

A Well-Organized Model in Cloud Computing Platform for Data Accessing



T.R.Saravanan, K.Uma, C.RameshKumar, M.Basha Khaja

Abstract: *Cloud Computing is a trending technology. The main benefit is user will pay only for the resources which have been utilized in the cloud services. Data which are stored in cloud can be accessed by the people from anywhere in the world using internet connection. Because of difficulties in data access and lack of security, in the current database system people are moving to Cloud Service Provider (CSP). Network backup and recovery method are used in CSP so there is no data loss in case of hardware failure. In this paper, we planned an efficient model in cloud computing for data accessing which will reduce the search time of providing the public key of the data owner. Not only data storage and security, data access also plays an important role to consume less time. So, in this proposed system we are going to increase the time efficiency for the data accessing.*

Keywords: *Encryption, Data decryption, Data Storage, Cloud service Provider, Data access protocol.*

I. INTRODUCTION

In IT sector, utilization of the cloud computing progressively increased. It allows the consumer to obtain the services when they are requested for it. In this environment, consumers are not concerned about the hardware and software. Nowadays, cloud computing approaches are used for developing most of the business models. It has three important unit particularly cloud service provider (CSP), consumer and owner of the data (DO). Network services are offered and handled by the CSP. Data are stored in the cloud server by DO and for retrieving those data, consumer should send request to the server. In the cloud server crucial problems are created by the hackers. If we try to implement cloud environment using ACM, then it will lead us to number of issues like high cost for searching, system overhead, data accessing time will be high. According to the requirement, we have proposed new efficient model for data accessing in the cloud computing. Each user profile is recorded in the CSP. User profile will be based on the interest of the user in

the cloud server. For monitoring user profile, the temporary list which is maintained by CSP that supports fast data accessing. When users want to access data he/she will make a request to the server. A query is executed by the CSP that matches the data type in the available list with the data type requested by the user for identifying the public key of data owner (PKOWN). If we get the correct match of the data type, data owner can be found quickly, we will issue the PKOWN to the user. CSP doesn't look for PKOWN in the whole Dos which will result in low searching time. After finding the PKOWN, User will simply ask for secret key and authorization it easily. In this way data accessing time will be minimized automatically.

II. PROPOSED METHOD

UCON [1] is a theoretical model which provides ability of making decision to the users. It contains all the benefits of the traditional ACM. Negotiation module is involved in this UCON for improving the flexibility of the service. When request of the user is not matched with the access policy, request of the user is not aborted immediately. It will offer a further chance to access data [10][11]. Data access request is acknowledged as per the attributes of the user. Meaningful attributes are assigned to data. Access tree is used for characterizing each user's access structure. For managing the key dummy attribute is used in ABAC. All the jobs are handled by the CSP. User access rights are kept secret and user secret key responsibility are achieved [2]. CSP maintains the purpose tree. Edges display the relationship between the purposes. If users want to access data from cloud server, access purpose have to match with intended purpose. Request for accessing data is approved only if access purpose and intended purpose are matched [3]. In TTAC[4] concentrates on security mechanisms of the data. Before storing the data into the cloud, data owner uses access policy for encryption [12]. On receiving the request for data access, it checks whether temporal constraint is fulfilled in policy P concerning with current time (tc). Authorized user will use their private key with access rights to decryption. The advantages of TTAC are flexibility, supervisory and privacy protection. TTAC restrict the user's access privileges by allocating time for data access [13]. In GBAC[5] [7], based on the secure gateway it proposes private virtual cloud. Each user gets validated in own cloud to achieve peer cloud access. Using third parties, it will provide protected communication path for user to communicate with other cloud. Gateway methodology is used construct the secured path [14].

Revised Manuscript Received on December 30, 2019.

* Correspondence Author

T.R.Saravanan, Department of CSE, Jeppiaar SRR Engineering college, Chennai-603103,

K.Uma*, School of Information Technology and Engineering, VIT University, Vellore, India,

C.Ramesh Kumar, School of Computing Science and Engineering, Galgotias University, Uttar Pradesh, India.

M.Basha Khaja, Wipro Technology, Software engineer, Ireland, United Kingdom,

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an [open access](http://creativecommons.org/licenses/by-nc-nd/4.0/) article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

It will search for the file in complete database which will increase the search time and maintaining cloud database is complex [15][16].

