ISSN: 0974-5823 Vol. 7 No. 12 December, 2022

International Journal of Mechanical Engineering

The Shared Cloud Data Security Technique Schemes For An Efficient File Access Control

Sudhakar Veledendi
Department of Computer Science & Engineering, S.R. University, Ananthasagar, Hanamakonda, Warangal, Telangana, India.

Niranjan Polala
Department of Computer Science & Engineering, Kakatiya Institute of Technology & Science, Warangal, Telangana, India.

Tarasvi Lakum*
*Department of Computer Science & Engineering, Kakatiya Institute of Technology & Science, Warangal , Telangana, India.

***Corresponding author: -** Tarasvi Lakum
Department of Computer Science & Engineering , Kakatiya Institute of Technology & Science, Warangal , Telangana, India, E-mail:- tarasiru1@gmail.com

Abstract:
Through cloud services, the cloud based users and organizations are storing and sharing the data in the advanced cloud computing environment. However, the recent cloud data breaches have raised privacy and secure concerns in the cloud managed data, due to vulnerability in untrusted cloud access control system. Designing an efficient trusted access control system in cloud is still challenging. We are implemented three objectives.

First objective on variation of decisional learning parity with noise (DLPN) named as Key-Ordered DLPN based security algorithm. It uses DLPN by extending it to a even-odd-order scheme, depend by the value of probability distribution of odd and even bits for encryption, where odd and even bits are the input integer values for key generation algorithm.

The second objective on Mutual Query Data Sharing Protocol (MQDS) to overcome the encryption or decryption time limitations of existing protocols like Boneh, RSA, Multi-bit TRLPN, Ring-LPN cryptosystem, KO-DLPN and KD-CS protocol's. This scheme is to provide the security for the authenticated user data among the distributed physical users and devices.

Third objective on the Key-Signatures Search Scheme provides confidential hosted-file data access, by role-based public key-revoking. With this, the cloud data security is made through the access enforcement, access revocation and hosted-file key management.

INTRODUCTION:

Cloud computing is the utilization of computer resources as a service delivered through the internet on demand. It is primarily centred on the outsourcing of data and programmes, which were formerly held on users' pcs, to remote servers (data centers) that are owned, maintained, and governed by third parties. Data security is a major issue in cloud computing. With the development of cloud computing data security becomes more and more important in cloud computing.

Cloud computing issues were divided into three groups: 1-data security challenges arising from single cloud features against traditional infrastructure, 2-data security issues arising from the data life cycle in cloud computing (data stored, processed, and transferred), 3-data security issues arising from data security attributes (confidentiality, integrity and availability)[1].

- **Data confidentiality:** It is the process of protecting data from illegal access and disclosure from outsourced server. This problem occurs when sensitive data is outsourced to the cloud server.

- **Data integrity:** Integrity refers to data protection from unauthorized changes, whether intentional or accidental. These changes include creating, deleting, and writing.

  Data outsourcing: users are relieved from the burden of data storage and maintenance. When users put their data on the cloud, the data integrity protection is challenging lightweight data integrity verification scheme suitable for thin clients. A single encryption key and two random sequence generators are needed for implementing this scheme. This scheme lacks the ability to protect the data from malicious modifications.
- **Data availability:** Data availability means that information must be available when authorized persons need it. Compare to data confidentiality and integrity in cloud environments, data availability issue has not yet been attracted the attention of researchers.
- Regular backups and storing in multiple disaster recovery sites for improving the data availability in times of disasters. Though the disaster management is part of the SLA with the main storage provider, availability can be increased by duplicating the data in other storage providers.
- **Data encryption:** cloud data secure cryptographic schemes (like encryption or authentication protocols) are appealing for theoretical and practical reasons. So, there is a need of gentle introduction to provable security using AES based schemes as examples. Starting from pseudorandom generators and symmetric key encryption, over secret-key authentication protocols. Through the constructions of public-key identification.
- **RSA (Rivest–Shamir–Adleman):** Is an asymmetric cryptographic algorithm used to encrypt and decrypt messages. It becomes difficult to find the decryption key under the large integer's factors. In LWE (learning with error) is used in public key cryptosystem design and applications of data encryption in cloud computing, like RSA. But LWE public key size is too large, and the reduction of this size is a public problem, so there is a need of learning parity with noise (LPN), which is special case of LWE, with small public key and provide a secure encryption through without errors [2-4].
- **LPN:** LPN [5][6] computational version is an analogue of linear codes decoding through random numbers, is an NP-complete problem. The problems available are made in to two non-trivial solving methods; one is a type of method which intends for all possible noise vectors to be intended and the other which has a sub index time complexity. In this , a matrix LPN problem is considered to solve the encoding error problem through damgård's scheme.
- **DLPN:** DLPN in this the public key becomes small, having a random public and private key vectors $a \in z_2^n$ and $s \in z_2^n$ respectively. If an attacker gets $(a, \langle a,s\rangle+e)$, where $e \leftarrow ber_\tau$, occurring only between $0< \tau <1$.

But the noise rate of lpn the distribution is $0< \tau <0.5$, through which attacker is able to differentiate the random $r \leftarrow z_2$ and sampling $\langle a, r\rangle$ elements, which should be solved through public-key encryption scheme for DLPN, to improve the security of the scheme[5].

Based on above existed techniques we have implemented first scheme ie. "A Key-Ordered Decisional Learning Parity with Noise (DLPN) scheme for public key encryption scheme for Public key encryption scheme in cloud computing multi-bit public key encryption scheme is providing the correctness and chosen plaintext attack security.

To overcome the drawbacks of first scheme, second scheme has developed i.e "Mutual query data sharing protocol for public key encryption through chosen-ciphertext attack in cloud environment" an identity-based authenticated data sharing protocol in providing the secure data sharing for inverse cipher enhancement.

Few limitations of second scheme overcome by third scheme i.e "An Efficient File Access Control Technique for Shared Cloud Data Security through Key-Signatures Search Scheme." Provably secure with sharing aggregate keys for large data sharing on the cloud environment is the proposed for a provable cryptosystem-based block cipher technique in achieving large data sharing for large block bit usage.

A KEY-ORDERED DECISIONAL LEARNING PARITY WITH NOISE (DLPN) SCHEME FOR PUBLIC KEY ENCRYPTION SCHEME IN CLOUD COMPUTING.

