TIME OPTIMIZATION FOR AUTHENTIC AND ANONYMOUS GROUP SHARING IN CLOUD STORAGE

IAEME Publication

IAEME PUBLICATION

International Journal of Computer Engineering & Technology (IJCET)
Volume 9, Issue 2, March-April 2018, pp. 16–31, Article ID: IJCET_09_02_002
Available online at
http://iaeme.com/Home/issue/IJCET?Volume=9&Issue=2
Journal Impact Factor (2016): 9.3590(Calculated by GISI) www.jifactor.com
ISSN Print: 0976-6367 and ISSN Online: 0976–6375

TIME OPTIMIZATION FOR AUTHENTIC AND ANONYMOUS GROUP SHARING IN CLOUD STORAGE

Muthireddy P, Manjula S H and Venugopal K R
Department of Computer Science and Engineering,
University Visvesvaraya College of Engineering,
Bangalore University, Bengaluru-560001, Karnataka, India

ABSTRACT

The Cloud computing is a rising technique which offers information sharing are more ***efficient****,* ***effective*** *and* ***economical*** *approaches between group members. To create an authentic and anonymous information sharing, IDentity based Ring Signature (ID-RS) is one of the promising method between the groups. Ring signature conspire grants the chief or data owner to authenticate into the framework in an anonymous way. In conventional Public Key Infrastructure (PKI) informa*tion sharing plan contains certificate authentication process, which is a bottleneck due to *its high cost for consumption of more time to signature. To maintain a strategic distance from this issue, we proposed* ***Cost Optimized Identity-based Ring Signature with forward secrecy*** *(****COIRS****) scheme. This plan evacuates the traditional certificate verification process. Just once the client should be confirmed by the chief giving his public details. The time required for this procedure is relatively not as much as customary public key framework. If the secret key holder has been compromised, all early generated signatures remain valid (Forward Secrecy). This paper examines how to optimize the time when sharing the documents to the cloud. We provide a protection from collision attack, which means revoked users will not get the original documents. In general better efficiency and secrecy can be provided for group sharing by applying approaches.*

Key words: Anonymity, Authenticity, Forward secrecy Group sharing, Ring signature.

Cite this Article: Muthireddy P, Manjula S H and Venugopal K R, Time Optimization for Authentic and Anonymous Group Sharing in Cloud Storage. *International Journal of Computer Engineering and Technology,* 9(2), 2018, pp. 16-31.
http://www.iaeme.com/IJCET/issues.asp?JType=IJCET&VType=9&IType=1

1. INTRODUCTION

The Cloud computing is an Internet based technology because of its widespread and popular use.

It empowers the both clients and enterprises to keep their data in cloud storage and permits resource sharing [1], [2], [3], [4]. The Cloud computing is generally utilized in view of its two primary applications, which are as per the following:

- The Vast amount of information storage: The Cloud storage enables the clients to store the documents on clients ask. Cloud storage gives the advantage to store the gigantic measure of the storeroom.
- Allows users to easily share their data: The Cloud computing technology provides another facility that is to easily share files to the public and to the individual.

It permits sharing of information through an outsider which turns out to be all the more financially valuable. Security of both the information and group member's personalities are most significant notion in cloud computing. Consider a *Smart Grid* example is as shown in figure. 1, the client's in the smart grid may get their information use record with no encoded format and they get urged to impart their private data to others. It allows sharing of data through a third party which becomes more economically useful. Privacy of both the data and group member's identities are most significant notion in cloud computing. Consider a *Smart Grid* example as shown in figure. 1, user's in smart grid may get their data usage file without any encrypted format and they get encouraged to share their private information with others.

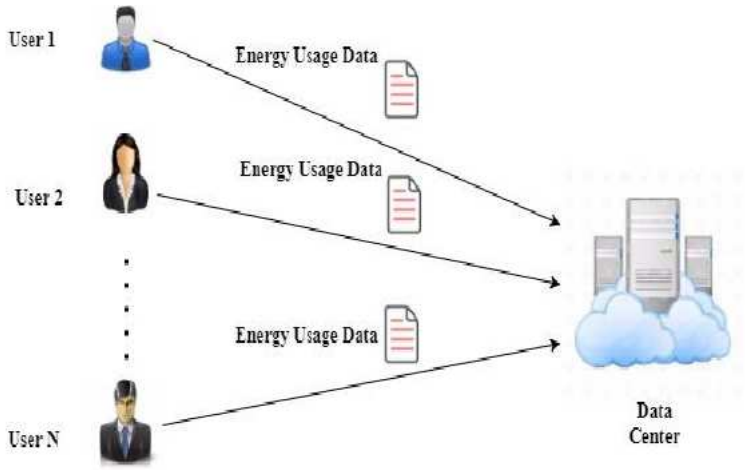

Figure 1 File Data Sharing in Smart Grid.

Consider an example, if the user wants to upload their files to the cloud platform like Microsoft Azure, from that gathered copy of energy data files several statistical copies are created. Anyone could match the data files about energy consumption with others. This may lead to critical problems to energy usage while accessing, analyzing and responding back to the cloud. Because of its openness, deployment of data sharing took place in a standalone background, it is open to several secrecy problems [5], [6]. There are many secrecy criteria to be reached in order to achieve *data efficiency* and *secrecy*, i.e.,

Authenticity of Data: The signed data usage file would be confusing in the example of smart grid, if that data file is copied by the adversaries. At the same time this type of problems can be solved by using some cryptographic techniques such as digital signatures, hash functions, encryption or decryption techniques or message authentication techniques. User might face other issues in smart grid system like *anonymity* and *efficiency.*

Data Anonymity: The signed energy usage file is enclosed with huge amount of information of consumers, sharing in the smart grid is processed in fine grained fashion. Then the signed energy file anyone can copy the information of consumers from the system. The copied information may be of electrical utilities used for a particular time etc., therefore, it is not easily possible to hold the anonymity condition of consumers.

Data Efficiency: The smart grid (it is an electric grid consisting a variety of operational, vitality measures, smart apparatuses, sustainable power source assets, smart meters) for data sharing system contains a large number of users, to save the consumption of energy from such smart grid systems. A realistic system must decrease its communication cost and computation as less as possible or else it would lead to energy wastage, this is against to the aim of smart grid.

