# Implementation of Design and Deployment of Secure Sharing Protocol using TTP via Cloud Computing

## Kamini H. Gonnade<sup>1</sup>, Fazeel Zama<sup>2</sup>

Student, Computer Science and Engineering, WCEM, Nagpur University, Nagpur, India

<sup>2</sup>Assistant Professor, PG Computer Science and Engineering, WCEM, Nagpur University, Nagpur, India

Abstract: In this paper, our main issue is an authorization and providing the data security for various applications in web services in a network. Cloud Computing is a revolutionary IT field and we are using this technology for various purposes. With the increasing use of the data sharing in distributed systems such as online social networks or cloud computing, there is increasing in concerns for data security while distributing or sharing data. Here, Ciphertext policy attribute-based Encryption(CP-ABE) is becoming cryptographic solution to above issue of secured data sharing among network. Also, we will have these achievements :1) key escrow problem could be solved by escrow-free key issuing protocol, where key is generated using the secure two-party computation between the key generation center and the data-storing center 2) fine-grained user revocation per each attribute could be done by using anonymous id algorithm where sharing of data will be done on attribute basis.

Keywords: Data integrity, Data sharing, attribute-based encryption, removing escrow, privacy protection.

#### 1. Introduction

Cloud Computing is a revolutionary IT field in today's world. With the recent development in network and computing technologies, people can share their private data with their closed one's among network. So, for sharing data, the use of cloud computing is increasing. People can share their private data through online social media like Facebook, what's app, etc. In this way, due to the development and increasing use of internet, people from various parts of world are coming closer. Also, while sharing the data among network, some security problems and access control problem may arises, which we have to handle in this paper. Improper use of the data by the storage server or unauthorized access by outside users could cause threats to data. People would like to make their sensitive or private data only accessible to the authorized people with credentials they specified. (ABE) is a promising Attribute-based encryption cryptographic approach that achieves a fine-grained data access control. A Ciphertext policy attribute-based Encryption (CP-ABE) is cryptographic solution to the issue of secured data sharing among network. This will enable data owners to define their own access policies over user attributes and enforce the policies on the data to be distributed or shared among different people in network. Thus, each user with a different set of attributes is allowed to decrypt different pieces of data per the security policy.

Also, while using CPABE, some problems may occurs. The key generation center (KGC) generates private keys of users by applying the KGC's master secret keys to users' associated set of attributes. As there is only one person who is responsible for making key, we cannot trust on that person. Because KGC is generating key, so if possible KGC can also decrypt it and we can loose security while sharing data. So, we have to solve this problem. Another challenge is key revocation. some users may change their attributes at some time, and so some private keys might be compromised, then the key revocation or update for each attribute is necessary in order to make systems secure.

#### 2. Existing System

In existing system, they have used following methods:

#### 2.1. Two Party Computation(2PC) protocol

The Two party computation protocol helps to share data securely. Following things are achieved in existing system.

#### 2.1.1. Key Escrow Problem

The very first problem occurs is key escrow problem which is resolved by a key issuing protocol and the main task of the key issuing protocol is that the key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol between the KGC (Key Generation Centre) and the data-storing center with their own master secrets. The 2PC protocol restricts them from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone. Hence, users are not required to fully trust on either the KGC or the data storing center in order to protect their data to be shared. Data confidentiality and privacy can be cryptographically enforced against any curious KGC or data-storing center.

#### 2.1.2. Fine Grained User Revocation:

The immediate user revocation can be done via the proxy encryption mechanism along with the CP-ABE algorithm. Here, the attribute group keys are selectively distributed to the valid users in each attribute group, then those are used to re-encrypt the cipher text encrypted under the CPABE algorithm. The immediate user revocation enhances the backward/forward secrecy of the data on any membership changes. Data owners need not be concerned about defining any access policy for users, but the data owner just need to define only the access policy for attributes as in the previous ABE schemes. Therefore, the proposed scheme is the most suitable for the data sharing scenarios where users encrypt the data only once and upload it to the data-storing centers and leave the rest of the tasks to the data-storing centers such as re-encryption and revocation.

