ISSN 2278-3091
Volume 9, No.5, September - October 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse12952020.pdf
https://doi.org/10.30534/ijatcse/2020/12952020

Integrated Security, Authentication and Decentralized Access Control (ISADA) Framework Based on Novel Key Exchange Mechanism for a Public Cloud Environment

S.Ramalakshmi[1], Dr.V.Vallinayagi[2]

[1]Research scholar, Reg No: 18221262162004,Department of Computer Science,
Sri Sarada College for Women, Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli–627012,
lakshmigana2011@gmail.com.
[2]Head & Associate Professor, Department of Computer Science,
Sri Sarada College for Women, Tirunelveli–11.

ABSTRACT

In modern days cloud computing has found its application to a great extent. People are sure that it will be the future technology that occupies digital world, but the security related issues need to be overcome. By using cloud computing, users can access their data from remote servers through internet. Cloud computing provides cheaper and faster services to users. At the same time there is security issues associated with cloud such as data loss, abuse of data, cyber security attacks and so on. While off-shoring sensitive data through third party cloud servers, access control ensures that an unauthenticated person cannot access data without user's knowledge. This research paper proposes a Data security and User centric access control framework which provides two levels of security and multilayer access control mechanism by using key exchange. This mechanism allows user to store shuffled and encrypted data in a cloud server which is only accessed by the authenticated users. A novel key management mechanism is used to achieve multilayer access control. User centric access control makes this mechanism more vigorous because there is no need for third party auditors and key service providers. All the communications and key transactions are only between the owner of the data, consumer of the data and the cloud host. This proposed framework (ISADA) gives a better solution for broken access control under horizontal privilege escalation.

Key words : Cloud computing, Remote servers, Data loss, Cyber security, Cloud servers, Access control, User centric access control, Shuffled and Encrypted data, Third party auditors, Key service providers, Broken access control, Horizontal privilege escalation.

1. INTRODUCTION

Cloud computing provides so many services like SAAS, PAAS, IAAS. Cloud storage services have raised their quality to a great extent today. Today's digital trade systems have increased the demand for off shoring data. Regarding data security, data from different users can be stored and accessed on various servers or virtual machine (it may or may not be stored on a single server) [33]. Sometimes a server can allow unapproved access and it leads to an attacker to hack user data without any notice, so instead of depending server security mechanism client can secure their data at their end. Meanwhile instead of using Key Distribution Centers (KDC) and Third Party Auditors (TPA) key management and verification can be done between data owner, consumer and host.

The Proposed framework provides a two layer security mechanism which shuffle and encrypt user data at the client end. Key contributions of this proposed work (ISADA) are as follows,

i) When considering about access control mechanism owner and consumer of data need to register themselves to the cloud server. Registration includes inherence and knowledge factors.
ii) Owner can upload shuffled and encrypted files along with the visible key and the list of consumers who can access the particular file.
iii) Consumer's identity will be verified through knowledge and inherence factors by means of password and biometric. After verification consumer can view the list of files which are permitted by the owners to access.
iv) If the consumer wants to access the file then he needs to get permission from the owner by sending a file request.

v) After approving consumer's request owner will send a set of keys named as visible key, decryption key and reshuffling key to the consumer's mail. At the same time owner generate another one key named as invisible key and sends to the cloud host. This key is called invisible key because it is unknown to consumers.

vi) At the consumer end, by providing this visible key to the cloud server, another key will be regenerated and verified. This key is named as invisible key; this process is done without user's knowledge.

vii) After verification of these keys now the consumer is allowed to access, decrypt and reshuffle the data.

This framework is applicable for an individual user and an organization. Data shuffling, encryption and multilayer access control mechanism joined together to achieve a better security and access control in a public cloud architecture. Meanwhile this work provides a better solution for broken access control.

Organization of the paper

The remainder of this paper is structured as follows. Problem statement, objective and significance of the proposed work are presented in Section-2, Section-3 indicates related work and existing solutions, and Section-4 represents cloud computing attacks and access control mechanisms. Section-5 presented the basic workflow of the proposed system, visible and invisible key generations; Section-6 presents key management. Section 7 deals with attack analysis, crypt analysis and efficiency analysis of the proposed framework.

2. PROBLEM STATEMENT, OBJECTIVE AND SIGNIFICANCE OF THE PROPOSED WORK

Problem Statement

Existing solutions uses Encryption for cloud data security and Key Distribution Center (KDC) to distribute and manage keys. At the same time Third Party Auditors (TPA) are involved to do key verification. So, if the key distribution center fails then it leads to the unavailability of data. At the same time there is no such appropriate solution for broken access control.

Objective

The main objective of this work is to propose a cloud architecture that employs a user centric access control using multiple key exchange mechanism without the need of KDC and TPA. This architecture solves the problem about data security, authentication and access control. This also protects user data from broken access control attacks.

Significance of the Work

The proposed architecture implements shuffling and encryption for data security. And also provides an authenticated communication between owner, consumer and cloud host. User centric access control mechanism for better cloud environment.

