

# Verifiable data distribution technique for multiple applicants in a cloud computing ecosystem

Jayalakshmi Karemallaiah, Prabha Revaiah

Department of Computer Science & Engineering, Dr. Ambedkar Institute of Technology, Bangalore, India

## Article Info

### Article history:

Received Sep 1, 2022

Revised Nov 7, 2023

Accepted Nov 30, 2023

### Keywords:

Cloud architecture

Cloud computing

Data sharing

Data storage

Security

## ABSTRACT

Cloud computing is the most exploited research technology in both industry and academia due to wide application and increases in adoption from global organizations. In cloud, computing data storage is one of the primary resources offered through cloud computing, however, an increase in participants raises major security concerns, as the user has no hold over the data. Furthermore, recent research has shown great potential for efficient data sharing with multiple participants. Existing researches suggest complicated and inefficient cloud security architecture. Hence, this research work proposes identifiable data sharing for multiple users (IDSMU) mechanism, which aims to provide security for multiple users in a particular cloud group. A novel signature scheme is used for identifying the participants, further verification of the Novel Signature Scheme is proposed along with a retraction process where the secret keys of the participant and the sender is cross-verified; at last, a module is designed for the elimination of any malicious participants within the group. IDSMU is evaluated on computation count and efficiency is proved by comparing with an existing model considering computation count. IDSMU performs marginal improvisation over the existing model in comparison with the existing model using the novel signature scheme.

*This is an open access article under the **CC BY-SA** license.*



## Corresponding Author:

Jayalakshmi Karemallaiah

Department of Computer Science and Engineering, Dr. Ambedkar Institute of Technology

Bangalore, India

Email: jayalakshmi\_112@rediffmail.com

## 1. INTRODUCTION

Cloud computing has emerged from the development of distributed architecture computation, it has added additional promise for users' computation as it aides several characteristics including flexibility, scalability, and pay-as-you-go service. It enables the vendors for renting service as per requirement. The application can be used or accessed irrespective of the place; the user tries to gain access, which is linked by their services. Various services are used by the customer across the internet, some of which include storage of data, databases, software, networking, and servers. The technology consists of a number of shared resources that are provided on demand of the user as a service that is metered. The evolution of cloud computing is from the utility and grid application as well as services of computing [1]–[3]. The cloud has application models through which services are offered. The classification of these models is as follows: private, public, hybrid, and community cloud. The private cloud refers to the use of cloud services for an internal organization, where the infrastructure of the cloud is modified according to the organization. The public cloud refers to the services that are commonly shared through the internet to various organizations. The performance of cloud services has also developed and reported to increase business over the years.

However, the security of cloud computing has many challenges that yet have to be overcome [4], [5]. There are various types of services that are offered by cloud, these services include platform as a service (PaaS), infrastructure as a service (IaaS) and software as a service (SaaS). PaaS provides various testing, developing, and delivering as well as management environments. IaaS provides the use of IT based infrastructures, which include servers, virtual machines, operating systems, networks and storage. SaaS is used for the delivery of various applications over the internet. Software applications can be maintained like security patches and software updates. Cloud also offers another service called as server less computing, where the functionality of building applications is focused without any time wasted on the management of servers. The provider manages the setup as well as the server management [6], [7].

The components of cloud computing include three distinct parts: the front end, the platform back end, lastly, a network and delivery that is based on cloud. The architecture of cloud computing is made up of two similar parts, one part consists of Interactions with the client and the other part is used for the service providers of the cloud. The SaaS suggests that the data is encrypted by the user although the application models are a new invention in cloud computing. Figure 1 shows the major cloud security components such as compliance, production, access and identity, production, availability, response, and trust. Moreover, the designed cloud model should comply with these components to be secure, distributed, and efficient data sharing especially when there are multiple participants involved [8].

