International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 24 (2017) pp. 15715-15722

Proposed Framework with Comparative Analysis of Access Control & Authentication based Security Models Employed over Cloud

Amit Wadhwa[1]
Research Scholar, Department of Computer Science & Engineering,
JaganNath University, Jaipur, Rajasthan, India.
Orcid Id: 0000-0002-1736-4850

Vinod Kumar Gupta[2]
Research Supervisor, Department of Computer Science & Engineering,
JaganNath University, Jaipur, Rajasthan, India.

Abstract

Cloud computing is a booming technology defined as abstraction of different computing resources as like hardware or software provided over a network in the form of a specific service. It's a rapidly emerging technology in the market from quite some time now and considerable research work related to its security perspective are going on it. Security of data present over a cloud and accessible to CSP has been considered as a major issue in recent times. These types of services could end up with attacks or threats like malicious insider attack, Man in middle attack and dictionary attacks to name a few. Apart from this providing security to data revolving around the cloud environment is governed with access control security provisions or models implemented over a cloud. In the past, several authors have presented various access control and user authentication models or schemes which are being used over cloud based environments and were either providing secure access control or authentication based security. Some proposed frameworks also provide combination of both access control and authentication based security models which were not that efficient or secure. Here in this paper, initially major access control models and authentication schemes proposed earlier for a cloud environment are analyzed and compared over selected characteristics. Secondly, a Multi-Security Level Based Authentication and Access Control Model (i.e. MLBAAC) is proposed here followed by its hypothetical analysis on above selected characteristics.

Keywords: Cloud Computing(CC), Access Control, Authentication, Security

INTRODUCTION

As per the NIST definition of cloud computing it's a phenomenon of on demand network access providing access to a shared pool of resources which can be easily configured and provisioned with minimal effort. The vast area and domain of Cloud computing is being rapidly growing over the years which has revolutionized the use of information technology in today's environment. Millions of its customers are benefitted by adopting it across their infrastructure. As the field is vast growing and rapidly evolving so it encounters a lot of challenges related to security of its critical as well as non-critical data. Main issue is that, data is being stored over third-party premises, requiring access to it through an authorized and secure platform.

In today's challenging environment of technology, day by day a lot of emerging security challenges or issues have been faced by Cloud Computing, where leakage or loss of critical data, its privacy, account/service based attacks like insider attacks or hacks and other vulnerabilities are major ones to make out. Various security issues affect every prospect of this technology, prospects like Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) are among them. All MNC's like Google, Microsoft and IBM are providing cloud based solutions to the people through these service delivery models. As all these service delivery models are facing challenges of security threats so it's important to provide a secure access of cloud services to its users through these delivery models. And not only security of data and services is important looking at customer's perspective but also authenticating right user to be able to access right set of services is also a major area of concern for Cloud service providers.

The paper has been organized or arranged as follows: initially the problem or issues related to data access control and authentication are discussed followed by an overview of some techniques for data access control and authentication mechanisms. Next section discusses about recent literature consisting of models and techniques presented in some of the earlier published work related to access control and authentication based security over a cloud. Then next section focusses upon identifying and defining certain required and important features or properties which could be used for modelling and analyzing a secure cloud based system. Properties identified are further used for making a theoretical analysis and weighted analysis of various models and techniques discussed, for providing data access control and authentication related security over a cloud. In next section, proposed multi-security model (i.e. MLBAAC) of access control and authentication based protection for securing cloud processes and critical data is being presented. Later in end, the proposed model is analyzed based on properties discussed above and a conclusion is made based on the analysis drawn.