## **3. Data Sharing Architecture**

#### 3.1. System Description and Key Management

#### 3.1.1. Key Generation Center

It is a key authority that generates public and secret parameters required for CP-ABE and it is in charge of issuing key, revoking key and then updating attribute keys for users. It also grants differential access rights to individual users based on their attributes. This key generating center is quite honest in doing their task, but we have to prevent encrypted data so that security should be maintained.

## 3.1.2. Data-Storing Center

It is an entity that provides a data sharing service. It is in charge of controlling the accesses from outside users to the storing data and providing some contents services. Also, the data-storing center is another key authority that generates personalized user key with the help of KGC, and issues and revokes attribute group keys to valid users per each attribute, which are used to enforce fine-grained user access control. The data storing center is also trustworthy like KGC.

## 3.1.3. Data Owner

It is a client who owns data, and wishes to upload it into the external data-storing centre for ease of sharing or for cost saving. A data owner can send any type of data, whatever data he wants to send to other person. A data owner is responsible for defining (attribute-based) access policies, and enforcing it on its own data by encrypting the data under the policy before distributing it.

## 3.1.4. User

It is an entity who wants to access the data from owner. If a user possesses a set of attributes satisfying the access policy of the encrypted data and is not revoked in any of the valid attribute groups, then user will be able to decrypt the cipher text and obtain the data. So the user will get the data securely and here sharing of data will occurs



Figure 1: Architecture of data sharing system

#### 3.1. Threat Model and Security Requirements

#### **3.1.1. Data confidentiality:**

Unauthorized users who do not have enough attribute satisfying the access policy should be prevented from accessing the plaintext of the data. So, we can prevent data to be accessed by every user.

#### 3.1.2. Collusion resistance:

Collusion resistance is one of the most important security property required in ABE systems. As the number of users increases, there may be chances of collusion in network. We should handle it properly.

## 4. Proposed System

We have added some points in existing system.

## 4.1. Two Party Computation(2PC) protocol:

## 4.1.1. Escrow-Free Key Issuing Protocol for CP-ABE:

The KGC and the data-storing center are involved in the user key issuing protocol. In this protocol, a user is required to contact the two parties before getting a set of keys and the secret key is generated through the secure 2PC protocol between the KGC and the data-storing center. Both KGC and data storing center generates their own master key's and issue independent key components to a users. Then, the user is able to generate the whole secret keys with the key components separately received from the two authorities, here KGC and data storing center. The secure 2PC protocol restricts them from knowing each other's master secrets so that none of them can generate the whole secret keys of a user alone. As none of them will be able to know each other's master key, so security will be maintained while sharing the data among network. To make the key issuing protocol escrow free, the CPABE works as follows.

## 4.1.1.1. Key generation:

The KGC and the data-storing centre both are involved in the following key generation protocol.

Data stori	ng center	К	GC	
$x = (\alpha + r_t)\beta$ $\tau \in_R Z_p^*, A = g^{x/r}$ $D = B^r$	$ \underbrace{ \begin{array}{c} & 2PC \\ & \\ & \\ \hline & \\ & \\ & \\ & \\ & \\ & \\ & \\$	→	<i>B</i> =	$A^{1/\beta^2}$



#### 4.1.1.2. Key Update:

When a user comes to hold or drop an attribute, its corresponding key should be updated to prevent the user from accessing the previous or subsequent encrypted data for forward or backward secrecy, respectively. Also, the key update procedure is done by the KGC when it receives a join or leave request from a user for some attributes. On

Paper ID: SUB154865

Volume 4 Issue 5, May 2015 <u>www.ijsr.net</u> Licensed Under Creative Commons Attribution CC BY receiving the request from user, the KGC notifies the data storing center of the event and sends the updated membership list of the attribute group to it. After receiving the notification from KGC, the data storing center reissues the key for that attribute group and so the sharing will be done even after updating key for attribute group.

