Accepted Manuscript

MGPV: A novel and efficient scheme for secure data sharing among mobile users in the public cloud

Pandi Vijayakumar, S. Milton Ganesh, Lazarus Jegatha Deborah, S.K. Hafizul Islam, Mohammad Mehedi Hassan, Abdulahmeed Alelaiwi, Gibancarlo Fortino

PII: S0167-739X(18)32657-8
DOI: https://doi.org/10.1016/j.future.2019.01.034
Reference: FUTURE 4727

To appear in: *Future Generation Computer Systems*

Received date : 29 October 2018
Revised date : 19 December 2018
Accepted date : 15 January 2019

MGPV: A novel and efficient scheme for secure data sharing among mobile users in the public cloud

Pandi Vijayakumar[1], S. Milton Ganesh[1], Lazarus Jegatha Deborah[1], SK Hafizul Islam[2], Mohammad Mehedi Hassan[3,*], Abdulahmeed Alelaiwi[3] and Gibancarlo Fortino[4]

[1]Department of Computer Science and Engineering, University College of Engineering Tindivanam, Tindivanam, Tamilnadu, 604001, India, Email: {vijibond2000, softengineermilton, blessedjeny}@gmail.com,
[2]Department of Computer Science and Engineering, Indian Institute of Information Technology Kalyani, West Bengal 741235, India, Email: hafi786@gmail.com
[3]Chair of Smart Cities Technology, College of Computer and Information Sciences, King Saud University Riyadh 11543, Saudi Arabia, Email: mmhassan@ksu.edu.sa, aalelaiwi@ksu.edu.sa
[4]Department of Informatics, Modeling, Electronics, and Systems, University of Calabria, Italy Email: giancarlo.fortino@unical.it

Abstract—With the significant popularity and utility, the web services have uniquely emerged as a new paradigm shift to many enterprises such as banking, government applications, telecom sectors and other solution providers. When web services are integrated with cloud services, web services achieve more flexibility and performance. Hence, through a web service, a mobile phone user can upload sensitive documents to cloud and share them with employees and customers, but the security in the cloud is yet to be completely resolved. Recently, the authors Zhu and Jiang have securely shared group keys among cloud users without secure communication channels. But, we have recently proved that, the existing method is susceptible to man-in-the-middle attack and message modification attack. A new protocol termed as MGPV has been proposed in this research work which averts all the possible attacks. It minimizes the computation complexity and ensures that the documents are accessible only by valid group users. It ensures that even the group manager and the cloud cannot access the documents stored in the cloud. The experiments conducted on the mobile cloud environments reveal that this protocol is worthy of implementation in the real world scenarios.

Keywords—Security, Access controls, Man-in-the-Middle attack, Message Modification Attack, Data encryption

1 INTRODUCTION

WITH the advent of customized web services, mobile phones and cloud storage, the secure sharing of sensitive documents among mobile users has become very common now-a-days [1], [2], [29], [30], [31], [35], [36]. It is more convenient for a mobile user to share a document with his peers through a web service. Because of the ubiquitous use of mobile phones and cloud computing, this scheme of sharing documents among the mobile user community is increasing exponentially day by day. In a typical context, a manager of a reputed company may want to share some sensitive documents with the employees of his company. Obviously, the manager would prefer to store the document from his mobile into the cloud using a web service due to the elastic nature and ease of use of cloud and web services [3], [4], [29], [30]. Though a web service is a viable option for mobile users to upload the documents, the documents if stored in a private file server, may need consistent support from maintenance personnels and security experts. But, if the user uploads a file to cloud storage, then the server maintenance and security issues are performed by cloud service providers. Additionally, the flexibility in computing, storage and licensing issues are vested with the cloud service providers themselves. Thus, web services when integrated with cloud services complement each other and emerge as a more powerful paradigm to solve the document storage and retrieval purposes.

Since the present day android powered mobile phones come with more than 2 GB of RAM and 2 GHz of computational capability, access to web services and storage applications in the cloud have become very handy [5-7], [41][42]. Hence, if a web service is available, a manager (cloud user) shall upload the business related documents to the public cloud not only for easy storage and retrieval purposes, but for their sharing among other users as well [8].

In such a scenario, though many users attempt to utilize the sharing facilities through public cloud servers, attacks on the cloud storage by hackers and other fraudsters seem to be increasing in the recent past. It can be seen that, the attacks on the cloud and web services have been a matter of common scenario [9], [10], [32], [33], [34] which are yet to be completely resolved [37], [38]. Moreover, a mobile phone user can create hypersensitive documents through a web application. These documents are hosted in the cloud service which could be shared with their peer employees and valuable customers. In connection to this, since the data to the cloud passes through a public channel, the security concern is usually compromised in certain situations. Therefore, the clear idea and motivation behind this research work aims at resolving such security issues.

In this context, Zhu and Jiang in 2016 have proposed a collusion resistant scheme which enables the secure document storage and sharing among the members of a dynamic group in the public cloud [11]. They claimed that, without employing the secure communication channels, they can securely transfer the keys to the group users.

An attacker can make use of Man-in-the-Middle (MITM) attack and the message modification attack as cited in [28] to break the scheme proposed by Zhu and Jiang in [11]. Hence, in this research work, we have taken the attacks on the Zhu and Jiang's work into consideration and proposed a novel collusion aware protocol which can be employed in a mobile user environment for enabling the mobile users to share documents through the public clouds without the fear of being fiddled with by attacker.

Following are the objectives of this novel research work. 1) To propose a novel collusion aware document storage technique called Modified Group key Protocol Version (MGPV) based on Zhu and Jiang's scheme [11] which is free from MITM attack, message modification attack and other possible attacks, 2) To minimize the computational complexity incurred during the upload and download of document in the cloud server, 3) To introduce a novel protocol which ensures the document confidentiality between data owner and mobile cloud users even restricting the group manager and the cloud server from accessing the document.

The rest of this research contribution has been organized in such a way that Section 2 surveys the recent works in line with the proposed work which strive to share the data among other users in the cloud environments. The merits and limitations of the protocols under consideration have been analyzed. section 3 presents the proposed protocol in the context of mobile cloud users and the cloud storage. Section 4 analyses the proposed protocol against the possible attacks and section 5 provides a detailed discussion of the results obtained during the implementation of this research work. Finally, section 6 concludes this research work.

2 A BRIEF OVERVIEW OF THE LITERATURE

The past literature can be spotted with numerous worthwhile secure methods which strives to improve security to group communication among multiple users. All of these schemes try to improvise upon the existing schemes in way or the other to enable secure group communication.

A past work proposed in 2003 by Kallahalla et al. is one such work which incurs an overhead due from frequent updating of the keys pertaining to various file blocks [3]. This work supports frequent join and leave operation by multiple users simultaneously.

A similar work in the same year was proposed by Goh et al. which concentrates on ensuring secure group key management with novel procedures for the key revocation operation [12]. Also, another work in 2005 had some contribution to do with the constant size with regard to the privately kept keys and the encoded text [13]. Nevertheless, these works relatively fallback in efficiency as a new group key being generated if a new user is part of the group or an old user leaving the same.

In the successive year, a new policy named Key-Policy Attribute-Based Encryption (KP-ABE) was put forth to enforce improved security for communication between a group of entities [14] and Lu et al. had earned the credit for introducing a secure scheme based on provenance to enforce the group security [15].

But, a recent scheme put forth in 2016 by Vijayakumar et al. had made efficient use of the technique hidden inside Chinese Remainder Theorem (CRT) for the secure transportation of the group key to its members. This work in spite of showing a low computational complexity suffers from frequent leave and join operations demanding the computation of new key for secure communication between the group members utilizing mobile phones for the same.

A recently introduced scheme [17] called Mona ensures secure uploading and downloading of secret documents between the corresponding group members and a similar scheme for providing similar security service was proposed by Zhou et al. [18] which provides access to the contents based on the user roles. The work proposed in [19, 20] demonstrate the task of improving group communication as well.

But, in spite of the multiple existing schemes, the scheme cited in [11] seems to be most recent work in this line to securely transport the private group keys over the public medium. It is a novel and highly worthwhile protocol. But, the hackers are recklessly determined and lurking to find any slightest loophole to attack the existing protocol proposed by anyone. In this way, the protocol proposed by Zhu and Jiang is not an exemption. Thus, despite being a highly efficient and trustworthy protocol, this falls prey to the MITM attack.

