Attribute-based Encryption Scheme for Secure Multi-group Data Sharing in Cloud

Md. Azhar Islam and Sanjay Madria, Department of Computer Science

(In IEEE *Transactions on Services Computing*,, 2022)

Problem Statement

- When data is stored in cloud or untrusted remote server, it is very challenging to share that data securely if multiple groups of user exist.
- Designing a data sharing scheme in such a scenario needs to achieve following goals:
  - Scheme should be scalable with number of user
  - Member leaving or new member joining cost should be minimal
  - Ensures Forward and Backward Secrecy
  - Group level data isolation
  - Cross-group data sharing
  - Store and share data securely within group members using existing untrusted public cloud
  - Fine grained access control in shared data
  - Prevent collision attack

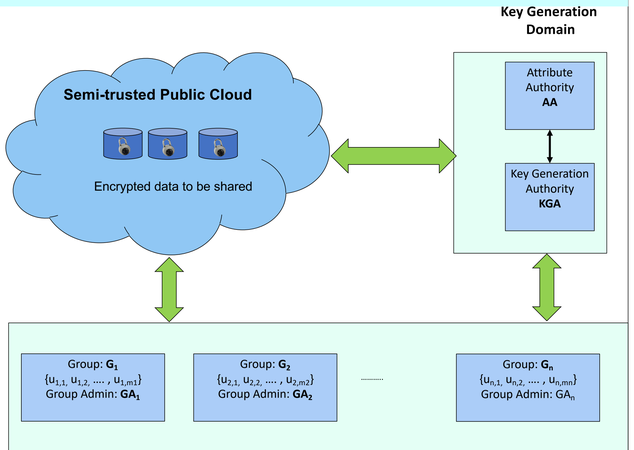
Challenges

- Handle membership change event without affecting keys of currently active users
- Enable on demand cross-group data sharing at file level granularity without affecting all files
- Preventing key-escrow problem

Threat Model

- Public Cloud will try to learn plaintext from stored cypher-text
- Member of one group with same attributes should not be able decrypt data of other group
- A compromised user other than the file owner will try to modify access policy of the file
- Multiple users may collude with each other and try to decrypt cypher text that can not be decrypted individually
- Revoked user may collude with cloud to decrypt data
- Assumption:
  - Cloud is semi-trusted that means it follows the protocols
  - User of one group does not share his TGDH key tree secret key with members of other groups

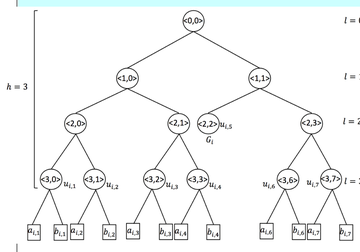
System Architecture



Scheme	Security assumption	Model	Outsourced Decryption	Verifiability	Revocation	Unlimited joining	Multi-group	Collusion resistant
DASS [8]	Decisional PB-DHE	Standard	✗	✗	✓	✗	✗	✗
Hur-I [13]	Generic Group	RO	✗	✗	✓	✗	✗	✗
Hur-II [7]	Generic Group	RO	✗	✗	✓	✓	✗	✗
PIRATTE [6]	Generic Group	RO	✗	✗	✓	✓	✗	✗
VO-ABE [17]	Decisional q-PBDHE	Standard	✓	✓	✗	✗	✗	N/A
CryptCloud+[5]	l-SDH	Standard	✗	✗	✓	✗	✗	✓
Flexible [12]	Generic Group	RO	✓	✗	✓	✓	✗	✓
UserCol [14]	Generic Group	RO	✗	✗	✓	✗	✗	✓
Ours	CDH	RO	✓	✓	✓	✓	✓	✓

Comparison with related schemes in terms of security and functionality.