3. RELATED WORKS & EXISTING SOLUTIONS

A secure cloud computing model based on manual data classification, classified data are encrypted by using different encryption algorithms. It minimizes the overhead and the processing time essential to secure data through using different security mechanisms [1]. Major growth and major drawbacks of cloud computing was discussed. Cloud has good solution to increase productivity in much area such as cost effectiveness .A classification, business models and research directions of cloud computing are discussed, says that there is not more transparency available at which location the data is stored. So security and trust is the major research issue [2].Cloud data is moving to the unknown destination, so there is a need for effective security mechanism. Hybrid Cryptographic Algorithms are proposed [3]. Data integrity, data loss and secure data access is the major issues in cloud, so here the data has been converted into more scalable and flexible form to add more security at access levels [4]. Three ways are introduced to achieve data security, that are i) Data transmission, ii) Data isolation, iii) Data wiping, IPsec, VPN and SSL are able to incorporated within cloud to improve the data security [5]. Solutions for some security issues in cloud are introduced that are i) Intrusion detection system, ii) Cloud computing security gateway [6]. Proposed additional securities for a secured cloud computing such as physical security, cloud OS security, data security, virtual cluster security, data security, SaaS/PaaS security [7]. Different encryption algorithms used in cloud computing are compared with each other [8]. Different security algorithms used in cloud was analyzed [9].Protect the data in the cloud database server cryptography is one of the method. Analyzed various symmetric and asymmetric algorithms used in cloud [10].Data classification used to achieve high data security and effective use of encryption algorithms .Data stored in the cloud

are manually classified and based on this classification various encryption algorithms are used [11]. Survey about classification techniques used in cloud computing and for security AES, hybrid encryption algorithm, homomorphism encryption schemes are used [12]. Data classification technique is used to improve cloud security. Data are classified under three different criteria Access control, Content, Storage. According to this classification security considerations can be applied [13]. Proposed a secure cloud computing model based on manual data classification, classified data are encrypted by using different encryption algorithms. It minimizes the overhead and the processing time needed to secure data through using different security mechanisms [14]. New solution is proposed to enhance user authentication and in cloud computing using biometrics with multifactor authentication mechanisms [15].This paper reviews and discusses the most important issues raised by biometrics and presents a secure authentication protocol skeleton [16].This paper comprehensively reviews multimodal recognition using ear pattern and finger print data, it is concluded that further research should investigate fast and fully automatic ear-finger print multimodal systems robust to occlusions and deformations [17]. Authentication using Biometric and secure data storage is discussed in this book. Cloud storage platform, distributed storage, Performance of the authentication system are the topics covered here [18]. This paper will enlighten the various improved methods for dealing with data security in the domain of biometrics, cryptography, public key infrastructure and Cloud Standards in the venture of Cloud Computing [19] It has been proven that Blowfish has fastest encryption time and decryption time, required less amount of storage and it also records highest average entropy per byte of encryption compared to other symmetric encryption algorithm [20]. By using hierarchical structure and clock this framework assures a best way of access control mechanism [21]. In the proposed model Multi Agent based System (MAS) is represented to define the accessibility and functionality of the access control mechanism [22]. A cloud access control system is introduced a WISP technology that means a Wireless Identification and Sensing Platform (WISP) tags are combined with customized motions. Users are permitted to pass the access control system only if they operate user defined motions correctly [23]. In this research paper a policy based encryption system introduces which address so many problems at the same time it assures access control in open stack swift [24]. In this proposed work encryption and authentication system is introduced mean while this application uses a group key system which means a group of user. File encryption system is used to enhance the group key formula [25]. Hybrid security algorithm is used to enhance data security in cloud. Data migration is the major consideration of this work. Comparisons are done by bandwidth, encryption, decryption and key generation time [26]. A reliable encryption system with advanced key management schemes with decentralized access control mechanism is proposed [27]. Multifactor biometric authentication mechanism is implemented. Iris, finger print, facial recognition, voice recognition are the factors used for authentication [28]. This paper made a comparative analysis of authentication and access control based security models employed over cloud and concludes with a new framework "MLBAAC" model for cloud [29]. A set of cryptographic keys are used to avoid the involvement of third parties and access control is lays in the organization itself not in the cloud. Role based access controls with multiple cryptographic keys are proposed [30]. An algorithm for data shuffling is proposed named as "Dual Shuffling", this algorithm is incorporated with blowfish and comparisons are done. At the end it achieves better data security instead of single encryption [31].

4. CLOUD COMPUTING ATTACKS AND ACCESS CONTROL MECHANISMS

Together with the advancement of cloud computing, security attacks are also increased [32]. The important attacks cloud faces are,

1) Broken access control attacks.
2) Side channel attacks
3) Authentication attacks
4) Denial of Service (DOS) attacks.
5) Man in the middle attack.
6) Inside job attacks.

Because of these attacks, a trusted security mechanism is needed before uploading data into the cloud server. At the same time access control is a procedure or mechanism that allows, restricts or denies access to a system [22]. There are three main types of access control models used in cloud are,

1) Mandatory Access Control.
2) Discretionary Access Control.
3) Role Based Access Control.