To overcome above metrics and provide more secure in data sharing COIRS model is introduced and it reduces group accessing time and cost of the files. We dedicate this paper to examining essential goals for understanding the three properties as described above.

- Data Authenticity
- Anonymity
- Efficiency

Instead of those secrecy issues there are other secrecy tools, such as availability (even under network attacks, service is being provided at an acceptable level) and access control. We discussed how our COIRS model is used in identity based cryptosystem and advantages in big data system in next part.

1.1. Identity Based Cryptosystem

Shamir [7] has introduced the first IDentity-based cryptosystem. It removes the necessity for proving the validity of Public Key (PKey) certificates, the maintenance in conventional public key infrastructure is both cost and time consuming. By collecting the publicly known users unique identity like address or email-id for the public key of the user is calculated. In ID-based Cryptosystem, private keys can be generated by a private key generator and later master-secret for users is calculated. Identity-based cryptosystem scheme removes the necessity of certificate validation, which is a part of traditional PKI and links an implicit PKey to all members inside the system. In ID-based signature, one does not require to validate the certificates first which is a contradiction to the conventional public key infrastructure. The removal of such certificate verification makes the entire verification process more effective. This would definitely lead to a major save in both computation and communication cost when huge number of consumers are involved (smart-grid). Here we assign some cost value to particular file to optimize the overall cost required for the process. One constant cost value for the file is assigned. The file size increases then their cost value varies. RS is a group focused signature along with secrecy assurance on signer. The client can sign secretly in the interest of a group's individual choice, while individuals are absolutely ignorant of signature generated using their identity information. Verifier can check that a data has been signed by one of the individuals of the group. However the real character of the signer isn't being shared. RS could be utilized for the application of whistle blowing [8] and an anonymous authentication for groups [9]. Numerous different applications which don't need group development stage however require signer secrecy.

1.2. An Advantage in Big Data System

Because of its normal structure, ID-based framework has a positive advantage in Big Data. RS in ID-based framework has an imperative favorable position over its partner in ordinary open key framework, for the most part in the huge information diagnostic scheme. Consider an event including 20,000 individuals in the group, the signature verifier of a traditional PKI based framework should approve all 20,000 certificates first, then one can take out the actual message verification process along with the signature. Unlike traditional PKI, in ID-based RS just the ring client's information along with the message and signature sets are required. Subsequently, we would be able to eliminate the expensive certificate validation process, which spares a lot of calculation time and execution time. As the quantity of clients in the ring builds, sparing will be more basic if a more elevated amount of secrecy is needed.

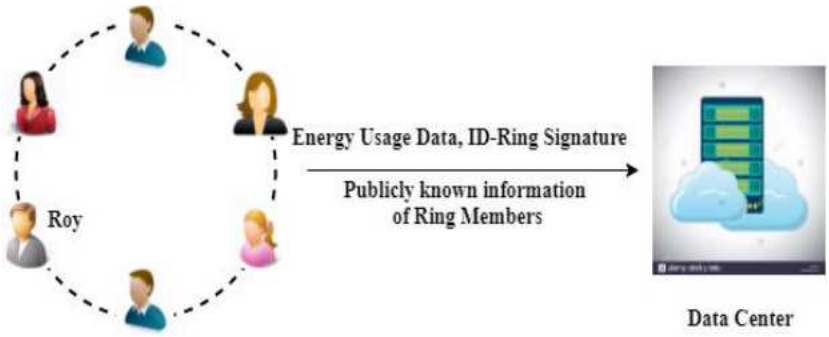

Figure 2 Identity Based Ring Signature.

As outlined in figure. 2, ID-based RS plot is more preferable, where huge number of individuals are involved with the framework like smart grid framework is as following:

- The vitality information proprietor (say, Roy), first make a ring or group by choosing a group of clients. This stage just requires public information of the users, similar to changeless or private locations, and Roy does not require the relationship between any ring individuals.
- Roy uploads his private details of electronic utilization, along with a group signature and the identity details of all group individuals.
- By approving the produced ring signature, one can be ensured that the information or message is certainly conveyed by a legitimate occupant, meanwhile we cannot find out actual signer of the group. Anonymity of the message provider is guaranteed along with the data or message authenticity. At the same time the verification process is highly efficient because it does not include any certificate verification method.

By adding more users in the ring one can achieve a higher level protection, but the possibility of key disclosure might increase. Key exploration is the real disadvantage of ordinary advanced signatures. Assume the SKey of a user is compromised, every single past signature of that client becomes valueless: future signatures are rejected and also already issued signatures can't be trusted. It doesn't resolve the issue of forgeability for past produced signatures.

1.3. Motivation

Key Exposure: The idea of forward secrecy is proposed to protect the legitimacy of past signatures regardless of the possibility that the present SKey holder is compromised.

Big Data Key Exposure: The exposure of key in a RS scheme [8] is more serious issue: suppose a user's private key is uncovered by any unauthorized user then user can develop a legitimate ring signatures of any records in the interest of that ring. Indeed, even more in

worst condition, the ring can be characterized by his own choice. Even one cannot recognize whether a ring signature is created preceding the key introduction or by which client. Subsequently, forward secrecy is a necessary prerequisite for all frameworks to share information. This consumes more *time* and high *cost*, to overcome these issues, we proposed Cost Optimized Identity-based Ring Signature with forward secrecy (COIRS) scheme.

1.4. Contribution

A creative idea called ID-based forward secure ring signature [8] is introduced which is an essential key for developing a COIRS framework. It gives a formal clarification on IDbased forward secure RS; we exhibit a solid outline of COIRS scheme, no past ID-based RS scheme had the property of forward secrecy, we demonstrate the secrecy of the proposed method under the standard RSA model assumption. Use of COIRS plan contains:

- The disposal of expensive certificate verification process makes it versatile and particularly reasonable for enormous information explanatory condition.
- The secret key is small in size.
- Exponentiation is done in key update process.
- We are calculating the energy usage required by the data owner to upload files to the cloud and downloading energy for the data centre for providing files to the clients.
- We are determining the time required by the data owner to sing the energy usage of the files and data centre to download the files requested by the clients.