Moreover, for ensuring secure group communication, many protocols have been proposed. A number of protocols have been proposed using CRT for efficient communication in networks with reduced computational cost for key management. Vijayakumar et al. [22, 23] have proposed novel methods for secure multicast communication with relatively less overheads. Moreover, they have introduced a new rotation based algorithm to enhance the security supporting both batch leave and join operations [24]. The work proposed by Vijayakumar et al. achieve less computational complexity for efficient group communication with the application of CRT. Many other protocols have been proposed in the literature for similar security services among the group members [21], [25], [26], [27], [40].

Though the work proposed by Zhu and Jiang in 2016 as referred in [11] is the recent scheme to enable secure group communication, the works presented in [28] clearly prove that this scheme can be broken through two of the most popular attacks. They are MITM attack and the message modification attack. Moreover, the work described in [28] puts the work proposed by Zhu and Jinag in [11] at jeopardy and hence paves the demand for another work in this line to fill the gap created by the attacks. The architecture of the proposed system and the notations used in the existing protocol are mentioned in [11]. This scheme was invented by Zhu and Jiang in 2016 which has been a novel and secure protocol of its kind in providing secure group communication over public communication channel. But, the more recent work as portrayed in [28] analyses this work in all aspects and had proved that this scheme in [11] can be prone to MITM attack and the message modification attacks.

3 PROPOSED MODIFIED GROUP KEY PROTOCOL VERSION

The proposed protocol consists of the following five phases offered as appropriate web services. They are system initialization by the group manager, mobile user registration phase, file upload by the mobile user, file download by mobile user and the mobile user revocation phase. Also, the proposed protocol consists of three major entities such as mobile user (MU), group manager

(GM) and the cloud service provider (CSP). The notations used in the proposed protocol are described in Table 1.

TABLE 1

NOTATIONS AND THEIR MEANING

S.No.	Notations	Meaning
1.	G_1, G_2	Additive cyclic group
2.	q	Prime number which is the order of the additive cyclic groups G_1, G_2
3.	P, G, W, Y, X	Points in the group G_1 generated by group manager in which G is kept as secret
4.	Z	Point in the group G_2
5.	f	Hash function $\{0,1\}^* \rightarrow Z_q^*$
6.	f_1	Hash function $\{0,1\}^* \rightarrow G_1$
7.	γ, l	Random numbers of the group manager from Z_q^*
8.	a_i, b_i	Random numbers generated by mobile user i from Z_q^*
9.	ID_i	The identity of mobile user i
10.	pk_i	Public key of mobile user i
11.	sk_i	The corresponding private key to pk_i
12.	ac_i	Account number of the mobile user i
13.	$Enc_E()$	Symmetric encryption algorithm using the document encryption key E
14.	$Aenc_{sk_i}()$	Asymmetric encryption algorithm using the secret key sk_i of the mobile user i
15.	U	Point generated by group manager during mobile user registration
16.	ru_i	Random number for mobile user i generated by the group manager
17.	rt_i	Corresponding random number of group manager for ru_i of mobile user i. It is generated by the group manager
18.	S_1, S_2	Points computed by group manager corresponding to the user i
19.	ID_{doc}	Identity of document i
20.	doc	Sensitive document to be uploaded and downloaded securely
21.	L_1, L_2, L_3	Parameters computed by group manager for the corresponding mobile user i during the file upload process
22.	rd_i	Random number selected by the group user for secure document download
23.	$D1_i, D2_i$	Parameters computed by mobile user i for secure document download
24.	t_i	Time at which the document with identity Doc_i was uploaded to the CSP
25.	α_i, β_i	Secret parameters generated by the group manager for each user with identity ID_i to enable secure communication between the cloud server and the mobile user with identity ID_i
26.	r_i	Random number i selected by group manager during the registration of mobile users
27.	K_g	Group key used by group manager to encrypt documents from mobile user
28.	μ	Temporary value containing the hidden group key K_g
29.	ek_i	Random key selected by the mobile user to compute the document encryption key E
30.	$Enc_{K_g}()$	Symmetric key encryption algorithm using the group key K_g

3.1 System initialization by the group manager

The GM proposes a bilinear map system which consists of $S = (q, G_1, G_2, e(.,.))$ where G_1 and G_2 are additive cyclic groups based on the same prime order q and $e: G_1 \times G_1 \rightarrow G_2$.

1. The GM randomly selects two points P and G from G_1 and also selects three random numbers $\gamma, l \in Z_q^*$.
2. Computes four parameters such that $W = \gamma.P, Y = \gamma.G, X = l.P$ and $Z = e(P, G)$.
3. The GM publishes the parameters such as $S, P, W, Y, X, Z, f, f_1, Enc(), Aenc()$ where f is a hash function: $\{0,1\}^* \rightarrow Z_q^*$, f_1 is also a hash function $\{0,1\}^* \rightarrow G_1$ and $Enc()$ is a symmetric encryption algorithm and $Aenc()$ is an asymmetric encryption algorithm.
4. The GM keeps the parameters such as G, γ, l as secret parameters.

3.2 Mobile user registration phase

In this phase, a mobile user registers with the GM to get the secret parameters in order to securely upload and download files to/from the cloud server.

1. The MU sends (ID_i, pk_i, a_i, ac_i) as a request to the GM where ID_i, pk_i, ac_i refer to the identity, public key and the account number for payment by MU to the CSP and a_i is a random number from Z_q^*.

2. After receiving the request from MU, the GM chooses a random number $r_i \epsilon Z_q^*$ and computes $R = e(P, P)^{r_i}$ and $U = (r_i + l.\gamma.a_i.f(ID_i \| pk_i \| ac_i)).P$. Then, it sends the newly computed parameters R and U to the MU. The main difference between our protocol and the existing

work [11] is that, the secret parameter l is multiplied with $\gamma.a_i.f(ID_i\|pk_i\|ac_i)$ to generate U.

3. After receiving R and U from GM, the MU confirms whether these parameters have come from the legitimate GM. To verify that, the MU separately computes $R.e(a_i.f(ID_i\|pk_i\|ac_i).W,X)$ and $e(U,P)$ and checks whether $R.e(a_i.f(ID_i\|pk_i\|ac_i).W,X) \stackrel{?}{=} e(U,P)$. The proof is given below.
$$\begin{aligned}&R.e(a_i.f(ID_i\|pk_i\|ac_i).W,X)\\ &= R.e(a_i.f(ID_i\|pk_i\|ac_i).\gamma.P,l.P)\\ &= R.e(\gamma.a_i.f(ID_i\|pk_i\|ac_i).P,l.P)\\ &= R.e(P,P)^{l.\gamma.a_i.f(ID_i\|pk_i\|ac_i)}\\ &= e(P,P)^{r_i}.e(P,P)^{l.\gamma.a_i.f(ID_i\|pk_i\|ac_i)}\\ &= e(P,P)^{r_i+l.\gamma.a_i.f(ID_i\|pk_i\|ac_i)}\\ &= e(U,P)\end{aligned}$$
4. If the verification succeeds, the MU sends $ID_i, b_i, Aenc_{sk_i}(ID_i,a_i,ac_i)$ to GM where b_i is a random number from Z_q^*.
5. The GM decrypts $Aenc_{sk_i}(ID_i,a_i,ac_i)$ using the public pk_i of the user and checks whether the ID_i in the decrypted message is equal to ID_i in the message. It also checks whether a_i is equal to the same a_i which was received in the first step. Now, the GM chooses $ru_i, rt_i \in Z_q^*$.Then, the GM sends $Aenc_{pk_i}(ru_i,rt_i,a_i,b_i)$ to the corresponding MU. The GM also computes $\alpha_i = rt_i.G, \beta_i = G.\frac{a_i}{rt_i+a_i}$ and adds ID_i, α_i and β_i of the corresponding user in the group user list (GUL) as depicted in Table 2. Finally, the GM sends the group identity ID_{group}, the updated GUL, the timestamp t_i and the signature $Sig(GUL)$ to the CSP.
6. The MU decrypts $Aenc_{pk_i}(ru_i,rt_i,a_i,b_i)$ received from GM using the corresponding private key sk_i and verifies whether the a_i, b_i from the decrypted message are the ones which were sent by this MU. Followed by this, MU stores ru_i and rt_i in its local database.
7. The CSP, on receiving the updated GUL from the group manager, verifies the freshness of the message through t_i and also verifies the authenticity of the GM as cited in [11] as follows
$$\begin{aligned}e(W,f_1(GUL)) &= e(\gamma.P,f_1(GUL))\\ &= e(P,\gamma.f_1(GUL))\\ &= e(P,Sig(GUL))\end{aligned}$$
8. If the verification is successful, the GM replaces the old GUL with the new one.