This research paper proposes a new way of secured, user centric and decentralized access control mechanism.

5. BASIC WORKFLOW OF THE PROPOSED FRAMEWORK

Proposed system mode consists of three major parts that are Data owner, Data consumer, Cloud Server. All the request and response are managed between these three parties. There is no need for third party auditors (TPA) and key distribution centers (KDC).

5.1. Workflow

The proposed workflow contains the five different phases that are listed below.

1) Registration
2) File upload
3) Visible key generation
4) Invisible key (or) Hidden key generation
5) Accessing permission

5.1.1. Registration Phase with Knowledge and Inherence Factors

Registering the details of owner and consumer is the prior work to be done. During registration, owner and consumer have to provide username, password, mail id and biometric impression of the owner and consumer. This method of registration including Knowledge and Inherence factors of owner and consumer.

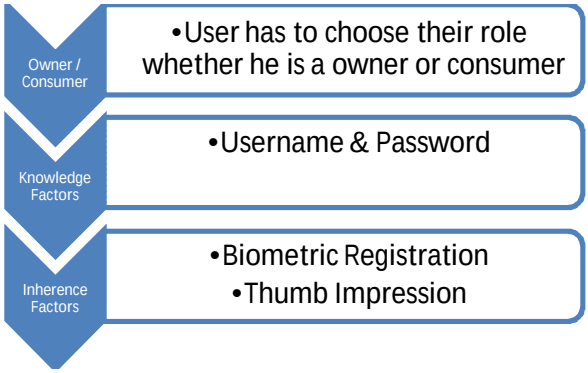

Figure 1: Registration Factors

Once registration has been completed, the user must login with the exact information that was provided. If there is any mismatch in the details then the user will not be allowed for further processing. Particularly user must provide registered username, password and biometric impression. After verification of these credentials now the user can be allowed for file upload/file request page.

5.1.2. File Upload &Visible key generation

Before uploading a file, owner must shuffle and encrypt the file by using dual shuffling incorporated with blowfish algorithm[31].Now along with the protected file, visible key has been uploaded in the cloud server by the owner of the file.

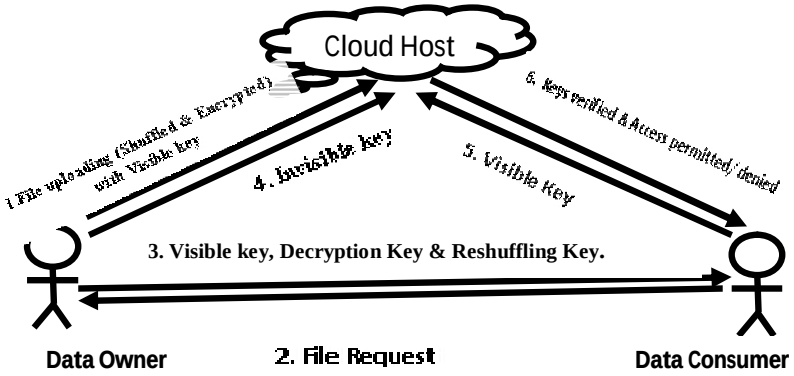

Figure 2: Workflow Directions of Proposed Framework

5.1.3. Visible key generation

The owner check the attribute set of the user. If the user has the valid permission then a key named visible key will be sent to the user and the cloud host. For each file request visible key will vary. Along with the visible key, decryption and reshuffling key has also been sent to the consumer. These keys are sent to consumer's registered mail.

If an owner wants to upload a file then at that time visible key also has to be uploaded along with the file. This visible key will vary for each and every file of the owner. Consumer can use the visible key only for the particular file of the owner. The below table describes the notations that are used in visible key generation algorithm.

Table 1: Notations used in Visible Key generation algorithm.

Notation	Description
O_n	Name of the nth owner
LO_n	length of the nth owner name
Rnum	Random number between 1000 to 9999
LF_i	Length of the ith file name uploaded by the nth owner.
K_1	Calculated Key value before round function.
VK	Generated Visible Key.

Visible Key Generation Algorithm

1. Owner wants to upload a file to cloud host.
2. Along with file visible key has to be generated and uploaded.
3. Taking the name of the owner (O_n).
4. Find the length of the owner name (LO_n).
5. Find Rnum.
6. Find the length of the file name which needs to be upload $L(F_i)$
7. Generate K_1. $\mathbf{K_1=(LO_n*Rnum)/LFi}$.
8. Generate Visible Key $\mathbf{VK=Round(K_1).}$

5.1.4. File Request & Invisible key generation

To download any file from the cloud server then the consumer needs to send a file request to the corresponding owner.

Invisible Key Generation

This key is also known as "Hidden Key", it is generated and sent to the host for authentication. Invisible key is generated by using user's registration details. So, it will vary for each and every user. If a user tries to produce visible key of another user (broken access control attack) then his/her access will be denied by verifying this invisible key. This key is generated by the owner and sent to the cloud host at the time of file request. At the time of verifying visible key, cloud host regenerates the invisible key by using user's registration details. If it matches then only the user is permitted for further processes. This invisible key generation is done without user's knowledge to avoid broken access control attack. The below table describes the notations that are used in Invisible key generation algorithm.