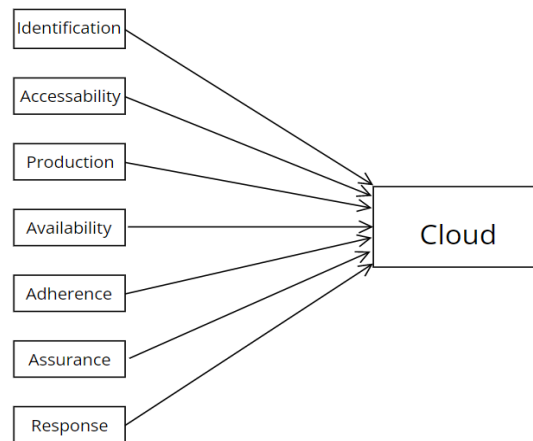


Figure 1. Cloud security component

Various constraints and problems occur with respect to the privacy and security of the data that is being sent within the medium that is open. The mechanisms for the security of this network are attractive as well as tough. Prior to the design of any algorithm or mechanism for security, the focus of the developer should lie on the possible attacks on the algorithm pertaining to security. It is possible for each algorithm to oppose various attacks based on its properties as well as the algorithm that is selected about its requirement; the developer has to perform this big challenge. Eventually, constant monitoring is required for the protection of the data from these attacks. The attacks, which threaten the network, have been vastly categorized into passive attacks and active attacks. The attack is classified as an active attack if the resources of the system can be altered or its operations are affected. A passive attack is when the information is collected in opposition to obtaining the information accessed. These attacks include breaking the site, service denial, usage of resources, deception of active attacks, breaching of data during traffic in the network, sniffing, collecting of information that is sensitive possessed by passive attacks. A huge count of researchers has dedicated their attempts to propose schemes that are reliable for data searches that are secure within the cloud [9], [10]. From a decade data is generated exponentially, it can be accessed very easily with effective cost by leaps, and bounds. The data volume may be increased from Terabyte (TB) to Petabyte (PB) because 2.5 quintillion bytes of data may be gathered per day. The data involves text files that are plain, images of various sizes and formats as well as multimedia files. The transmission of data over the channel of communication without the main task being disclosed. Various mechanisms for security that include policies for access control, cryptography, digital signatures, and steganography. are used in order to avoid the threats that are unauthorized. The most commonly used is cryptography for the protection of data. Furthermore, the contribution of this proposed work is as given below: (a) this research work proposes identifiable data sharing for multiple users (IDSMU) mechanism, which aims for providing the multiple participants, data-

sharing model in the cloud. (b) IDSMU creates general participants-key (GP-key) for secure access of data; further, with the help of a manager, it creates the trusted participant's group, and a later novel signature scheme is proposed to trace the identity of participants. (c) IDSMU is evaluated considering the computation count; also, further evaluation is carried out by comparing with the existing model. (d) A Verification of the Novel Signature Scheme is proposed along with a retraction process where the secret keys of the participant and the sender is cross verified. (e) A fault detection process is performed for the elimination of any malicious participants within the group.

This particular research work is organized as follows: the first section starts with the background of cloud computing along with security concerns and architecture of the cloud along with different services of cloud. This section ends with the motivation and contribution of research work. Further, the second section discusses the related work of existing models along with their shortcomings. The third section proposes IDSMU along with the proposed architecture, mathematical model, and algorithm. The fourth section evaluates the model by comparing it with the existing model at client side and server side.