Organization: In section 2, we give related work on forward secrecy to provide authentication access and cost optimization. In section 3, we describe architecture of COIRS model. In section 4, we discuss mathematical model of COIRS scheme. In section 5, we deal on experimental analysis. We concluded our model in section 6.

2. RELATED WORK

Liu *et al.,* [10] proposed a novel that can completely maintain fine-grained update request and authorized auditing by providing a proper examination for feasible forms of fine-grained data updates. Based on the above idea enhancement is made, that can significantly diminish communication expenses for verifying small updates, and significantly reduce the overhead for big-data applications. Yang *et al*., [11] studied first outlined an evaluating structure for distributed storage frameworks and proposed an efficient and protection safeguarding inspecting convention. Then, they stretched out evaluating algorithms to help the information dynamic operations, which is efficient and provably secure. The examination and re-enhancement comes about in demonstration that proposed evaluating conventions are secure and efficient, particularly it reducing the calculation cost. Nabeel *et al.*, [12] proposed a vital issue in broad daylight mists by which to specifically share reports in view of fine-grained Access Based Control Policy Scheme (ACPS). An approach is to scramble records fulfilling diverse strategies with various keys utilizing an open key cryptosystem, for example, property based encryption, as well as intermediary re-encryption.

Dai *et al*., [13] examined inventions to diminish essentialness use by server farms considering the position of virtual machines onto the servers in the server farm shrewdly. This examine as various programming issue, show it in NPhard, by then research two eager guess estimations, slightest essentialness virtual machine and minimum correspondence virtual machine arranging calculation, to take in the imperativeness while satisfying the inhabitant's organization level understandings. Bera *et al.*, [14] exhibits the speedy paced change of vitality structures that requires sharp systems to support constant control and checking with

bidirectional correspondence and power streams. To focus on tried and efficient, proficient, secured and fiscally overview on control organization essentials. Li *et al*., [15] chipped away at in spite of the way that, it suggested that a half breed cloud may save cost differentiated and amassing an extraordinary private cloud, broad renting expense and correspondence cost are still displayed in such a world view. The best strategy to enhance such operational cost winds up clearly one important stress for the SaaS providers to get the hybrid cloud figuring world view.

Yang *et al*., [16] introduced novel methodologies in light of compiler code examination that reasonably decrease the traded data measure by trading only the essential store objects and the stack diagrams extremely referenced in the server. The tests show that the diminished size positively impacts the trade time itself and in addition the general ampleness of execution offloading and in the long run, improves the execution of flexible dispersed registering out and out the extent that execution time and essentialness use is concerned. Yao *et al*., [17] manufactured a novel structure named cost streamlining for web content multihoming. COMIC dynamically changes end-customers' loads among server ranches and CDNs with a specific end goal to confine the substance advantage cost. To ensure predominant for content passing on, content diministration utilizes an advancement known as substance multihoming: substance are delivered from various topographically appropriated server cultivates and passed on by various scattered substance dissemination frameworks. The power costs for server ranches and the usage costs for CDNs are genuine supporters of the substance advantage cost. As power costs change transversely finished server homesteads and utilize costs vary across finished CDNs, arranging server ranches and CDNs has a tremendous result for propelling substance advantage cost.

Trombetta *et al*., [18] suggested three traditions handling this issue on disguise based, hypothesis based k-mysterious and secret databases. The traditions rely upon most likely comprehended cryptographic assumptions, and we give theoretical examinations to prove their soundness and test results to speak to their profitability. Zhou *et al*., [19] proposed an arrangement that empowers a relationship to store data securely in an open cloud while keeping up the delicate information related to the affiliation's structure in a private cloud. Customers of open distributed computing don't know where their data is secured. They have a misinformed judgment of losing their data [20]. Zhou *et al*., [21] learned about the troubles of controlling organization rates and applying the N-Technique to enhance operational cost inside an execution. The cost work has been made in which the costs of vitality use, structure clock and server start-up are out and out considered. Yu *et al*., [22] have developed an effective id-based limit ring mark plot. Edge ring signature engages any gathering of t substances instantly selecting optional n-t components to make a straightforwardly verifiable t-out-of-n edge signature for the advantage of the whole assembling of the n components, while the bonafide financiers remain a baffling. Bellare *et al.*, [23] contemplated a forward secure digital signature schemes, it is a computerized signature chart in which open key is settled yet puzzle signature key is revived at steady between times so as to give a forward secrecy appropriately, bartering of the secret key does not empower the contradict to deliver the signatures identifying with the past. This can be useful to ease the mischief caused by key presentation without requiring the dispersal of keys.

3. COIRS MODEL

In this section, we are discussing the mathematical assumption, secrecy model and designed architecture of COIRS secrecy model.

3.1. Mathematical Assumption

Definition: Let $M = uv$, where u and v are two b-bit prime numbers where $u = 2u' + 1$ and $v = 2v' + 1$ for some primes u', v'. Let r be a prime, $r > 2^{\ell}$ for a some constant parameter ℓ, where $gcd(r; \phi(M)) = 1$. Let x is a random element in Z_M^*. We say that an algorithm A resolve the RSA dilemma if it accept an input the tuple (M, r, x) and outputs an element z such that $z^r = x \bmod M$.

3.2. Secrecy Model

Cost Optimized Id-based Ring Signature (COIRS) scheme is a part of Probabilistic Polynomial Time (PPT) algorithms. This PPT contains the following operations:

Setup:

- Input ← 1^{γ} Prm, MSGG, S).
- Results ← PKG generates Master Secret key (MSkey) and parameter list Prm.

Extract:

- Input← *Prm*, an identity $ID_i \in \{0,1\}^*$, 1^{γ}, *MSkey*.
- Results ← Users Secret Key $(SKey_{i,0}) \in K$ such that the secret key is valid for time $t = 0$. When we say identity ID_i corresponds to user secret key $SKey_{i,0}$ or vice versa, we mean the pair $(ID_i, SKey_{i,0})$ is an input-output pair of *Extract* with respect to *Prm* and *MSkey*.

Update:

- Input ← $SKey_{i,t}$ for a time period t.
- Results ← New user Secret Key $SKey_{i\,t+1}$ for the time period $t+1$.