Major Problems Pertaining to CC Environment

Problems prevalent in field of Cloud Computing related with data access to be handled securely and requirement for need of providing better access control and authentication based mechanisms:

i. No Transparency and Data Control[1]: Once data is on third party server, control of its movement is not with user, its only with service provider (Cloud Service Provider i.e. CSP) and if some data loss happens then user is unaware about it till it tries to access that data again sometimes later. As transparency to accessing user's data is absent so user don't know about the time, place and procedure by which the data is processed [1]. Its being the need of the hour that systems required the knowledge of what happens with the data over cloud or any third-party premises. If transparency is not their then it might incur huge loss of data [1].

ii. Dependency on CSP and Trust Related Issues [1]: If there is an issue with the CSP, user services might get affected and he/she can't do anything about it as generally there is no contract laid between CSP and service receiver i.e. user [1]. As there is no contract so user is bound to provider as changing provider won't be easy and would be a difficult task at that point for user. If further any problem arises, user have no proof to ask CSP about the issues

Considering these issues and challenges, access control and authentication based security has become an important issue to look forward and take seriously for both, cloud providers and users. Considering these issues and their seriousness over cloud implementation different access control algorithms and frameworks have been formulated and put forward by many researcher's, providing an effective solution for all access control problems of cloud users but still there is scope for improvement where a better and more effective framework could be designed considering these issues.

Apart from using different access control mechanisms there are various user/service authentication mechanisms used to provide trustworthy and authorized access to the cloud environment. One of the commonly used authentication mechanism[2] is password-based in which users provide the password to access their accounts. The technique of using passwords is so simple thing that most of the time it comes out to be vulnerable to dictionary or Man in the Middle attacks[2] to name a few.

Considering these requirements, this paper focusses on providing an effective framework suitable for and addressing both the security chucks. Further to it, this paper gives an insight about different access control and authentication mechanisms being deployed and adapted across many organizations working in cloud environment. So, major focus of this paper is providing a comparative theoretical analysis of different access control mechanisms adopted and presented by users and their shortfalls, along with it various authentication mechanisms being formulated for secure access to cloud environment. The algorithms or techniques presented earlier as well as proposed afresh in this paper are compared on certain considered parameters with specific weightage for making the hypothetical analysis.

OVERVIEW OF ACCESS CONTROL AND AUTHENTICATION MECHANISMS

Here in this section, various access control and authentication mechanisms currently being followed and provisioned over cloud are discussed.

Access Control Mechanisms

i. Identity based encryption/authentication [1]: Identity based encryption or authentication is a public key cryptography based technique in which a private Key generator is used. It generates a pair of keys known as master keys [1], i.e. public key and private key. For generating public key its created and made unique by fetching and using unique information relating to user. With the unique Private key generated using the private key generator a user can decrypt the file. User identities are being identified using private key generated as output of private key generator. The only major drawback of this technique is that the private key generator should be online all the time and must be trusted for generating unique private keys and supposed to not retain them.

ii. Role based model [1]: Here in this type of model for access control security data owner is the one which has control over who can have access to its data which is encrypted by user at its end before uploading it over a cloud. Role are being assigned to cloud data users keeping in mind the responsibilities and user qualification required to achieve this. Special roles are assigned with set of permissions only to specialized designated users to have data access. Role assigning to user is the responsibility of role manager and in case of discrepancy revoke it from the user [1]. So, unauthorized users are identified using roles with their specialized assignment and dependency.

iii. Attribute based Encryption [1]: In this encryption scheme, to quantify and analyze user identity and for encryption and decryption processes a group of attributes are used. Authorized agent generates public key and master keys as per attributes of the user [1]. Data encryption using public key is performed by its owner, and user private key would be used for data decryption. As per the encryption scheme discussed here the access policy has been classified into two types as- key-policy attributes based encryption and cipher text policy attributes based encryption [1], [2]. Further to it, advantages for the approach are reducing communication overhead in network and providing fine grained level of access control.

iv. Key-Policy based Encryption: In this encryption

scheme, it requires an association or linkage between the encrypted text and set of attributes, trusted authority issues a private key[1] whose access structure is like a tree and which describes this user's identity [1]. The data file of user could be only recovered if encrypted text attributes are satisfied by access policy in private key. This type of technique could be not justifiable or suitable for some requirements of systems where data owner doesn't have trust or having trust issues with key issuer and where there are scalability issues with levels of attributes.