#### 4.1.2. Encryption and Decryption:

The encryption and decryption of data is processed using RSA algorithm. Here we are implementing RSA algorithm to encrypt and decrypt the data by particular users so that security will be maintained while sharing the data and also the data will be read by only users to which data belongs. The RSA algorithm is as follows:

- Choose two large prime numbers p and q.
- Calculate n=p\*q.
- Select the public key (i.e., encryption key ) e such that it is not a factor of
- (p-1) and (q-1).
- Select the private key (i.e., decryption key) d such that following equation is true:
- $(d^e) \mod (p-1)^e(q-1) = 1$
- For encryption, calculate the cipher text to the receiver.
- Send CT as the cipher text to the receiver.
- For decryption, calculation the plain text PT from the cipher text CT as follows :
  - $PT = CT^d \mod n$

#### 4.2. Anonymous ID Algorithm

Our next most useful task is fine grained user revocation which will be possible by implementing Authorization ID algorithm. Here, an algorithm for anonymous sharing of private data among N parties is developed. Also, this technique is used iteratively to assign these nodes ID numbers ranging from 1 to N. This assignment of ID's is anonymous such that the identities received are unknown to the other members of the group. This assignment of serial numbers allows more complex data to be shared and has applications to other problems in privacy preserving data mining and the collision avoidance in communications and distributed database access. Here, the required computations are distributed without using a trusted central authority. This algorithm is basically used to share complex data among network by creating unique Id for each user so that no other user will know the ID of each other.

## 4.2.1. Secure Sum Algorithm:

Random numbers transmitted by secure sum algorithm:

Nodes	$\hat{r}_{i,1}$	$r_{i,1}$	$r_{i,2}$	$r_{i,3}$	$r_{i,4}$	$d_i$	$\hat{d}_{m{i}}$
$\overline{n_{i=1}}$ :	13 - 6 + 8 = 15	13	-10	6	-3	6	8
$n_{i=2}:$	7 - 10 + 9 = 6	7	3	-5	5	10	9
$n_{i=3}:$ -	-8 - 6 + 5 = -9	-8	11	12	-9	6	5
$n_{i=4}$ :	6	6	-8	-5	9	<b>2</b>	2
s: =	18	18	-4	8	2	T = 24	24

Algorithm is as follows:

- Given nodes  $n_1, \ldots, n_N$  each holding an data item  $d_i$  from a finitely representable abelian group, share the value  $T=\sum d_i$  among the nodes without revealing the values  $d_i$ .
- Each node  $n_i$  , i =1,....,N chooses random values  $r_{i,1,\ldots,,}r_{i,N}$  such that  $r_{i,1+\ldots,+}r_{i,N}$  =  $d_i$

- Each "random" value  $r_{i,j}$  is transmitted from node  $n_i$  to  $n_j$  node . The sum of all these random numbers  $r_{i,j}$  is, of course, the desired total T.
- Each node  $n_j$  totals all the random values received as:  $s_{j=r_{1,j+}r_{N,j}}$
- Now each node n<sub>i</sub> simply broadcasts s<sub>i</sub> to all other nodes so that each node can compute:

 $T=s_1+\ldots+s_N$ 

#### 4.2.2. Transmitting simple data with secure sum

#### 4.2.2.1. Anonymous data sharing with power sum

Given nodes  $n_1, \ldots, n_N$  each holding a data item  $d_i$  from a finitely representable field F , make their data items public to all nodes without revealing their sources.

• Each node n<sub>i</sub> computes d<sub>i</sub><sup>N</sup> over the field F for n=1,2,....,N. The nodes then use secure sum to share knowledge of the power sums:

i=1, $i=1$ ,
--

• The power sums  $P_1, \ldots, P_N$  are used to generate a polynomial which has  $d_1, \ldots, d_N$  as its roots using Newton's Identities as developed in [30]. Representing the Newton polynomial as

 $p(x)=c_N x^N + \ldots + c_1 x + c_0$ the values  $c_0, \ldots, c_N$  are obtained from the equations:

$$\begin{split} c_N &= -1 \\ c_{N-1} &= -\frac{1}{1}(c_N P_1) \\ c_{N-2} &= -\frac{1}{2}(c_{N-1} P_1 + c_N P_2) \\ c_{N-3} &= -\frac{1}{3}(c_{N-2} P_1 + c_{N-1} P_2 + c_N P_3) \\ c_{N-4} &= -\frac{1}{4}(c_{N-3} P_1 + c_{N-2} P_2 + c_{N-1} P_3 + c_N P_4) \\ c_{N-m} &= -\frac{1}{m} \sum_{k=1}^m c_{N-m+k} P_k \end{split}$$

• The polynomial p(x) is solved by each node, or by a computation distributed among the nodes, to determine the roots  $d_1, \ldots, d_N$ .

