart from this role relationship management by updating the inheritance framework also detailed in this work. However these suggestive measures does not provide for greater flexibility to meet the cloud requirements.

Consequently, how to securely and efficiently share user data is one of the hardest challenges in the scenario of cloud computing [25]. An efficient encryption technology described in [26] tackles the challenge of secure data sharing. The secret key of user is represented by an attribute set and cipher text is associated with defined access structure by data owner. User can decrypt the received cipher text, if and only if the attribute set matches the access structure. Implementing CP-ABE directly in cloud create some open problems. Fully trusted Key Authority (KA) has the responsibility to issue secret key. This may lead to a security risk known as key escrow problem.Bo Lang et al discussed about the problems in cloud computing with focus on access control and data security. As laid out by Cloud Security Alliance, enhanced data protection is achievable only with encrypted form of data handling. Although existing data security techniques provides for better data protection they do not provide for efficient access control. When RBAC is used alone data access permissions are assigned through roles results in lack of fine-grainedness. Likewise when CP-ABE is used alone it results key breach issues and cloud learning of data and user behaviors. In order to solve this problem a self-contained data security model was proposed by Lang et al. They have utilized the merits of Role Based Access Control (RBAC) and Cipher Text Based Attribute Based encryption (CP-ABE). By combining these two techniques a better access control is achieved along with data security. Although this scheme able to achieve remarkable efficiency in terms of protection and access management, the futility of the methods lies in the requirement of heavy computational loads. Also the computational burden for encryption and decryption needs to be fulfilled by the owner and user rather than the cloud server.

Yu et al [27] provides for a comprehensive access control mechanism that achieves scalability, fine-grainedness and

confidentiality of data access over cloud environment. In this module individual data user specific exclusive access framework was employed at the same time preventing the cloud servers from obtaining data content or access privilege related information. Initially each data is encrypted with Key Policy Attribute-Based Encryption (KP-ABE) in which each data set is encrypted with attributes and their corresponding public key module. On the other hand, each data user will be having a tree alike access structure defined with the data attributes. The user must be complying with the access structure in order to successfully decode the message. Although KP-ABE achieves fine grained data access it has heavy computational burden underlying that paves way to combine two other cryptographic techniques such as Proxy Re-Encryption (P-RE) and Lazy Re-Encryption (L-RE).

A bidirectional verification based security scheme was proposed by Bin et al, in which a two way authentication will be done to ensure better data security. At the first level a Third Party Auditor will verify the credentials and permissions of data user. The verification will be followed by returning a logic based output to cloud service provider. The cloud service provider can verify the third part auditor in required cases, apart from the logic based output received from third party auditors; the CSPs can authenticate the users directly. Further in this scheme data files are split into number of blogs where each blog will have a signature tag which will be shared with the CSP by the data owner. The CSP will verify the signature tag for each block of data received from cloud users to verify whether data block was tampered.

However this scheme draws large computational overhead especially for larger data files. These computational requirements are peak during the verification stage and may not be needed for the data owner's normal requirement. This additional peak overload issue causes instability in the performance of cloud server [28].A cloud computing adoption framework was developed by Chang et al aimed at providing data security. In the multilayered security protocol, intrusion protection is achieved with a firewall setup at the first layer. An identity management layer with three sub groups namely users, servers, and security manager. The third layer is a convergent encryption layer in which all the data will undergo a validation test. If any attack is detected or if any data is tampered with an isolation module will separate them from other modules [29], [30],[31]. This scheme provides for a comprehensive security to data stored in cloud; however transmission time security breaching were not included in the frame work. This protocol needs complex architectural setup for all the entities involved in cloud such as user, data owner, key manager and server.

A feedback based dynamic security model was proposed by Chen et al. According to this scheme the security arrangements and feedback were grouped as physical security, network security, host security, application security and data security. Each layer will have separate provision for monitoring threats. This threat monitoring module analyses any risky objects and determines the overall weakness of the particular segment. The feedback is given to a protection enforcement module which will enforce necessary requirements in order to overcome the weakness [32]. The major drawback in this scheme is lies in its design which is purely abstract without any technological detail. A number of works related to access control has been surveyed and found that access control in cloud is an important requirement for scaling the cloud services to a higher level with greater security, privacy protection and confidentiality. Improving confidentiality along with flexibility is the key recruitment of access control in current scenario. Securing the data along with user role related data such as user behaviour attributes also phenomenon for the cloud. A number of potential vulnerabilities were found in the current literature of cloud access control. These gaps can be overcome by providing greater flexibility and confidentiality simultaneously achieving simplicity of design and lower computation overhead

3. Proposed Architecture

The proposed architecture for cloud computing encompassing the features of data security with chaos based encryption, flexible access control with hybrid RBAC and Chaos encryption and data Anonymization are detailed in this section.