Authentication Mechanisms

i. Simple Authentication Framework: This type of authentication requires the use of simple password based technique for authorized access to the user areas or services [3]. But analysis shows that these design and techniques are vulnerable to man in the middle attacks and some sort of dictionary attacks. Considering this it was not adjudged as the possible solution for many domains over cloud and its environments.

ii. Anonymous Password Mechanism: In this mechanism, the user without revealing about its identity tries to connect to the server in an anonymous way and thus preventing easy un-authorized access and which thereby securing it from the dictionary attacks [3]. Though, probability of guessing attack is still possible in these types of systems.

i. Biometric Authentication: It uses a technique where user's biometric traits are used as replacement for passwords. Biometric traits could be iris or facial features [3]. In these systems, ideal or authorized user detection and authentication requires the system to check for either of face, iris or fingerprints considered as biometric traits. Accuracy could be affected by altered facial expressions or dirty fingers of user accessing his information [3]. For this requirement is that system should be trained to record and match corresponding biometric traits requiring high data storage.

ii. Smart Card Authentication: This requires use of smart cards for securing highly sensitive data or information. In one of the solutions proposed by one author it requires the use of password, smart card and public key technique for authentication and key distribution [3]. Advantage of the technique would be to ease out the issue or burden of remembering long length difficult passwords. The main disadvantage is that if the smart card is lost then there is no security provided in that circumstances [3]. Also, it's a costly solution issuing and creating smart cards for each user.

LITERATURE REVIEW OF SOME MODELS

This section focusses upon and gives light onto various earlier presented models or techniques on access control and authentication or a combination of both. In the past, many different models or techniques have been proposed by researchers over the years giving idea about the vast nature and scope of the area of concern.

F. Fatemi Moghaddam in 2014 proposed a scalable and efficient user authentication scheme for cloud environments. It presents a client based user authentication model for confirming about the identity of user [4]. It uses a plugin (client based user authentication agent) installed on user's web browser downloaded from service provider's website with a unique code [4] for installing extension on web browser, thereby effectively confirming the identity of user without much dependency on the service provider's server. Apart from this it also uses a Modified Diffie Hellman Agent [4][1,2] to allow unregistered devices to access cloud servers. It also uses a cloud based SAAS application for confirming with the process of new device registration [3]. User authentication and encryption process burden is removed from main server by servers independently used for storing authentication and cryptography resources. Cryptography agent was also used to encrypt the resources before storing on server using Hybrid encryption algorithm based on RSA [4]. Advantage of the whole system is enhanced reliability and rate of trust on cloud based environments. It provides features of scalability, efficiency and security. Security is provided by securing system for Man in Middle attack, Brute Force Attack and Timing Attack [4].

Auxilia M. and K. Raja in 2014 discussed various access control models also one proposed for dynamic access control. It uses various rules laid down earlier for providing access to cloud user data being used in various access control models[5]. Various access control models discussed are MAC (Mandatory Access Control), DAC (Discretionary Access control) and RBAC (Role Based Access Control) [6]. It proposes a dynamic access control model which is based on interrelationship between data requestor, Data requested and action being performed on data [6]. These features are stored in form of access control policies on cloud environment. Then the theoretical analysis of interoperability support is made for various models discussed with proposed dynamic model for access control and it was found out that adopting DAC approach would result in very high support for interoperability among various entities.

S. Niu et. al. in 2015, presented a scheme providing effective and secure access control mechanism or system. It's designed to work for securing access control systems [5]. And for that a comprehensive framework for access control based on attribute encryption is presented for use with lightweight devices adopting cloud platform or resources to outsource encrypt and decrypt operations. It uses the principle of CP-ABE[5] (Ciphertext policy-Attribute Based Encryption), [6, 7] scheme proposed earlier by Ren. K, et. al. and uses following attributes like ESP, DSP and SSP thereby achieving encryption and

decryption processes and moving their computational task to cloud environment [5]. Using this approach moves the burden of encryption and decryption computation task from user to cloud environment, thereby reducing the computation requirements for user terminal and providing a secure access control process. The system allows to perform performance evaluation of the system having separate encryption and decryption procedures to move computation cycles to cloud environment.