The variation of decisional learning parity with noise (DLPN) named as key-Ordered DLPN based security algorithm is presented in this . The proposed scheme uses DLPN by extending it to a even-odd-order scheme, depend by the value of probability distribution of odd and even bits for encryption, where odd and even bits are the input integer values for key generation algorithm.

This states that the probability distribution of odd and even bits are ordered based on the key generation, the process of odd and even bits resolving for the solution of DLPN attacker problems, thus, it provides more correctness and security proof. Through the learning parity with noise (LPN), DLPN and RSA algorithms, the proposed system is evaluated, to measure the encryption time, public key and ciphertext bits.

To provide securing the data in confidential and an authorized encryption. And has become required in providing protection to the information from an unauthenticated users. The information required should be made available to the authorized users and to be protected from unauthorized users by creating it unavailable. Through which the availability, confidentiality and integrity of data become necessary for the security of data.

Recently, encrypted security became a ideological research area, with a process of keeping the data in a server and encrypted form of data is communicated, in a way for the purposed users can have access and process. Cryptography broadly made in to symmetric and public-key. In asymmetric cryptography, public key is used for encryption process and private key is used for decryption process. The prior is more important and secure than the later for cryptography, which depends on the length of the key used and of cryptography made during the computations.

From the survey s, motivated with the challenges in cryptography, a variation of DLPN with two order bits has been proposed, where the keys are dependent of LPN variables and is possible to enhance the scheme by odd and even bits with newly computed bits during the process of encryption and decryption. Increased key generation time can be reduced by increasing the process of coding, it made a big-task in the implemented method provide security for the process from attacks and made secure.

This chapter provides new constructions of encryption schemes from a variant of DLPN. First contribution is to introduce a DLPN variety problem with s ← ber^nxn_τ within the assumptions of normal DLPN problem. As a second contribution a key-bit is constructed into vector-bit through cryptographic operations.
The third contribution the odd and even plaintext-bits are ordered in a multi-bit level based on the encryption and decryption algorithm of the public key. This scheme is a minimization to the LPN and DLPN problem and is efficient as the surveyed schemes.

RELATED
Many schemes have been proposed for public key cryptography. In this , the contributions is on RSA algorithm, LPN and DLPN.

In RSA algorithm, it becomes difficult to find the decryption key under the large integers factors. An enhanced RSA algorithm is proposed by factorizing and deriving the key variable and considering the third prime number by making the complexity more and robust. A new factors should be replaced to increase the complexity at cryptography process to reduce the track back difficulty in the product of three prime numbers, by achieving the increased time complexity.

In LPN, the problems available are made in to two non-trivial solving methods, one is a type of method which intends for all possible noise vectors to be intended and the other which has a sub index time complexity$2^{O(n/\log n)}$. And this complexity is increased further in to $2^{O(n/\log\log n)}$with the sampling time of$n^{1+\varepsilon}$.

Further improvements in the algorithm with less running time are to be made, and there is a need of polynomial time algorithms to solve the variety of LPN problems.

LPN instances creation, so a need of a design for LPN based cryptographic applications, through symmetric encryption in public key scheme. In, a LPN based on public key encryption is proposed with the noise ration of $\tau \approx 1/\sqrt{n}$. However, in all the variants of, an encoding error prevails which is a non-negligible. To solve these, in this work, a matrix LPN problem is considered to solve the encoding error problem through Damgård's scheme.

In DLPN, the problem is to vary between the uniform distribution over the Z value and the number of samples given by the oracle LPN. It can be formulated by an optimization solution ie., by using random matrix A with a random column vector c over Z, to find the vector v to maximise the equations of the scheme Av=c. This illustrates a problem of decrypting a NP-hard, which is a random linear code. To solve these variants of LPN problems, require sub-exponential queries during the sub-exponential time. The DLPN is a variant of LPN_1 problem, introduced in with a distributed secret s is a uniform random variable and throughBer_{τ}^{k}. Here noise parameter made non-constant and it depends on the value of k, through a linear number of queries which are arbitrarily polynomial and matrix version of LPN_1.

A public key cryptosystem based on LPN1 is given as $\left|Pr_{s,A,e}[D(A, A \cdot s \Theta e) = 1 - Pr[D(A,r) = 1]]\right| \geq \epsilon$, where $A \leftarrow B_{\mu}^{q \times n}, s \leftarrow Z_2^n, e \leftarrow B_{\mu}^{q}$ and U_q is a uniform distribution over Z_2^q. The $LPN_{n,\mu,n+q}$problem is hard makes the problem of $Knapsack - LPN_{n,\mu,n+q}$ problem becomes hard.
The DLPN problem is hard compare to LPN problem defined above, which leads to more complex results in public encryption key schemes, to make it available the design is made in black-box manner from the available DLPN problem identified, which is made for noise of $\mu = \omega(1)/\sqrt{n}$.

Proposed Key Encryption Scheme
Proposed scheme uses two prime messages in an order with the increased size. The message noise of these two orders generate the public key (P), a variable O and private key (Q). P and Q are generated as with O parameter considered. Random messages Even() and Odd() are required to create the prime messages. It takes a time in generation of secure key using Even() and Odd() messages and find the noise in the message and time taken is also less by dividing them in to two categories, which makes the reduce in complexity of the algorithm.

The value of O is generated in a random way and these values are transmitted through a sequence of newly generated ie., O_EO as a public key. It continues with the P and Q through the regenerative O and O_EO sequences, so it becomes difficult to the attackers to enter the system which is encrypted, which helps system to improve the security.

Proposed key encryption scheme algorithm is described as follows.

- **Mathematical representation of DLPN with two order bits algorithm**

1. KO-DLPN of ko_keygen(1^n, τ) takes n as integer and τ as noise rate, by choosing a random matrix.
2. KO-DLPN of ko_enc() is divided in to two parts.

- First is even(), where m is converted to a even-square matrix, if m_e=1, for e-th column of is 1 and similarly at each entry of the e-th column is 0, e.g., $m=(0,1,1,1)^t$, then, by choosing.
- And second is odd(), where m is converted to a odd- square matrix , if m_e=0, each entry of the e-th column of is 0 and similarly at each entry of the e-th column is 1, e.g., $m=(1,0,0,0)^t$, then , by choosing.