The illustrative figure of the proposed cloud computing architecture is provided in figure 1. This architecture consists of five main segments namely the data owner (DO), Cloud Service provider (CSP), Key Management module (KM), Data user (DU) and Transmission Space (TS). The data owner is the ultimate owner of the data who may avail cloud services from a CSP for the purpose of storage or data processing or allowing publication to the data users of his choice. The data owner's data may be his private data and DO shall allow data access to only trusted users. The data owner's main concern with respect to his data stored on CSP is security and privacy concerns. He may need to protect his data from malicious attacks originating from unknown sources. At the same time, the CSP is a third party service provider to the DO; hence CSP may not be trustable to the DO. So DO needs to protect his data from the cloud server where it was stored. Otherwise his data may illegally accessed by CSP for another activities.

The DO prior to sending his data to the cloud server belongs to CSP, needs to encrypt his data. In this architecture a chaos based key generation is implemented as an attempt to provide greater security against any attacks. Normally encrypted data are subject to a number of attacks, in which attackers either obtain the key series or decipher data directly.

In the chaos based encryption, the data owner uses a sharable identity element (ID) to generate the key serials. The ID used to generate the key serials are not known to the CSP. In chaos based encryption, the ID is taken as the initial value and key series are generated based on Logistics mapping or Henon mapping approach. Logistics mapping generated a one-dimensional series of keys that meant for text encryption. Henon mapping generates two dimensional key serials that can be used to encrypt multimedia data such as images and videos. Since the key series generated using the chaos theory are highly random they are highly resistive to any type of attacks. These keys are used to encrypt data with simple XOR operation.

After encrypting the data with key serials generated by chaos theory, the data is transmitted to the cloud server through the transmission space assumed as unsecured channel and stored in the cloud servers. It is important to note that since the data is already encrypted, it is free from any type of attacks and

securely reaches the server. At the server the DO's data in the encrypted form is stored. Apart from sending the data, the DO also sends a list of user roles and their respective access structure. The access structure will contain the hierarchical base on which the data shall be shared with the data user with respect to his/her role. Each data user will be broadly classified as registered user and unregistered user. Within the registered user category a number of sub categories of roles are defined with each role having a specific access structure. On the other hand the unregistered or public cloud users will be treated as per the access structure assigned to them. Along with access structure the public users will be not allowed to view the entire data. Each data is masked prior to sending to the unregistered users.

The cloud servers will store the data in encrypted form, execute the role based access policy based on access structure, implements data masking, encrypts data prior to sending to the data users. Apart from these operations the cloud server also runs a trust module. The trust module in cloud server is responsible for dynamic learning and classification of users into trustable and non-trustable category. Initially each user either it be registered user or unregistered user allowed to access data based on their assigned access structure. When a user tries to access the data breaking his/her predefined access structure, the dynamic trust manager activates and started logging the user behavior. When a user exceeds the threshold set for breaking his access structure, he/she classified as un-trustable and lowers his access privileges. The learning and classification is done with the help of a neural network based Bayesian classifier algorithm. The trust manager not only regulates and monitors users for trust enforcement. But it also plays an important role in implementing greater flexibility during an emergency scenario. If a data user wants to access the data belongs to data owner in an emergency scenario, then the trust authenticates the user with third party authorities or with law enforcement agency based trusted authorities. Once authenticated the particular user is allowed to access the data with a break the glass provision on the emergency situation.

On the other hand, the data owner can also define emergency access policies by registering it as a role. In this case the data owner will have a separate key stored in the key management module which is normally attributed to the physiological parameters of the data owner say ECG pattern or thump impression. If a health care provider wants to access the data owner's private health recorder in an emergency situation, he may use the data owner's physiological data to authenticate with the key manager and access the data with break the glass provision. This provision adds greater flexibility to the access control in an emergency situation.

The key management module is again run on separate cloud infrastructure which is different from that of the cloud server used to store data. For greater efficiency the data owner may run his own key management module if requires, since the computational resources needs to run a key management module proposed here is very minimal. The KM acts as key sharing module between data owner and data user. The DO's ID used to generate keys was shared with data user. It is important to note that by implementing a separate key management module, the CSP will not have knowledge about the keys. When a user wants to access data he authenticates with the key manager after successful authentication. The key manager shares the DO's id with the data user. In case of registered user the KM will obtain the customized private id of the data user from DU. After obtaining DO's key id, the user will contact the cloud server and authenticates once again with his ID. The cloud server will authenticate the user with the ID it received from the KM dynamically. Once authenticated the user is allowed to access data assigned to his user id. The cloud server encrypts the data with the key series generated by chaos theory keeping the private user id as the initial value. In this way the already encrypted data on the cloud is re-encrypted once again. The encrypted data is transmitted to the user. The user after receiving the data will perform a double decryption with his key and the key id received from key manager. In this way the data is decrypted and accessed. If an unregistered user tries to access data from the server, he will not be able to authenticate himself; hence he will be treated as an unregistered user. The unregistered user will be allowed to access only the data access policy defined for his role. Apart from this, the data transmitted to him will be masked with suppression or generalization based data Anonymization technique combined with chaos based encryption.