G. P. Kanna et. al in 2016 as author for the work presented an approach for enhancing the security of outsourced cloud data using keyword encryption and hybrid cryptography technique [2]. It compared encryption, decryption, execution and throughput time for specifying the results. It proposes an identity based hybrid encryption method (RSA with ECC) [2]. Final comparison is being made between proposed technique of identity based hybrid encryption method and simple IBE[8,9] [2] (Identity Based Encryption Scheme) which is further configured using hybrid encryption and proxy re-encryption techniques. The idea is to encrypt the data before storing onto cloud and for this initially user identity is used to encrypt the user data along with hybrid encryption algorithm[2]. Then the receiver identity and keyword for ciphertext generation is encrypted using proxy re encryption and sent to receiver along with things generated at first step.

F. Rehman et. al. in 2016 presented a work on passphrase based authentication framework to be implemented over cloud [3]. It provides a comparative analysis of various multifactor authentication techniques and security frameworks adopted on cloud platforms. Also, presents three factor paraphrase based authentication model for secure authentication[3,10,11,12] Initially using private-public key pair system user's request is generated and private key is made secure over network using a passphrase (a random phrase acting as password or key which is hard to guess by anonymous intruder). After that for secure authentication one time authentication request is pushed to user's mobile device having a secure mobile application to approve access to cloud environment. Here, apart from normal procedures for protection a passphrase[3] method is also adopted for providing additional security to public private key pairs which in turn makes it more useful and less vulnerable than previous approach described above.

Form this review of various techniques of access control and authentication one can conclude that none of these models had focused upon a specific user access control framework or model. Leading to this, we are motivated towards providing a better and specific access control framework which would be specifically focusing towards a new dimension towards access control security.

ANALYZING DISCUSSED MODELS AND TECHNIQUES

Based on the above discussed literature for access control and authentication frameworks or models, this section initially focusses on defining certain features or characteristics that could be used for drawing the analysis of various models and frameworks discussed along with the one proposed for providing a better solution based on identified features. Features are being identified through the literature and some of the other systems discussed and presented in past for providing a secure and sound access control and authentication based system. Features are categorized under two umbrellas: To start with there are, approach and system design based features while others are the system supporting certain characteristics or not.

Following are the listed features or properties (from P1 to P9) to be considered:

- P1 - Simplistic Approach: It specifies the order of simplicity of system's operation for the technique or model under consideration.
- P2 - Efficient System Design: This parameter considers how much feasible and efficient the system design is to be implemented over a cloud.
- P3 - Working Complexity: It identifies how complex the system design is and how much complex is the working principle of the model or approach.
- P4 - Practical Feasibility: It tells about the practical feasibility of the system model or design. Checks for is the design practically feasible to be implemented or not.
- P5 - Supporting Choice Based Security: It tells user about whether it's a system supporting choice based security or not as an advantage.
- P6 - Supporting Enhanced Authentication: This property is about whether enhanced level of authentication is supported by system or not.
- P7 - Support for Security levels: It specifies that whether the model allows for support for varied security levels or not.
- P8 - Support for Efficient User control: It qualifies the system supporting efficient user access control.
- P9 - Integrated Access Control and Authentication Support: It signifies that whether the system or model is providing integrated support for both access control and authentication or not.

These above discussed nine features are used here in this work or the analysis and drawing a suitable conclusion as which model would serve better for implementing it over a cloud environment. Prospective values chosen for every property discussed above are: Low, Moderate, High, Very High with weights being assigned from 1 to 4 respectively. In case where the property is not supported by any of the considered models, the NO or N.S. (not supported) would be the value assigned for it having a weight 0 associated with it. So, for a model to be found as effective and better as compared to other in consideration, weighted summation of these values would be done for each of the models and based on it analysis will be drawn. The model with highest value of W^m would be assumed as best among all. There is an exception to the above rule of

weight assignment for complexity feature as low complexity is presumed better for a model to be adopted. So, for the complexity property the weights assigned are in reverse order of the one mentioned above for other properties.