TABLE 2
UPDATING THE GROUP USER LIST

Identity	Secret parameter 1	Secret parameter 2
ID_1	α_1	β_1
ID_2	α_2	β_2
…	…	…
ID_m	α_m	β_m

3.3 File upload by mobile user

Let us assume that an MU wants to upload a document to the CSP securely through the corresponding web service.

1. The MU randomly selects a symmetric encryption key $ek_i \epsilon Z_q^*$ and computes $E = Z^{ek_i}$. Also, it selects a suitable identity ID_{doci} for the document to be uploaded and encrypts the document using a symmetric encryption algorithm as $Enc_E(doc)$. Also, MU computes two parameters $L_1 = W.ek_i$, $L_2 = P.ek_i.f(a_i\|b_i\|ru_i)$. Then, the MU sends the message ID_i, ID_{group}, $Enc_{ru_i}(ID_i, ID_{doci}, Enc_E(doc), L_1, L_2)$ to the GM.
2. Upon receiving the message from the mobile user, the GM finds that the user with the identity ID_i has sent an encrypted document to be uploaded to the CSP. Then, the GM retrieves the secret parameter of the mobile user. Firstly, the GM retrieves the secret parameter ru_i which is stored in its local database and decrypts $Enc_{ru_i}(ID_i, ID_{doci}, Enc_E(doc), L_1, L_2)$ to get the parameters such as $ID_i, ID_{doci}, Enc_E(doc), L_1, L_2$. Then, it checks whether the ID_i in the decrypted part of the message is the same as the ID_i present in the message. Now, the GM randomly selects a group key $K_g \epsilon Z_q^*$ and ensures that the value of K_g is very much smaller than the values of ru_i in order to exploit the facility supported by CRT. Subsequently, the GM re-encrypts the document as $ED = Enc_{K_g}(Enc_E(doc))$. In order to hide the group key K_g, the GM computes the temporary value μ such that, $\mu = K_g + \prod_{i=1}^{n} ru_i$ where, ru_i is the secret parameter shared between GM and the corresponding mobile user i. Moreover, to enable the receiver to compute the decryption key, GM computes $L_3 = G.\frac{1}{\gamma+f(a_i\|b_i\|ru_i)}$ and let $LD = L_1, L_2, L_3$. Let us also assume that $DL = (ID_{group}, ID_{doci}, ED, \mu, LD)$. Now, the group manager computes $\sigma_{DL} = \gamma.f_1(DL)$ which is the signature of GM and sends $DL = (ID_{group}, ID_{doci}, ED, \mu, LD), \sigma_{DL}$ to the CSP. Also, the GM creates the updated data list DL to the CSP which is mentioned in Table 3.

TABLE 3
UPDATING THE DATA LIST

Document ID	Timestamp
ID_{doc1}	t_1
ID_{doc2}	t_2
…	…
ID_{docn}	t_n

Followed by that, the GM sends $DL, sig(DL), t_i$ to the CSP where $sig(DL) = \gamma.f_1(DL)$, and t_i is the timestamp at which the signature is generated.

3. Upon receiving this message, CSP verifies the authenticity of the DL by checking whether $e(W,f_1(DL)) \stackrel{?}{=} e(P,Sig(DL))$ as follows.

$$\begin{aligned}e(W,f_1(DL)) &= e(P,Sig(DL))\\ &= e(P,\gamma.f_1(DL))\\ &= e(P,f_1(DL))^{\gamma}\end{aligned}$$

$$= e(\gamma.P, f_1(DL)) = e(W, f_1(DL))$$

3.4 File download by mobile user

The MU, using the file download web service, wants to securely download the document with identity ID_{doci} from the cloud server and it performs the following steps as described below.

1. The MU randomly selects $rd_i \epsilon Z_q^*$ and computes $DK = Z^{rd_i}$. Then, encrypts the identity of the document and the identity of the user as $RD = Enc_{DK}(ID_{doci}, ID_i, rd_i)$. Also, it computes $D1_i = P.\frac{rd_i}{rt_i + a_i}$ and $D2_i = rd_i.P$. Then, the MU sends $(ID_i, ID_{group}, RD, D1_i, D2_i)$ to the CSP.
2. The CSP sees the ID_i in the message and retrieves the corresponding $\alpha_i = rt_i.G, \beta_i = G.\frac{a_i}{rt_i + a_i}$ from its database. Now, the CSP finds the decryption key DK to decrypt the message from MU as follows.
$$e(D1_i, \alpha_i)e(D2_i, \beta_i)$$
$$= e(D1_i, rt_i.G)e\left(D2_i, G.\frac{a_i}{rt_i + a_i}\right)$$
$$= e\left(P.\frac{rd_i}{rt_i + a_i}, rt_i.G\right)e\left(rd_i.P, G.\frac{a_i}{rt_i + a_i}\right)$$
$$= e(P,G)^{\frac{rd_i}{rt_i + a_i}.rt_i}e(P,G)^{rd_i.\frac{a_i}{rt + a_i}}$$
$$= e(P,G)^{\frac{rd_i.rt_i + rd_i.a_i}{rt_i + a_i}}$$
$$= e(P,G)^{\frac{rd_i(rt_i + a_i)}{rt_i + a_i}}$$
$$= e(P,G)^{rd_i}$$
$$= Z^{rd_i}$$
$$= DK$$
Now, the CSP decrypts RD as $Dec_{DK}(Enc_{DK}(ID_{doci}, ID_i, rd_i))$ and gets access to ID_{doci}, ID_i, rd_i and compares this ID_i with the ID_i sent along with RD in the message. The CSP also checks whether this ID_i is present in the GUL as mentioned in Table 2. If successfully verified, then the CSP assumes that the user with ID_i is a valid user of the group. Moreover, this DK can be calculated only with the parameters α_i and β_i sent to the CSP by the GM during the corresponding mobile user registration process.
Then, CSP retrieves L_1 and L_2 from LD of the corresponding document and computes $S_1 = rd_i.L_1$ and $S_2 = rd_i.L_2$. Finally, the CSP sends S_1, S_2, L_3, μ, ED to the MU who has sent the request for file download.
3. User does the decryption of the encrypted document as follows.
Firstly, the MU retrieves the group key K_g such that $K_g =$ μ $mod\ ru_i$. Then, the user decrypts the double encrypted document as $Dec_{K_g}(ED) = Dec_{K_g}\left(Enc_{K_g}(Enc_E(doc))\right)$ and gets access to $Enc_E(doc)$ which is encrypted using the key $E = Z^{ek_i}$.

Secondly, MU finds the encryption key $E = Z^{ek_i}$ as follows.

$$e\left(S_1, \frac{1}{rd_i}.L_3\right)e\left(S_2, \frac{1}{rd_i}.L_3\right)$$
$$= e\left(rd_i.L_1, \frac{1}{rd_i}.L_3\right)e\left(rd_i.L_2, \frac{1}{rd_i}.L_3\right)$$
$$= e(L_1, L_3)^{rd_i.\frac{1}{rd_i}}e(L_2, L_3)^{rd_i.\frac{1}{rd_i}}$$
$$= e\left(W.ek_i, G.\frac{1}{\gamma + f(a_i\|b_i\|ru_i)}\right)$$
$$e\left(P.ek_i.f(a_i\|b_i\|ru_i), G.\frac{1}{\gamma + f(a_i\|b_i\|ru_i)}\right)$$
$$= e\left(\gamma.P.ek_i, G.\frac{1}{\gamma + f(a_i\|b_i\|ru_i)}\right)$$
$$e(P,G)^{\frac{ek_i.f(a_i\|b_i\|ru_i)}{\gamma + f(a_i\|b_i\|ru_i)}}$$
$$= e(P,G)^{\frac{\gamma.ek_i}{\gamma + f(a_i\|b_i\|ru_i)}}e(P,G)^{\frac{ek_i.f(a_i\|b_i\|ru_i)}{\gamma + f(a_i\|b_i\|ru_i)}}$$
$$= e(P,G)^{\frac{ek_i.(\gamma + f(a_i\|b_i\|ru_i))}{\gamma + f(a_i\|b_i\|ru_i)}}$$
$$= e(P,G)^{ek_i}$$
$$= E$$

Thus, the MU decrypts the encrypted document as $Dec_E(Enc_E(doc))$ and gets the document which is a sensitive one.