Group Key Calculation



TGDH Key tree

$$BK_{<l,k>} = g^{K_{<l,k>}} \quad mod \quad p \quad (1)$$

$$SK_{<l,k>} = (BK_{<l+1,2k+1>})^{K_{<l+1,2k>}} \quad mod \quad p$$

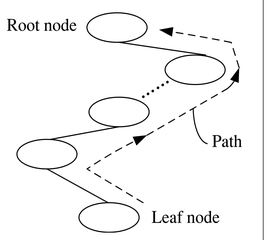
$$= (BK_{<l+1,2k>})^{K_{<l+1,2k+1>}} \quad mod \quad p \quad (2)$$

$$= g^{K_{<l+1,2k>}K_{<l+1,2k+1>}} \quad mod \quad p$$

Group Key calculation Formula

Group Admin's calculation of group public and private key

Round	level l	Secret key $K_{<l,k>}$	Blinded key $BK_{<l,k>}$
1	2	$K_{<2,0>} = (BK_{<3,0>})^{K_{<3,1>}} = g^{K_{<3,0>}K_{<3,1>}}$	$BK_{<2,0>} = g^{K_{<2,0>}}$
		$K_{<2,1>} = (BK_{<3,2>})^{K_{<3,3>}} = g^{K_{<3,2>}K_{<3,3>}}$	$BK_{<2,1>} = g^{K_{<2,1>}}$
		$K_{<2,2>} = s_i$	$BK_{<2,2>} = g^{s_i}$
		$K_{<2,3>} = (BK_{<3,6>})^{K_{<3,7>}} = g^{K_{<3,6>}K_{<3,7>}}$	$BK_{<2,3>} = g^{K_{<2,3>}}$
2	1	$K_{<1,0>} = (BK_{<2,0>})^{K_{<2,1>}} = g^{K_{<2,0>}K_{<2,1>}}$	$BK_{<1,0>} = g^{K_{<1,0>}}$
		$K_{<1,1>} = (BK_{<2,2>})^{K_{<2,3>}} = g^{K_{<2,2}K_{<2,3>}}$	$BK_{<1,1>} = g^{K_{<1,1>}}$
3	0	$K_{<0,0>} = (BK_{<1,0>})^{K_{<1,1>}} = g^{K_{<1,0>}K_{<1,1>}}$	$BK_{<0,0>} = g^{K_{<0,0>}}$



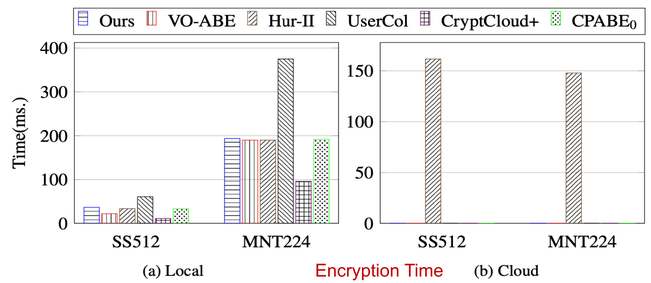
Technical Details

- Data owner will encrypt a file using symmetric encryption key K as CT_F
- Then K is encrypted using our key escrow-free CP-ABE scheme as CT_{Read}
- A file signature key K_{Write} is chosen and it is also encrypted using CP-ABE scheme as CT_{Write}
- Possession of K gives one read permission on file while K_{Write} gives one write permission.
- Owner creates signature on <ID, CT_{Read}, CT_{Write}, PK_{Write} > with his signing key
- Owner also creates a signature on encrypted file CT_F
- Group denominator secret is encrypted with the current TGDH public key
- Owner then send all the information as the ciphertext CT_{Full} to the cloud and cloud stores the encrypted file as following format:

ID	CT_{Read}	CT_{Write}	CT_G	σ_1	σ_2	PK_{Write}	CT_F

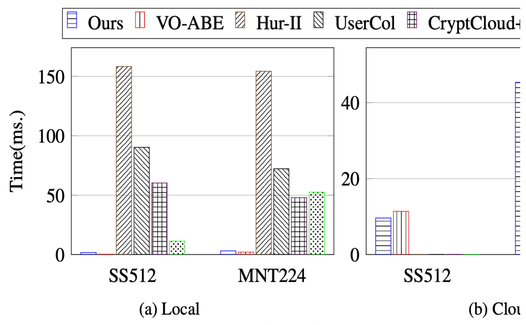
permission-metadata | *verification-metadata*

- Later, any legitimate user can download encrypted files from cloud and decrypt it if he has proper access right.