Table 2: Notations used in Invisible Key generation algorithm

Notation	Description
C_n	Name of the nth Consumer
C_n ASC	ASCII value of C_n
C_n Sum	Sum of ASCII Value
$AvgN_1$	Average of ASCII
RSC_n	Random shuffling of Consumer name
RSF_n	Random shuffling of file name
$RSCF_n$	Starting 50% letters from RSC_n and RSF_n
$RSCF_n$ASC	ASCII value for $RSCF_n$
S_n	Sum of $RSCF_n$ASC
$AvgN_2$	Average of S_n
IVK	Invisible Key.

Invisible Key Generation Algorithm

1. Find C_n.
2. Calculate the ASCII values for C_n (C_n Asc).
3. Calculate sum of ASCII (C_n Sum).
4. Fin average of the ASCII (AvgN1).
5. Perform random shuffling of consumer name and file name (RSC_n and RSF_n).
6. Take the starting 50% letters from RSC_n and RSF_n ($RSCF_n$).
7. Calculate ASCII for $RSCF_n$($RSCF_n$ASC).
8. Find sum of the ASCII Values $\mathbf{S_n= SUM (RSCF_n)}$.
9. $\mathbf{AvgN_2= Avg (S_n).}$
10. Invisible Key $\mathbf{IVK = (VK+AvgN_1)-AvgN_2.}$

5.1.5. Verification

Visible key must be submitted to the cloud server for verification. If the key matches with the visible key stored in the cloud server then secondary key is regenerated and verified by the cloud host for authentication purpose. Visible and Invisible key is varying for each file request.