In AACM [6][8] [9], discuss about various access control methods used in cloud. It speaks about who provides access to data, advantages and disadvantages in those methods [17]. Only authorized users can obtain data from the cloud server and unauthorized users are denied from accessing the data [18].

III. PROPOSED METHOD

A. System Model

- It contains CSP the main handler who provides place to store the data and other facilities of cloud to data owners, the operators(users) who may use the cloud, by help of n no. of servings with finite space and potential.
- Data owners, they use the cloud database for storing their data and files. Cloud Service
- Users(Operators), Individuals who wants to retrieve the data as well as any kind of document or any needed accessibility from the Cloud Service Provider. They should authorized themselves by Cloud Service Provider, So only the authorized users have the right to access or communicate with the server. The Architecture of the system is shown in Figure 1.

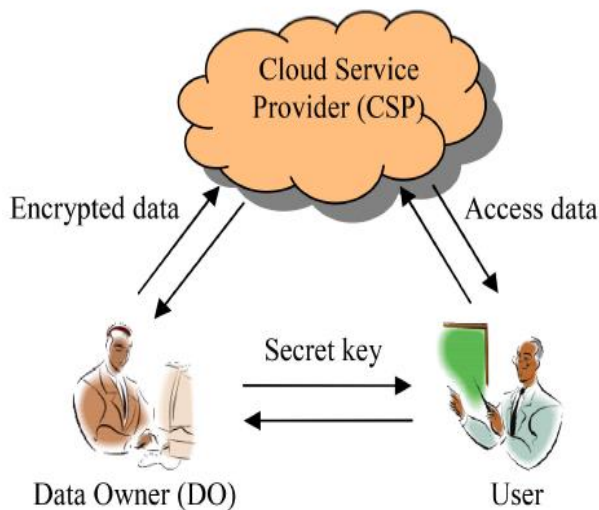


Fig.1. The proposed system Architecture

The proposed system has various steps for storing data,

1. Data is encrypted by the DO using secret key
2. Individual private key of the DO is used then uses the service provider's public key for data encryption.
3. Secret key is distributed with authorized users only.

In the proposed model, data owner comes to online for issuing the secret key and authorize to the users and after issuing authentication details DO will go offline. Data owners are not recommended to be online all the time. Because of this, system overhead is minimized. Temporary list is maintained for monitoring the user's profiles which will help in database maintenance.

B. Objective

Main goal of work to be done is to minimize the time of finding the file or data in cloud; so that the cloud service provider could provide the DOWN in minimum time with this the working or taking the data from the cloud time should be minimum. the operators can pay a few to get the service from the cloud which they want to access .Cloud Service Provider is responsible for monitoring and maintaining the databases in a well-organized way.

IV. METIERIALS AND METHODS

Here in this scheme, Cloud Service Provider keeps a OWN Table (OWN_LIST) basically made with the Operator's profile, which includes number of five columns.

Operator Group (OPR_GROUP): Number of groups which are in the OWN_LIST.

Operator ID (OPR_ID) : the ID of the operators who accessed same type of data item with same format or kind of similar data.

Data Format: contains the format of the data such as JPEG, PNG, MP3, etc.

Operator Group time and Date (OPR_GROUP_T&D):The time and date on which specific Opr_GROUP is made.

Operator time and date (OPR_T&D): last time accessed data time of an operator.

In these five fields OPR_ID is least recently used column. For reducing the accessed time in a cloud and making it fast OWN_LIST is used .For operating the data , operator should be authorized ,ID plays an important role while searching the operator in OWN_LIST. Because of the data type the time is reduced and there is no need to search the entire database so that the operator can be found easily and fast. The time is reduced by using OWN_LIST. Table shows the discussed columns. Main Operations on OWN_LIST in proposed scheme are operator authorizations which are to be made on the data, operations performed on the OWN_LIST, storing of data and using or accessing the data as shown in Table 1.

A. User Authorisation

The operators which have registration in cloud can only have the right to access data. Operators first send the registration request to the cloud service provider. Operator is authenticated by his/her digital signature and CSP collects operator's all important information. Acknowledgment of registration is sent by the CSP. After this, DOWN is provided to the operators by CSP, with DOWN they ask to the Data Owners to fetch the key which is secret to all known as secret key and certification. Data owners cross check the operator's authenticity from the CSP. Data owner will only send the Secret key and certification if the operator is authorized, if not data owner will reject the request made by them.