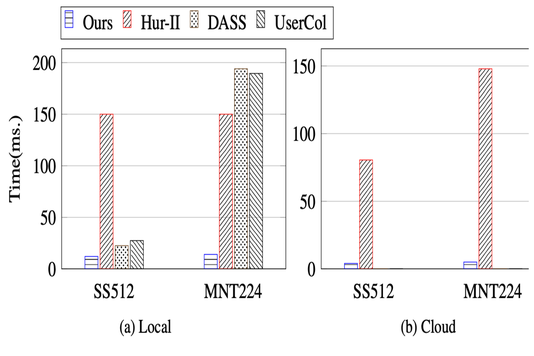


Encryption Time

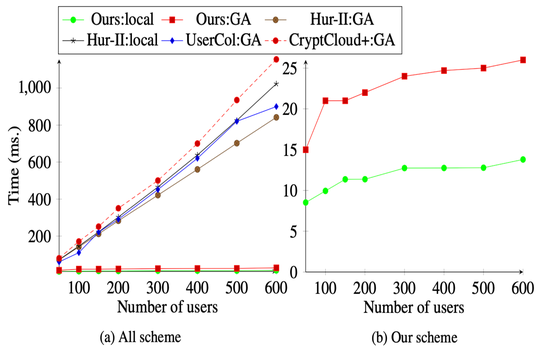
Experiment Results



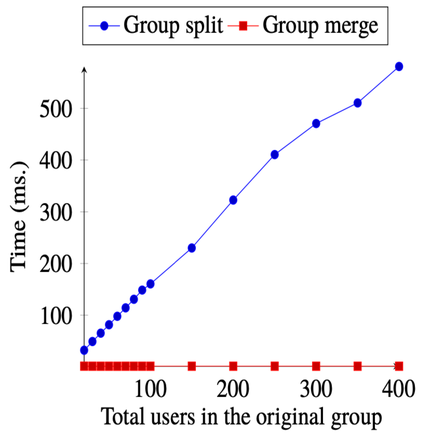
Decryption Time



Re-encryption



Re-keying time



Group spit and merge cost

Scheme	Ciphertext size	Secret key size	Public key size
DASS [8]	$(2a+1)\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_T\rvert + \lvert\mathbb{C}\rvert$	$(b+1)\lvert\mathbb{G}_1\rvert + (\log m)\lvert\mathbb{K}\rvert$	$(u+2)\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_T\rvert$
Hur-I [13]	$(2a+1)\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_T\rvert + \lvert\mathbb{C}\rvert$	$(2b+1)\lvert\mathbb{G}_1\rvert + (\log m)\lvert\mathbb{K}\rvert$	$2\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_T\rvert$
Hur-II [7]	$(2a+1)\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_T\rvert + \lvert\mathbb{C}\rvert$	$2(b+1)\lvert\mathbb{G}_1$	$3\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_T\rvert$
VO-ABE [17]	$(2a+1)\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_T\rvert + \lvert\mathbb{C}\rvert + l_2$	$(b+3)\lvert\mathbb{G}_0\rvert + \lvert p\rvert$	$(u+2)\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_T\rvert$
PIRATTE [6]	$(a+1)\lvert\mathbb{G}_1\rvert + a\lvert\mathbb{G}_2\rvert + \lvert\mathbb{G}_T\rvert + \lvert\mathbb{C}\rvert$	$2b\lvert\mathbb{G}_1\rvert + (b+1)\lvert\mathbb{G}_2\rvert + 2\lvert p\rvert$	$2\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_2\rvert + \lvert\mathbb{G}_T\rvert$
CryptCloud+ [5]	$(2a+5)\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_T\rvert + \lvert\mathbb{C}\rvert$	$(b+4+2\log m)\lvert\mathbb{G}_1\rvert$	$(u+6)\lvert\mathbb{G}_1\rvert + 3\lvert p\rvert$
Flexible [12]	$(2a+6)\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_T\rvert + 2\lvert p\rvert + \lvert\mathbb{C}\rvert$	$(b+4)\lvert\mathbb{G}_1\rvert + 2\lvert p\rvert$	$3\lvert\mathbb{G}_1\rvert + 2\lvert\mathbb{G}_T\rvert + \lvert p\rvert$
UserCol [14]	$(4a+ra+1)\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_T\rvert + \lvert\mathbb{C}\rvert$	$4b\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_T\rvert$	$2(u+3)\lvert\mathbb{G}_1\rvert + 2\lvert\mathbb{G}_T\rvert + (2m-1)\lvert p\rvert$
Ours	$(2a+1)\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_T\rvert + \lvert\mathbb{C}\rvert + l_2$	$2b\lvert\mathbb{G}_1\rvert + 2\lvert p\rvert$	$2\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_T\rvert$