In this architecture, any security breaching during transmission or during storage inside server is inhibited. The hybrid RBAC and chaos based access control together with the trust manager platform enhances greater flexibility together with enhanced confidentiality. The data Anonymization is carried out in the encrypted form hence assures data security along with privacy. The following encryption and decryption is performed whenever a chaos based encryption or decryption is evoked in the modules.

4. Data Encryption Algorithm

Text and image reverted into secret code with Figure 2. Minimum rounds will yield great performance in cloud with low communication and computational cost.

The algorithm for working inside each sub module of the proposed architecture is given as follow as

Date Owner

1. D← ENC(K_1,d_1)
2. R← RDEF(D,U_i)
3. SND(D,R) → CSP
4. SND(U_i,R,K_1)→ KM

Key Manager

1. REC(U_i,R,K_1)←DO
2. If REQ from user Ui, AUTH if U_i∈U SND(K_1)&& REC(K_2)
   else SND(K1)
3. SND (K_2)→CSP
4. If REQ from DO , UPDATE(U,R)

Cloud Server

1. If REQ from User Ui, AUTH if Ui∈U,R,
   SND E← (ENC(D_r,K_2); D_r∈DR
   else SND(M← MSK(ENC(D)))
2. LOG(U_i)// trust manger log

Registered User

1. SND (Ui,K_2)→KM
2. RCV(K_1), SND(Ui)→ CSP

3. RCV(E),
4. $E_1 \leftarrow DEC(E,K_1)$
5. $E_2 \leftarrow DEC(E_1,K_2)$

Unregistered user

1. SND (UR_i)→KM
2. RCV(K_1), SND(URi)→ CSP
3. RCV(M),

$ME \leftarrow DEC(M,K_1)$

5. Experimental Evaluation

To evaluate the performance of encryption and decryption time for logistic and henon map, we have implemented the chaos based encryption and decryption module in MATLAB 2012a. The module was simulated with the help of a Pentium Dual Core Processor, 2.30 GHz speed, 2 GB memory.

5.1 Security Analysis

In this section, a thorough security analysis has been carried out to demonstrate the robustness of the proposed scheme. A good cryptosystem should resist all kinds of known attacks, which can be discussed in the following,

i. Brute Force Attack (Exhaustive search attack)
ii. Statistical attack
iii. known/chosen plaintext attack and
iv. differential attack

Theorem 1: (Brute Force Theorem) The chaos crypto system is ξ- computationally secure against brute force attack for all possible keys 'k' with lyapunov exponent 'λ'. Let x_0 [correct] and x_0' [wrong] be the initial condition over space 'S' of dimension ' d' for the sampling period 'T', shows that the key space is nonlinear to derive an unpredictable orbit say S^d .

Proof:

Assume that key k = (x_0, φ, T_0) where 'x_0' as initial condition, 'φ' as activation component, 'T_0' as Transient (initial time of sampling period)

i.e. $$\left| x_0 - x_0' \right| \geq \xi \quad (1)$$

Cipher text 'Ci' of message Pi is deduced as

$$C_i = E\left(k, \left[C_{i-1} \oplus P_i\right]\right) \quad (2)$$

For space 'S',

$$\exists_x \left\{ x \in S \mid L(x_0) = S \right\} \quad (3)$$

$$\forall_{x_0} \in \left[0, N^s\right) \quad (4)$$

Where N represents the number of values with respect to diffusion nature.

Therefore, if 0<ξ<S is the distance between two keys x_0 and x_0' , then maximal security is attained after initial transient ie T> T_0.

Estimation for T_0 is taken from ξ. $N^{S.T0} = N^S$ which gives large number of keys, deriving that, it is hard to succeed brute force attack.

$$T_0 = \frac{x_0 - \log \xi}{S} \quad (5)$$

Insider Attacks

A malicious insider has full and direct access to the data. This is the most prevalent type of attack in relation to data sharing in the cloud . They can do anything they wish with the data, including selling them for profit.

Proof: Cloud provider does not have full and direct access to the data owner's data, Since all the data stored in the cloud server are in encrypted form. The key series used for encryption are highly random non-predictable keys generated with chaos theory. It validates that any insider attack shall be void and the attacker may not able to understand the message content.

Sniffing Attacks (Man-in-the-middle attack)

Attackers intercept the public communication channels and retrieve sensitive information, such as passwords. Such attacks are likely to be successful when there are no forms of encryption, when data is sent over public communication channels.

Proof: The data transmitted over the transmission is space is subject to man-in the middle attack. In this proposed scheme all the communication over the transmission is carried out in encrypted form only. Hence this scheme protects data content from any man-in-middle attacks.

Privacy of data against cloud

There is no phase in our approach, where the cloud stores the plaintext 'M' and key 'k'. The data is stored in encrypted form and the secret key is not stored in the cloud. This ensures that the data is protected from service provider and unauthorized user. More important, cloud has low chance to compromise with key manager.