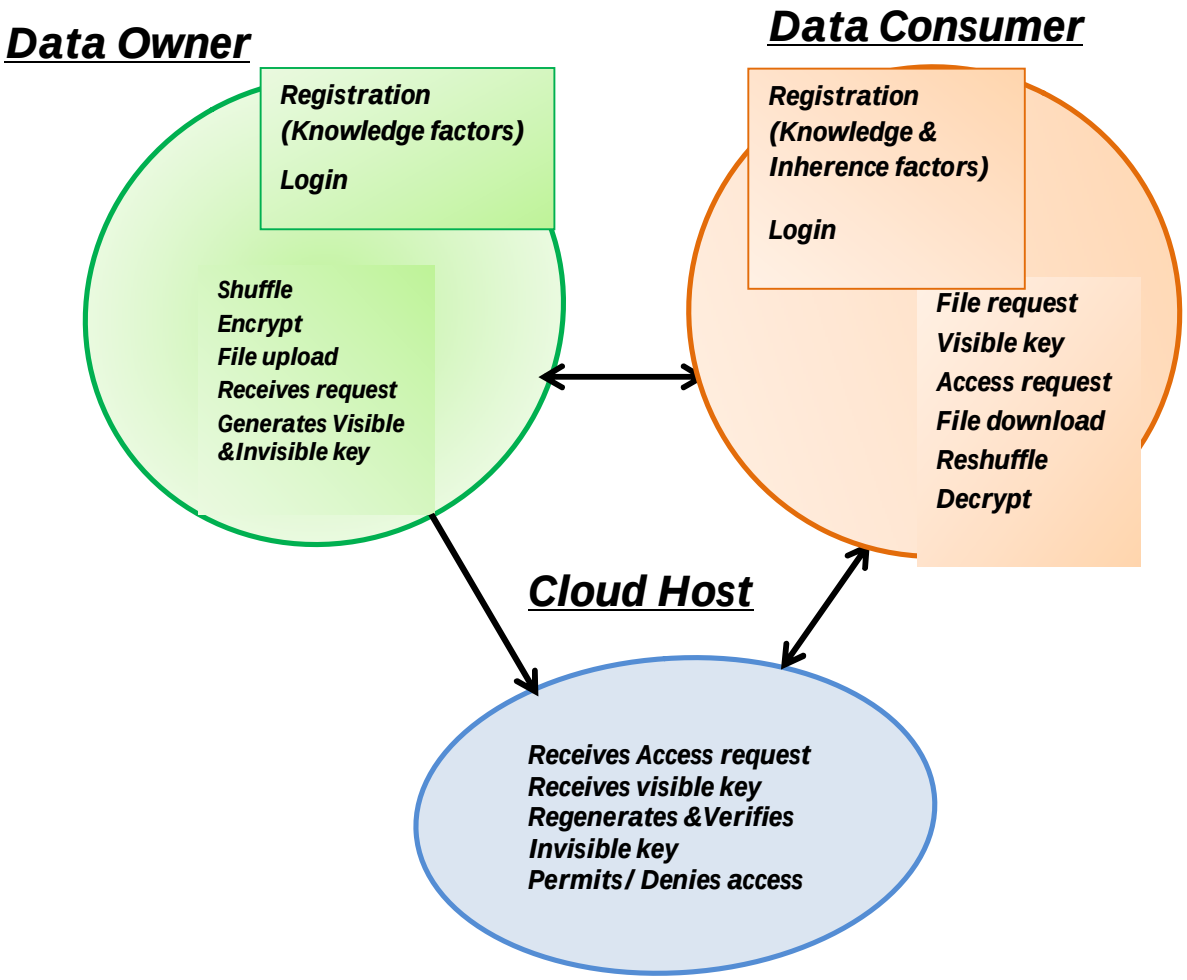

Figure 3: Class Diagram of Proposed Workflow

5.1.6. Access permission

After the verification of visible and invisible key now the consumer is allowed to access the particular file. Consumer can decrypt and reshuffle the file by using decryption and reshuffling key given by the owner. The access permission is limited for ten days. After ten days consumer can't access the file with the same permission.

6. KEY MANAGEMENT

The proposed framework applies various keys at different stages of the application. That are,

- **Visible key** – This key is generated by the owner when the consumer request the file and it will be shared with consumer after checking consumer's access rights. The same key is stored also in cloud server for verification of the consumer.
- **Invisible key** – This key is generated by the owner with the user's registration details. So, it will vary for each and every user. This key is generated and sends to the host without consumer's knowledge. Then the cloud hosts regenerate it with the user's credentials and verify the particular user is an authenticated person.
- **Decryption key** – This key is used to decrypt the file and it is shared by the owner to the consumer.
- **Reshuffling key** – This key is used to reshuffle the file after decryption and this is also shared by the owner with the consumer.

7. EXPERIMENTAL SETUP & RESULT ANALYSIS

Various types of attacks and prevention vectors provided by the proposed work are analyzed. Time taken at the owner side, host side and consumer side with different file sizes are examined. For this experiment a laptop with 2.10 GHz C.P.U., 2 GB RAM, Intel Pentium Processor and Windows 7(32-Bit) is used in which the text data are stored. Implementation is done under Python spyder 3.1.4. It is the scientific Python development environment. Python spyder is a powerful Python IDE with advanced editing, interactive debugging, testing and introspection features. SQLite system software is used to store users' data. It is a relational database management system and it is easy to embed it into the end program.

7.1. Attack Analysis

An attack indicates a way by which a hacker can get access to a system or a server to deliver malicious outcome. Types of attacks include viruses, email attachments, deception, and pop-up windows and so on. Except deception all the above mentioned attacks involves programming. In deception attack a human operation is trapped thus breaking the system defense walls.

Table 3: Attack Analysis with Proposed Framework.

S.No	Name of the Attack	Description	Proposed Action Plan
1	**Insider Attacks**	It is a security attack to an organization and it causes from the employees of the organization. People those who have authorized access misuse that access to create negative impact on organization's information or systems	**Invisible key generation & regeneration** An invisible key is generated by an owner with the name of the consumer and it is regenerated by the cloud host to verify the consumer authentication. It is done without consumer knowledge.
2	**Cloud Malware Injection Attacks**	This attack is done to take control of user data in the cloud architecture. To achieve this, hacker can insert an infected service implementation module to SaaS or PaaS. When the cloud system trusts then it will redirect user data request to the hacker module and then it initiates the execution of malicious code.	**Shuffling and Encryption of Data**. It is achieved in all the three stages that are, i) At the owners side ii) In transit iii) At rest

3	**Password Discovery Attacks**	Attackers use so many techniques to steal passwords stored or transmitted by a user to launch this attack. It includes Guessing, Dictionary, Video recording and Brute force attacks	**Knowledge + Inherence Factor Authentication** Biometric fingerprint authentication included with static password.
4	**Broken Access Control Attacks**	When a user may perform an action or access data of another user within the same level of permission then this will comes under Horizontal Privilege Escalation. This attack will occur when users can act outside of their intended permissions. This attack leads to unauthorized access, information disclosure and alteration or destruction of data. This will usually occur with inappropriate implementation of authentication mechanism.	**Invisible Key Generation** This research work leads a result to this problem in the form of "Invisible key". This key generation and verification is done without consumer knowledge so it is very difficult to hack or breach by another consumer.

7.2. Cryptanalysis

Under this section, the security measures of proposed system in the aspects of authentication, sensitivity and integrity.

Sensitivity

In the proposed work, there is a two level of data security is provided. One is shuffling and the other is encryption. Shuffling is done by Dual shuffling algorithm and encryption process done by Blowfish algorithm. It is proved that Dual shuffling incorporated with Blowfish will achieve better security. At the same time shuffling, encryption, reshuffling and decryption processes are done only in client and server ends so the data is secure in transit and also at the rest. Meanwhile it's impossible to hack or seal the key.

Authentication

In the proposed work, to achieve authentication knowledge and inherence factors are used. Username and password is the basic knowledge factors and it is used for data owners. Biometric fingerprint authentication is the inherence factor and it is used for data consumers along with knowledge factors.
It provides a rigid authentication mechanism because of the combination of knowledge and inherence factors.