B. Data Storage

For storing data some techniques is there, which are at data owner's end and CSP's end. They are as follows:

Data Owners: Storing of data, a secret key is generated by data owners, encryption of data is done with the help of secret key and encrypt with PRKDO.

Data owners again perform the encryption to the full message with the help of PBK, and a bunch is made of 3-layers of encryption method:

- Secret key is used by data owners to encrypt.
Data → ECsck (Data)
- DOs use the PRKDO to encrypt ECsck (Data).
ECsck (Data) → ECPRKDO {ECsck (Data)}
- At the end, DOs uses the PBK to perform encryption ECPRKDO {ECsck (Data)} and certifies. A bunch is made by owners of data DO and received by CSP
- CSP: As soon as Cloud Service Provider gets the bunch from data owners, they perform the decryption by using PRK. Again, the bundle is decrypted using DOWN.
- The CSP performs decryption on the bunch by utilizing the PRK.

- ECPRKDO {ECsck (Data)} and Cert ← DCPRK [ECPBK [ECPRKDO {ECsck Data and Cert}]
- Once more the CSP uses the DOWN to perform decryption on the bunch.
ECsck (Data) and Cert ← DCDOWN [ECPRKDO {ECsck Data}] and Cert
Again the CSP uses DOWN to decrypt the Bundle.
ECsck (Data) and Cert ← DCDOWN [ECPRKDO {ECsck (Data)}] and Cert
- Cloud Service Provider stores the certificate and ECsck (data) on their databases for after wards or for future references as the Provider does not know the secret key how to perform decryption the data.

Table-1: Example of OWN_LIST

Operator Group (OPR_GRP)	Operator's ID (OPR_ID)	Data Type	Operator Group time and date (OPR_GRP_T&D)	OPR's time & date (OPR_T&D)
1	198	MP3	07.56 22-11-11	07.08 16-09-15
	033			06.09 17-08-14
	613			09.21 11-07-15
	561			05.22 13-06-15
2	042	JPG	19.45 21-09-11	23.45 21-08-11
	872			22.21 20-11-11
	763			20.15 19-10-11
	225			07.15 15-11-09
50	546	DOCX	09.35 22-07-10	16.23 18-03-13
	657			17.41 03-02-13
	877			10.42 12-03-13
	657			17.41 03-02-13

C. Operations Performed On the Own List

Before you begin to format your paper, first write and save the content as a separate text file. Complete all content and organizational editing before formatting. Please note sections A-D below for more information on proofreading, spelling and grammar.

- *Inserting ID of operator in the OWN_LIST Algorithm:* For insertion firstly provider performs a check for operator's authorization, found that the operator is unauthorized, the process is terminated. If not the value of C and M and are assigned in count1 and count, after this provider have a check on group field of operator. if group is full operator is called by Provider. Function of delete an entire group ,Addition of data and A's id OPR_GRP z OPR_ID and OPR_GRPz Data, so that M have fields of operator and data of A has a check in OPR_GRP and OPR_ID Field. Checking of empty storage if it is there addition of A data is performed in OPR_GRP x OPR_ID. if not the deletion and update and add of A's data in OWN_LIST.
- *Deletion:* Deleting contains two possibilities. Deletion of operator's id from the OPR_ID column and

- deletion of a full OPR_GRP present in the OWN_LIST.
- *Deleting operator's id in OWN_LIST REMOVEOPR_ID OPR_GRP Algorithm:* For deletion
- id of operator from column of the OPR_ID column, Provider searches full OPR_GRPs and current OPR_ID. when Search of LRU operator ID, it assigns 1, thus, deletion is done from OPR_ID column. Then, OWN_LIST is goes under pupation and stops the procedure.
- *searching an Owners's ID insides OWN_LIST for providing the DOWN:* operator request for a data request, firstly, after that provider perform checking whether the operator's authorization is there or not If the operator is unauthorized terminates the process then and their Otherwise, for all OPR_GRP fields, other is performed. Provider checks A Data across the OPR_GRPxData.Satisfaction is their if, Provider have a search of the data and owners of the data after this only they provides the DOWN If not, invalid. Table 2 shows the symbols and notation descriptions.