User Revocation

When the access right of the user is revoked, the key corresponding to the user are removed from the key manager. This is most suitable way when compared to re-encryption and redistributing keys to the remaining users.

Large data sizes

This work focused on health applications. The data is the combination of text and image with large size. The proposed SCBEA generates symmetric key that will be able to handle the encryption of the large data.

5.2 Performance analysis

The performance of the proposed method is analysed with various metrics such as i) Key Size ii) Encryption and Decryption Time iii) Storage Cost iv) Throughput v) Statistical Analysis and vi) Access Control

i. Key Size Attack Time

The attack time is referred as the time taken for the attacker to break the keys .The attack time for different algorithms such as AES, DES and SCBEA were analyzed and the comparison chart is shown in Table 1.

Table 1: Comparative analysis of Key Size vs Attack Time

	DES	AES	SCBEA
Key Size	56	256	infinity
Attack Time	1.37×10^{11}	1.02×10^{8}	No Known attack

It is observed that the attack time for AES algorithm tends to be low when compared to other two algorithms; whereas the attack time of the DES algorithm is moderate. Due to increasing key size no known attack for SCBEA and provide protection against attacks.

ii. Encryption and Decryption Time

The encryption time can be measured as the time that an encryption algorithm takes to produce a cipher text from a plaintext. The decryption time can be measured as the time that an encryption algorithm takes to produce a plain text from a ciphertext. The encryption and decryption time for different algorithms such as AES and SCBEA were analysed and the comparison chart is shown in Figure 3.

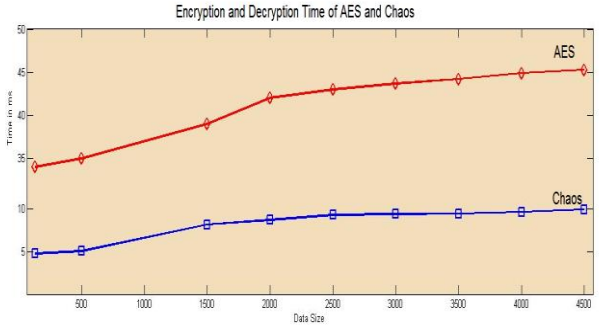

Figure 3: Encryption Time for different Data Sizes

By analyzing Figure 3, it is noticed that AES algorithm has higher encryption and decryption time. The encryption and decryption time of the SCBEA tends to be lower when compared to the AES algorithm.

iii. Storage Cost

Comparative analysis of various Data Size vs Storage Cost is depicted in figure 4. It is noticed that AES algorithm has higher cost than Chaos.

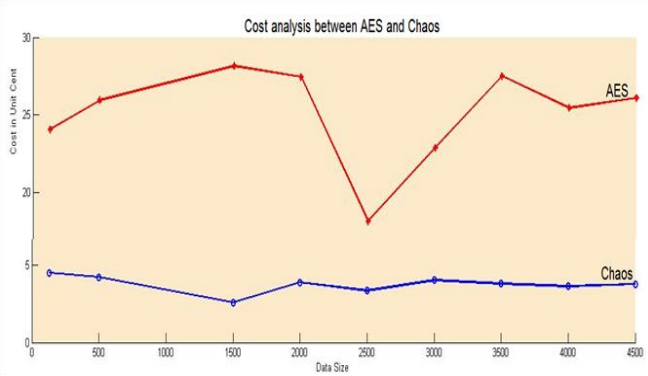

Figure 4: Cost Analysis between AES and Chaos

iv. Throughput

Throughput can be calculated using the following formula in equation (6).

$$\text{Throughput} = \frac{\text{plaintext size encrypted/decrypted}}{\text{Encryption/Decryption Time}} \qquad (6)$$

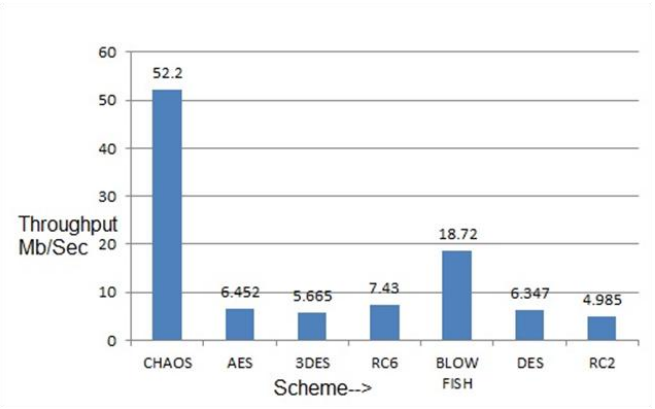

Figure 5: Throughput for different Scheme

By analyzing the Figure 5, it is noticed that AES and DES algorithm have similar Throughput. The throughput of the CHAOS tends to be higher when compared to the AES and DES, Triple DES, RC6, Blow Fish, RC2 algorithms.

v. Statistical Analysis

Statistical analysis is a common and effective way to analyze a cryptosystem. Consequently, a good cipher should be robust against any statistical attack. In order to prove the security of the proposed image cryptosystem, the following statistical tests are performed and it is shown in Figure 6.

vi. Access Control

An access structure based control technique was used in combination with RBAC and chaos encryption. The access structure based access control is similar to that of a Role Based Access Control except the fact that roles permissions are defined through an access structure. Also each data access is controlled not only based on the role assignment but also with an encryption technique. The data send to the user is in the encrypted form and user alone can decipher and read it.