Integrity

Integrity means unforgeability. A visible and invisible key generation gives two levels of access control policy. One is with the knowledge of the data consumer and the other one without the consumer's knowledge. This key generation are done by data owner and verified by the cloud host. Invisible key is regenerated and verified by the cloud host. At the same time invisible key is generated by using consumer registration details so this is difficult to cease. Without invisible key verification the consumer will not be permitted to access the data. So, this achieves betterment in integrity.

7.3. Efficiency Analysis

Based on the existing and proposed model for access control, security and authentication particular features could be used for efficiency analysis. These features are being identified by the existing models. Following are the list of features,

i) **F1-Support for Multilevel Security** – It specifies the security mechanisms provided to the user data. Proposed model supports multilayer security.

ii) **F2-Support for Multifactor Authentication** -- It specifies the authentication mechanism provided by the model.

Proposed model supports multifactor authentication.

iii) **F3-Efficient User Access Control** -- It indicates the access control mechanism provided by the model. Proposed model supports multi key exchange access control.

iv) **F4-Integrated Security, Authentication and User Access Control –** This feature measure about the integrated mechanism of security, authentication and access control. Proposed model achieves this integration.

v) **F5-Support for Data Security at all the three levels** -- This feature describes whether the model achieves data security at the owner side, in transmit and at rest . Proposed model achieved these three levels of data protection.

vi) **F6-Key Distribution without KDC** -- This feature describes the methods for key distribution. Again KDC is a third party, so key distribution without KDC is considered as a better approach. In the proposed model key distribution is done by the owner itself.

These former discussed features are analyzed here and provides a better conclusion as which model would perform better for a public cloud environment. Prospective values for every feature include:
Yes, No with weights**1** and **0** respectively. The weight measures of six features are mentioned in the below table. The model with the highest weighted average value would be considered as best among all the models. By using this weight calculation measures an effective model can be identified with the comparison of all features.

Table 4: Features with Weightages

Feature	Weight
F4	6
F1	5
F2	4
F3	3
F5	2
F6	1

.

Weighted average is calculated for all the six measures with existing and proposed model by using the formula,

$$X = \frac{\sum_{i=1}^{n} w_i x_i}{\sum_{i=1}^{n} w} \quad \text{----------(1)}$$

X = Weighted Average
x= 1 or 0
w_i = Weight age

Analysis of Existing and Proposed Models

Hereafter listing the above mentioned features needed for analyzing and a representational art of selected models for Security, Authentication and access control are compared and drawn. The weight age values for various features and their average weight are being laid out here as shown in Table 1 and chart1 represents the comparison of average weight of every model.

Table 5: Weights are calculated for various models based on various features (F1 – F6).

Ref.No	Support for Multi Level Security	Support for Multi Factor Authentication	Support for Efficient User Access Control	Integrated Security, Authentication and User Access Control	Key distribution achieved without KDC	Support for Data Security at all the three levels	Total Weight
Weight age	2	3	4	1	6	5	
[26]	Yes	No	No	No	No	No	0.095
[27]	Yes	No	Yes	No	No	Yes	0.524
[28]	No	Yes	Yes	No	No	No	0.333
[29]	Yes	No	No	No	No	Yes	0.333
[30]	No	Yes	Yes	Yes	No	No	0.381
ISADA	Yes	Yes	Yes	Yes	Yes	Yes	1.000