Sign:

- Input ← Parameter list *Prm, t*, group size n of length polynomial in γ, a set $L = ID_i \in \{0,1\}^* \mid i \in [1, n]$ of n user identities, $MSg \in MSGG$ and $SKey_{\pi,t} \in K$, $\pi \in [1,n]$ for time t
- Results ← signature $\alpha \in S$.

Verify:

- Input ← parameter list *Prm, t*, group size n of length polynomial in γ, a set $L = ID_i \in \{0, 1\}^* \mid i \in [1, n]$ of n user identities, $MSg \in MSGG$ and a signature $\alpha \in S$.
- Results ← generated signature $\alpha \in S$ is valid or invalid.

Correctness:

A (1, n) COIRS scheme should satisfy the verification on correctness signatures signed by honest signer are verified to be invalid with negligible probability.

3.3. Architecture of COIRS Scheme

The architecture of Cost Optimized Identity based Ring Signature with forward secrecy (COIRS) scheme is illustrated in figure 3. The architecture mainly consists of four components:

- User
- Admin
- Private Key Generator (PKG)

- Public Cloud

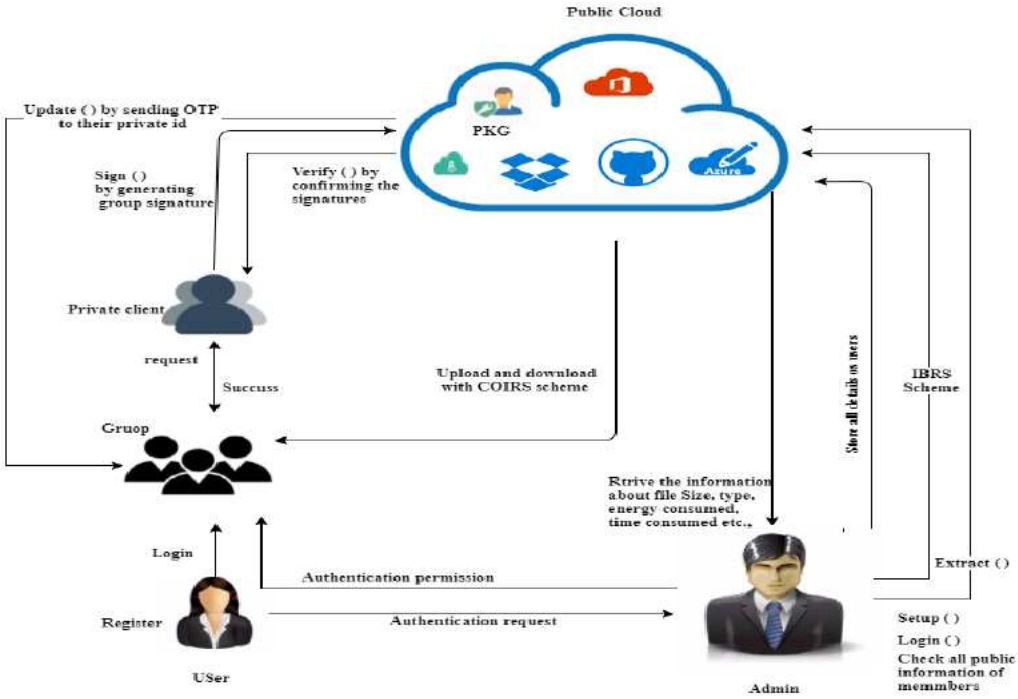

Figure 3 Architecture of COIRS scheme.

User: User is the one who wants to share their personal information to others or they wish to keep secret or confidential data hidden from unauthorized persons. In COIRS scheme, user registers to a cloud by filling all his details. Admin or manager of the particular group grants the authorization permission to users to perform the desired upload/download operations. By agreeing terms and conditions of the registered cloud, user can perform the upload and download the operations. After logging in to the particular group by getting OTP to user *email id* which is entered while registering at the first time. The user becomes a group member in addition the user has rights to perform the tasks. For every task of a group signature is generated by a particular user on behalf of the group to maintain secrecy and forward secrecy to avoid unauthorized access.

Admin: Admin gives access to the registered users before performing the tasks. Admin then collects all registered user's public details and uploads his information with user's details to maintain the users log records. Admin will keep the information about file details of all the user details, accessing details etc.

Private Key Generator (PKG): It generates the private keys for all registered users and these key will be vary every time while performing new task. PKG sets up the group's average time, to calculate the average time required by the group to upload and download the files.

Public Cloud: Public cloud is the cloud infrastructure where any user can access the information from the cloud. Here there are several cloud service providers like *Microsoft Azure, Dropbox, Google*$^{+}$*, Amazon*, etc., these service providers provide the services to requesting users by using some algorithms to maintain privacy and secrecy of the data.

4. MATHEMATICAL MODEL OF COIRS SCHEME

In this section, we are going to give the description and analysis of our COIRS scheme. The different notations for efficiency is shown in table 1.

4.1. The Design

Assume that the user private key and group member identities are valid up to *T* periods and do the time period intervals as public ans set the message space MSGG = (0, 1)*

Setup: Let γ is a secrecy parameter using as input to a setup phase, the *PKG* generates two random b-bit prime numbers *u* and *v* such that $u = 2u' + 1$ and $v = 2v' + 1$ for some primes u', v'. It computes $M=uv$. For fixed parameter ℓ, it selects a random prime number *r* such that $2^{\ell} \leq r \leq 2^{\ell+1}$ and $gcd(r, \varphi(M)) = 1$. It selects two hash functions HF_1: 0, 1* $\rightarrow Z_N^*$ and HF_2: 0, 1* $\rightarrow$ 0,1$^{\ell}$. The public parameters *Prm* are $(b, \ell, r, M, HF_1, HF_2)$ and the *MSkey* is *u,v*.

Extract: The PKG generates the user secret key for user i, with user's identities $IDi \in$ 0, 1* requests for a secret key at time period *t* (integer), where $0 \leq t \leq T$.

$SKey_{i,t} = [HF_1(ID_i)]^{1/r^{(T+1-t)}} \bmod M$.

Update: $SKey_{i,t}$ as a input for a time period t, if t < T the user updates the secret key as $SKey_{i,t+1} = SKey^{r}_{i,t} \bmod N$. Or else, the algorithm yields ⊥ means the secret key has expired.