Simple RBAC is widely used access control however it suffers from Trojan horse attack. In this work, data access is double secured with access control and mechanism hence any Trojan horse attack is nullified. Although an attacker able to break the access structure, he will be stopped at the initial authentication level itself. Further if he able to access any data by breaking the RBAC, the chaos based encryption embedded in the data secures the data. The attacker will not be able to access the data since the data is encrypted with highly random non predictable key serials generated with Chaos based concept.

The figure 7 indicates the disk space requirements of various access control mechanism such as simple RBAC, DAC, MAC and the proposed access structure -Chaos combination. It is important to note that in the proposed system occupies only a minimal disk space compared with other techniques. Unlike other techniques, in the proposed system only the access tree is stored for each role and data is driven dynamically when the users tries to access it. Since the data is already in encrypted form by Chaos encryption, there is no need to separate them based on their roles fearing cross role attacks. This ensures greater access control along with data protection at a predominately low computational requirement.

6. Conclusion

This paper presents a novel architecture that provides enhanced key management without interpreting data stored in cloud. This architecture has new and significant features like high scalability for both organizations and health care systems. Secure protocol usages leverage control on client data, multi-tenancy, privacy and trust. The proposed work eliminates the compromise of key manager and cloud service provider. More importantly, key manager is a separate cloud with enforcement activities. Also it greatly reduces computational overhead occurred in conventional techniques. This will provide privacy for potential security breaches in cloud by anonymizing encrypted data. Altogether this approach is a comprehensive cloud security model.

References

[1] Kushida, Kenji E., Jonathan Murray, and John Zysman, "Cloud computing: from scarcity to abundance," *Journal of Industry, Competition and Trade*, vol.15, no. 1, pp. 5-19, 2015.

[2] Lang, Bo, Jinmiao Wang, and Yanxi Liu, "Achieving Flexible and Self-contained Data Protection in Cloud Computing", *IEEE Access*, 2017.

[3] Rimal, Bhaskar Prasad, Admela Jukan, Dimitrios Katsaros, and Yves Goeleven, "Architectural requirements for cloud computing systems: an enterprise cloud approach", *Journal of Grid Computing* 9, no. 1, pp. 3-26, 2011.

[4] Rochwerger, Benny, David Breitgand, Eliezer Levy, Alex Galis, Kenneth Nagin, Ignacio Martín Llorente, Rubén Montero et al., "The reservoir model and architecture for open federated cloud computing" ,*IBM Journal of Research and Development*, vol. 53, no. 4, pp.4-1,2009.

[5] Jaeger, Paul T., Jimmy Lin, and Justin M. Grimes, "Cloud computing and information policy: Computing in a policy cloud?," *Journal of Information Technology & Politics* ,vol.5, no. 3,pp.269-283,2008.

[6] Arinze, Bay, and Murugan Anandarajan, "Factors that determine the adoption of cloud computing: A global perspective", *Enterprise Information Systems and Advancing Business Solutions: Emerging Models: Emerging Models, pp.* 210-223,2012.

[7] Armbrust, Michael, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee et al., "A view of cloud computing," *Communications of the ACM* ,vol. 53, no. 4 ,pp.50-58,2010,.

[8] Pearson, Siani, and Azzedine Benameur, "Privacy, security and trust issues arising from cloud computing," *IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), 2010*, pp. 693-702, 2010.

[9] Karadsheh, Louay, "Applying security policies and service level agreement to IaaS service model to enhance security and transition", *computers & security*, vol.31, no. 3 315-326, 2012.

[10] Anand, Priya, Jungwoo Ryoo, and Hyoungshick Kim, "Addressing security challenges in cloud computing–a pattern-based approach" ,

[11] Lan Zhou, Vijay Varadharajan, and Michael Hitchens, "Secure Role-Based Access Control on Encrypted Data in Cloud Storage," *IEEE Transactions on Information Forensics and Security*, vol.12, 2013.

[12] J. Hur, D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems", *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 7, pp. 1214-1221, 2011.

[13] J. Hur, "Improving security and efficiency in attribute-based data sharing", *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 10, pp. 2271-2282, 2013.

[14] J. Li, X. Chen, C. Jia, W. Lou, "Identity-based encryption with outsourced revocation in cloud computing", *IEEE Transactions on Computers*, vol. 64,no. 2, pp. 425-437, 2015.