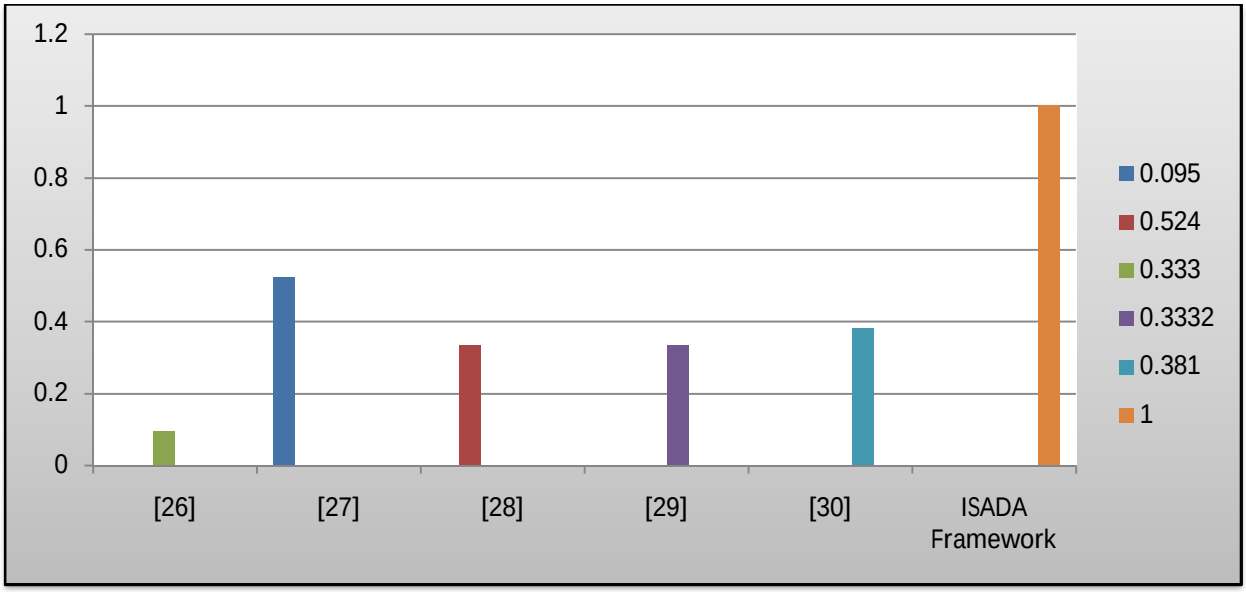

Chart 1: Weights for various models based on various features (F1 – F6).

Table 5& Chart 1 show the yes/no values for the various models for the above said properties. These values are being used to conclude for a better integrated framework to implement in a public cloud environment. Total weight for each model is calculated by using formula (1). At the end it has been proven that proposed integrated Secured, Authenticated and User Access Control framework achieves maximum weight compare to all other existing models so it leads to a decision that proposed integrated framework is more effective and secured one for public cloud infrastructure.

8. CONCLUSION

This proposed framework (ISADA) is thoroughly a well organized one for providing secure access control in cloud computing. This model assures secured, authenticated and authorized access control mechanism. It is a decentralized and user centric access control method. This framework achieves both security and access control in cloud computing. Registration is done by using inherence and knowledge factors of authentication which enhances first layer authentication. In the second layer this model only deals with data owner, consumer and cloud server. This framework ensures access control without the need of third party auditors and key distribution centre. This work provides a novel methodology for key management and double layer authentication meanwhile security is achieved in two steps that are shuffling and encryption. At the end it has been proven with the attack analysis, crypt analysis and efficiency analysis that Integrated Security, Authentication and Decentralized Access control (ISADA) framework based on novel key exchange mechanism is efficient, decentralized and prevent attacks for a public cloud environment.

REFERENCES

[1] Amol C. Adamuthe, Vikram D. Salunkhe, Seema H. Patil ,Gopakumaran T. Thampi , “Cloud Computing– A market Perspective and Research Directions”, I.J. Information Technology and Computer Science, 10, 42-53, , 2015.

[2] Prof Dr.Christof Weinhardt, Arun AanandaSivam, Dr.Benjamin Blau Borrisov, Thomos Meinl, Dr.JochenStober,”Cloud Computing – A Classification Business Models and Research Directions”, DOI 10.1007/s 12599-009-0071-2.

[3] Hatem M. Abdul Kader, Mohie M. Hadhoud, Salah M El-Sayed, DiaSalamaAbdElminaam, “Performance Evaluation Of New Hybrid Encryption Algorithms To Be Used For Mobile Cloud Computing”,International journal of technology enhancements and emerging engineering research, vol 2, issue .4 63 ISSN 2347-4289.

[4] R. BalaChandar, M. S. Kavitha and K. Seenivasan,”A proficient model for high end security in cloud computing”, Ictact journal on soft computing, volume: 04, issue: 02, January 2014.

[5] Raj Kumar, "Research on Cloud Computing Security Threats using Data Transmission", International Journal of Advanced Research in Computer Science and Software Engineering. Volume 5, Issue 1, January 2015.

[6] Smita Parte, NoumitaDehariya, "Cloud Computing: Issues Regarding Security, Applications andMobileCloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering. Volume 5, Issue 3, March 2015.

[7] ChangyouGuo, and XuefengZheng,"The Research of Data Security Mechanism Based on Cloud Computing ", International Journal of Security and Its Applications Vol. 9, No. 3 (2015), pp. 363-370.

[8] Rachna Arora, AnshuParashar,"Secure User Data in Cloud Computing Using Encryption Algorithms ", International Journal of Engineering Research and Applications (IJERA). Vol. 3, Issue 4, pp.1922-1926, Jul-Aug 2013.

[9] Randeep Kaur, SupriyaKinger,"Analysis of Security Algorithms in Cloud Computing ", International Journal of Application or Innovation in Engineering & Management (IJAIEM). Volume 3, Issue 3, March 2014.

[10] Vishal R. Pancholi, Dr. Bhadresh P. Patel, "Enhancement of Cloud Computing Security with Secure Data Storage using AES", IJIRST – International Journal for Innovative Research in Science & Technology| Volume 2 | Issue 09 | February 2016 .

[11] PankajPali,Saurabh Sharma," Security Model for Cloud Computing by using Data Classification Methodology", International Journal Of Innovative Research & Development. Vol 5 Issue 2, January, 2016

[12] Prakash Sawle, TruptiBaraskar," Survey on Data Classification and Data Encryption Techniques Used in Cloud Computing", International Journal of Computer Applications (0975 – 8887) Volume 135 – No.12, February 2016.