- **Solution equations for DLPN with two order bits algorithm**

1. KO-DLPN of ko_keygen(1^n, τ): compute , to return with key.
2. KO-DLPN of ko_enc(pk,m) is divided in to two parts.
   First is even(), returns to ciphertext c=(c_{even} and c_2) where the computations are $c_{even}=ra+e_{even}$ and $c_2=rb+e_2+m^{even}$ with e_{even} <-$ber^{1*n}\tau$ and e_2<-$ber\tau^{n*n}$.
   Second is odd(), returns to ciphertext c=($c_1$and c_{odd}) where the computations are $c_1=rb+e_1+m^{odd}$ and $c_{odd}=ra+e_{odd}$ with e_{odd} <-$ber^{n}\tau$ and e_1<-$ber\tau^{n*n}$.
3. KO-DLPN of ko_dec(sk,c), returns (c_1 and c_{even})*s+(c_2 and c_{odd}).
4. Key generation time

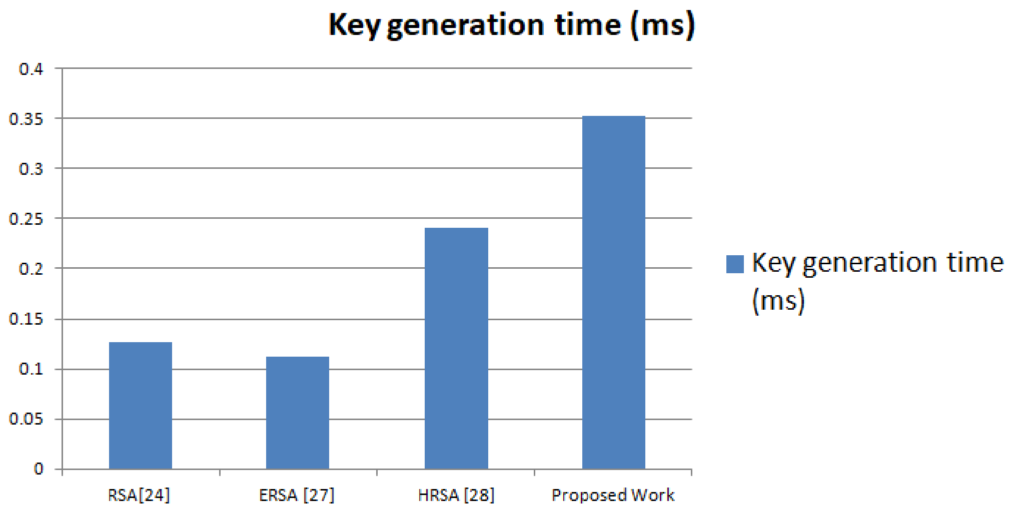
Method	Public key size(bit)	Ciphertext size(bit)	Encoding error
Damgård for bit=1	$2n^2+2n$	n+1	Yes
PPKE based LPN for bit=1	$2n^2$	2n	No
Proposed for bit=1	n^2	N	No
Damgård's for bit=multi	$4n^2$	2n	Yes
PPKE based LPN for bit=multi	$2n^2$	$2n^2$	No
Proposed for bit=multi	$2n^2$	n^2+1	No

Table 1: COMPARISON BETWEEN PROPOSED AND DAMGÅRD SCHEMES AND PPKE BASED LPN.

All the above are w.r.t to LPN, the multiplications and additions have made the computational time to reduce. Proposed is similar to PPKELPN but proposed increases slightly in public key and ciphertext in both the scenarios and decryption error can be neglected. From the table 2 , the key generation time of proposed is better than the reviewed s. From the experiments it is proved that proposed key generation time is higher than RSA, table 2 shows these results.

Security level (128 bits)	Key generation time (ms)
RSA	0.127
ERSA	0.112
HRSA	0.241
Proposed	0.352

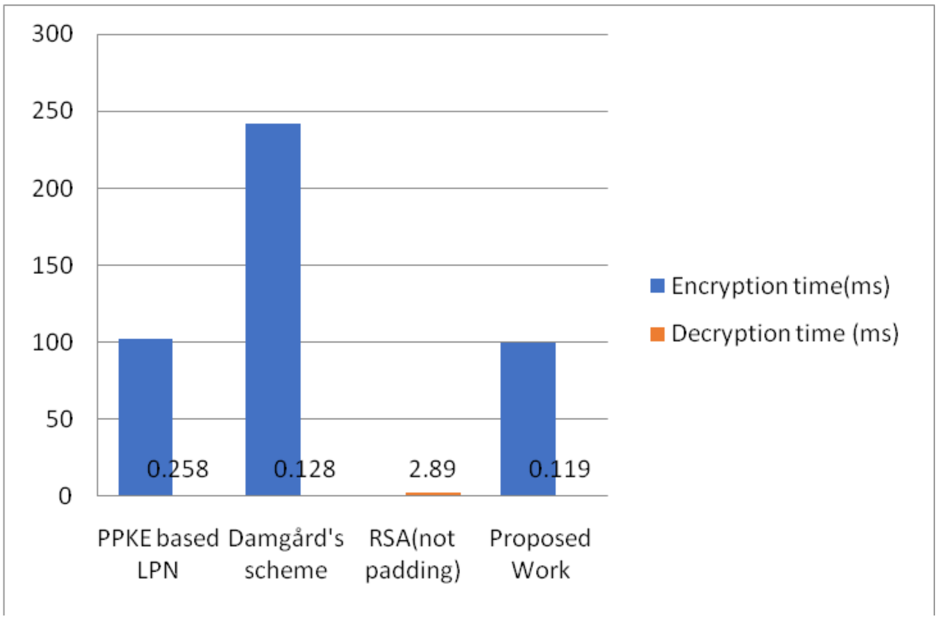
Table 2: COMPARISON BETWEEN PROPOSED AND RSA, ERSA, HRSA IN KEY GENERATION TIME.



- **Encryption time and decryption time**

Security level (128 bits)	Encryption time(ms)	Decryption time (ms)
PPKE based LPN	102.10	0.258
Damgård's scheme	241.70	0.128
RSA(not padding)	0.060	2.890
Proposed	99.85	0.119

TABLE 1.2 Comparison between proposed and reviewed in encryption time and decryption time.