Sign: To sign a message $MSg \in (0,1)*$ in time period *t* where 0 ≤ t ≤ T, on behalf of a ring of identities L= $ID_1,.....,ID_n$ a user with identity $ID_\pi \in L$ and secret key $SKey_{i,t}$:

- For all $i \in 1,.....,n,$ choose random $A_i \in Z_M^*$ *and* compute

  $R_i = A_{\pi}^{e^{(T+1-t)}} \bmod M$ and $h_i = HF_2(L,m,t,ID_i,R_i)$

- Choose random $A_\pi \in Z_M^*$ and compute

  $R_\pi = A_{\pi}^{e^{(T+1-t)}} \bmod M * \Pi_{i=1,i\neq\pi}^{n} HF_1(ID_i)^{-h_i} \bmod M$ and

  $HF_\pi = HF_2(L,MSg,t,ID_i,R_\pi)$

- Compute $SKey_{i,t}^{h_\pi} \Pi_{i=1}^{n} A_i \bmod M$.

- Output the signature for the list of identities *L*, the message MSg and the time period *t* as $\gamma = (R_1...R_n, h_1...h_n, s)$.

Verify: To verify a signature *α* for a message MSg, a list of identities *L* and the time period *t*, check whether $h_i = HF_2(L,m,t,ID_i,R_i)$ for i = 1,...,M and $\gamma^{e^{(T+1-t)}} = \Pi_{i=1}^{n} HF_1(ID_i)^{h_i} \bmod M$. We will get valid output if all equality's satisfied. Otherwise the result will be invalid.

Table 1 Notations for efficiency comparison

Notation	Definition
Pkey	Public Key
1^{γ}	Security Parameter
M	Group Size
Prm	Public System Parameter
L	List of Identities of all Users
MSkey	Master Secret Key
MSg	Message
K	User Secret Key Space
S	Signature Space
MSSG	Message Space
ID	Identity of User
G	Cyclic Bilinear Group
SKey	Secrete Key
α	Signature
t	Time

4.2. Correctness

We are checking whether our secrete key is valid or not by considering the equations on left hand side with the right hand side. The secret key verification becomes success then LHS=RHS.

$\gamma^{e^{(T+1-t)}} = \Pi_{i=1}^{n} (R_i HF_1(ID_i)^{h_i}) \bmod M$

$LHS = \gamma^{e^{(T+1-t)}}$

$= ((SKey_{\pi,t})^{h_\pi} * \Pi_{i=1}^{n} A_i \bmod M)^{e^{(T+1-t)}}$

$= ((HF_1(ID_\pi)^{1/r^{(T+1-t)}})^{h_i} * \Pi_{i=1}^{n} A_i \bmod M)^{e^{(T+1-t)}}$

$= (HF_1(ID_\pi)^{h_\pi} * \Pi_{i=1}^{n} (A_i)^{r^{(T+1-t)}} \bmod M)$

$RHS = \Pi_{i=1}^{n} R_i * HF_1(ID_i)^{h_i} \bmod M$

$= \Pi_{i=1,i\neq\pi}^{n} (R_i * HF_1(ID_i)^{h_i})) * R_\pi HF_1(ID_\pi)^{h_i} \bmod M$

$= \Pi_{i=1,i\neq\pi}^{n} (A_i^{r^{(T+1-t)}} * HF_1(ID_i)^{h_i})) * A_i^{r^{(T+1-t)}} * \Pi_{i=1,i\neq\pi}^{n} HF_1(ID_i)^{-h_i})) * HF_1(ID_\pi)^{h_\pi} \bmod M$

$= \Pi_{i=1}^{n} (A_i^{r^{(T+1-t)}} * HF_1(ID\pi)^{h_\pi} \bmod M$

=LHS

Therefore, LHS= RHS.

4.3. Algorithms

Algorithm 1 Forward secrecy

procedure SIGNATURE

Variables: User, Group Signature, Time, Admin.

Start:

$U_i \leftarrow$ *User*, Log in to the cloud system.

$A_i \leftarrow$*Admin*, Authentication permission to user U_i.

At time T_i, user uploads a file F_i.

$G_s \leftarrow$ Group Signature, generated by the cloud authority,

where $G_s \in (U_i, T_i)$.

At T_{i+1}, G_s is invalid.

User is not able to access the data using other person's signature key.

End.

Algorithm 2 Average time calculation for the file size F_i

procedure AVERAGETIME

Variables: System Time, Time periods, Amount.

Start:

$T_i \leftarrow$ System Time in ms.

Call Forward Secrecy Function

Time periods T are divided into four time slots like 100, 200, 300, 400 ms.

$A_i \leftarrow$ Average time.

$C_i \leftarrow$ Count of the group.

$TotalTime \leftarrow = A_i / C_i$.

Result= TotalTime * F_i, where *i* is an integer value i.e F_1 = 1024 kb and F_2= 2048 kb.

For Upload or download a file of size F_1= 1024 kb and F_2 = 2048 kb.

Compute $T_i \leftarrow$ Result/Time period time slot, where *i* is integer

End.

Our COIRS scheme proposed Algorithm 1 provide a better secrecy to user's files. In forward secrecy algorithm as name depicts it provides one step more secrecy for being accessed by the unauthorized users. We use asymmetric cryptographic technology with random variables. In forward secrecy technique at each stage the group signature is being produced, it means, if the secrete key holder compromised with others the secrecy of current file as well as past signatures being exposed by unauthorized users. To overcome this problem, asymmetric cryptography technique is used to generate different signature at every encryption and decryption process. Algorithm 2 computes the average time required for our COIRS model to upload the file where file sizes are 1024 kb and 2048 kb. As the size of the file increased the time required by the data owner to upload the files to the cloud becomes increases. The Time period is divided into 4 time slots, 100, 200, 300 and 400 ms. Total time is calculated separately for all time periods. It is calculated as,

$$\text{TotalTime} = Ai / Ci \quad (1)$$

Here, we are considering two constant file sizes are 1024 kb and 2048 kb. We calculate the average time to both these files is shown in figure 6, figure 7, figure 8 and figure 9.

5. EXPERIMENTAL ANALYSIS

In this section, we are analyzing our COIRS scheme on the bases of the *time* evaluation.