Total weight for model is calculated by following formula:

$$W^m = \sum_{k=1}^{n} p^k * wi^k \, , \forall \, (0 \leq wi \leq 4) \ldots\ldots\ldots\ldots (1)$$

where in this equation,

W^m – total weight calculated for model/framework 'm'

p^k – property under consideration with $1 \leq k \leq 9$

wi^k – weight associated with considered property

Analysis of Models and Techniques

Here after listing the above features required for analyzing and depicting a summative analysis of our selected models for authentication and access control, a comparative analysis of the various access control and authentication based techniques or models under consideration is being drawn. The values for various properties corresponding to various algorithms or techniques and their weighted assignments under consideration are being laid out here as shown in the Table 1 and Table 2 respectively,

Table 1 Comparative analysis of Various Authentication and Access Control models

Models	Features								
	Simplistic approach	**Efficient System Design**	**Working Complexity**	**Practical Feasibility**	**Supporting Choice Based Security**	**Supporting Enhanced Authentication**	**Support for Security levels**	**Support for Efficient User control**	**Integrated Access Control and Authentication Support**
Simple Authentication Framework	High Simplicity	Moderate	Low	Very High	NO, (Not Supported)	NO, (Not Supported)	NO, (Not Supported)	NO, (Not Supported)	NO, (Not Supported)
Anonymous Password Authentication	High Simplicity	Moderate	Low	Very High	NO, (Not Supported)	Yes, (Low Support)	Yes, Low	NO, (Not Supported)	NO, (Not Supported)
Biometric Authentication	Low Simplicity	Low to Moderate	High	High	NO, (Not Supported)	Yes, (Moderate Support)	Yes, Moderate	NO, (Not Supported)	NO, (Not Supported)
Smart Card Authentication	Low Simplicity	Low to Moderate	Moderate	Moderate	Yes, (Low Support)	Yes, (High Support)	Yes, Moderate	NO, (Not Supported)	NO, (Not Supported)
Password-based Two Factor Authentication	Moderate Simplicity	Moderate	High	Moderate	Yes, (Moderate Support)	Yes, (High Support)	Yes, Moderate	NO, (Not Supported)	NO, (Not Supported)
Scalable and Efficient User Authentication Scheme	Moderate Simplicity	Moderate	High	High	NO, (Not Supported)	Yes, (High Support)	Yes, Low	Yes, High	NO, (Not Supported)
DAC[6] (Discretionary Access Control)	Moderate Simplicity	Moderate	Low	Moderate	Yes, High Support	NO, (Not Supported)	Yes, Moderate	Yes, High	NO, (Not Supported)
MAC[6] (Mandatory Access Control)	Low Simplicity	Moderate	High	Moderate	Yes, Moderate Support	NO, (Not Supported)	Yes, Moderate	Yes, Moderate	NO, (Not Supported)
RBAC[6] (Role Based Access Control)	High Simplicity	Moderate	Moderate	Moderate	Yes, High Support	NO, (Not Supported)	Yes, Moderate	Yes, Very High	NO, (Not Supported)

Table 2 Weights Calculated for Various Models Based on various properties (P1 to P9)

Models	Properties with Weight Assignments									
	P1	P2	P3	P4	P5	P6	P7	P8	P9	Total Weight, W^m
Simple Authentication Framework	3	2	4	4	0	0	0	0	0	13
Anonymous Password Authentication	3	2	4	4	0	1	1	0	0	15
Biometric Authentication	1	2	2	3	0	2	2	0	0	12
Smart Card Authentication	1	2	3	2	1	3	2	0	0	14
Password-based Two Factor Authentication	2	2	2	2	2	3	2	0	0	15
Scalable and Efficient User Authentication Scheme	2	2	2	3	0	3	1	3	0	16
DAC (Discretionary Access Control)	2	2	4	2	3	0	2	3	0	18
MAC (Mandatory Access Control)	1	2	2	2	2	0	2	2	0	13
RBAC (Role Based Access Control)	3	2	3	2	3	0	2	4	0	19

Table 1 above shows the prospective values assigned to various models for said properties and is being used to draw a conclusion for a better model for cloud. As shown in the above Table 1 the models or techniques discussed here are not satisfying many of the properties under consideration. Apart from this if all these models and techniques are analyzed based on weighted values of properties mentioned earlier and total weight is being calculated as per formula given in equation (1), for most of these, weighted values for the associated techniques or frameworks are not even above 20 or are just near 50% of the maximum weight which could be assigned. So, it shows that there is a lot of scope for improvement in those areas where these models are lacking. A better and more effective and secure framework could be proposed which could satisfy most of the properties discussed above.