MQDS FOR PKE THROUGH CCA IN COUD ENVIRONMENT

An identity-based authenticated data sharing protocol is the solution to provide secure data sharing for inverse cipher enhancement. We are Implemented a Mutual Query Data Sharing Protocol (MQDS), this protocol main intention is to provide security for the authenticated user data among the distributed physical users and devices. The MQDS protocol designed in such a way to resist the Chosen Ciphertext Attack (CCA) under the hardness solution for the query shared- strong diffie hellman problem.

RELATED LITERATURE

Security for public-key encryption schemes [7-8] is formally defined, through semantic security of a message encryption keeping the attacker from computing the message without the encryption key and message.

They provided this by: two plaintexts; a ciphertext c that encrypts the plaintexts in a feasible way, and mounting a chosen-plaintext attack security system called 'CPA-security' but this semantic security could not provide decryption device security against an attacker.

In the settings of decryption is made in-distinguish ability through the appropriate non-adaptive case. The semantic security models provide the extensions of the Chosen-Ciphertext Attacks, with in-distinguish ability. Security against CCA were defined, to provide additional security when using these CCA systems in general security applications. There are numerous applications[9-13] of the above said decryption service[14-15], to distribute security service in a key recovery mechanism, by allowing decryption of specified messages.

The process of decryption is done by authenticated user, but if a specified party is capable to decrypt the ciphertext, then the decryption services is to be organized.

The process of decryption based on mutual query data sharing protocol, the security provision is through the mutual authentication by an identity-based protocol, by demonstrating session key authentication and user key attack computations. In the proposed mutual query pre-based solution, the authentication is not transparent as key-pair. The file encryption and sharing is performed through a randomly generated number to perform symmetric encryption of the cdo credentials based. The CDO experience in using the encryption process is enhanced by multicast mechanism of the CDO key-pair, so that the user key-pair are provided with three-registration authentication service.

- The evaluation of proposed with the existing data sharing protocols. A Chosen Cipher Text Attack (CCA) is an attack model for cryptanalysis.
- The proposed method contains three phases
  Initiation
  Encryption and sharing
  Accessing and decryption
- **Initiation:** The CDO owner generates a multimedia file to share in the cloud, for that CDO owner need a PKG to run setup file based algorithm with security parameters and authentication credentials *k*, in order to produce parameters and master private key (MSK).
- **Encryption and sharing:** primary CDO wants to share a file with secondary CDO perform below tasks. 1. For a set of group's u, set of individual user's v in cloud CC, the multimedia message file m is created.

2. For the u and v, the encryption process is initiated by encrypt (u,v,m,parameters) keyword passing the cloud software platform. 3. Primary CDO has a symmetric encryption key, which is a randomly generated number assigned to each CDO.

Through this, the encrypted m is sent to public net along with the CDO identifier keywords. 4. The decrypted m file is stored in the cloud server center and can be decrypted by cc with keywords shared by primary CDO. 5. Now primary CDO, multicasts the decrypted keywords through CC to the u and v through a client device such as mobile or pc.

- **Accessing and decryption:** secondary CDO performs the following tasks to decrypt the multimedia message file.

a) Through the credentials and authentication process, the secondary CDO gets in into the cc to access the cloud shared files.
b) With the received keywords, the secondary CDO owner searches for the m file based on the query of the keywords. The m file based through keywords are analysed multiple times, until the m file is found. As the m file is found, the secondary CDO owner data center

(DC) is to be determined by the primary CDO owner cc, whether secondary CDO owner is authorized to receive the m file. As the cc founds the presence of access grant for secondary CDO owner, the symmetric encryption process initiated with the use of randomly generated number along with the encryption id of cloud service is shared with the dc over a public cloud net. After receiving the encryption id, the dc at the secondary CDO owner performs the symmetric key decryption algorithm

c) After the decryption process through public key, the secondary CDO owner needs to encrypt the message m file into ciphertext (CT). For this, secondary CDO owner asks private key to PKG of dc cloud service provider. Through the private key, the extract () algorithm is performed.

d) The key-pair is being used in the above steps, based on private and public keys, after extract () algorithm, the decrypt (msk, id, ct, params) =m algorithm is executed and received at the secondary CDO owner cloud software platform.

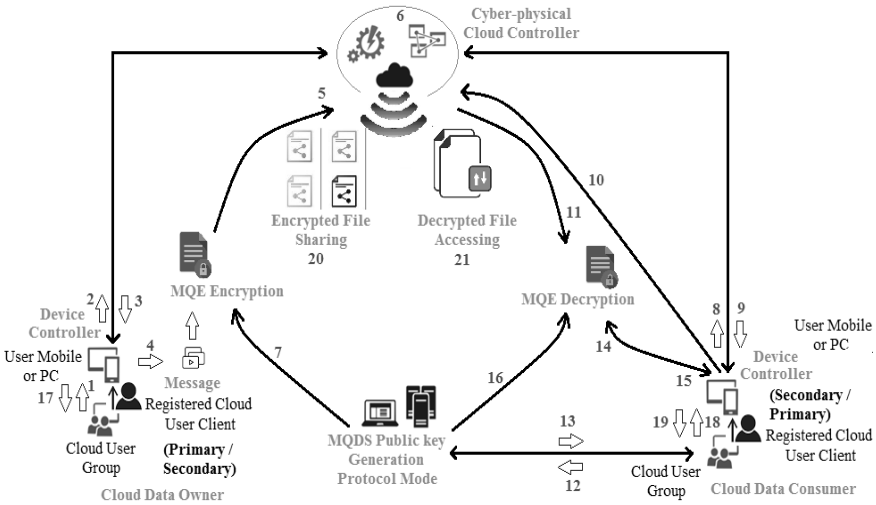
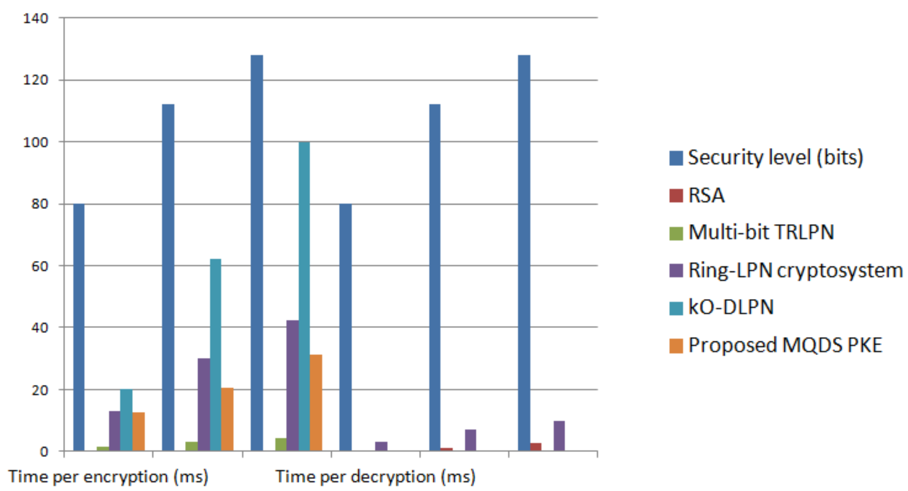