[15] Karadsheh, Louay, "Applying security policies and service level agreement to IaaS service model to enhance security and transition," *computers & security*, vol.31, no. 3 pp. 315-326, 2012.

[16] Subashini, Subashini, and Veeraruna Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of network and computer applications* ,vol.34, no. 1,pp. 1-11,2011.

[17] Padhy, Rabi Prasad, Manas Ranjan Patra, and Suresh Chandra Satapathy, "Cloud computing: security issues and research challenges," *International Journal of Computer Science and Information Technology & Security (IJCSITS)*, vol.1, no. 2, pp.136-146, 2011.

[18] Varadharajan, Vijay, and Udaya Tupakula, "Security as a service model for cloud environment," *IEEE Transactions on Network and Service Management*, vol.11, no. 1 60-75, 2014.

[19] J.M.bohli, N.Gruschka, M.Jensen, L.L.Iacono and N.Marnau, "Security and privacy- enhancing multicloud architectures", *IEEE Trans. Dependable Sec. Comput.*,vol. 10,no. 4, pp. 212-224,2013.

[20] Y.Wu, Z.Wei, and R.H.Deng, "Attribute-based access to scalable media in cloud assisted content sharing networks", *IEEE Trans. Multimedia*,vol.15,no.4,pp.778-788,2013.

[21] C.Wang, S.S.M Chow, Q.Wang, K.Ren, and W.Lou," Privacy-preserving public auditing for secure cloud storage", *IEEE Trans. Comput.*, vol.62, no.2, pp.362-375, 2013.

[22] T. Yang, C. W. Wu, L. O. Chua, "Cryptography based on chaotic system", *IEEE Transactions on Circuits & Systems I Fundamental theory & Applications*, vol.44, no. 5, pp. 469-472, 1997.

[23] Khan, Abdul Raouf, "Access control in cloud computing environment," *ARPN Journal of Engineering and Applied Sciences* 7, no. 5, 613-615, 2012.

[24] Ferraiolo, David, Rick Kuhn, and Ravi Sandhu. "Rbac standard rationale: Comments on" a critique of the ansi standard on role-based access control", *IEEE Security & Privacy*, vol.5, no. 6 , 2007.

[25] K. Liang, W. Susilo, and J. K. Liu,"Privacy-preserving ciphertext multisharing control for big data storage," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 8, pp. 1578–1589, Aug. 2015.

[26] Z. Zhou, D. Huang, and Z. Wang, "Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption," *IEEE Trans. Comput.*, vol. 64, no. 1, pp. 126–138, Jan. 2015.

[27] Yu, Shucheng, Cong Wang, Kui Ren, and Wenjing Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," *Infocom, 2010 proceedings IEEE*, pp. 1-9,2010.

[28] Feng, Bin, Xinzhu Ma, Cheng Guo, Hui Shi, Zhangjie Fu, and Tie Qiu, "An Efficient Protocol With Bidirectional Verification for Storage Security in Cloud Computing," *IEEE Access* ,vol.4,pp.7899-7911,2016.

[29] Chang, Victor, and Muthu Ramachandran, "Towards achieving data security with the cloud computing adoption framework," *IEEE Transactions on Services Computing*, vol.9, no. 1, pp.138-151,2016.

[30] R. Thandeeswaran, M A Saleem Durai,"DPCA: Dual Phase Cloud Infrastructure Authentication", *International Journal of Communication Networks and Information Security (IJCNIS)*, Vol. 8, No. 3, December 2016.
[31] Zakia El uahhabi, Hanan El bakkali," Calculating and Evaluating Trustworthiness of Certification Authority", *International Journal of Communication Networks and Information Security (IJCNIS)*, Vol. 8, No. 3, December 2016.
[32] Chen, Xuexiu, Chi Chen, Yuan Tao, and Jiankun Hu, "A Cloud Security Assessment System Based on Classifying and Grading", *IEEE Cloud Computing* ,vol.2, no. 2 58-67,2015.

Appendix 1: Notations used in Algorithm

Notation	Meaning
D	Data
ENC	Encryption
K1	Data owners key id
D1	Data subset
R	Role
RDEF	Role definition
U	User set
SND	Send
KM	Key manager
REC	Receive
REQ	Request
DO	Data owner
K2	Data user key
AUTH	Authentication
UPDATE	User grant or revocation update
E	Encrypted data
D_r	Data assigned to Role r
M	Masked Version of ENC data
MSK	Data anonymization
LOG	Trust Monitoring and logging
CSP	Cloud service provider
E_1	Data encrypted with K_1
E_2	Data encrypted with K_1 and K_2
ME	Masked Data