## 2. RELATED WORK

Security plays an important role in the generalization of cloud computing which leads to global acceptance of cloud computing (CC) service; existing related work of security focused on the various security solution, which includes security policy implementation and technology. In this section, this research focuses on several related work that has been conducted earlier. In [4] author has the process of cryptography that involves key generation is split into three classes. Initially, the service model of encryption that is based on support vector machine (SVM) for the generation of the key is from the encryption mode of operation that is conventional additional towards few improvements. In order to complicate the process, the techniques of optimization are considered for the generation of the key in accordance with two various models of application that are used for computation for a cloud environment that is more secure. In [11] paper, a scheme for data protection that is verified and searchable from an aided third party is proposed. This uses the technology of cloud computing. To understand the protocol better, firstly, a system model that is user differentiated is introduced along with a structure for data storage that is cubic. Based on the structure of the data and system model, the integrity of the data that the users have downloaded or uploaded is reviewed at any given time and encrypted keywords are used to search the scholarly data online [12]. in order to aid the retrieval of efficient cipher text and keep up with the challenging performance, this paper proposes an encryption scheme that is lightweight attribute-based searchable encryption (LABSE), which recognizes the access control that is fine gained and the keyword search. During the reduction of the overhead for computation of the devices that are resource-constrained [13]. The proposed work is an authentication user group that is content-centric to assure the accuracy and security of the data shared. The proposed authentication scheme for the group user uses the content of the user for the generation of the feature vector of the user. Moreover, the authentication scheme for the group that is based on every user's identity can assure the security of the network before the data is being shared. Additionally, the network operations that are regular remain unaffected and are not damaged due to the incidents that happen over the process of authentication.

In [14], the focus lies on the IoT for industries where the storage of raw information in these devices is not advised due to their storage capacity constrain as well as their threats relating to security. The paper emphasizes on resolving the issues that are caused by deployment of these devices in remote areas by development of a framework that is achieved by combination of cloud computing as well as fog computing. The raw information that is gathered and stored is done with the help of a cloud sever or an edge server for data that is not time sensitive and time sensitive respectfully. In [15], the challenges that are faced by internet of service (IoT) devices with edge computing is tackled by developing a mechanism based on trust calculations for the edge IoT devices by using the feedback information. The paper [16] shows that although cloud services are extensively being used there is a hesitation among its users to share important information due to the security concerns that arise due to cloud. In order to resolve these challenges an encryption mechanism is proposed which is based on identity. This mechanism is combined with the revoking storage; this methodology has been proposed prior which is proved to be unsuccessful. Whereas the scheme proposed in this paper shows an improvised technique. In [17], a framework is proposed for cloud computing combined with edge computing with respect to IoT devices. The general risks mainly data leakage relating to combined storage of edge and cloud are handled in this paper. In [18], the focus lies in the emerging technology of data group sharing. The paper highlights the data sharing mechanism by using building blocks for a group signature. The security of this data group sharing technology is shown in this paper. In paper [19], confidentiality issues arise when user valuable information or data is stored in cloud services. The storage of information in a domain outsider owner's trust leads to confidentiality concerns. A solution to resolve this problem is proposed in this paper, where a protocol is developed for sharing and management of secret group

key for protection against unauthorized access of the stored and communicated information. The key is used in the data encryption process along with a secret key distribution technique is used for the group distribution of the key using the protocol. In [20], an IoT-based cloud approach is considered due to the lack and inefficiency of IoT devices for computation and storage. The paper proposes a framework, which evaluates the security of the services that is provided by the cloud. An assessment is performed for cloud security, which evaluates its service. This is performed by using a security metrics dataset and a real-world dataset for web-services [21]. Proposed an application layer based signal scrambling scheme (to scramble the healthcare information, a tiny data is utilized). A random number generator or a piece of data is utilized for the tiny data derivation (that increases the flexibility of the scheme) [22]. Provided a six-step based framework. These steps are: (i) the preliminary selection, (ii) systems entity's selection, (iii) technique selection, (iv) patient's physiological parameter's assessment, (v) security analysis, and (vi) performance estimation.

### 3. PROPOSED METHODOLOGY

The widespread utilization of CC in information technology makes it easy adoption for standalone as well as distributed approaches. However, several service owners are still in doubt about CC adoption due to data security. Moreover, in the related work section, several approaches have been discussed and it requires to development of an efficient architecture. The protection of data or the privacy of data is an essential necessity for every paradigm relating to computing. Particularly, considering cloud computing, the data is operated and managed by a third party. Therefore, user data security could be breached for the archetype cloud computing. One such method for data protection with the cloud is through data encryption, which is made inarticulate.