Figure 1: Proposed MQ-PKE based cloud net model for cloud security.

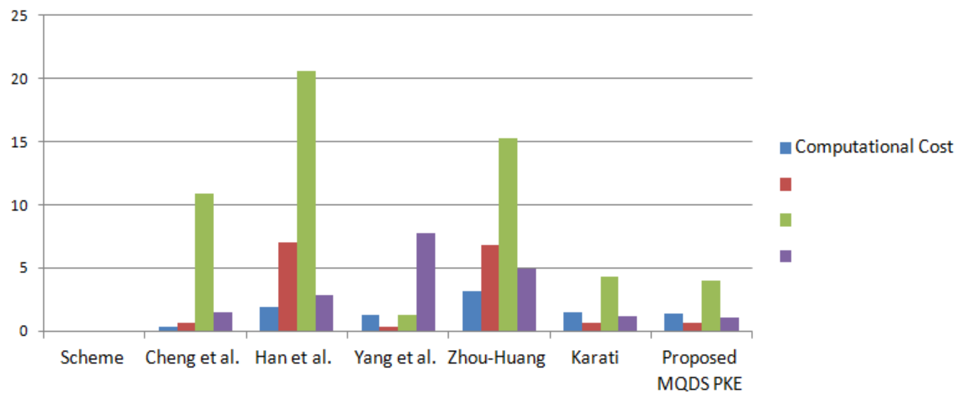
	Time per encryption (ms)			Time per decryption (ms)		
Security level (bits)	80	112	128	80	112	128
RSA	0.010	0.030	0.060	0.140	0.940	2.890
Multi-bit TRLPN	1.400	3.100	4.400	0.052	0.098	0.128
Ring-LPN cryptosystem	13.20	29.90	42.20	3.10	6.90	9.70
kO-DLPN	20.12	62.11	99.85	0.061	0.089	0.119
Proposed MQDS PKE	12.80	20.40	31.20	0.021	0.044	0.087

Table 2.0: Encryption/decryption times for comparison



Scheme	Computational Cost			
	Setup	Extract	To Upload	To Download
Cheng et al.	0.311	0.645	10.88	1.422
Han et al.	1.866	6.995	20.64	2.798
Yang et al.	1.245	0.311	1.244	7.773
Zhou-Huang	3.108	6.842	15.296	4.972
Karati	1.458	0.640	4.340	1.156
Proposed MQDS PKE	1.394	0.612	4.012	1.098

Table 2.1: Time (ms) required by different algorithms



Scheme	Encryption	Decryption	Key generation	Cipher text overhead
Boneh	3.5 f-exps	1.5 exp+1 pairing	4 f-exps	2. L_{BG}+704
KD_CS	3.5 f-exps	1.5 exps	3 f-exps	2. L_{DDH}+128
Proposed MQDS PKE	3.5 f-exps	1.5 exps +2 pairing	5 f-exps	2.L_{MQDS} +1024

Table 2.2: Efficiency comparison for CCA-secure encryption schemes

AN EFFICIENT FILE ACCESS CONTROL TECHNIQUE FOR SHARED CLOUD DATA SECURITY THROUGH KEY-SIGNATURES SEARCH SCHEME

Through cloud services, the cloud based users and organizations are storing and sharing the data in the advanced cloud computing environment. However, the recent cloud data breaches have raised privacy and secure concerns in the cloud managed data, due to vulnerability in untrusted cloud access control system. However, designing an efficient trusted access control system in cloud through enabling a cryptographically file access control technique is still challenging. In this research contribution, a cloud data security system for an efficient file access control technique that provide practical trusted security for shared cloud data is proposed. Proposed file access control technique revokes Key-Signatures Search Scheme which provides confidential hosted-file data access, by delegating role-based public key-revoking in cloud hosted environment to update encrypted data.

In Key-Signatures Search Scheme, the cloud data security is made by encrypting the file by a hosted-file key management, which records hosted-file and its revocation keys simultaneously for key-access enforcement and file-access revocation. In each hosted-file revocations, cloud administrator checks for any in-secure data breach, if found, for that particular hosted file a new revocation key is updated and request for a new encrypted hosted-file with updated file-access permissions.

With the significant advancements in distributed cloud computing [16] [17] [18], users and organizations are finding it progressively engaging to store and share information through cloud administrations. Cloud administration providers give abundant cloud based administrations, going from limited scope individual administrations to huge scope industrial administrations. However, recent information breaches, like, releases of private photographs, have raised concerns with respect to the protection of cloud-managed information.

All things considered [19] [20] [21], a cloud specialist provider is generally not secure because of plan drawbacks of software and frame vulnerability. As such, a basic issue is the manner by which to enforce information access control on the possibly untrusted cloud [22] [23].

To overcome these issues [24] [25] [26], this work present file Access control technique through Key-Signatures Search Scheme (Access-KSS), a cryptographically implemented unique access control system on un-trusted cloud[27] [28]. Access-KSS delegates the cloud to refresh encrypted files in permission revocation.