5.1. Time Analysis

In our COIRS model, we evaluate the time using two entities *Data owner* and *Data center*. For time analysis, experiments were conducted by taking some constant files to generate the accurate analysis. Our analysis for uploading time (or energy) for each file when user uploads different file sizes. As the file size increased the time required by the data owner to upload the file is as shown in figure 4. For uploading and downloading we are taking some constant file sizes i.e., 100 kb, 200 kb, 300 kb, 400 kb, 500 kb, 1000 kb, 2000 kb etc. In figure 5, we have shown the time required for COIRS model to download the different files such as 100 kb, 200 kb, 300 kb, 400 kb, 500 kb, 1000 kb, and 2000 kb. As the size of the file increased with increases time for upload/download a file.

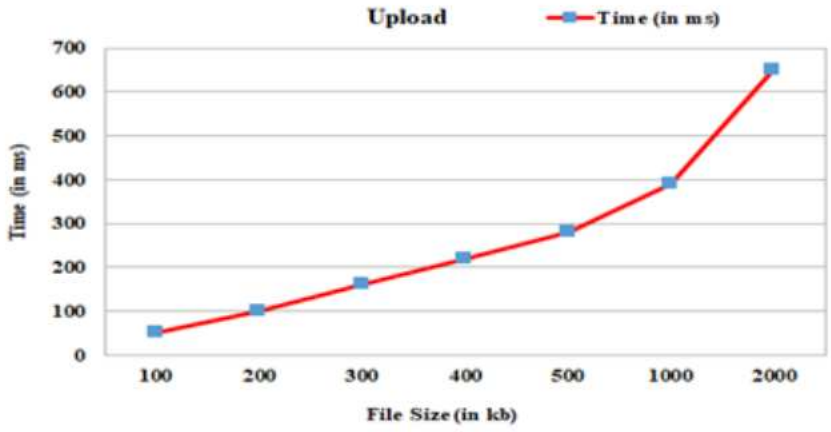

Figure 4 The Time consumption to upload different file sizes using COIRS scheme.

5.2. Implementation and Experimental Results

We calculated the analysis of our COIRS model with respect to three entities: *Data owner*, *Data center* and *Private key generator*. All analysis were conducted 20 times to gain an average results. For different groups with different size. Group 1, Group 2 and Group 3

contains 5, 10 and 20 users respectively. The count 'C' increases group by group, the average time required by the groups to sign energy usage data with different choices of M and T, where M is the number of users. The experiments were

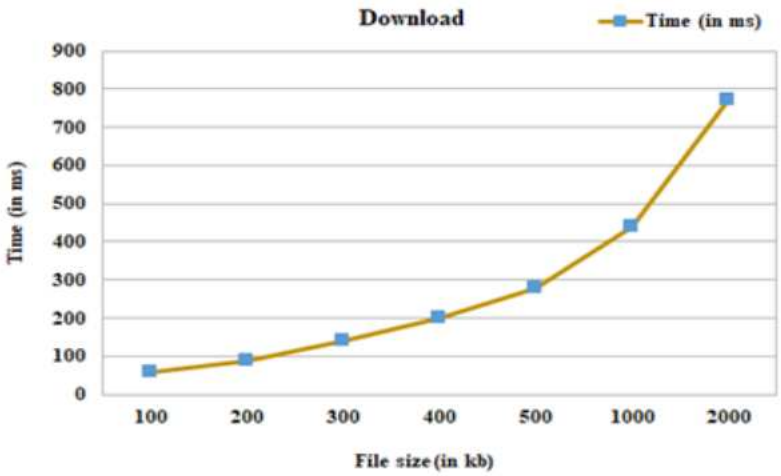

Figure 5 The Time consumption to download different file sizes using COIRS scheme.

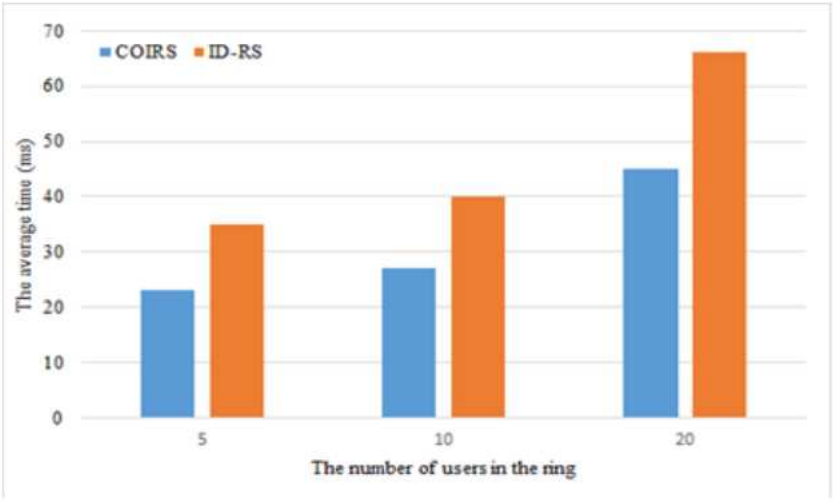

Figure 6 The average time for the data owner to sign energy usage data, |F| = 1024 kb.

Taken for the two constant file sizes F = 1024 kb and F = 2048 kb. In Table II shows the average time for the private key generator (PKG) to setup the system. The PKG took 80 and 1040 ms to setup the whole system for F = 1024 kb and F = 2048 kb respectively. In figure 6 depicts the average time for the the data owner to sign energy usage data file F is 1024kb using COIRS and ID-RS model. The ID-RS scheme consumes more time to sign when compare to COIRS scheme. In figure 7 depicts the average time for the data owner to sign energy usage data with constant file size F=2048 kb with different choices of M and T. This requires authenticated users only upload or download files. In group sharing decreases *time* and *cost* using COIRS scheme.

In ID-RE uses individual authentication, therefore more time for sign and consumes more energy. The test bed for the user is a personal computer built in with DELL i5 workstation inbuilt with 2.0 GHz, Intel Xeon dual-processor with 8 GB RAM and running on Windows 8 Professional 64-bit OS. The Time slices T were increased by multiples of 100 up to 400.