#### 3.1. System modelling

Figure 2 shows the system model of the proposed architecture; the general system model is designed based on user preference. For instance, a user with a similar domain tends to store the data in one particular data where the other members can have access. Moreover, these members are required to be genuine; this model tends to make the group data sharing not only efficient but also secure. In order to make it secure, the signature phenomena are utilized.

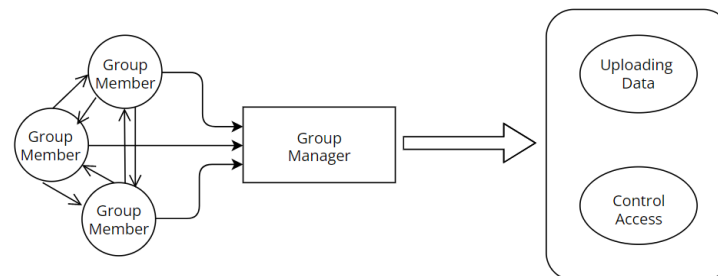


Figure 2. proposed IDSMU model

The proposed Security model in Figure 2 comprises the three modules; the first module is a cloud that provides the users with unlimited storage. In addition, does not modify any data Second module is the Manager who is directly responsible for parameter generation of the designed model. The third module refers to the number of users based on the designed communication model. Further, there are three types of connection. Connection 1 indicates the registration and revocation, connection 2 is consensus development among users to generate the key, and connection 3 is identifying the participants. In Proposed Model IDSMU (Identifiable Data Sharing for multiple users)-mechanism, users register to the group manager for data sharing; the job of revocation is also carried out by the manager based on key generation.

#### 3.2. Server-side modeling for key generation

In Client-side modeling, key is generated; IDSMU generates the key through two distinctive steps for participants. Key is generated based the on designed structure of  $(w, l + k, 1)$ ; this structure is designed according to the selection of prime number participants. However, considering the participants with a prime number might not be sufficient for the generation of keys as few messages might go missing. Thus, trusted members are created to support the data sharing along that also helps in creating the GP-key.

Trusted participants (TP) selects the trusted participants to create the key. Trusted participants are the one that has a good reputation in a particular group, it is denoted as  $m_q - m$ . In order to select the trusted participant need to submit  $\varphi_j$  which indicates the identity to register with the manager to obtain the secret key  $(w_j, Z_j)$ . Once the registration and selection of trusted participants are completed. Normal participants and trusted participants requires two steps to generate the general participants. Further, the structure is designed for the  $o$  participants that need to share the data.

**3.2.1. Generation of participant’s signature**

Each participants chooses random number  $q_j$  as the secret key to compute  $L_j = d(H, q_j R_j)$  the that helps in generation of general participants-key in particular group among the participants. Further, each participants member  $j$  adopts the algorithm of Participants signature (PSign) for creating a signature on message with given secret key  $(Z_j, w_j)$ . Meanwhile participants receives message  $C_k = (L_k, \delta_k)$  from participants  $k$ . Further, key generation is parted into four scenario; in case of first scenario first participants requires receiving message from  $k$  participants. In case of second scenario, member participants requires to receive message from participant’s  $k$  along with first participants. In case of third scenario, for participants  $j$ , it needs to receive the message from participant 0 and participants  $k$ . Remaining participants receives message from participants  $k$  and  $((j - 1)/l)$ . Table 1 presents the algorithm for signature generation. Moreover, in order to design the algorithm few parameters needs to be computed, these parameters are computed through (1) and (2). In (1) and (2) parameter helps in generating the hash for signature.