Table-2: Notation and their description

Notation	Description
PBK	Provider's public key
EC	encryption
PRK	Provider's private key
DC	decryption
PBKUSR	public key of the user
Cert	certificate
PRKUSR	operator's private key
SCK	secret key or data decryption key
PRKDO	private key of the DO
OPR_GRP _x Data	data belong to x th OPR_GRP
OPR_GRP _x OPR_ID	OPR_ID belong to x th OPR_GRP
OPR_GRP _z OPR_ID	OPR_ID belong to z th OPR_GRP
OPR_GRP _z Data	data belong to z th OPR_GRP
OPR_GRP _x	x th OPR_GRP
OPR_ID _y	y th Operator ID
OPR_ID _{new}	OPR_ID field after processing
OPR_ID _{prev}	OPR_ID field before processing
A _{data}	A's requested data type
EC _{SCK}	encryption with the Secret key
DK _{SCK}	decryption with the Secret key
EC _{PBK}	encryption with the PBK
EC _{PRK}	encryption with the PRK
DC _{PRK}	decryption with the PRK
DC _{PBK}	decryption with the PBK
EC _{PRKDO}	encryption with the PRKDO
DC _{PRKDO}	decryption with the PRKDO
EC _{PBKUSR}	encryption with the PBKUSR
EC _{PRKUSR}	encryption with the PRKUSR
DC _{PRKUSR}	decryption with the PRKUSR
DC _{PBKUSR}	decryption with the PBKUSR

Insertion Algorithm for an operator's ID in the CSP_LIST

```

If A==Authorized operator's ID
    Count ← N, count1 ← C
    if count ≠ FULL
        for all Ux ∈ M
            if Adata==OPR_GRPxdata
                for all ux ∈ M' in Ux
                    if count1 ≠ FULL
OPR_GRPxOPR_ID ← OPR_GRPxOPR_ID ∪ A
                    else REMOVEOPR_ID (OPR_GRP)

OPR_GRP OPR_ID ← OPR_GRPiOPR_ID ∪ A
                End for
            End for
        End for
    Else

```

```

z ← REMOVEOPR_GRP()
OPR_GRPzOPR_ID ← OPR_GRPzOPR_ID ∪ A
OPR_GRPzdata ← Data
UPDATE OWN_LIST
else
STOP

```

Algorithm for deletion of a operator's ID in OWN_LIST

```

for x=1 to N
    for y=1 to C
        I ← SEARCHiru(OPR_IDy)
OPR_IDnew ← OPR_IDprev - I
        End for
    End for
UPDATE OWN_LIST
STOP

```



Algorithm for deletion of full OPR_GRP column from the OWN_LIST

SEARCH LRU OPR_GRP
DELETE entries of xthOPR_GRP
UPDATE OWN_LIST
STOP

Algorithm to perform search for a DO's ID from the OWN_LIST

If A == Authorized operators ID
For x=1 to N
If A_{data} == OPR_GRP_{xdata}
SEARCH data from the record of OPR_GRP_x
SEARCH data owner of the requested data
PROVIDE DOWN TO A
else
Display INVALID data type
End for
else
STOP

D. Data Access

Data can be accessed only by sending the request to the server, Cloud Service Provider informs to the Operators that they have the key to decrypt the data and certifications from data owners for performing decryption by which they can use it for the first time. After authorization of operators CSP needs the data. Operators have to initiate data for request to obtain for the needed time. Hereafter accessing there is no use of certification and Secret Key from owners. At first they got all this details. Steps are,

- I: A request is been made by the operators to the provider. Encryption is performed by the provider to DOWN by using private key of them PRK and PUBUSR, after this operator has it and have the DOWN after decryption.
- II: Secret key and Certification is taken after the request to Owners. Operators with the help of PRKUSR for encryption of the message, and then, uses the DOWN once more for encryption purpose. Owners with help of PRKDO, hereafter uses PBKUSR for decryption of the message.
- III: Operator's authenticity from Cloud Service Provider is validated by data owners.
- IV: Authorized operators will only get the certificate and secret key by DO.

SCK and Cert → EC_{PRKDO} (SCK and Cert)

EC_{PRKDO} SCK and Cert → EC_{PBKUSR} { EC_{PRKDO} (SCK and Cert)}

EC_{PBKUSR} { EC_{PRKDO} (SCK and Cert)} → Operator

- V: Operators with the help of PRKUSR and DOWN decryption of the message.