The choice  $c_N$ =-1, chosen for consistency , may be replaced by  $c_N$ =1 .or any other nonzero value. Also, note that in the typical case F=GF(P) , the solution for the  $c_i$  requires finding the multiplicative inverse of the coefficients 2,3,....,N modulo P . While the Euclidean algorithm could be used, the inverses 1/x can easily be computed in the order by the formulae:

$$q = P/x + r; \quad 1/x = -q(1/r) \pmod{P}$$

After the integer division with remainder r, 1/r will already be known, since  $r{<}x$  .

Volume 4 Issue 5, May 2015 <u>www.ijsr.net</u> Licensed Under Creative Commons Attribution CC BY

International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Powers of	7 DATA VA	LUES $d_i$ C	hosen by I	Each Node
	Mo	DDULO $P =$	= 11	
$d_i^e$	e = 1	e = 2	e = 3	e = 4
$n_{i=1}$ :	6	3	7	9
$n_{i=2}$ :	10	1	10	1
$n_{i=3}$ :	6	3	7	9
$n_{i=4}$ :	2	4	8	5
$\sum d_i^e$	$P_1 = 2$	$P_2 = 0$	$P_3 = 10$	$P_4 = 2$

# 5. Experimental Result

As per the implementation, results are been shown in paper.

aren Kiaya (2PC)	Key Gener	wites
pen Database	Prime Ne. 1 12	Alpho : D.A
eral Delabave	Boars (0,0	Laubia: 2
ergt Jarabasa	Initialize Key Pairs	
an and index	Fublic - Kitys : 0., a ROA public +ep, 1550 bits mit out, at 1045/20208-10592/862182/1607508204 public exponent 02037	0000000542004779003847500+0848400+18965
	Filiate Keys: can security ta RSePrivateCriffeyingiQ#543	id .

Figure 3: Result of key generation

Secret Keys (2PC)	es GPG) Selet Dates Be : C'Uses Kansin/Delide Physic coerdant databar bankbank.cov						B	onse									
ogenerate	1.00						0				~				0		0
Encript Database	^	1.00	16			P.	4	14	1	÷		P		n	0	P	u.
	30-	. Joo.	- M	.60	308	33.	70.	78	10	-1947	7k_	-0u.	108-1	'00.	M.	30.	X.,
entert Clatabase	30	- 10.	100-1	-pn.	10	1787	20	700	100	79	.00	19		-1		194	240
care for carefording	14	10.	20	- 20-	-	4165	Jac.	200		11	2	100	4	220	÷.	100	
	10	100	100	700	- 10	1300	744	Date:	100	- 10	apr.	100	2	100		144	100
Apland Database	50	-11	1	100	100	0	142	200	100.0	2	100	204	4	G	0	140.1	100
	14	100	Tal.	-		242	100	2007	100	- 44	10.10	141	-	124		Add .	100
construction of the	10		100	- Sec	2.	202	Sec	780	400.0	14	100	140	÷	110	-	14	100
owniese Databa.	39	34	100	120	100	147	140	'00'	708	6	100	151	2	-1	8	100	100
	41	200.	-	'ber	200	221	145	'no'	100	34	100	57	2	4 .	ů.	100	100
	43	20.	100	"pri-	10	-41	'ves'	303	·ce.,	17	'001	313	4	547	2	141.	195
	39	56.	100.	'50.	'80'	9374	'yes'	'no"	105.	20	10	273	1	-1	0	141.	1681
	43	'20.	****	'30	'80"	264	'ves'	'no'	108.	17	'301'	113	2	-1	0	"un	514*
	36	"to	100	'ter	'no'	1100	10	'no'	"ce	12	31.	328	2	-1	0	340.1	'10'
	20	nt.	Sec	'20	'no"	502	'10'	"no"	'ce	20	'apr'	261	1	-1	0	Ten.	300
	31	"bl	· '#1	'50.	'80"	360	'yes'	"yes"	*ce.,	29	"jen"	89	1	241	1	Tal.	146
	40	100.	m.,	'ter	'80"	194	'80'	"yes"	10e.,	29	'30.	189	2	-1	ô.	198	111
	56	30.	10.	100.	'no'	4073	'00'	'no'	100.0	27	31.	239	5	-1	0	50.	'84'
	37	"ad.,	21.	"ler	"no"	2347	'yes"	"no"	'ce.,	20	"apr"	114	1	162	2	"fat	100'
	25	"H.,	31.	"pri_	160.	-221	A60.	'no"	101.0	23	18.	250	1	1	0	VI.,	194"
Over	31	36	WL.	'se	.40,	132	'80'	'990'	'0¢	7	M.,	148	1	152	.1	38.	'NI'