$$\begin{aligned}
 S_1 &= \varpi \cdot T \\
 S_2 &= \varrho \cdot U \\
 S_3 &= Z_j + (\varpi + \varrho) \cdot G
 \end{aligned}
 \tag{1}$$

$$\begin{aligned}
 Q_1 &= s_\varpi \cdot T \\
 Q_2 &= s_\varrho \cdot U \\
 S_3 &= f(S_3, O)^{s_w} \cdot f(G, V)^{-s_\varpi - s_\varrho} \cdot f(G, V)^{-s_\varpi - s_\varrho} \\
 Q_4 &= s_w \cdot S_1 - \xi_1 \cdot T \\
 Q_5 &= s_w \cdot S_1 - \xi_1 \cdot T
 \end{aligned}
 \tag{2}$$

Table 1. Signature generation	
<i>Input is given as a secret key <math>(Z_j, w_j)</math>,</i>	
<i>message and system parameters</i>	
Step1: selection of random number	$\varpi, \varrho, s_\varpi, s_\varrho, s_w, s_{\xi_1}, s_{\xi_2} \in Y_p'$
Step2: settings up numbers	$\xi_1 = w_j \varpi, \xi_2 = w_j \varrho$
Step3: compute $S_1, S_2, S_3, Q_1, Q_2, Q_3, Q_4, Q_5$	
Step4: Generate hash value with $b = g_1(L, S_1, S_2, S_3, Q_1, Q_2, Q_3, Q_4, Q_5)$	
step 5: compute $q_\varpi, r_\varrho, r_w, r_{\xi_1}, r_{\xi_2}$	
step6: Generation of group signature	$\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$
Step7: return output as $\delta$ on message $L$	

Once each participant in a particular group receives the particular message, which further contributes to creating the general participants -key from participants, a signature is verified with the message validity. After successful verification, each participant computes.

$$B_{k,j} = \prod_{w \in ED_{k-j}} L_w, (w < m, j < m)
 \tag{3}$$

Participants  $i$  receives message as  $D_k = \{B_{k,j}, \delta_k\}$  form other participants such that  $i \in E_j$  where  $B_{k,j}$  is for creating a particular group signature by participants  $j$  with algorithm 1. Each participant verifies the message validity, if verification is valid then the Group key is computed through the (4).

$$J = L_j (\prod_{w \in ED_{k-j}} B_{k,j})
 \tag{4}$$

Further, each participant in the group-access the General participant's key that can be utilized for ensuring security in the cloud.

### 3.3. Verifying the generated signature at client side

The integrity if the data is tested by a verification scheme that is proposed in this paper. This is an essential step in the authentication process of the key. In the proposed work, we specify the verification for the group signatures that are required for authorization process. This verification of the group participants is performed when the manager sends an information for authorization. Each participant can verify the message that is received by an algorithmic flow that is proposed. Consider the input message that is received by the participants to be  $N$  and this message has a novel signature that is denoted as  $\sigma$ . System parameters are the constant parametric values that has the directories for services relating to data that include storage of various types of files such as rejected, log, target, cache, temporary and source. The parametric values used in this proposed work are given as  $(O, B, U, G, V)$ .for the verification process, the resulting value is true or false which means the secret key verification is successful or has failed. We perform the following calculations to show the verification process of the Novel Signature Scheme.

$$\overline{Q_1} = s_a \cdot B - c \cdot S_1 \quad (5)$$

$$\overline{Q_2} = s_\beta \cdot B - c \cdot S_2 \quad (6)$$

$$\overline{Q_3} = [(\hat{e}(S_3, V))^c \cdot (\hat{e}(O, O))^{-c}] \cdot \hat{e}(S_3, O)^{s_x} \cdot \hat{e}(G, V)^{s_a - s_\beta} \cdot \hat{e}(G, O)^{s_{\delta_1} - s_{\delta_2}} \quad (7)$$

$$\overline{Q_4} = s_x \cdot S_1 - s_{\delta_1} \cdot B \quad (8)$$

$$\overline{Q_5} = s_x \cdot S_2 - s_{\delta_2} \cdot U \quad (9)$$

$$c' = g_1(N, S_1, S_2, S_3, \overline{Q_1}, \overline{Q_2}, \overline{Q_3}, \overline{Q_4}, \overline{Q_5}) \quad (10)$$

If the values of the participants match the hash values, then verification process is rendered as successful and if the values do not match then there is an error that occurs in the verification process implying that it has failed.