ECPRKDO (SCK and Cert) ←

DC_{PRKUSR} [EC_{PBKUSR} { EC_{PRKDO} (Sec and Cert) }]

Sec and Cert ← DC_{DOWN} { EC_{PRKDO} (SCK and Cert) }

- VI: Operators with the help of PRKUSR for encryption of the certificate, once more uses the PBK for encrypting. This is sent to the provider by the operator

Cert → EC_{PRKUSR} (Cert)

EC_{PRKUSR} Cert → EC_{PBK} { EC_{PRKUSR} (Cert) }

EC_{PBK} { EC_{PRKUSR} (Cert) } → CSP

- VII: decryption of the message by CSP.
 EC_{PRKUSR} (Cert) ← DC_{PRK} [EC_{PBK} { EC_{PRKUSR} (Cert) }]

Cert ← DC_{PBKUSR} { EC_{PRKUSR} (Cert) }

- VIII: CSP can only provide data to operators if the certification which is present matched with the present which is used to request the data.

ECSCCK (Data) → EC_{PRK} { $ECSCCK$ (Data) }

EC_{PRK} $ECSCCK$ Data → EC_{PBKUSR} [EC_{PRK} { $ECSCCK$ (Data) }]

EC_{PBKUSR} [EC_{PRK} { $ECSCCK$ (Data) }] → Operator

- IX: Operators with PRKUSR plus PBK for decryption of the message. Finally decryption is performed with the help of secret key to fetch the original data.

V. RESULTS AND DISCUSSIONS

After a deep analysis and research, we found that few operations have executed for checking the model in comparing to the other existing methods: PBAC, GBAC and UCON. There are few rules/protocols that they are taking as the main schemes for the simulation as these are same to the existing scheme of ACM. We have proved that that our algorithm is efficient in data accessing and saves the user time. CPU occupation is calculated for the proposed work in different types of scenarios for data searching time or giving the public owner, now the average data is taken in order to calculate the time taken in unalike plot. Figure 2 shows the result of system configuration. The data set result has shown in Figure 3.

EK_{PRSP} { EK_{Sec} (Data) } ← DK_{PRUSR} [EK_{PUUSR} [EK_{PRSP} { EK_{Sec} (Data) }]]

EK_{Sec} (Data) ← DK_{PUSP} [EK_{PRSP} { EK_{Sec} (Data) }]

Data ← DK_{Sec} { EK_{Sec} (Data) }

In this model, because of menacing search time the access data time is reduced for providing the PUOWN. In the existing schemes, the accessing time is drastically increased in the same manner of the search time. The performance result has shown in Figure 4.

A. Creation of virtual machines

- A virtual environment is used Cloud Sim 3.0.3 in this paper for evaluating the performance purpose.
- Now divided the RAM into four types of virtual machines (VMs): User-Type I (500 Million instruction per second, 512 MB), User-Type II (1000 Million instruction per second, 1 GB), User-Type III (1500 Million instruction per second, 1.5 GB) and User-Type IV (2000 Million instruction per second, 2 GB). Every virtual machine has the bandwidth of 1 GB/s.
- Dynamic memory is added in the Cloud Sim which helps us to get the exact source. A resource is allocated in the virtual machine after the cloudlet is executed. There are few classes which are modified for achieving dynamic resource, which are namely: -



- 1st one is: CloudletScheduler.
- 2nd is: powerhost
- 3rd is: VM
- 4th is: VMScheduler.