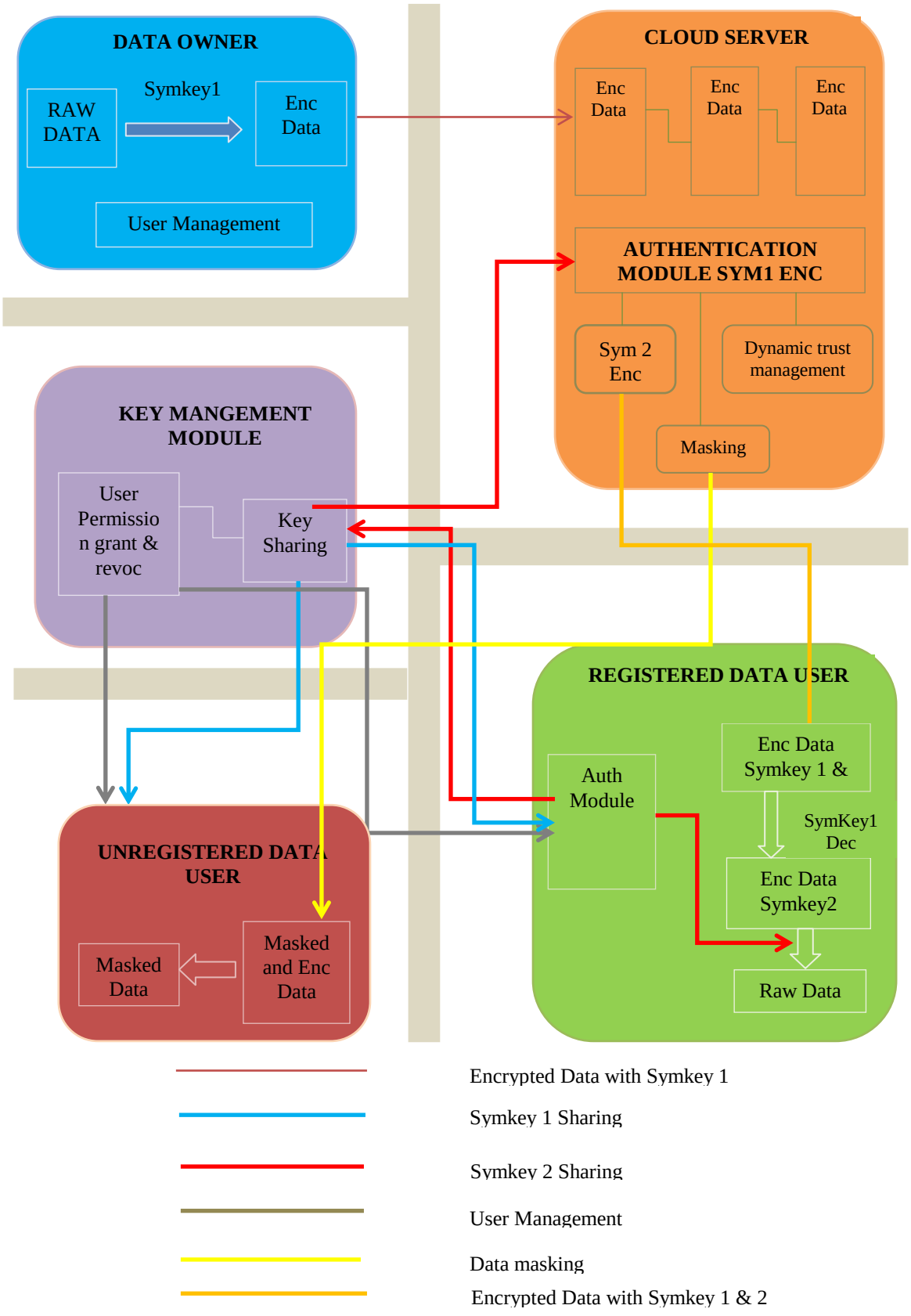

Figure 1: A comprehensive cloud security and privacy protection architecture

function $Data\_Encryption\_text\_image(p_i)$ **returns** $Ciphertext(C_i)$, or failure