The validity of the participants who have sent the message to other participants is performed by verification retraction of the message senders. This process is determined by using the novel group signature denoted as  $\sigma$ , the parametric values used here are  $P_0, P_1, P_2$ . There are retraction keys that are stored in the retraction list given as  $Z_0, Z_1, Z_2 \dots Z_M$ . This results in the verification retraction being invalid or is valid. A temporary variable is set to  $\hat{e}(S_1, G_1) \cdot \hat{e}(S_2, G_2)$ . If the temporary variable is equal to  $\hat{e}(S_3 - Z_j, G_0)$ , where  $j$  is any given value of the retraction keys between 1 to  $M$ . Then, the verification is considered as invalid when then temporary variable is not equal to  $\hat{e}(S_3 - Z_j, G_0)$ , the verification is valid.

### 3.4. Discarding the participants

The malicious practice of some members in the group is predicted to destroy the security of the by generation of sub level keys among the group. The generation and distribution of the keys within the group leads to security breaches, this is avoided by only one key being generated that is unique to the particular participant and is destroyed after its use. The process of fault detection is thoroughly explained in this section, where a participant has to submit the signature as well as the retraction keys. After this is completed, it has to satisfy (11) for the verification process,

$\{M, H C_{gm}, Z_j | 0 \leq j \leq u - 1\}$  which has to be verified by the participants;

$$M = g_2 \left( HC_j \parallel |HC_{gm}| \parallel t \mid 0 \leq j \leq m - 1 \right), HC_{gm} \text{ is the ID of the group} \quad (11)$$

this expression is given by the group for all the participants to verify using their signature of group and the sub keys  $Z$  of every member. A common key denoted as  $\mathbb{C}$  is given for each member to verify using (12),

$$\mathbb{C}^d = \prod_{j=0}^{m-1} Z_j \text{ where } d \text{ is a non-zero integer } d \in Y_p \quad (12)$$

if the (12) is satisfied for every participant of the group then a common key  $\mathbb{C}$  is confirmed. If the equation is not satisfied it results in performing fault detection. In this case, the participant  $l$  who has not satisfied the equation sends a fault detection report to the group authority using (13),

$$M, HC_l, \tau_l, N_x \ x \in D_l \in l \quad (13)$$

the report sent is inclusive of the secret key of the participant  $l$  and the message  $N$ . It is verified if the message sent by the participant  $l$  to the group is the same message or if the message is being varied. This report has to be sent by the participant  $l$  under time  $t$  and the participant  $l$  shall be terminated from the group if the attempts failed cross a limit  $\varphi$ . The participant  $l$  shall also be terminated from the group if the report response is not sent by time  $t$ . Therefore, it is concluded that the participant  $l$  is involved in malicious activities or is under a service attack. If both of these conclusions are not met then the fault detection process is run for the rest of the participants.

### 3.5. Key update

The key updating process takes places in two phases: firstly, updating the common key  $\mathbb{C}$  for the entire group and updating the secret key of individual participants. Considering the re-encryption as well as the control over access and authentication, the data is not shared at the cloud server due to the collision and with the participant with detected faults. The common key is updated in a fixed interval of time and during this process, the retraction list is cleared. The private keys are also update during the change of a group participant. A random key is generated for the new participant, which is replaced at the cloud after the verification of the signature is successful.