Figure 4: Result of database access

Keel Keys (2PC)	A state	Guery Data	1.0.0				Eng	rent Diata
	38	"agnas."	maniet.	"secondary"	'70'	424	787	700"
open Dutatione	34	"blue-collar"	"manled"	"secondary"	'na'	1031	"yes"	'ra'
	3.9	"0448-008ar"	"manied"	"primaty"	"04"	111	"80"	"no"
stick Descena	34	"bise-coltar"	"manied"	"primaty"	"64"	455	"yka"	"ng"
(pr) answer and	27	"senices"	"single"	"pecondary"	"tha"	195	"102"	*na*
	32	"management	"single"	766807	'700"	3616	'80"	700
Database	\$7	"bize-collar"	"manied"	"secondary"	'na'	54093	"ma"	'na'
	41	"weekbown"	"single"	"tettian"	"04"	1567	"80"	"10"
Protect of the local division of the local d	41	"aldman."	"manued"	"Tertian"	"64"	\$420	"yk2"	"ng"
case	30	"admin."	"single"	"tertian"	"tha"	291	"80"	"na"
	36	"Mie-collar"	"divorce d"	"secondary"	'700"	2843	'80"	700
anana -	1.3							
in the second se	+							
	6 2020 000002 0000002 000000 00000 00000 00000 00000 00000 00000 00000 00000 00000 00000 00000 00000 00000 000000	ACCOR (WORC) 9	+ 0 05469 to 1 1004 to 1004	CINCLE ACTION	C Dey Liste, Dro BCCC DroCW DroCW Discussion Call Constant Sign(1-1A)	- Wat dist	AUTOHIC CO: 2 224/9/ ACCITENUISI 400000 22 520000 22 520000000000000000000000000000000000	07 -/ 00100 07 /0 be-0 F01010000 00 s0a0 '5 0 j05 0 y-0 90000,000k