3.5 Mobile user revocation by group manager

Through the mobile user revocation in web service, an MU with the identity ID_i requests the GM for user revocation from the group. To achieve user revocation, GM and CSP perform the following steps.

1. GM downloads the GUL as mentioned in Table 2 from the CSP and removes the details such as ID_i, α_i, β_i from the downloaded GUL.
2. GM downloads the document $ED = Enc_{K_g}(Enc_E(doc))$ of the MU which was encrypted using the current group key K_g.
3. GM randomly selects a new group key $K'_g \varepsilon Z_q^*$ such that the value of K'_g is very much smaller than the value of ru_i of all the users to enable CRT to hide it. It also computes μ′ such that $\mu' = K'_g + \prod_{j=1\ and\ j \neq i}^{n} ru_j$ where j refers to the number of active users in the group.
4. Now, the GM re-encrypts the document using the new group key K'_g such that $ED' = Enc_{K'_g}(Enc_E(doc))$ and computes a fresh signature $\sigma'_{DL} = \gamma.f_1(DL)$ and sends $DL = (ID_{group}, ID_{doci}, ED', \mu', LD)$ and σ'_{DL} to the CSP.
5. Receiving this message from GM, the CSP verifies the validity of the received signature $\sigma'_{DL} = \gamma.f_1(DL)$ by checking $e(W, f1(DL)) \stackrel{?}{=} e(P, Sig(DL))$ and if successful, updates the details of the corresponding document in Table 3 with the new timestamp. Moreover, CSP replaces the old value of DL with the recently received values.

4 Security Analysis of the Proposed Protocol

The proposed protocol has been designed in such a way that it is resistant to all the attacks. In this section, the security of MGPV protocol is provided during MITM attack, message modification attack and masquerading. Moreover, the proposed protocol is checked as to whether it preserves the forward and backward secrecies and ensures secure key distribution.

4.1 Man-in-the-Middle attack

In this attack, an attacker who is present in the middle between two legitimate entities intercepts the communication between them without their knowledge. The protocol in [11] is susceptible to MITM attack as clearly explained in [28]. The attack made in the protocol is as follows. During the registration process, by substituting $W = \gamma.P$, the attacker tries to compute the value of

U which is composed of $r.P$ and $\gamma.P.v_1.f(pk_a\|ac\|ID_i)$ such that $U = r.P + \gamma.P.v_1.f(pk_a\|ac\|ID_i)$. In this case, the value of $\gamma.P$ can be easily substituted with the value of W as it is a public parameter. But, in the proposed protocol, in order to protect the registration process from MITM attack, U is computed as $U = \left(r + l.\gamma.v_1.f(ID_i\,\|pk_i\|\,ac_i)\right).P$ in which case, the value of $l.\gamma.P$ cannot be computed by the attacker by any means and hence, the registration process is secured from the MITM attack.

4.2 Message modification attack

In this attack, an attacker tries to alter, insert or delete some portions of the message sent by the sender to the receiver. As pointed out in [28], the attacker has the chance to retrieve the secret key $KEY = (x_i, A_i, B_i)$, the attacker can modify the message $Enc_{B_i}(ID_{data}, C_1, C_2, C, t_{data})$ by decrypting it using B_i without the knowledge of the sender and the receiver. In the protocol proposed in this manuscript, the attacker has been restricted from computing the value of the parameter U which means, there is no change to derive the private key shared between the group manager and the mobile user. Thus, the proposed protocol is free from the message modification attack.

4.3 Masquerading

In the protocol proposed in [11], the attacker has access to $KEY = (x_i, A_i, B_i)$ and hence can masquerade as a legitimate cloud user by sending $ID_{group}, ID_i, Enc_{A_i}(ID_{data})$ to the CSP. The CSP being unaware of the attack being made, will send $DF = \left(ID_{group}, ID_{data}, CE, EK, t_{data}\right), \sigma_{DF}$. Since the attacker has access to $V_i = f(B_i)$, he can easily derive the group key K and hence can decrypt the C to get the actual document sent by the sender. In the proposed protocol, since the private keys are securely distributed between GM and MU, the attackers have no chance of getting access to the sensitive document sent by the sender of the message. Thus, the proposed protocol averts any masquerading by the attackers.

4.4 Key distribution

The main objective of the proposed work is that of securely distributing the secret keys between the group manager and mobile users over insecure channels. In order to securely distribute the private keys, in this research work, the MU who wants to register himself with the GM, initially sends his public key pk_i and his identity ID_i along with a random number a_i specific to this communication. GM authenticated himself by sending U, R to the MU. In order to modify the value of U, an attacker ought to compute $U = \left(r + l.\gamma.v_1.f(ID_i\,\|pk_i\|\,ac_i\,)\right).P$ for some unknown $l.\gamma\,\epsilon\,Z_q^*$ which is infeasible due to decisional Diffie-Hellman problem. Moreover, the secret key for document encryption ru_i is sent by GM as $Aenc_{pk_i}(ru_i, a_i, b_i)$ to MU which can be decrypted only the corresponding MU alone. Thus, the secure key distribution is ascertained in the proposed MGPV protocol.

4.5 Forward and Backward Secrecies

Whenever a mobile user wants to upload a document, he encrypts the document as $Enc_E(doc)$ where $E = Z^{ek_i}$ in which ek_i is the secret key randomly selected by the respective mobile user MU_i. When the document is uploaded by the cloud user and the while document reaches GM, the GM re-encrypts the document using the group key K_g such that $ED = Enc_{K_g}\left(Enc_E(doc)\right)$ and hides the group key k_g such that $\mu = K_g + \prod_{i=1}^{n} ru_i$. The temporary value μ is made from the secret parameter ru_i of each of the group members.

In this case, it has become clear that, a user who does not have the value of ru_i cannot retrieve the group key K_g. Thus, a user can access the encrypted documents only during his presence in the group. Moreover, if an MU joins the group or leave the group, the group key K_g is newly computed rejecting any room for forward or backward accesses. Thus the proposed protocol ensures the forward and backward secrecies of the system.

5 RESULTS AND DISCUSSION

The proposed scheme is compared with other existing schemes such as Mona proposed by Liu et al. [17], RBE method proposed by Zhou et al. [18], Delerablee et al.'s ODBE protocol [20], Liang et al.'s scheme [39] and Zhu and Jiang's scheme [11]. The comparison of the security performance in Table 4 shows the capabilities provided by the proposed scheme.

The significance of the proposed MGPV protocol can be understood from the fact that, when a sensitive document is shared by an MU through GM, even the GM cannot decrypt the document and view the contents. The authenticated group users alone can decrypt the document and access the contents. But, in the scheme proposed by Zhu and Jiang [11], the GM is assumed to be fully trusted by the other parties. This means that, a document shared by a data owner can be decrypted by the GM. Thus, the GM has access to all the documents shared by any of the group user. But, the proposed scheme ensures the confidentiality of the document between the document owner and the document receivers alone and restricts the GM and CSP from accessing the document.

The proposed protocol called MGPV has been simulated using pbc library and the results thus obtained are compared with Mona proposed by Liu et al. in [17], RBE proposed by Zhou et al. [18], Liang et al.'s scheme [39] and the protocol proposed by Zhu and Jiang in [11]. The experiments were conducted such that G_1 consists of elements of size 161 bits and G_2 consists of elements of size 1024 bits. The elliptic curve has been selected such that it has a group order of 160 bits. The setup for mobile user and group manager has been made in cygwin tool in a computer with 2.8 GHz Core i3 processor, 4GB DDR3 RAM and with the Windows 7 operating system installed in it. The cloud server has been simulated in cygwin tool installed in a computer of 3.2 GHz Core i5 processor of 64 bits with 8GB DDR3 RAM containing Windows 7 operating system.

Let us assume that the time required to perform an addition operation, point multiplication operation, multiplication operation, exponential operation, hash operation, pairing operation, division operation, encryption operation, point addition and decryption operation be represented by T_A, T_{PM}, T_M, T_E, T_H, T_P, T_D, T_{Enc}, T_{PA} and T_{Dec} respectively.