## 4. PERFORMANCE EVALUATION

Cloud Computing technologies have become more preferable computational models due to their characteristics like cost-effectiveness, flexibility, and scalability. However, the performance of cloud computing is directly affected as the user has no control over the data, especially in the case of multiple participants involved in a particular group. In this section, IDSMU is evaluated and performance is analyzed, in order to evaluate the performance, python is used as the programming language with a system configuration of windows 10 packed with 16 GB RAM and 4GB NVidia graphics. Further, a model is evaluated considering the client-side and server-side by varying the number of computation counts from 10 to 100. In order to prove the model efficiency, the proposed model is compared with two baseline models [23], [24] and the existing model [25].

### 4.1. Server-side evaluation

Figure 3 presents the client-side computation cost evaluation considering the time in seconds as the parameter. Moreover, in the case of client-side evaluation which can also be referred to as the key generation. IDSMU is evaluated with comparing with three mechanism considering 10 different computation count as 10 to 100; considering instances of 10 to 100 computation counts, existing mechanism does not perform well i.e. in order to generate the key secure VDB takes more time in comparison with other mechanism with required time of 0.13, 0.4, 0.6, 0.8, 1, 1.15, 1.26, 1.5, 1.75 and 2.15 respectively. Further novel- DB takes less time than secure-VDB with time requirement of 0.125, 0.2, 0.23, 0.3, 0.35, 0.3, 0.5, 0.55, 0.65 and 0.7 respectively. A verifiable scheme performs better than the other model with seconds of 0.1, 0.15, 0.225, 0.2, 0.25, 0.25, 0.45, 0.5, 0.6 and 0.65 in respective manner. However, in comparison with all these mechanisms, proposed mechanism IDSMU requires 0.004540992, 0.00766, 0.004521227, 0.00995, 0.004767766, 0.009976, 0.004631673, 0.0099, 0.00465587 and 0.009925549 respectively.

### 4.2. Client-side evaluation

Figure 4 presents the server side evaluation which is also known as the verification of key based on the computation count of 10, 20, 30, 40, 50, 60, 70, 80, 90 and 100. In client side evaluation, key verification is carried out for different computation count i.e. from 10 to 100; existing model i.e. verifiable scheme performs better for key verification. Moreover, least performed model is secure-VDB, which requires 0.25, 0.45, 0.75, 0.8, 1.1, 1.35, 1.6, 1.75, 2.1 and 2.3 in respective manner for 10 to 100 Computation count. Further, novel-VDB requires 0.2, 0.25, 0.55, 0.5, 0.8, 0.75, 1.1, 1.25, 1.6 and 1.75 respectively for computation count 10 to 100. Verifiable-scheme is optimal when compared to above discussed method with required time of 0.125, 0.15, 0.26, 0.25, 0.45, 0.52, 0.6, 0.55, 0.8 and 0.85 respectively. However, proposed model IDSMU is most efficient with time required to verify the key is 0.005243778, 0.006999922, 0.003568935, 0.007794452, 0.002598095, 0.00816344, 0.002682917, 0.00654999, 0.002575437 and 0.006519957 respectively for computation count of 10 to 100.

### 4.3. Signature generation

Signature generation is one of the modules designed for secure implementation of IDSMU as given in Table 1. Figure 5 shows the time required to generate a signature for computation counts of 10 to 100

given as 0.003196383, 0.003095162, 0.003421823, 0.002821046, 0.003031621, 0.005085568, 0.003010011, 0.002807465, 0.00482555 and 0.002807465 respectively. Figure 6 presents the graphical presentation of improvisation over the other model; it is observed that, as number of computation count increases there is increase in improvisation.