Figure 5: Result of Encrypting data using RSA

A Kens (2017)						00	olipticata	
Nontrane of 1	100000000000000000000000000000000000000	IN BRIDGHT	or warmen and the	100.000	101210-00110-001	THE STREET	WARDON TO MAN	annin
a Theorem	1, 180° (1. #NOCCO_C)(1	P06222 22	- Sec	IDM (BET3/62)	111112780.088	CO.TWO C.UC	-315M2 C	202
- Sector	CT 1400 A 1581	1 3 5 YO W 1 3	2000 S 230G	10000	2 2001WBP		******	1
of Control on a	The name har per	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		Contraction of the second	Law	Aller Trees		
producer	10 /01/01/04 (D1/11/	0.00.000.0	THE DERPTS	055 5(5685 )	ATTAC AND	10.0044	IPRR Sa	ion.
-	0d 262cCHGCUC5CaChi	020-12-282	CC 0000000	00k+FN2 12.	0 -920100	CCCKOP ICK	DwCC/mC	180
prusises -	13021622 92222222	100125128	總(2122,22%2)	000056061(10	1111/0422			
1	52422°C					1999		
ad Database	281-0 00 060Vex(200	7911 _014	124 J 1903X	2 DO028	004040208	0000	1798483	55
	and the party and the second							
	analy Million a Ma	the second of the		citate deste e	3414202 22	Name and	(m *5855(5	822
	100W 1101111K 00/4	ONISSISE 2	12	-1012 842 2	341,7101 21	Nauran 816	(m *5#25(5	M21
load Databa	TOW DECEMBER OF	Watestof 1	12	Marine	M.A.O. 1.	N 0.4	(m *2822)2	
load Databa	1000 1111111 000	owsester a	12		M.A.O. 1.	N	(***2822)2	
load Databa.	1000 1105105K 00/4 R	wanter	'secondary'	-jui: en J	424	'Yaa''	(m *2822)2 /82*	
toed Databa	illiyw liffilir od/s " "admo" "bue-cetar	Wanter Wanter	"Secondary" "Secondary"	101. 64. 1 10 10	424	544" 544"	(m *5855)5 'Na' 'Na'	и <u>с</u> ,
toed Databa	ilow Ilothick colid 'somn' 'bue-ceter 'bue-ceter 'bue-ceter	Warket Warket Warket Warket	12 "Secondary" "Secondary" "Secondary"	10.00.1	424 1901 111	544" 544" 110"	(m *5855)5 'hs' 'hs' 'hs'	
toed Defette.	100w 1101011x 00/4 "admin" "bue-celter "bue-celter	Warket Warket Warket Warket	12 "Secondary" "Secondary" "Secondary" "Secondary" "Secondary"	22 22 22 22 22 22 22 22 22 22 22 22 22	424 1801 111 455	562" 562" 762" 762"	(m *2822)2 '82' '82' '82' '82'	
toed Databa	VENW FIFTHER DO	manie manie manie manie manie	12 "Secondary" "Secondary" "primary" "Secondary"	20.00.1 20.00 20.0	424 1801 111 455 -195	544" 544" 545" 744" 545"	(m *2822)2 192* 192* 192* 192*	12
0046 (Datacos	VERW EXCERTS OF	Manied Manied Manied Manied Manied Single	'secondary'' 'secondary'' 'secondary'' 'secondary'' 'secondary'' 'secondary'	10.00.1 10 10 10 10 10 10 10	424 1891 111 425 -195 3016	544" 544" 744" 744"	(m*19822)2 '82' '82' '82' '82' '82'	M-2
toed Dataton.	100w 1000000 00 bus catur bus catur bus catur bus catur Senios? 'nangemet bus catur	Market Market Market Market Market Singlet Market	12 "Secondary" "Secondary" "Secondary" "Secondary" "Secondary" "Secondary"	******	424 1901 111 455 -195 3816 1000	544" 544" 544" 544" 544" 544" 544"	1972) 1974 1974 1974 1974 1974 1974 1974	
000 d Datassa.	Victoria Antonia Victoria Victoria Victoria Victoria Victoria Victoria	manie manie manie manie manie manie manie manie manie manie manie	Necendary" "Secondary" "Secondary" "Secondary" Secondary" "Secondary" "Secondary" "Secondary"	201001.10 20100.10 20100.10 20100.10 20100.10 20100.10 20100.10 2010	424 1801 111 455 -196 3016 1400 1507	542' 542' 102' 542' 102' 102' 102'	100202 m) 100 100 100 100 100 100 100 100	W2
000 d Dateroa	Warms' Tou cattar Tou cattar Tou cattar Tou cattar Tou cattar Yaaugamat Tou cattar Yaaugamat Uutower Yaang	manie manie manie manie manie single single manie single	12 Secondary Secondary Secondary Secondary Secondary Secondary Secondary Secondary	द्वस्यस्य इत्यस्यस्य	424 1891 111 455 -195 3016 1000 1900 1900	583' 583' 783' 783' 783' 783' 783' 783' 783' 7	10000000000000000000000000000000000000	W2
0000 (Datason 30 30 30 30 30 30 30 30 30 30 30 30 30	Admin' Dua-attur Dua-attur Dua-attur Dua-attur Santosi Yaangamatt Dua-attur Yaangamatt Dua-attur Yaangamatt Dua-attur Yaangamatt	Warted Warted Marted Marted Marted Single Marted Marted Marted Marted Marted Marted	12 Secondary Secondary Secondar Secondar Secondar Secondar Secondar Secondar Secondar	244444 244444 2444444	424 1001 111 465 -195 3016 1507 540 541	542' 542' 742' 742' 742' 742' 742' 742' 742' 7	100202 (1) 100 100 100 100 100 100 100 100 100 1	W-2
100 m () Sectors	Stroye SESSER OF 4	Market Market Market Market Market Singkt Singkt Singkt Singkt	12 "Seconday" Seconday" Seconday" Seconday Seconday Seconday Seconday Seconday Seconday Seconday Seconday	[ब्दददददददद	424 1601 111 455 -195 3156 14000 1507 5406 251 251	542' 542' 545' 545' 545' 745' 745' 745' 745' 745	ישר ישר ישר ישר ישר ישר ישר ישר ישר ישר	