[13]RizwanaShaikha, Dr. M. Sasikumar,"Data Classification for achieving Security in cloud computing", Procedia Computer Science 45 (2015) 493 – 498.

[14] Lo"aiTawalbeh, Nour S. Darwazeh, Raad S. Al-Qassas and Fahd AlDosari," A Secure Cloud Computing Model based on Data Classification", First International Workshop on Mobile Cloud Computing Systems, Management, and Security. Procedia Computer Science 52 (2015) 1153 – 1158

[15]Shabana Ziyad and A. Kannammal, "A Multifactor Biometric Authentication for the Cloud", Computational Intelligence, Cyber Security and Computational Models, Advances in Intelligent Systems and Computing 246, DOI: 10.1007/978-81-322-1680-3_43, _ Springer India 2014.

[16]. Ga¨el Hachez, Francois Koeune, Jean-Jacques Quisquater,"BIOMETRICS, ACCESS CONTROL, SMART CARDS: A NOT SO SIMPLE COMBINATION", Work partially done within the European IST project BANCA.

[17]. R. Parimala, C. Jayakumar, "Providing Authentication by Using Biometric Multimodal Framework for Cloud Computing", International Journal of Computer Science and Information Technologies, Vol. 6 (5), 2015, 4507-4511.

[18] Giovanni L. Masala, Pietro Ruiu, and Enrico Grosso," Biometric Authentication and Data Security in Cloud Computing", Chapter-19,Springer International Publishing AG 2018 K. Daimi (ed.), *Computer and Network Security Essentials*,DOI 10.1007/978-3-319-58424-9_19.

[19] Yuvraj Gupta, "Enhancing Data Security in Cloud Computing", International Journal of Scientific & Engineering Research, Volume 3, Issue 12, December-2012 ISSN 2229-5518.

[20] Mohammed Nazi Abdul Wahid, Abdurrahman Ali, BabakEsparham and Mohamed Marwan,"A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention", Journal of Computer Science and Application technology.

[21] BIBIN K ONANKUNJU, "Access control in cloud computing", International Journal of Scientific and Research Publications, Volume 3,Issue 9, September 2013, ISSN 2250 -3153.

[22] Mansura Habiba, Md.Rafiqul Islam, A B M Sawkat Ali, "Access control management for cloud",12th IEEE International conference on Trust, Security and Privacy in Computing and Communications.

[23] Sonam Chugh, Sateesh Kumar Peddoju, "Access control based data security in cloud computing", International Journal of Engineering, Research and Applications (IJERA),Vol 2,Issue 3,May-June 2012, pp.2589-2593.

[24] Enrico Bacis,Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, Marco Rosa and Pierangela Samarati, "Access control management for secure cloud storage",Springer Berlin/ Heidelberg 2016.

[25] Biaokai Zhu Jumin Zhao Dengao Li Hong Wang Ruiqin Bai Yanxia Li Hao Wu,"Cloud access control authentication system using dynamic accelerometers data", Special issue paper 2018, willeyonlinelibrary.com/journal/cpe.

[26]

K.Sakthidasan@Sankaran,N.Vasudevan,V.R.Prakash and P.Kumara Guru Diderot, "Access control based efficient hybrid security mechanisms for cloud storage", International Conference on Communication and Signal Processing", April 4-6, 2019, India.

[27] Savanth Chintoju," An application for Decentralized Access Control Mechanism on Cloud Data Using Anonymous Authentication", Repository the St.Cloud State, St.Cloud State University, 12-2016.

[28] Jihad Qaddour, "Multifactor Biometric Authentication for Cloud Computing", the Seventeenth International Conference on Networks, IARIA – 2018, ISBN: 978-1-61208-625-5.

[29] Amit Vadwa,"Proposed Framework with Comparitive Analysis of Access Control & Authentication Based Security Models Employed Over Cloud ", International Journal of Applied Engineering Research, December 2017.

[30] Maheshkumar.M et al., "Rule Based Access Control System In Cloud Based Environment", International Journal of Advance Research, Ideas And Innovations In Technology, ISSN: 2454 – 132X, Volume 5, Issue 3, 2019.

[31] S.Ramalakshmi, V.Vallinayagi," Dual Shuffling Algorithm Incorporated With Blowfish (DS-BF) to Elevate Data Security in Cloud Storage", International Journal of Advanced Science and Technology", Vol 29, No 3, (2020).

[32] O.S.Abdul Qadir, Dr.G.Ravi, "Dual Objective Task Scheduling Algorithm in Cloud Environment", International Journal of Advanced Trends in Computer Science and Engineering, Volume 9, No.3, May-June2020, https://doi.org/10.30534/ijatcse/2020/07932020

[33] Olga I. Vaganova, Zhanna V. Smirnova, Ekaterina V.Vovk, Anastasia A. Kapina, Elena A. Chelnokova, "Comparative analysis of Cloud Technologies", International Journal of Advanced Trends in Computer Science and Engineering, Volume 9, No.3, May - June 2020, https://doi.org/10.30534/ijatcse/2020/12932020.