In Access-KSS, a file or document is encrypted by a symmetric key list which records a file key and a succession of revocation keys. In a revocation, the executive transfers another revocation key to the cloud, which encrypts the file or document with an another layer of encryption and updates the encrypted key list likewise. Same as previous s[29-32], having a honest-but-curious cloud, i.e., the cloud is honest to perform the re-encryption of files or documents and appropriately update previous encrypted files or documents however is interested to passively assembling sensitive data or information. Although the essential thought of layered encryption is straightforward, it involves tremendous specialized challenges. For example, the size of key list and encryption layers would increment as the quantity of revocation tasks, which causes extra decryption overhead for clients to get to documents. To overcome such an issue, Access-KSS is proposed. A provable crypto system-based block cipher technique is the solution to achieve large data sharing for large block bit usage.

The key-signatures search scheme provides confidential hosted-file data access, by role-based public key-revoking with this, the cloud data security is made through the access enforcement, access revocation and hosted-file key management.

As a result, proposed technique enforces the file access control providing efficiency, which does not require re-submission of keys and security, by key-revoking scheme.

- Cloud data security frame and system implementation is made in the proposed to demonstrate the cloud data security and efficiency of the proposed technique. Access-KSS develops new techniques using light weight symmetric encryption scheme with three methods.
- First, Access-KSS proposes key-signatures encryption technique to assign the cloud to refresh strategy information. For a file or document, the administrator attaches another revocation key toward the finish of its key list and requests the cloud to refresh this key list in the policy information.
- The size of the key list anyway increments with the revocation activities, and a client needs to download and decrypt an enormous key list in each file access. To overcome this issue, Access-KSS utilizing the key rotation method to compactly encrypt the key list in the policy information. Therefore, the size of the key list keeps the same regardless of revocation activities.
- Second, Access-KSS proposes flexible role-based encryption procedure to designate the cloud to update file or document information. For a file or document, the administrator requests the cloud to encrypt the file or record with another layer of encryption. Additionally, the size of the encryption layers increments with the revocation tasks, and a client needs to decrypt on multiple times in each file or document access.

To overcome this problem, Access-KSS enables the administrator to characterize a tolerable bound for the file or document.

When the size of encryption layers arrives at the bound, it tends to be made not to increment anymore by assigning encryption tasks to the cloud. Subsequently, the administrator can flexibly change a tolerable bound for each file or document to accomplish a balance among effectiveness and security. During the activity of a file or document, its encryption layers constantly increment until a pre-defined bound is reached.

- Third, Access-KSS proposes role-based access revocation and hosted file key management encryption methodology to occasionally refresh the symmetric key list of the file or document and eliminate the bounded encryption layers over it through wiring activities.
- In explicit, the following user to write to the file or document encrypts the writing content by another symmetric key list containing another record key, and updates the key list in the policy information. With this technique, Access-KSS occasionally eliminates the limited encryption layers of file or documents while amortizing the weight to a huge number of writing clients. Proposed design uses the following notation: u is a user, r is a role, p is a permission, f_n is a file name of a file f, c is a

ciphertext (either symmetric or public encryption), and v is a version number.

The proposed scheme shown in figure 1, follows the following implementation method:

➢ Design and analyze Access-KSS based on the role-based access control (RBAC) model named, which is widely used in practical applications. RBAC model describes permission management with abstraction: roles describe the access permissions associated with a particular (class of) job function, users are assigned to the set of roles entailed by their job responsibilities, and a user is granted access to an object if they are assigned to a role that is permitted to access that object.

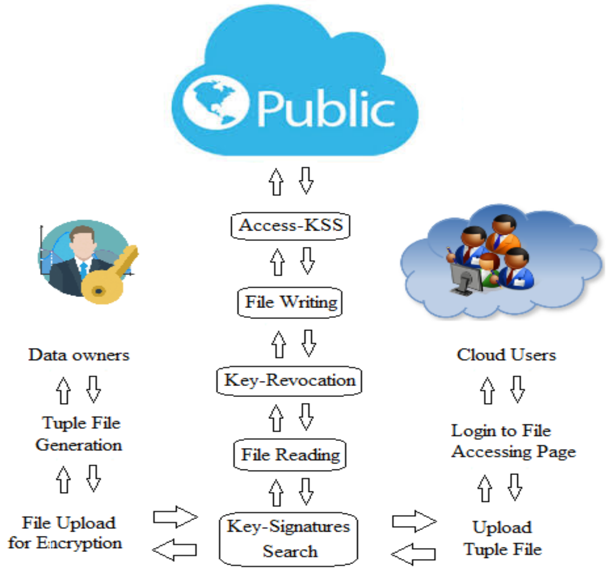


Figure 2: Access-KSS Scheme Flow Diagram

- Access-KSS use three types of files to store metadata for file management.

1. Users: a record (u, ek_u) contains a user identity u and the encryption key ek_u of u.
2. Roles: a record (r, ek_v) contains a role identity r and the encryption key ekvr of r.
3. Files: a record (fn) contains the file name fn of a file.

Key-signatures search management

- In proposed system, the administrator, roles and users are associated with cryptographic keys. Access-KSS introduce them as follows.
- 1. Administrator keys: the administrator plays a role of super user in the system. It has an encryption key pair (ek_{su}, dk_{su}) of a public key encryption scheme and a signature key pair (sk_{su}, vk_{su}) of a digital signature scheme. The encryption key pair is also used by a user to create a special fk tuple when adding a new file into the system.
- 2. User keys: a user read key of u is an encryption key pair (ek_u, dk_u) of a public key encryption scheme. This key is used to encrypt/decrypt rk tuples for u.
- 3. Role keys: a role key of r is an encryption key pair (ek_r, dk_r) of a public key encryption scheme. This key pair is used to encrypt/decrypt fk tuples for r.
- 4. File keys: a file key of f_n is a symmetric key list (k^0, k^1...k^t) of a symmetric key encryption scheme and a rotation key pair ($rsk_f n$, rpkfn) of a key rotation scheme. (k^0, k^1...k^t) is used by users to encrypt the f tuple of f_n, and ($rsk_f n$, $rpk_f n$) is used by the administrator to compactly store (k^0, k^1... K^t) in the fk tuple of f_n.