Group key computation and retrieval cost is shown in Table 5. It is observed that, for 10 users, MGPV takes 0.3 ms which is 96.41 ms less than Mona, 7.29ms less than Zhu and Jiang scheme, 12.79 ms less than Zhou et al.'s scheme and 19.69 ms less than Liang et al's scheme. Also, for 100 users, MGPV takes 3.001 ms which is 959.48 ms less than Mona, 67.59ms less than Zhu and Jiang scheme, 73.09 ms less than Zhou et al.'s scheme and 196.999 ms less than Liang et al's scheme respectively. Hence, the results show that the proposed scheme achieves less group key computation overhead compared to other works. Similarly, for group key retrieval, MGPV achieves less computational complexity. For 50 users MGPV incurs 0.005 ms which is 16.94 ms and 29.99 ms, 40.39 ms, 71.19 ms less than Mona, Zhu and Jiang's scheme, Zhou et al.'s scheme and Liang et al.'s scheme respectively.

TABLE 4
COMPARISON OF THE SECURITY PERFORMANCE

Scheme vs parameter	**Secure Key Distribution**	**Secure user revocation**	**Anti-collusion attack**	**Confidentiality between data owner and data user only**	**MITM attack**	**Message Modification attack**
Mona	no	no	no	no	no	no
Zhou et al.'s scheme	no	no	no	no	no	no
Liang et al.'s scheme	no	Yes	yes	no	no	no
Zhu and Jiang's scheme	no	Yes	yes	no	no	no
MGPV protocol	yes	Yes	yes	yes	yes	yes

TABLE 5
GROUP KEY COMPUTATION COST

Scheme vs computation cost	**Group key computation Cost by GM (ms)**		**Group key verification and retrieval cost by the user (ms)**	
	Cost for 1 user (ms)	**Cost for n users (ms)**	**Cost if only 1 user exists in the group (ms)**	**Cost if n users exist in the group (ms)**
Mona	$2T_{PM} + 1T_P + 1T_E$	$(n+1)T_{PM} + n(T_P + T_E)$, n refers to the number of revoked users	$8T_{PM} + 4T_{PA} + 5T_P + 1T_H$	$(nT_M + 1T_{PM}) + (8T_{PM} + 4T_{PA} + 5T_P + 1T_H)$, n refers to number of revoked users
Zhu and Jiang	$1T_{PM} + 1T_E$	$1T_{PM} + nT_E$	T_{PM}	nT_{PM}
Zhou et al. scheme	$1T_E + 1T_E + 1T_E + 1T_E + 1T_H + 1T_E + 1T_{PM} = 4T_E + 1T_H + 1T_E + 1T_{PM}$	$1T_E + 1T_E + 1T_E + nT_E + 1T_H + 1T_E + 1T_{PM} = 4T_E + nT_E + 1T_H + 1T_{PM}$	$1T_E + 1T_E + 1T_E + 1T_E + 1T_H + 1T_E + 1T_{PM} = 4T_E + 1T_H + 1T_E + 1T_{PM}$	$1T_E + 1T_E + 1T_E + (n-1)T_E + 1T_H + 1T_E + 1T_{PM} = 4T_E + (n-1)T_E + 1T_H + 1T_{PM}$
Liang et al. scheme	$1T_E + 1T_{PM} + 1T_E = 2T_{E+}1T_{PM}$	$n * (2T_E + 1T_{PM})$	$1T_E + 1T_{PM} + 1T_E + 1T_{PM} = 2T_E + 2T_{PM}$	$(n * 2T_E + 2T_{PM})$
MGPV Protocol	$1T_A + 1T_M$	$1T_A + nT_M$	$1T_D$	$1T_D$

Moreover, for 100 users, MGPV incurs 0.006 ms which is 16.99 ms, 59.99 ms, 75.39 ms and 141.19 ms less than Mona, Zhu and Jiang's scheme, Zhou et al.'s scheme and Liang et al.'s scheme respectively.

The computation cost of the uploading operation of a file of size 1KB with varying number of revoked users is calculated for the proposed MGPV protocol and compared its cost with the schemes such as Mona, Zhu and Jiang's scheme, Zhou et al.'s scheme and Liang et al.'s scheme. Table 6 shows the computational and communication complexities during file upload operation. Fig. 1 clearly points to the fact that MGPV achieves the less computation cost than Mona, Liang et al.'s scheme, Zhou et al.'s scheme and Zhu and Jiang's scheme. For instance, for 80

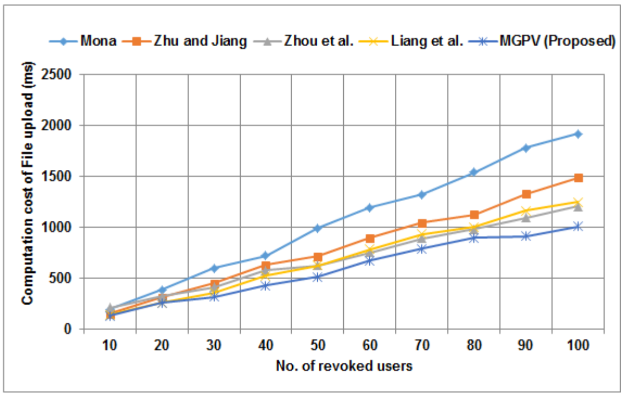

Fig. 1. Computation cost of file upload operation

file uploads, MGPV incurs 898.12ms which is 417.17ms, 227.98ms, 85.39ms and 103.88ms less than Mona, Zhu and Jiang scheme, Zhou et al. scheme and Liang et al. scheme respectively.

For 100 revoked users, MGPV incurs 1010.12ms which is 908.9ms, 475.0ms, 193.1ms and 239.80ms less than Mona, Zhu and Jiang's scheme, Zhou et al.'s scheme and Liang et al.'s scheme.

TABLE 6

COMPUTATION AND COMMUNICATION COST DURING FILE UPLOAD

Scheme vs cost towards file upload	Computation Cost of data owner towards 1 file upload with n revoked users (ms)	Communication Cost of data owner towards 1 file upload of size 1KB when there are n revoked users (bits)
Mona	$2T_{PM} + 1T_{PM} + 1T_{PM} + 1T_E + 1T_{Enc} + 1T_H + (9T_{PM} + 1T_A + 3T_{PA} + 3T_P + 3T_E + 5T_A) = 13T_{PM} + 4T_E + 1T_{Enc} + 1T_H + 4T_{PA} + 6T_A$	$ID_{group} + ID_{data} + C_1 + C_2 + C + f(\tau) + t_{data} + \sigma$ = 16+16+160+160+1024+256+ 24+(160+160+160+16+16+16+16+16+16) = 2232
Zhu and Jiang's scheme	$2T_{PM} + 1T_E + T_{Enc} + T_{Enc} = 2T_{PM} + 2T_E + 2T_{Enc}$	$ID_{data}, C_1, C_2, C, t_{data} = 16 + 160 + 160 + 1024 + 24 = 1384$
Zhou et al.'s scheme	$1T_E + 2T_H + 1T_E + 1T_E + 1T_{Enc} == 3T_E + 2T_H + 1T_{Enc}$	$Enc_K(M), C_1, C_2, C_3$= 1024+160+160+160 = 1504
Liang et al.'s scheme	$1T_P + 1T_E + 1T_{PM} + 1T_E + 1T_E + 1T_{PM} = 1T_P + 3T_E + 2T_{PM}$	$C_0, C_1, C_2, C_3 = 1184 + 160 + 160 + 160 = 1664$
Proposed MGPV protocol	$1T_E + T_{Enc} + T_{PM} + T_{PM} + T_{Enc} = 1T_E + 2T_{Enc} + 2T_{PM}$	$ID_i,\ ID_{group},\ Enc_{ru_i}(ID_i,\ Doc_i,\ Enc_E(doc), L_1, L_2)$ = 16 + 16 + (16+16+1024+160+160) = 1408

Similarly, the communication cost for the file upload of size 1KB shows that MGPV incurs less communication complexity than other schemes and is far better than them. The proposed method has been executed for a maximum of 10 revoked users.

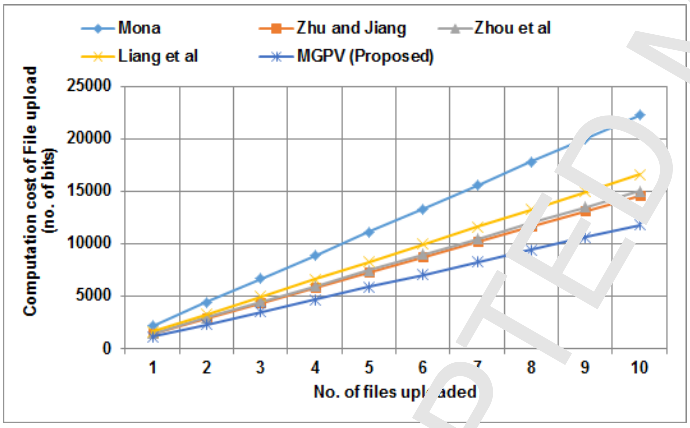

Fig. 2. Communication cost of file upload operation.