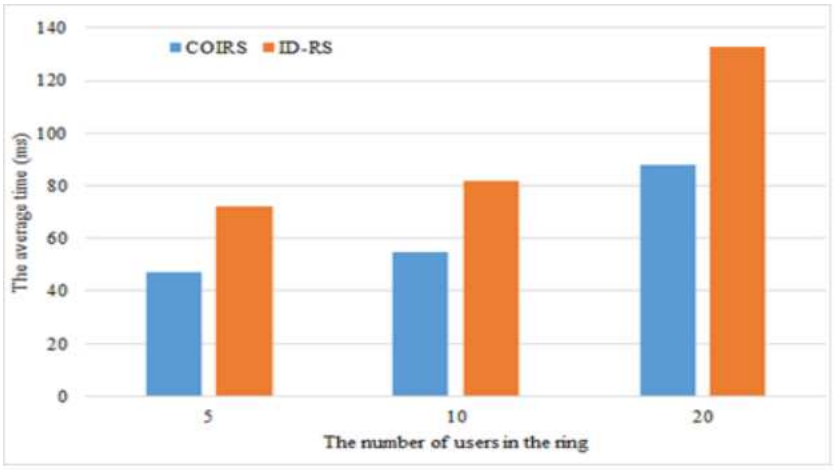

Figure 7 The average time for the data owner to sign energy usage data, |F| = 2048.

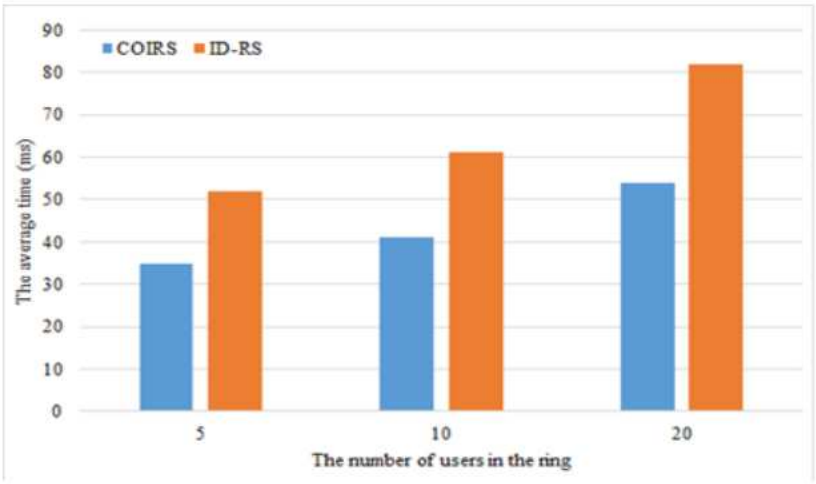

Figure 8 The average time for the data center to verify the ring signature, |F| = 1024 kb.

Table 2 Average time for the PKG to setup in COIRS system.

| M | (in kb)	Time (in ms)
1024	80
2048	1040

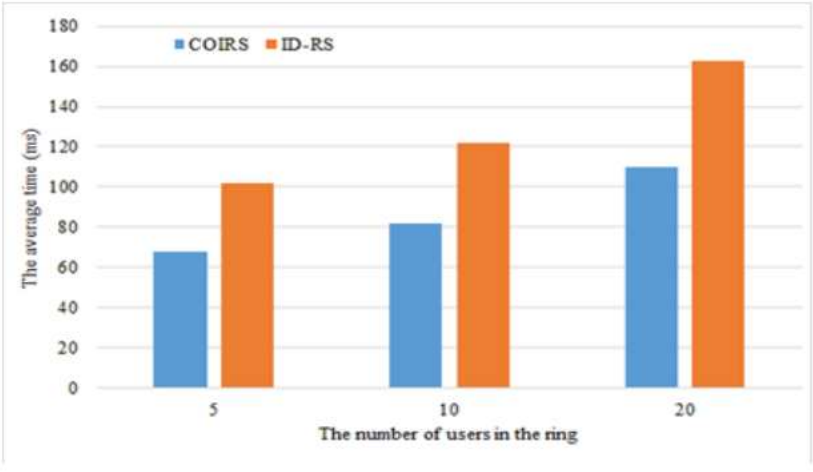

Figure 9 The average time for the data center to verify the ring signature, |F| = 2048 kb.

The individual time stamp of each group to verify the ring signature with different choices of M and T to upload/download a file. The average time for the data center to verify the ring signature of file F = 1024 kb and the average time for the data center to verify the ring signature file for F = 2048 kb is as shown in figure 9. This provides more security to the data because authorized users only share the files.

6. CONCLUSIONS

In group sharing scheme, to create an authentic and anonymous data sharing, Ring signature is one of the promising technique. *Ring signature* scheme permits the manager or data owner to authenticate into the system in anonymous manner. In conventional sharing scheme certificate authentication becomes a bottleneck because of high cost and more time consuming. To avoid this problem COIRS scheme is constructed. This scheme describes, suppose, the secret key holder has been compromised, all generated past signatures still remain valid. Discussed about how to optimize the time and cost when sharing the files to the cloud. Provide a protection to this scheme from collision attack, it means that revoked users cannot get the original documents and to reach high efficiency, implies that previous users not necessary to update their secret keys for the condition while new user enters the group or exit from the group. In generally high secrecy can be provided for group sharing, by applying all these approaches. COIRS scheme reduces signature *time* of file at data owner or provider and provides high *security* using Ring signature

REFRENCES

[1] P. Muthi Reddy, S. H. Manjula, and K. R. Venugopal, "Secure Data Sharing in Cloud Computing: A Comprehensive Review," International Journal of Computer (IJC), vol. 25, no. 1, pp. 80–115, 2017..

[2] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy Preserving Public Auditing for Secure Cloud Storage*," IEEE Transactions on Computers*, vol. 62, no. 2, pp. 362–375, 2013.

[3] 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,* vol. 24, no. 6, pp. 1182–1191, 2013.

[4] Z. Zhu and R. Jiang, "A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 1, pp. 40–50, 2016.

[5] S.-H. Seo, M. Nabeel, X. Ding, and E. Bertino, "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 9, pp. 2107–2119, 2014.