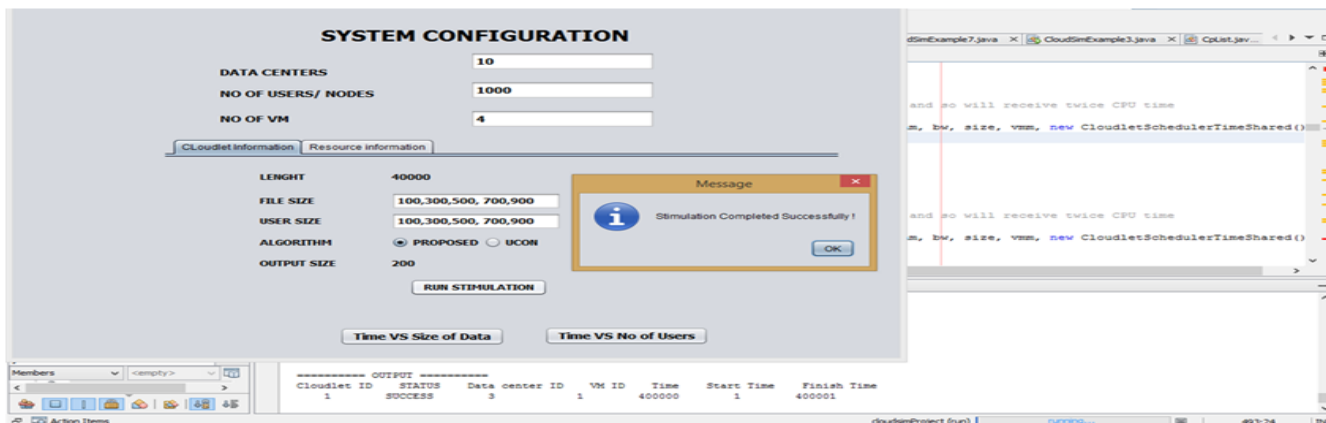


Fig.2. System Configuration



Fig.3. Performance of Time Vs Size

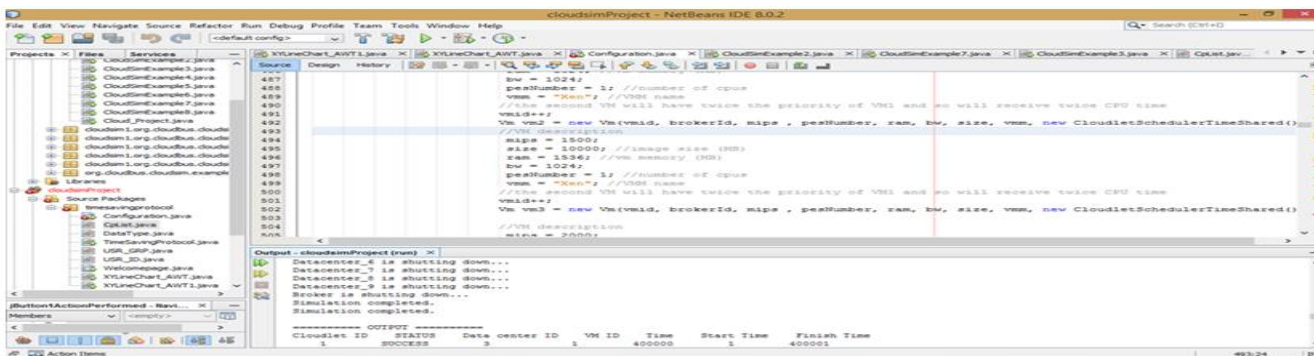


Fig.4. Data SET Result

VI. CONCLUSION

In this paper, a new access control scheme has been proposed we reduced the time for data accessing. As CSP list helps us to reduce the time for fast data access. So, here public is shared so that searching time can be reduced. When user tries to access the data, before that there is a process called user authentication, once authorized and validation done then he is sent to the page where he is only assigned or access, instead of searching in complete database. The data access time will be fast as it reduced the minimization time, so users can spend less time for utilizing the services. In the proposed scheme, the process time is minimized and the CSP list is easily maintained and monitors the database efficiently. Therefore after the full analysis and results we proved that

this method is being more efficient than the old or existing methods.

REFERENCES

1. Danwei, C., Xiuli, H. and Xunyi, R., Access control of cloud service based on ucon. In IEEE International Conference on Cloud Computing Springer, Berlin, Heidelberg, pp. 559-564, December.2009
2. Yu, Shucheng, Cong Wang, Kui Ren, and Wenjing Lou. "Achieving secure, scalable, and fine-grained data access control in cloud computing." In 2010 Proceedings IEEE INFOCOM, pp. 1-9. 2010.
3. Sun, Lili, and Hua Wang. "A purpose based usage access control model." International Journal of Computer and Information Engineering vol.4, no. 1, pp.44-51, 2010.