Fig.2 shows that, for 10 revoked users, MGPV sends 11840 bits which is 10840 bits, 2810 bits, 3200 bits and 4800 bits less than Mona, Zhu and Jiang's scheme, Zhou et al.'s scheme and Liang et al.'s scheme.

The computation cost of the downloading operation of a file of size 1KB with varying number of revoked users is calculated for the proposed MGPV protocol and other schemes for which the results are tabulated in Table 7 and displayed in the graph depicted in Fig. 3.

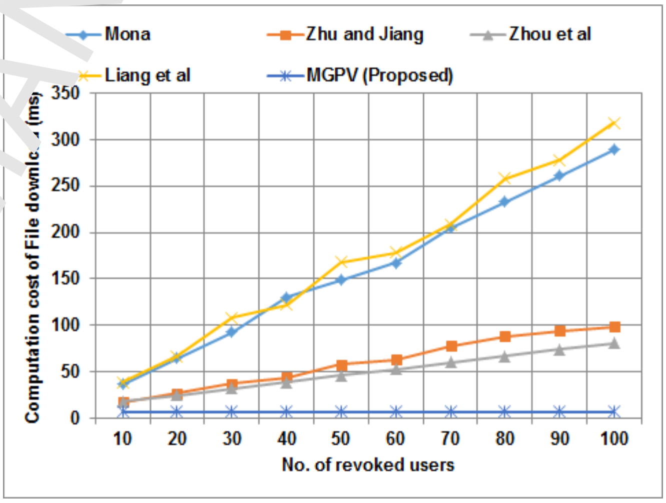

Fig. 3. Computation cost of file download operation

The table clearly portrays that when the number of revoked users increases, the complexity of the MGPV protocol incurs $O(1)$ due its nature of exploiting the famous CRT.

Thus, for 70 revoked users, MGPV takes 198.35ms, 71.22ms, 53.17ms and 201.57ms less than Mona, Zhu and Jiang's scheme, Zhou et al.'s scheme and Liang et al.'s scheme. For 100 revoked users, MGPV incurs 282.59ms, 91.78ms, 74.26ms and 311.66ms less overhead than Mona, Zhu and Jiang's scheme, Zhou et al.'s scheme and Liang et al.'s scheme.

The communication cost of the proposed protocol during file download is depicted in Table 8. Fig. 4 shows that MGPV constantly requires 2528 bits irrespective of the number of revoked users.

TABLE 7

COMPUTATION COST DURING FILE DOWNLOAD

Scheme vs computation cost	Cost of a data user towards 1 file download when there is one revoked group user (ms)		Computation Cost of a data user towards 1 file download when there are n revoked group users (ms)	
	Cost (ms)	Cost (ms)	Cost (ms)	Cost (ms)
Mona	$(8T_{PM}+5T_E+4P_A)+2T_P$ $+1T_M+1T_{Dec}$	$O(1)$	$(8T_{PM}+5T_E+4P_A)+n(2T_P+1T_M)$ $+n(1T_D+1T_M+1T_{PM})+2T_P+1T_M$ $+1T_{Dec}$	$O(n)$
Zhu and Jiang's scheme	$2T_P+1T_E+1T_{PM}+1T_{Dec}+$ $2T_P+1T_E+1T_{Dec}$= $4T_P+1T_{PM}+$ $1T_{Dec}+2T_E$	$O(1)$	$2T_P+nT_E+1T_{PM}+1T_{Dec}+2T_P+$ $1T_E+1T_{Dec}$= $4T_P+1T_{PM}+1T_{Dec}+(n+$ $1)T_E$	$O(n)$
Scheme by Zhou et al.	$2T_p+1T_E+1T_p+1T_p+$ $1T_{PM}+1T_H+1T_{PM}+1T_E+$ $1T_{Dec}$=$4T_p+2T_E+2T_{PM}+1T_H+$ $1T_{Dec}$	$O(1)$	$2T_p+1T_E+1T_p+1T_p+1T_{PM}+1T_H+$ $1T_{PM}+nT_E+1T_{Dec}$=$4T_p+1T_E+2T_{PM}+$ $1T_H+nT_E+1T_{Dec}$	$O(n)$
Liang et al.'s scheme	$1T_p+1T_p+1T_p+1T_{PM}$ $=3T_p+1T_{PM}$	$O(1)$	$3T_p+1T_{PM}+n*(1T_P+2T_E)+1T_P+2T_E$ $=4T_P+1T_{PM}+2T_E+n*(1T_P+2T_E)$	$O(n)$
Proposed MGPV protocol	$1T_D+1T_{Dec}+2T_P+1T_M+1T_{Dec}$ $=1T_D+2T_{Dec}+2T_P+1T_M$	$O(1)$	$1T_D+2T_P+1T_{PM}+1T_{Dec}+1T_{Dec}$	$O(1)$

TABLE 8

COMMUNICATION COST DURING FILE DOWNLOAD

Scheme vs communication cost	Communication cost of a data user towards 1 file download when there is only one group user (bits)		Communication Cost of a data user towards 1 file download when there are n group users (bits)	
	Cost (bits)	Cost (bits)	Cost (bits)	Cost (bits)
Mona	C_1, C_2, C, σ = (160+160+160+(160+160+160+16+16+16+16+16+16)) = 1056	$O(1)$	$C_1, C_2, C, \sigma, ID_{group}, n(A_1, x_1, t_1, P_1), Z_r, t_{RL}, Sig(RL)$ =(160+160+160+160+160+160+16 +16+16+16+16+16))+16+n(160+16+24+160)+160+24+160 = 1416 + (n*360)	$O(n)$
Zhu and Jiang's scheme	$ID_{group}, ID_{data}, CE, EK, t_{data}, \sigma_{DF}$ = 16+16+(160+160+1024)+1(1024)+24 +160) = 2584	$O(1)$	$ID_{group}, ID_{data}, CE, EK, t_{data}, \sigma_{DF}$=16+16+ (160+160+1024)+n(160)+24+160)=2424* (n*160)	$O(n)$
Zhou et al. scheme	$C_1, C_2, D, g^{p_{i,M(s)}}, g^{p_{k,N(s)}}, Aux_1, Aux_2$ =1024+160+160+480+256+256+160 +160 = 2656	$O(1)$	$C_1, C_2, D, g^{p_{i,M(s)}}, g^{p_{k,N(s)}}, Aux_1, Aux_2$ =1024+160+160+480+256+256+n*160+n* 160 = 2336+(2n*160)	$O(n)$
Liang et al. scheme	$C_0, C_1, C_2, C_3, id, T_i$ =1184+160+160+160+128+32=1824	$O(1)$	$C_0, C_1, C_2, C_3, id, T_i + n*(C_0, C_1, C_4) =$ 1184+ 160+160+160+128+32 +n*(160+160+160) = 1824+n*(480)	$O(1)$
Proposed MGPV protocol	S_1, S_2, L_3, μ, ED = (160+160+160+1024+1024) = 2528	$O(1)$	S_1, S_2, L_3, μ, ED = (160+160+160+ 1024+1024) = 2528	$O(1)$

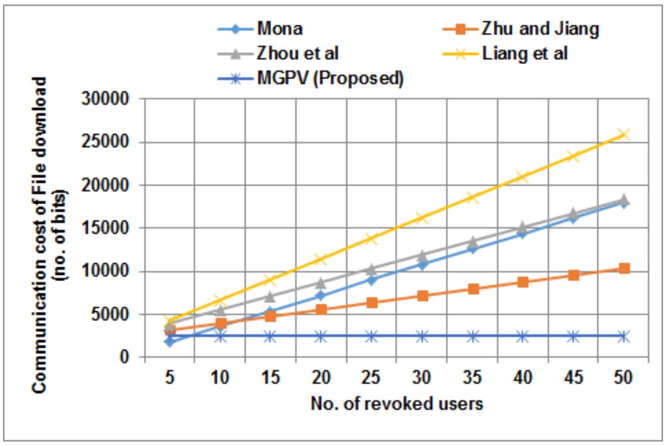

Fig. 4. Communication cost of file download operation

Rather, other schemes in the recent literature incur communication complexity proportional to the number of users. For instance, for 50 revoked users, the MGPV sends 2528 bits which is 15472 bits, 7896 bits, 15808 bits, 23296 bits less than Mona, Zhu and Jiang's scheme, Zhou et al.'s scheme and Liang et al.'s scheme. As the number of revoked users increases, there is an increase in the communication complexity in other schemes leading to more overhead. Thus, it is clear that the proposed MGPV protocol shows better performance compared to other schemes in the literature in terms of computational and communication complexities.