[6] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, T. V. X. Phuong, and Q. Xie, "A DFA-Based Functional Proxy Re-Encryption Scheme for Secure Public Cloud Data Sharing*," IEEE Transactions on Information Forensics and Security*, vol. 9, no. 10, pp. 1667–1680, 2014.

[7] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," *In Workshop on the Theory and Application of Cryptographic Techniques.* Springer, 1984, pp. 47–53.

[8] X. Huang, J. K. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, and J. Zhou, "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security," *IEEE Transactions on Computers*, vol. 64, no. 4, pp. 971–983, 2015.

[9] E. Bresson, J. Stern, and M. Szydlo, "Threshold Ring Signatures and Applications to Ad-Hoc Groups," *in Annual International Cryptology Conference*. Springer, 2002, pp. 465–480.

[10] C. Liu, J. Chen, L. T. Yang, X. Zhang, C. Yang, R. Ranjan, and R. Kotagiri, "Authorized Public Auditing of Dynamic Big Data Storage on Cloud with Efficient Verifiable Fine-

Grained Updates," *IEEE Transactions on Parallel and Distributed Systems,* vol. 25, no. 9, pp. 2234–2244, 2014.

[11] K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," *IEEE Transactions on Parallel and Distributed Systems,* vol. 24, no. 9, pp. 1717–1726, 2013.

[12] M. Nabeel, N. Shang, and E. Bertino, "Privacy Preserving Policy-Based Content Sharing in Public Clouds," *IEEE Transactions on Knowledge and Data Engineering,* vol. 25, no. 11, pp. 2602–2614, 2013.

[13] X. Dai, J. M. Wang, and B. Bensaou, "Energy-Efficient Virtual Machines Scheduling in Multi-Tenant Data Centers," *IEEE Transactions on Cloud Computing,* vol. 4, no. 2, pp. 210–221, 2016.

[14] S. Bera, S. Misra, and J. J. Rodrigues, "Cloud Computing Applications for Smart Grid: A Survey," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 5, pp. 1477–1494, 2015.

[15] S. Li, Y. Zhou, L. Jiao, X. Yan, X. Wang, and M. R.-T. Lyu, "Towards Operational Cost Minimization in Hybrid Clouds for Dynamic Resource Provisioning with Delay-Aware Optimization," *IEEE Transactions on Services Computing,* vol. 8, no. 3, pp. 398–409, 2015.

[16] S. Yang, D. Kwon, H. Yi, Y. Cho, Y. Kwon, and Y. Paek, "Techniques to Minimize State Transfer Costs for Dynamic Execution Offloading in Mobile Cloud Computing," *IEEE Transactions on Mobile Computing*, vol. 13, no. 11, pp. 2648–2660, 2014.

[17] J. Yao, H. Zhou, J. Luo, X. Liu, and H. Guan, "Comic: Cost Optimization for Internet Content Multihoming," *IEEE Transactions on Parallel and Distributed Systems,* vol. 26, no. 7, pp. 1851–1860, 2015.

[18] A. Trombetta, W. Jiang, E. Bertino, and L. Bossi, "Privacy-Preserving Updates to Anonymous and Confidential Databases*," IEEE Transactions on Dependable and Secure Computing,* vol. 8, no. 4, pp. 578–587, 2011.

[19] L. 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,* vol. 8, no. 12, pp. 1947– 1960, 2013.

[20] P. Muthi Reddy, Rekha Rangappa Dasar, R. Tanuja, S. H. Manjula, and K. R Venugopal, "Forward Secrecy in Authentic and Anonymous Cloud with Time Optimization," IEEE in Proceedings of the Fifteenth International Conference on Wireless and Optical Communications Networks (WOCN), ISBN: 978-1-5386-4798-1, 2018..

[21] A. C. Zhou, B. He, and C. Liu, "Monetary Cost Optimizations for Hosting Workflow-as-a-Service in IaaS Clouds," *IEEE Transactions on Cloud Computing*, vol. 4, no. 1, pp. 34–48, 2016.

[22] J. Yu, F. Kong, H. Zhao, X. Cheng, R. Hao, and X.-F. Guo, "Non Interactive Forward-Secure Threshold Signature without Random Oracles," *Journal of Information Science and Engineering,* vol. 28, no. 3, pp. 571–586, 2012.

[23] M. Bellare and S. K. Miner, "A Forward-Secure Digital Signature Scheme*," in Annual International Cryptology Conference*. Springer, 1999, pp. 431–448.

AUTHOR DETAILS

Muthi Reddy P is a full time Research Scholar in the Department of Computer Science and Engineering from University Visvesvaraya College of Engineering, Bangalore University, and Bengaluru, India. He was awarded Master of Technology in Computer Science and Engineering from Davangere University, Davangere. He obtained his Bachelor of Engineering degree in Computer Science and Engineering from BMS College of Engineering, Visvesvaraya Technological University. He was received the Diploma in Computer Science and Engineering from Govt. Polytechnic, Board of Technical Examinations, Karnataka. His research interests are in the field of Data Security, Data Sharing and IOT in the Cloud Computing.

Manjula S H is currently Associate Professor, Dept. of Computer Science and Engineering, UVCE, Bangalore University, Bengaluru. She has obtained B.E, M.Tech., Ph.D. in Computer Science and Engineering, Chennai. Her research interests are in the field of Wireless Sensor Networks and Data mining.

Venugopal K R is currently the Principal, University Visvesvaraya College of Engineering, Bangalore University, and Bangalore. He obtained his Bachelor of Engineering from University Visvesvaraya College of Engineering. He received his Masters degree in Computer Science and Automation from Indian Institute of Science Bangalore. He was awarded Ph.D. in Economics from Bangalore University and Ph.D. in Computer Science from Indian Institute of Technology, Madras. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science and Journalism. He has authored and edited 64 books on Computer Science and Economics, which include Petrodollar and the World Economy, C Aptitude, Mastering C, Microprocessor Programming, Mastering C++ and Digital Circuits and Systems etc., He has filed 101 patents. During his three decades of service at UVCE he has over 640 research papers to his credit. His research interests include Computer Networks, Wireless Sensor Networks, Parallel and Distributed Systems, Digital Signal Processing and Data Mining. He is a Fellow of IEEE, ACM and ISTE.