Comparison of storage and communication efficiency with other schemes

Scheme	Encryption	Decryption	
		local	cloud
DASS [8]	$(3a+1)C_1+C_T$	$(s+1)P + s(C_1+C_T)$	N/A
Hur-I [13]	$(3a+1)C_1 + C_T$	$(2s+1)P + C_1 + C_T\log a$	N/A
Hur-II [7]	$(3a+2m+3)C_1 + C_T$	$(3s+1)P + C_T\log a + (m+1)sC_1$	N/A
VO-ABE [17]	$(3a+1)C_1+C_T$	C_T	$(2s+1)P + aC_T$
PIRATTE [6]	$(a+1)C_1 + C_T + aC_2$	$(s+\log a)C_T + (3s+1)P$	aC_2
CryptCloud+ [5]	$(a+5)C_1 + C_T$	$2C_1 + sC_T + (2s+5)P$	N/A
Flexible [12]	$2(a+3)C_1 + 2C_T$	$4C_T$	$(2s+4)P + C_T\log a$
UserCol [14]	$(3a+ra+1)C_1 + C_T$	$(2s-1)C_T + (3s+1)P$	N/A
Ours	$2(a+1)C_1 + C_T + P$	$2C_T$	$(2s+1)P + C_1 + C_T\log a$

Comparison with other schemes in terms of computation cost.

Scheme	Key update		Re-encryption	
	user	Cloud/GA	Owner	Cloud/GA
DASS [8]	bC_1	0	$(3a+1)C_1 + C_T$	0
Hur-I [13]	bC_1	0	0	$(3a+1)C_1 + C_T$
Hur-II [7]	bmC_1	$2(m+1)C_1$	0	$(3a+1)C_1 + C_T$
PIRATTE [6]	0	amC_2	$(a+1)C_1 + C_T + aC_2$	0
CryptCloud+ [5]	0	$3mC_1$	N/A	N/A
Flexible[12]	$(b+1)C_1$	$2mC_1 + P$	0	$C_1 + P$
UserCol [14]	0	$(2m-1)C_1$	0	$(3a+2)C_1 + C_T$
Ours	$C_1\log m$	$(2\log m+3)C_1$	$C_1 + C_T + 2P$	0

Cost of group dynamic change

CONCLUSIONS AND FUTURE WORK

1. We proposed a directly revocable ABE scheme called ReVO- ABE using our proposed data structure called e-TGDH tree.

2. ReVO-ABE does not put any cap on the number of user revocation or joining.

3. A federated cloud architecture (using two clouds) and a novel key binding technique to prevent collusion attacks and achieve revocation under the assumption that at least one of the two clouds acts honestly

4. A multi-group secure data sharing scheme called DMG-SDS to demonstrate that our ABE scheme supports a muti-group setting .

5. We have only considered static access policy in this work; it will be interesting to see how it affects our system if dynamic access policy change is allowed.

M. A. Islam and S. K. Madria, "Attribute-Based Encryption Scheme for Secure Multi-Group Data Sharing in Cloud," in *IEEE Transactions on Services Computing*, vol. 15, no. 4, pp. 2158-2172, 1 July-Aug. 2022, doi: 10.1109/TSC.2020.3038836.