4. Zhu, Yan, Hongxin Hu, Gail-Joon Ahn, Dijiang Huang, and Shanbiao Wang. "Towards temporal access control in cloud computing." In 2012 Proceedings IEEE INFOCOM, pp. 2576-2580, 2012.
5. Wu, Yongdong, Vivvy Suhendra, and Huaqun Guo. "A gateway-based access control scheme for collaborative clouds." In the proceedings of 7th International Conference on Internet Monitoring and Protection. 2012.
6. Chunlin, Li, et al. "Multiple context based service scheduling for balancing cost and benefits of mobile users and cloud datacenter supplier in mobile cloud." Computer Networks vol.no.122 pp.138-152, 2017.
7. Namasudra, Suyel, and PINKI ROY. "A new table based protocol for data accessing in cloud computing." Journal of Information Science & Engineering Vol. 33,.pp. 3. 2017.
8. Namasudra, Suyel, and Pinki Roy. "PpBAC: popularity based access control model for cloud computing." Journal of Organizational and End User Computing (JOEUC) vol.30, no. 4 pp.14-31,2017.
9. Chard, K., Caton, S., Rana, O. and Bubendorfer, K., Social cloud: Cloud computing in social networks. In 2010 IEEE 3rd International Conference on Cloud Computing pp. 99-106, July 2010
10. Cloud Computing vs. Virtualization <http://www.learncomputer.com/cloud-computing-vs-virtualization>.
11. Andrew Joint and Edwin Baker, "Knowing the past to understand the present- issues in the contracting for cloud based services", Computer Law and Security Review 27, pp 407-415, 2011.
12. Vania Goncalves and Pieter Ballon, "Adding value to the network: Mobile operators' experiments with Software-as-a-Service and Platform-as-a-Service models", Telematics and Informatics 28, pp 12-21, 2011.
13. NIST, <http://www.nist.gov/itl/cloud/index.cfm>.
14. GTSI Group, "Cloud Computing - Building a Framework for Successful Transition," White Paper, GTSI Corporation, 2009.
15. T. Dillon, C. Wu and E. Chang, "Cloud Computing: Issues and Challenges", 24th IEEE International Conference on Advanced Information Networking and Applications, 2010.
16. P. Mell and T. Grance, "The NIST Definition of Cloud Computing" Recommendation of NIST, Special Publication 800- 145 2011 <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-45.pdf>.
17. Z. Wang, "Security and Privacy Issues Within Cloud Computing", IEEE Int. conference on computational and information sciences, Chengdu, China, Oct. 2011. [14] Ahmed Youssef and Manal Alageel "Security Issues in Cloud Computing", in the GSTF International Journal on Computing , Vol.1 No. 3, 2011.
18. Rajnish Choubey, Rajshree Dubey and Joy Bhattacharjee, "A Survey on Cloud Computing Security, Challenges and Threats", International Journal on Computer Science and Engineering (IJCSE), vol. 3, No. 3, 2011.

M.Basha Khaja is working as Software engineer in Wipro, Ireland, United Kingdom. His research area includes Image Compression, Software engineering, Data mining and Warehousing

AUTHORS PROFILE

Dr. T.R.Saravanan received the Master of Technology degree from the Sathyabama University Chennai, TamilNadu, India in 2007 and the Ph.D. degree from Sathyabama University, Chennai, Tamil Nadu, India in 2017. He is currently working as Assistant Professor in the Department of Computer Science and Engineering at Jeppiaar SRR Engineering College, Chennai, Tamil Nadu, India. His research interests are in Image Processing, Software Engineering, Mobile Computing and Cloud Computing.

Dr.K.Uma received her B.E Degree in Computer Science and Engineering from Annamalai University, Tamil Nadu, India in 2007 and M.E degree from Anna University, Tamil Nadu, India in 2009. She has completed her Ph.D. in Image Processing from Anna University Chennai, India in 2017. Currently she is working as Assistant Professor (Sr) in the School of Information and technology, VIT University, Vellore, India. She has published about 65 papers in both national, international journals and conferences. Her research area includes Image Compression, Software engineering, Data mining and Warehousing, Cryptography and Cloud Computing and Wireless Sensor Networks.

C. Ramesh Kumar received the B.E degree in Computer Science and Engineering from Anna University, TamilNadu, India, in 2005 and the M.E degree in Computer Science and Engineering from Anna University of Technology, TamilNadu, India, in 2011. He is currently pursuing the Ph.D. degree in Computer Science and Engineering at Galgotias University, Uttra Pradesh, India. His research interest includes network security, wireless body area network, wireless sensor network, cloud computing security.