6 Conclusions

Well known cloud service providers such as Amazon, Google, Microsoft and others enable a mobile user to share a document with his peers securely through web services. In this context, based on the web services, a novel collusion attack resistant scheme called MGPV for ensuring the security of shared documents among a group of mobile users in the cloud storage has been proposed in this research work. This scheme is an improvised version of the protocol proposed by Zhu and Jiang for document storage in the clouds in order to avoid its vulnerability to MITM and message modification attacks and it can be adopted for mobile user community pertaining to cloud storage environments. The proposed scheme has been implemented using a real world mobile user and the cloud environment setup. The experimental results ascertain the fact that the proposed work is secure against all the known attacks. The security analysis provided in this protocol ensures the capability of this work to be implemented by mobile users and the cloud service providers for sharing secure documents in the vulnerable cloud storage.

Acknowledgement

This paper was fully financially supported by King Saud University through the Vice Deanship of Research Chairs: Chair of Smart Cities Technology. Dr. Mohammad Mehedi Hassan is the corresponding author of this paper.

References

[1] D. Boneh, and X. Boyen, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT) (2005) 440-456. doi: https://doi.org/10.1007/11426639_26.

[2] A. Alzahrani, A. Nasser, and M. Sarrab, "Mobile Cloud Computing, Advantage, Disadvantage and Open Challenge". Proceedings of the 7th international conference on Euro American Association on Telematics and Information Systems (EATIS 2014) (2014). doi: 10.1145/2590651.2590670.

[3] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, K. Fu, and Plutus, "Scalable Secure File Sharing on Untrusted Storage". Proc.USENIX Conf. File and Storage Technologies (2003) 29-42.

[4] R. Buyya., R. Ranjan, and R.N. Calheiros, "InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services". LNCS, Vol. 6081 (2010) 13-31. doi: https://doi.org/10.1007/978-3-642-13119-6_2.

[5] X. Zhang, A. Kunjithapatham, S. Jeong, and S. Gibbs, "Towards an elastic application model for augmenting the computing capabilities of mobile devices with cloud computing". Mobile Networks and Applications, 16(3) (2011) 270–284. doi: 10.1007/s11036-011-0305-7.

[6] I. Giurgiu, O. Riva, D. Juric, I. Krivulev, and G. Alonso, "Calling the cloud: Enabling mobile phones as interfaces to cloud applications". Proceedings of the ACM/IFIP/USENIX 10th international conference on Middleware, Springer-Verlag, (2009) 83–102. doi: https://doi.org/10.1007/978-3-642-10445-9_5.

[7] S. Jeong, X. Zhang, A. Kunjithapatham, and S. Gibb, "Towards an elastic application model for augmenting computing capabilities of mobile platforms". Mobile Wireless Middleware, Operating Systems, and Applications, (2010) 161–174. doi: https://doi.org/10.1007/978-3-642-17758-3_12.

[8] M.R. Rahimi, J. Ren, C.H. Liu, A.V. Vasilakos, and N. Venkatasubramanian, "Mobile cloud computing: A survey, state of art and future direction," 19(2) (2014) 133-143. doi: https://doi.org/10.1007/s11036-013-0477-4.

[9] A. Bakshi, and B. Yogesh, "Securing Cloud from DDoS Attacks Using Intrusion Detection System in Virtual Machine". Second International Conference on Communication Software and Networks, ICCSN'10 (2010) 260-264,. doi: 10.1109/ICCSN.2010.56.

[10] M. Jensen, J. Schwenk, N. Gruschk, and L.L. Iacono, "On Technical Security Issues in Cloud Computing". IEEE conference on Cloud Computing, CLOUD'09 (2006) 109-116. doi: 10.1109/CLOUD.2009.60.

[11] Z. Zhu, and R. Jiang, "A secure anti-collusion data sharing scheme for dynamic groups in the public cloud". IEEE Transactions on parallel and distributed systems, 27(1) (2016) 40-50. doi: 10.1109/TPDS.2015.2388446.

[12] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage". Proc. Network and Distributed Systems Security Symp (NDSS), (2003) 131-145.

[13] D. Boneh, C. Gentry, and B. Waters, "Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys". Advances in Cryptology – CRYPTO, LNCS, 3621 (2005) 258–275. doi: https://doi.org/10.1007/11535218_16.

[14] V. Goyal, O. Pandey, A. Sahai, and B. Water, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data". Proc. ACM Conf. Computer and Comm. Security (CCS), (2006) 89-98. doi: 10.1145/1180405.1180418.

[15] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance:

The Essential of Bread and Butter of Data Forensics in Cloud Computing". Proc. ACM Symp. Information, Computer and Comm. Security (2010) 282-292. doi: 10.1145/1755688.1755723.
[16] P. Vijayakumar, S. Bose, and A. Kannan, "Chinese remainder Theorem based centralized group key management for secure multicast communication". Journal of IET Information Security (2013) 1-9. doi: 10.1049/iet-ifs.2012.0352.
[17] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud". IEEE Transactions on Parallel and Distributed Systems, 24(6) (2013) pp. 1182-1191. doi: 10.1109/TPDS.2012.331.
[18] Lan Zhou, V. Varadharajan, and M. Hitchens, "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage". IEEE Transactions on Information Forensics and Security, 8(12) (2013) 1947-1960. doi: 10.1109/TIFS.2013.2286456.
[19] X. Zou, Y. Dai, and E. Bertino, "A practical and flexible key management mechanism for trusted collaborative computing". The 27th IEEE conference on Computer Communications INFOCOM 2008, (2008) 1211-1219. doi: 10.1109/INFOCOM.2008.102.
[20] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys". Proc. Of 1st International Conference on Pairing-Based cryptography (2007) 39-59. doi: https://doi.org/10.1007/978-3-540-73489-5_4
[21] Yanji Piao, JongUk Kim, Usman Tariq, and Manpyo Hong, "Polynomial-based key management for secure intra-group and inter-group communication", Computers and Mathematics with Applications, Elsevier 65(9) (2013)1300–1309.
[22] P. Vijayakumar, S. Bose, A. Kannan and S. Siva Subramanian, "A secure key distribution protocol for multicast communication", in: P. Balasubramaniam (Ed.), Gandhigram-India, 2011, in: CCIS, Vol. 140, Springer, Heidelberg, (2011) 249–257.
[23] P. Vijayakumar, S. Bose and A. Kannan, "Centralized key distribution protocol using the greatest common divisor method", in Computers and Mathematics with Applications, Elsevier, 65(9) (2013) 1360-1368.
[24] P. Vijayakumar, S. Bose, and A. Kannan, "Rotation based secure multicast key management for batch rekeying operations", Springer 1(1) (2012) 39-47.
[25] P. Vijayakumar, R. Naresh, L. Jegatha Deborah and SK Hafizul Islam, "An efficient group key agreement protocol for secure P2P communications", Security and Communication Networks, Wiley, (2016).
[26] J. Zhou, and Y.-H. Ou. "Key tree and chinese remainder theorem based group key distribution scheme", J. Chin. Inst. Eng., 32(7) (2009) 967–974
[27] H. Wang, and B. Qin, "Improved one-to-many authentication scheme for access control in pay-TV systems", IET Inf. Secur., 6(4) (2012) 281–290.
[28] S. Milton Ganesh, P. Vijayakumar, L. Jegatha Deborah, and Md. Zakirul Alam Bhuiyan, "Attacks on the Anti-collusion Data Sharing Scheme for Dynamic Groups in the Cloud", SpaCCS 2017: Security, Privacy, and Anonymity in Computation, Communication, and Storage, Lecture Notes in Computer Science book series (LNCS-Springer) 10658 (2017) 457-467.
[29] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, and A. Konwinski, "A view of cloud computing", Commun. ACM, 53(4) (2010) 50–58.
[30] J. Flinn, S. Park, and M. Satyanarayanan, "Balancing performance, energy, and quality in pervasive computing". In: Proc. of the international conference on distributed computing systems (2002).
[31] X. Li, Y. Li, T. Liu, J. Qiu, and F. Wang, "The method and tool of cost analysis for cloud computing". In: Proc. of IEEE international conference on cloud computing (2009).
[32] L. Zhou, V. Varadharajan, and M. Hitchens, "Enforcing role-based access control for secure data storage in the cloud", Comput. J., 54(10) (2011) 1675–1687.
[33] M. J. Atallah, K. B. Frikken, and M. Blanton, "Dynamic and efficient key management for access hierarchies," in Proc. ACM Conf. Comput. Commun. Sec., (2005) 190–202.
[34] S. D. C. Di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in Proc. VLDB, (2007) 123–134.
[35] P. Vijayakumar, S. Milton Ganesh, L. Jegatha Deborah, and Bharat S Rawal, "A new SmartSMS protocol for secure SMS communication in m-health environment," Computers & Electrical Engineering, Elsevier. Accepted for publication, In Press.
[36] P. Vijayakumar, P. Pandiaraja, M. Karuppiah, and L. Jegatha Deborah, "An efficient secure communication for healthcare system using wearable devices", Computers & Electrical Engineering, Elsevier, 63 (2017), 232-245.
[37] P. Vijayakumar, Victor Chang, L. Jegatha Deborah, Balamurugan Balusamy, and P.G. Shynu, "Computationally Efficient Privacy Preserving Anonymous Mutual and Batch Authentication Schemes for Vehicular Ad Hoc Networks," Future Generation Computer Systems, Elsevier, 78(3) (2018) 943-955.
[38] S. Namasudra, P. Roy, P. Vijayakumar, S. Audithan, and Balamurugan Balusamy, "Time efficient secure DNA based access control model for cloud computing environment," Future Generation Computer Systems, Elsevier, 73, (2017) 90-105.
[39] K. Liang , J.K. Liu , D.S. Wong1, and W. Susilo, "An Efficient Cloud-based Revocable Identity-based Proxy Re-encryption Scheme for Public Clouds Data Sharing," in Computer Security - ESORICS 2014. Lecture Notes in Computer Science, 8712,(2014), 257-272.
[40] Huawei Zhao, Peidong Bai, Yun Peng, Ruzhi Xu, "Efficient key management scheme for health blockchain", CAAI Transactions on Intelligence Technology, IET, 3(2), (2018), 114 – 118.
[41] Min Huang, Yuefan Zeng, Lina Chen, Bo Sun, "Optimisation of mobile intelligent terminal data pre-processing methods for crowd sensing", CAAI Transactions on Intelligence Technology, IET, 3(2), (2018), 101 – 113.
[42] I. Mohiuddin, A. Almogren, M. Al Qurishi, M. M. Hassan, I. Al Rassan, G. Fortino. Secure distributed adaptive bin packing algorithm for cloud storage. Future Generation Computer Systems, 90, 307-316, 2019