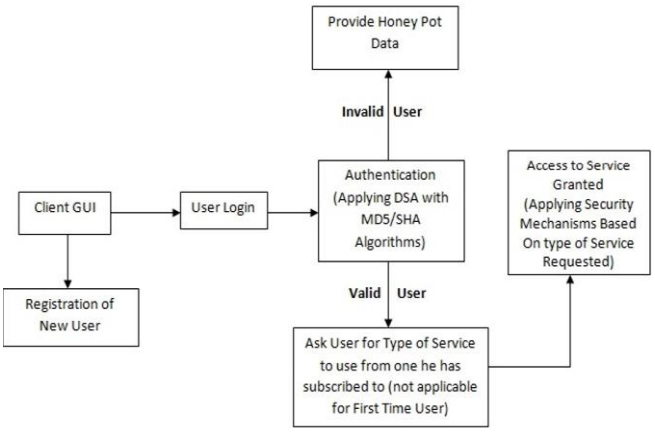

Figure 1: Suggested Framework relating MLBAAC Model [11]

PROPOSED MLBAAC MODEL AND ITS ANALYSIS

Here in this section a better and effective framework is being proposed to be implemented over a cloud environment providing the integrated access control security and secure authentication for cloud users. The proposed MLBAAC (i.e. Multi-Security Level Based Authentication and Access Control) Model is a security model or framework for providing Authentication and access control security using multi-level security approach. It provides various set of features employed at different levels to provide users with multiple levels of security. Apart from providing security for user's data at user view level it also stresses upon providing security to data at CSP view level. This means that the CSP files containing user related information like user's area based access credentials generally secured with cryptographic techniques would now be secured using a new proposed mechanism. So, to support and satisfy the above scenario a secure model or approach is being proposed here with features as depicted in Figure 1 below:

Features of "MLBAAC" Model

Technique used for "Multi-Security level based Authentications and Access Control Model" (MLBAAC) depicted by Figure 1 employs following features, as discussed here:

i. uses approach for digital signature and cryptography for secure authentication and data security.

ii. provides multiple security levels to cloud services and supports switching among them for enhanced security.

iii. provision for distributed, one time access key sharing mechanism (multi key division based authentication and access control with distributed access key distribution).

iv. option for service barring in unauthorized attempts.

v. choice based security provisions for sensitive and non - sensitive data.

vi. protection for critical and highly confidential or sensitive data

vii. randomized extension varying approach for critical CSP files having CSP view for confidential data

viii. Securing confidential data from database hijacking attacks

(making data of no use to hijacker using honey pots), faking identity of data for basic guessing attacks

ix. prevention man in middle attack using distributed key distribution model, prevention of malicious insider attack (helps to maintain Security of data maintained over a cloud with third party).

After laying out all these features, the proposed technique or model is analyzed based on the properties P1 to P9 as shown in Table 3,

Table 3 Analysis of MLBAAC model on suggested/selected properties

Property	MLBAAC Model	
	Value	**Description/Validation**
P1	Low Simplicity	It depends upon many access control layers or levels making it a less simpler approach.
P2	Moderate	System design is moderately supported and moderately feasible to plan.
P3	High to Very High	Requires or possess different levels of access increasing complexity from high to highest.
P4	Moderate to High	Practical feasibility is supported as a need for different level of security is desired.
P5	Yes, Very High Support	Provides very high support for Choice based security with different levels.
P6	Yes, High Support	Supports enhanced multi-layer authentication level using ASE and SHA
P7	Yes, Very High	Supports different Levels of security like Honey-Pot data and secured CSP data.
P8	Yes, High	Efficient User control is also provided with higher level
P9	Yes, High	Both techniques like access control and authentication are supported, providing integrated environment.
Total Weight = 24/36, i.e. approx. ~ 66.67%		

So, based on analysis of proposed model and weight assignment for defined properties, comparing it with other models by observing the total weight calculated for them as shown in Table 4 here,

Table 4 Comparison of Proposed Model with others based on Weight, W^m

Model/Technique	Total Evaluated Weight, (W^m)	Percentage Weight (in %)
Simple Authentication Framework	13	36.11
Anonymous Password Authentication	15	41.67
Biometric Authentication	12	33.33
Smart Card Authentication	14	38.89
Password-based Two Factor Authentication	15	41.67
Scalable and Efficient User Authentication Scheme	16	44.44
DAC (Discretionary Access Control)	18	50
MAC (Mandatory Access Control)	13	36.11
RBAC (Role Based Access Control)	19	52.78
Proposed MLBAAC Model	24	66.67

This above analysis as shown in Table 4 suggests that the proposed model i.e. MLBAAC, if properly implemented would prove to be an effective and efficient solution for security over the cloud based environment.