input: p_i, k, λ **//initial value positive lyapunov exponent is user id**

output: C_i

generate random key series $k_1, k_2, k_3, ...$

for each random key in keyseries (k) do

if key is consistent with assignment based on constraints

$Data\_Encryption\_text(p_i, k) \leftarrow p_i \oplus k$

$Enc\_text(C_i) \leftarrow Data\_Encryption\_text(p_i, k)$

$Data\_Encryption\_image(p_i, k) \leftarrow p_i \oplus k$

$Enc\_image(C_i) \leftarrow Data\_Encryption\_image(p_i, k)$

if $Enc\_text(C_i) \neq failure$ **then**

return $Composed\ text\ data$

end if

if $Enc\_image(C_i) \neq failure$ **then**

return $Composed\ image\ data$

end if

end if

end for

Figure 2: Chaos Theory based Encryption and Decryption is reverse process

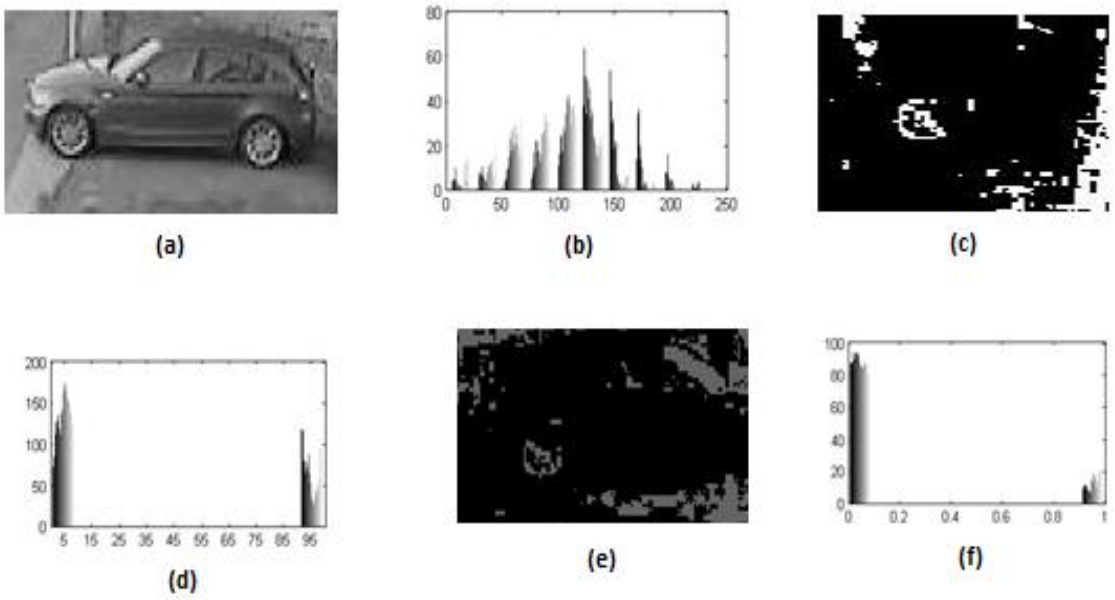

Figure 6: (a) Original Image (b) Histogram of image (c) encryption key (d) Histogram of encryption key (e) Encrypted image using chaos (f) histogram of encrypted image

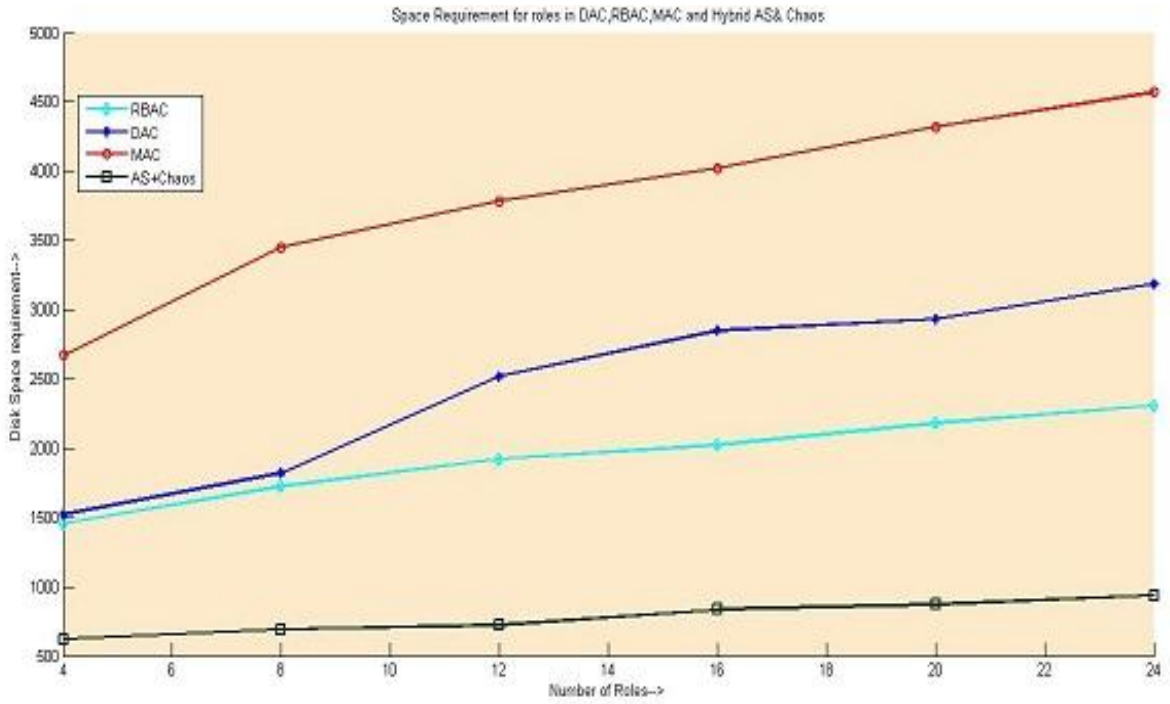

Figure 7: Disk space requirements for various access control techniques