Access-KSS scheme

- In response to data breaches security issues, this presents Access-KSS scheme

a) In Access-KSS scheme, a revocation file is accesses through encrypted by a defined symmetric key list through which it records a encrypted file key and a revocation layer sequences of revocation keys

b) In layers of key revocations, the authorized administrator provides a new revocation key to the cloud location, which encrypts the relocated file with a new layer of file encryption and updates the layers of encrypted key list with the file revocations

c) An append-aware file encryption strategy is presented to keep the size of the key constant with number of repetition times of revocation operations.

d) A time bound update file encryption data is presented to adjust the encryption key operation requests the cloud can encrypt the file with layers of encryption.

e) A repeated encryption is presented to refresh the symmetric key list of the revocation file and remove the time bounded encryption layers over it through overwrite operations.

f) Altogether, Access-KSS scheme achieves efficient key revocation, efficient file access mechanism and immediate key and file revocation simultaneously. For key and file revocation efficiency, Access-KSS scheme uses lightweight symmetric encryption scheme at the authorized administrator side as it does not need to re-encrypt and re-upload file data.

For time bound revocations, the key permissions of users are revoked in access time as the files are re-encrypted. To improve the file access efficiency, the files are still encrypted by lighten symmetric keys. Access-KSS compare the performance of the four systems in access revocation and file reading/writing

- Access-KSS only uses lightweight symmetric encryptions to encrypt file data and for access revocation, Access-KSS uses key-signatures encryption strategy to delegate the cloud provider to update rk/fk tuples. Access-KSS also uses adjustable role-based encryption strategy to delegate the cloud to update f tuples.

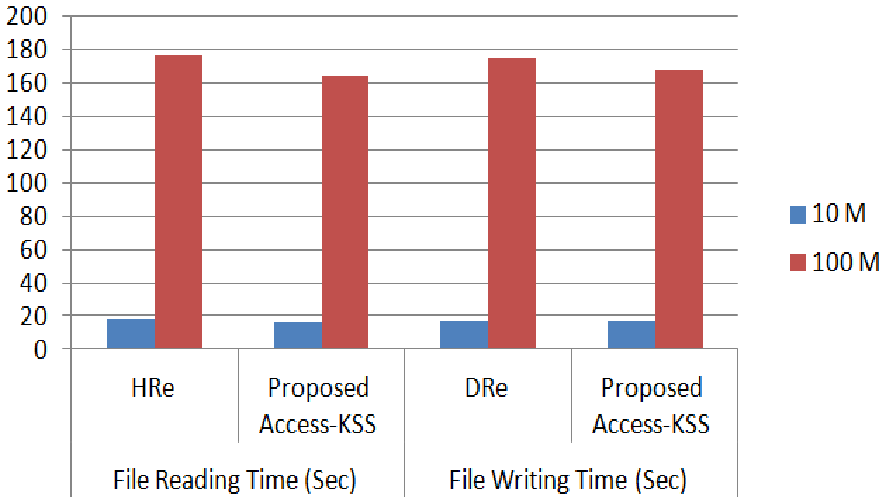
  As the administrator only sends symmetric keys for the cloud provider to encrypt files, it costs far less overhead to update f tuples than previous s.

Key-revoking scheme end-to-end experiments

- Access-KSS only uses lightweight symmetric encryptions to encrypt file data and for access revocation, access-kss uses key-signatures encryption strategy to delegate the cloud provider to update rk/fk tuples.
- Access-KSS also uses adjustable role-based encryption strategy to delegate the cloud to update f tuples. As the administrator only sends symmetric keys for the cloud provider to encrypt files, it costs far less overhead to update f tuples than previous s.
- For file read/write, Access-KSS constrains encryption layers over files to improve the efficiency of file read/write operations.
- In specific, Access-KSS uses the adjustable role-based encryption strategy to constrain the encryption layers in revocation operations and role-based access revocation encryption strategy to remove them periodically.
- The combination of the two strategies ensure that the encryption layer of each file is under an upper bound all the time. More interestingly, the administrator can adjust this upper bound to suit specific application requirements by combining the two strategies in a flexible way.

	File Reading Time (Sec)		File Writing Time (Sec)	
File Size	HRe	Proposed Access-KSS	DRe	Proposed Access-KSS
10 M	17.7	15.8	17	16.8
100 M	176.8	164.1	175.1	168

Table 3.0: Performance in File Reading and Writing



CONCLUSIONS:

A cryptography scheme under public key through DLPN assumptions is an important research, carrying many advantages comparatively. Due to decryption errors, the existing systems are still having problems, which have to be corrected. Through DLPN variant problem, a key-Ordered DLPN is proposed in this. There is a drastic change in the computing overhead of the proposed compared to the PPKELPN, Damgård's scheme and RSA. Proposed can withstand with the practical security like quantum attacks. A comparative result shows the proposed gives high security. A variant of multi-bit public key encryption scheme is the solution to provide the correctness and chosen plaintext attack security [33].

A new MQDS protocol is designed for cyber-physical cloud security and privacy systems based on the CDO pairing through chosen-ciphertext attack in the cloud environment for public key encryption scheme. In this MQDS, firstly a new CDO is registered to the cloud server and cloud service software. Secondly, the CDO sends the encrypted multimedia message in the form of file, to the registered CDO user. If this registered CDO user is untrusted, the cloud controller commands this information to client devices as the registered CDO user becomes trusted. The design and implementation of MQDS is demonstrated with security and correctness of the MQDS protocol, and the performance is evaluated [34]. This introduced Access-KSS, a frame that gives useful cryptographic implementation of dynamic access control in the potentially untrusted cloud provider. Access-KSS meets its objectives utilizing three strategies. Specifically, Access-KSS propose to designate the cloud to refresh the policy data in a privacy-preserving way utilizing a Key-Signatures encryption methodology. Furthermore, Access-KSS propose a role-based access revocation encryption technique to avoid the file or document understanding overhead. The hypothetical analysis and the performance evaluation show that Access-KSS accomplishes significant higher efficiency in access revocations [35].

ACKNOWLEDGEMENTS:

We are grateful to adminstration and Management of KITS Warangal and S.R University for their encouragement and support in the research.