CONCLUSION AND FUTURE DIRECTIONS

The paper discusses some of the existing authentication and access control techniques or models implemented over cloud architecture. Also, it discusses and defines properties which could be considered for effectively comparing and analyzing the discussed technique or models. Further we also proposed and discussed a multi security level based model, MLBAAC, providing both access control and authentication level security over cloud. The model also made-up to provide protection from man in middle attacks, malicious insider attacks, faking identity attacks and database hijacking attacks. The idea was further analyzed and conclusions are drawn coming out to be favoring the proposed solution providing better weight percentage compared to other discussed techniques or models. Further in future the simulations for the proposed model could be worked out using suitable cloud simulation tools like CloudSim or

Cloud Analyst, which could justify the model in more admissible way. Apart from this some other cryptographic algorithms or key distribution criteria could be chosen based on possible advantages to gain out of it.

REFERENCES

[1] R. Charanya and M. Aramudhan, "Survey on access control issues in cloud computing," *2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)*, Pudukkottai, 2016, pp. 1-4

[2] G. P. Kanna and V. Vasudevan, "Enhancing the security of user data using the keyword encryption and hybrid cryptographic algorithm in cloud," *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, Chennai, 2016, pp. 3688-3693

[3] F. Rehman, S. Akram and M. A. Shah, "The framework for efficient passphrase-based multifactor authentication in cloud computing," *2016 22nd International Conference on Automation and Computing (ICAC)*, Colchester, 2016, pp. 37-41

[4] F. Fatemi Moghaddam, S. G. Moghaddam, S. Rouzbeh, S. K. Araghi, N. M. Alibeigi and S. D. Varnosfaderani, "A scalable and efficient user authentication scheme for cloud computing environments," *2014 IEEE REGION 10 SYMPOSIUM*, Kuala Lumpur, 2014, pp. 508-513

[5] S. Niu, S. Tu and Y. Huang, "An Effective and Secure Access Control System Scheme in the Cloud," in *Chinese Journal of Electronics*, vol. 24, no. 3, pp. 524-528, 07 2015

[6] Auxilia M and K. Raja, "Dynamic Access Control Model for Cloud Computing," *2014 Sixth International Conference on Advanced Computing (ICoAC)*, Chennai, 2014, pp. 47-56

[7] S. Vishnupriya, P. Saranya and A. Rajasri, "Secure multicloud storage with policy based access control and cooperative provable data possession," *International Conference on Information Communication and Embedded Systems (ICICES2014)*, Chennai

[8] L. Gadhavi, M. Bhavsar, M. Bhatnagar and S. Vasoya, "Design of efficient algorithm for secured key exchange over Cloud Computing," *2016 6th International Conference - Cloud System and Big Data Engineering (Confluence)*, Noida, 2016, pp. 180-187

[9] S. Manjula, M. Indra and R. Swathiya, "Division of data in cloud environment for secure data storage," *2016 International Conference on Computing Technologies and Intelligent Data Engineering (ICCTIDE'16)*, Kovilpatti, 2016, pp. 1-5

[10] V. K. Pant, J. Prakash and A. Asthana, "Three step data security model for cloud computing based on RSA and steganography," *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, Noida, 2015, pp. 490-494

[11] A. Wadhwa and V. K. Gupta, "*Framework for User Authenticity and Access Control Security over a Cloud*," in International Journal on Computer Science and Engineering, vol. 06, no. 04, pp. 138-141, 04 2014

[12] M. K. Ibrahem, "Modification of Diffie-Hellman Key Exchange Algorithm for Zero Knowledge Proof," in Proc. International Conf. on Future Communication Networks (ICFCN), Baghdad, Iraq, 2012, pp. 147-152