#### Figure 6: Result of Decrypting data using RSA

1	2	Waty Presenting Data 3	itariag With Terare Do	-
	Ne	of Participeers 💿		-
	Give Permi	insing To Courts 1		-
	Terminole	Ter columns : 2 P.F.		
Assynto	Gae Per	Trission		iaerotyt 🔤 🗤
	Participent 1	Participent2	Participant 3	Participant 4
Prevate No.	7	4	6.7	20
Assign Mitro 11	4	1	)	1
- Andreso II		'	1	1

Figure 7: Result of creation of unique id for user

second carle (at or)		De	ers Authorized	Sets af Antibanes a	a View Data
and a second			Ciercial :	3	
Open Cambane	Anonymous ID of Uwe :			1	
Encript Database		Coing	nan to View:	244	
Decript Database					Downio
					Automatic Second
Dated Constraint	Sector 1	10	741	-	
	inaner.	100	764	Message	
ewnisad Calaba	'manied'	'no'	'hes'	1.1	
	"single"	'10'	'64'		
	.254 Be.	184	2987		Download And Access Successibly
	married	10	262.	-	
	maneg.	100	143		(111)
	Transfer of	100	Dest.		OK
	"wateria"	7007	"max"		
	"un con"	100	100	Art.	
	"manager"	2007	Teat.		
	"sit da"	100	1007		
	"mariad"	7007	7447		

Figure 8: Result of sharing data attribute-wise

# 6. Conclusion

The proposed scheme features a key issuing mechanism that removes key escrow problem during the key generation. This user secret keys are generated through a secure twoparty computation such that any curious key generation center or data-storing center cannot derive the private keys individually. The key generation takes place by two party computation protocol between KGC and data storing center. Also, the attribute wise sharing is possible using CPABE and anonymous ID algorithm where unique id is created for each user. Thus, the proposed scheme enhances data privacy and confidentiality in the data sharing system against any system managers as well as outsiders in the network.All this work is shown in this paper by implementing it.

## References

[1] Junbeom Hur, "Improving Security and Efficiency in Attribute- Based Data Sharing", 2013(reference).

- [2] Larry A. Dunning, Ray Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment",2013.
- [3] J. Anderson, "Computer Security Planning Study," Technical Report 73-51, Air Force Electronic System Division, 1972.
- [4] A. Shamir, "How to share a secret," *Commun. ACM, vol.* 22, no. 11, pp. 612–613, 1979
- [5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute- BasedEncryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.
- [6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy,pp.321-334.

# **Author Profile**



Kamini Hari Gonnade has received her B.E. in Computer Technology from Rajiv Gandhi College of Engineering Research and Technology, Chandrapur, Nagpur University in 2013. Currently, she is doing Master of Technology in Computer Science and

Engineering from WCEM Nagpur, Nagpur University. Her area of interest includes cloud computing and network security.