REFERENCES

1. An Overview on Data Security in Cloud Computing, Springer International Publishing AG 2018 R. Silhavy et al. (eds.), Cybernetics Approaches in Intelligent Systems, Advances in Intelligent Systems and Computing.
2. Arjun, U., Vinay, S.: A short review on data security and privacy issues in cloud computing. In: IEEE International Conference on Current Trends in Advanced Computing, pp. 1–5. IEEE (2016) .
3. A Review on Challenges of Security for Secure Data Storage in Cloud, Second International Conference on Smart Systems and Inventive Technology (ICSSIT 2019) IEEE Xplore Part Number: CFP19P17-ART; ISBN:978.
4. Zhimin Yu at all., A Practical Public Key Encryption Scheme Based on Learning Parity With Noise, Special Section On Information Security Solutions For Telemedicine Applications, IEEE Access, VOLUME 6, 2018, pp-31918-31923.
5. I. Damgård and S. Park, ``How practical is public-key encryption based on LPN and ring-LPN?'' Cryptol. ePrint Arch., Int. Assoc. Cryptol. Res., Tech. Rep., Jun. 2016. [Online]. Available: http://eprint.iacr.org /2012/699.pdf
6. Karati, R. Amin, S. K. H. Islam and K. R. Choo, "Provably secure and lightweight identity- based authenticated data sharing protocol for cyber-physical cloud environ-ment," in IEEE Transactions on Cloud Computing, pp. 1-14, 2018
7. L. Dang, J. Xu, X. Cao et al., "Efficient identity-based authenticated key agreement protocol with provable security for vehicular ad hoc nets," International Journal of Distributed Sensor Nets, vol. 14, no. 4, 2018.
8. S. Bala, G. Sharma, and A. K. Verma, "PF-ID-2PAKA: pairing free identity-based two-party authenticated key agreement protocol for wireless sensor nets," Wireless Personal Communications, vol. 87, no. 3, pp. 995–1012, 2016
9. He, N. Kumar, M. K. Khan, L. Wang, and J. Shen, "Efficient privacy-aware authentication scheme for mobile cloud computing services," IEEE Systems Journal, vol. 12, no. 2, pp. 1621–1631, 2018.
10. S. H. Islam and G. P. Biswas, "A pairing-free identity-based two-party authenticated key agreement protocol for secure and efficient communication," Journal of King Saud University—Computer and Information Sciences, vol. 29, no. 1, pp. 63–73, 2017.
11. He, N. Kumar, H. Wang, L. W ang, K.-K. R. Choo, and A. Vinel, "A provably-secure cross-domain handshake scheme with

symptoms-matching for mobile healthcare social net," IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 4, pp. 633–645, 2018.

12. Q. Feng, D. He, S. Zeadally, N. Kumar, and K. Liang, "Ideal lattice based anonymous authentication protocol for mobile devices," IEEE Systems Journal, vol. 13, no. 3, pp. 2775–2785, 2018.
13. C. Lin, D. He, X. Huang, K.-K. R. Choo, and A. V. Vasilakos, "BSeIn: a blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," Journal of Net and Computer Applications, vol. 116, no. 1, pp. 42–52, 2018.
14. Yu, H.; Yang, B. Low-computation certificateless hybrid signcryption scheme. Front. Inf. Technol. Electron. Eng. 18, 928–940, 2017.
15. Huang, Q.; Yang, Y.; Fu, J. PRECISE: Identity-based private data sharing with conditional proxy re-encryption in online social nets. Future Gener. Comput. Syst. 86, 1523–1533, 2018.
16. C. Jin and M. van Dijk, "Secure and efficient initialization and authentication protocols for shield," IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 1, pp. 156{173, 2019.
17. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, SIAM Journal on Computing, vol. 32, no. 3, 2003.
18. D. Boneh, K. Lewi, H. Montgomery, and A. Raghu Raghunathan, Key homomorphic PRFs and their applications, in CRYPTO, 2013.
19. D. Nali, C. M. Adams, and A. Miri, Using mediated identity-based cryptography to support role-based access control, in ISC 2004, 2004.
20. Gudes, The Design of a Cryptography Based Secure File System,IEEE Transactions on Software Engineering, vol. 6, no. 5, 1980.
21. E. Shen, E. Shi, and B. Waters, Predicate privacy in encryption systems, in TCC, 2009.
22. Ateniese, D. H. Chou, B. Medeiros, and G. Tsudik, Sanitizable Signatures, in proceedings of ESORICS, 2005.
23. J. Bethencourt, A. Sahai, and B. Waters, Ciphertext-policy attribute based encryption, in IEEE S&P, 2007.
24. J. Wang, X. Chen, J. Li, J. Zhao, and J. Shen, Towards achieving flexible and verifiable search for outsourced database in cloud computing, Future Generation Computer Systems, vol. 67, 2017.
25. J. Wang, X. Chen, X. Huang, I. You, and Y. Xiang, Verifiable Auditing for utsourced DOatabase in Cloud Computing, IEEE Transactions on Computers, vol. 64, no. 11, 2015.
26. A.L. Ferrara, G. Fuchsbauer, and B. Warinschi, Cryptographically enforced RBAC, in CSF, 2013
27. M. Barhamgi et al. Privacy in data service composition. IEEE Transactions on Services Computing, 2019.
28. M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, Dynamic and efficient key management for access hierarchies, ACM TISSEC, vol. 12, no. 3, 2009.
29. R. S. Sandhu, Rationale for the RBAC96 family of access control models, in proceedings of ACM shop on RBAC, 1995.
30. S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati,Over-encryption: Management of access control evolution on outsourced data, in VLDB, 2007.
31. S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, Encryption policies for regulating access to outsourced data, TODS, vol. 35, no. 2, 2010
32. A Key-Ordered Decisional Learning Parity with Noise (DLPN) Scheme for Public Key Encryption Scheme in Cloud Computing. Tarasvi Lakum, B.Thirumala Rao. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10, No. 11, 2019. (doi) : 10.14569/IJACSA.2019. 01011 21.
33. Review on Learning Parity with Noise based cloud computing. Tarasvi Lakum, B.Thirumala Rao. International Journal of Emerging Trends in Engineering Research, 8(10), 2020, 6859 – 6863. doi.org/10.30534/ijeter/2020/368102020.
34. MQDS for PKE through CCA in Cloud environment. Tarasvi Lakum, B.Thirumala Rao. International Journal of Electrical and Computer Engineering (IJECE), Vol 12, No. 1, January 2022.
35. An Efficient File Access Control Technique for Shared Cloud Data Security through Key-Signatures Search Scheme. B.Tirapathi Reddy, Tarasvi Lakum. Journal of Theoretical and Applied Information Technology (JATIT), January 2022, Vol 100 no.1.