Biography of Authors

P.Vijayakumar completed his Ph.D in Computer Science and Engineering in Anna University Chennai in the year 2013. He completed Master of Engineering in the field of Computer Science and Engineering in Karunya Institute of Technology in the year 2005. He completed his Bachelor of Engineering under Madurai Kamarajar University in the year 2002. He is presently working as Assistant Professor at University College of Engineering, Tindivanam. He is guiding for many Ph.D scholars in the field of network and cloud security. He has published various quality papers in the reputed journals like IEEE Transactions, Elsevier, Springer, IET, Taylor & Francis, Wiley etc. His main thrust research areas are Key management in Network Security and Multicasting in Computer Networks.

S. Milton Ganesh is doing Ph.D in Anna University Chennai and has received his B.Tech in Information Technology in 2004 and Master of Engineering in Computer Science and Engineering in 2007. He is presently working as Assistant Professor in the Department of Computer Science and Engineering at University College of Engineering, Tindivanam. His areas of research are computer networks and mobile security.

L. Jegatha Deborah completed Ph.D in Computer Science and Engineering in Anna University Chennai in 2013 and completed Master of Engineering in the field of Computer Science and Engineering in 2005. She completed Bachelor of Engineering in 2002. She is presently working as Assistant Professor in University College of Engineering Tindivanam and her research interests include database security and data mining.

SK Hafizul Islam received the M.Sc. degree in Applied Mathematics from Vidyasagar University, Midnapore, India, in 2006, and the M.Tech. degree in Computer Application and the Ph.D. degree in Computer Science and Engineering in 2009 and 2013, respectively, from the Indian Institute of Technology [IIT (ISM)] Dhanbad, Jharkhand, India, under the INSPIRE Fellowship PhD Program (funded by Department of Science and Technology, Government of India). He is currently an Assistant Professor with the Department of Computer Science and Engineering, Indian Institute of Information Technology Kalyani (IIIT Kalyani), West Bengal, India. Before joining the IIIT Kalyani, he was an Assistant Professor with the Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani (BITS Pilani), Rajastahn, India. He has more than five years of teaching and eight years of research experiences. He has authored or co-authored seventy five research papers in journals and conference proceedings of international reputes. His research interests include cryptography, information security, WSNs, IoT, and cloud computing. Dr. Islam is an Associate Editor for Wiley's "**International Journal of Communication Systems"** and "**Security and Privacy"**. He was a reviewer in many reputed international journals and conferences. He was the recipient of the University Gold Medal, the S. D. Singha Memorial Endowment Gold Medal, and the Savitri Parya Memorial Endowment Gold Medal from Vidyasagar University, in 2006. He was also the recipient of the University Gold Medal from IIT(ISM) Dhanbad in 2009 and the OPERA award from BITS Pilani in 2015. He is a senior member of the IEEE and a member of the ACM.

Mohammad Mehedi Hassan (M'12) is currently an Associate Professor of Information Systems Department in the College of Computer and Information Sciences (CCIS), King Saud University (KSU), Riyadh, Kingdom of Saudi Arabia. He received his Ph.D. degree in Computer Engineering from Kyung Hee University, South Korea in February 2011. He received Best Paper Award from CloudComp conference at China in 2014. He also received Excellence in Research Award from CCIS, KSU in 2015 and 2016 respectively. He has published over 100+ research papers in the journals and conferences of international repute. He has also played role of the guest editor of several international ISI-indexed journals. His research areas of interest are cloud federation, multimedia cloud, sensor-cloud, Internet of things, Big data, mobile cloud, sensor network, publish/subscribe system and recommender system. He is a member of IEEE.

Abdulhameed Alelaiwi is an Associate Professor of Software Engg. Department, at the College of Computer and Information Sciences, King Fahad University. Riyadh, Saudi Arabia. He has authored and co-authored many publications including refereed IEEE/ACM/Springer journals, conference papers, books, and book chapters. His research interest includes IoT, Edge, Cloud, software testing analysis and design, cloud computing, and multimedia. He is a member of IEEE.

Giancarlo Fortino is currently a Professor of Computer Engineering (since 2006) at the Dept. of Informatics, Modeling, Electronics and Systems (DIMES) of the University of Calabria (Unical), Rende (CS), Italy. He holds the "Italian National Habilitation" for Full Professorship. He has been a visiting researcher at the International Computer Science Institute, Berkeley (CA), USA, in 1997 and 1999, and visiting professor at Queensland Univ. of Technology, Brisbane, Australia, in 2009. He was nominated Guest Professor in Computer Engineering of Wuhan Univ. of Technology (WUT) on April, 18 2012. His research interests include distributed computing, wireless sensor networks, software agents, cloud computing, Internet of Things systems. He authored over 230 publications in journals, conferences and books. He is the founding editor of the Springer Book Series on Internet of Things: Technology, Communications and Computing and serves in the editorial board of IEEE Transactions on Affective Computing, Journal of Networks and Computer Applications, Engineering Applications of Artificial Intelligence, Information Fusion, Multi Agent and GRID Systems, etc. He is co-founder and CEO of SenSysCal S.r.l., a spinoff of Unical, focused on innovative sensor-based systems for e-health and demotics. He is IEEE Senior member.

Authors Photo

P.Vijayakumar

S. Milton Ganesh

L. Jegatha Deborah

SK Hafizul Islam

Mohammad Mehedi Hassan

Abdulhameed Alelaiwi

Giancarlo Fortino

Highlights

- Proposed a scheme for secure data sharing among mobile users in the public cloud
- Designed a collusion aware document storage technique to prevent various attacks
- Minimized the computational complexity incurred during the upload and download of documents
- Introduced a protocol to ensure the document confidentiality between data owner and data users