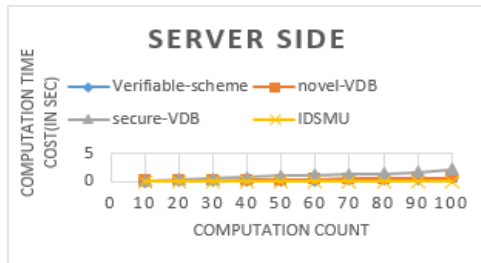


Figure 3. Server side evaluation

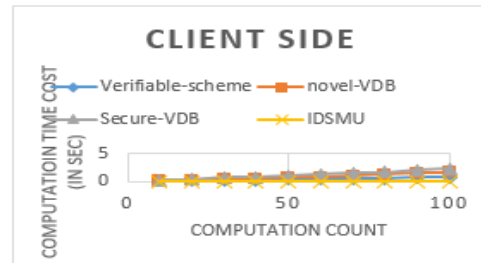


Figure 4. Client side evaluation

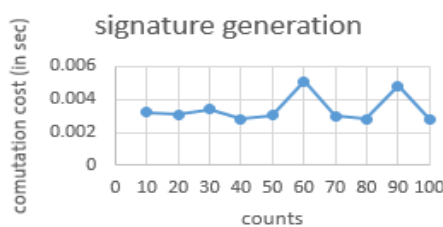


Figure 5. Signature generation

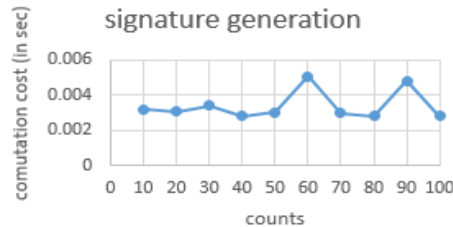


Figure 6. Percentage of improvisation

## 5. CONCLUSION

Security challenges and vulnerabilities arises through cloud computing service usage as currently CC is considered as the primary storage. Moreover, importance of security becomes more impactful in large organization where there are multiple participants in a particular cloud group. This organization requires integrity and confidentiality of data through cloud service providers. Hence, this research work proposes IDSMU mechanism, which aims for ensuring the secure data sharing with multiple participants in a group. IDSMU creates GP-key for secure access of data; further, with the help of a manager, it creates the trusted participant's group, and a later novel signature scheme is proposed to trace the identity of participants. A Verification of the Novel Signature Scheme is proposed along with a retraction process where the secret keys of the participant and the sender is cross verified. A detection process is performed for the elimination of any malicious participants within the group. IDSMU performs nearly 99% improvisation over the existing model in comparison with the existing model using the novel signature scheme, however considering the vulnerabilities of the cloud environment, it is important to consider the other security aspects, which need to be analyzed in the future.

## REFERENCE





- [1] M. Younis, W. Lalouani, N. Lasla, L. Emokpae, and M. Abdallah, "Blockchain-enabled and data-driven smart healthcare solution for secure and privacy-preserving data access," *IEEE Systems Journal*, vol. 16, no. 3, pp. 3746–3757, Sep. 2022, doi: 10.1109/JSYST.2021.3092519.
- [2] Y. Zhao, Y. Wang, X. Cheng, H. Chen, H. Yu, and Y. Ren, "RFAP: A revocable fine-grained access control mechanism for autonomous vehicle platoon," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 9668–9679, Jul. 2022, doi: 10.1109/TITS.2021.3105458.
- [3] A. Shankar, P. Pandiaraja, K. Sumathi, T. Stephan, and P. Sharma, "Privacy preserving E-voting cloud system based on ID based encryption," *Peer-to-Peer Networking and Applications*, vol. 14, no. 4, pp. 2399–2409, Aug. 2021, doi: 10.1007/s12083-020-00977-4.
- [4] F. Chen, Z. Li, C. Jiang, and J. Li, "Verifiable cloud data access: Design, analysis, and implementation," *IEEE Systems Journal*, vol. 16, no. 1, pp. 1135–1146, Mar. 2022, doi: 10.1109/JSYST.2020.3034105.
- [5] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, "A systematic literature review on cloud computing security: Threats and mitigation strategies," *IEEE Access*, vol. 9, pp. 57792–57807, 2021, doi: 10.1109/ACCESS.2021.3073203.
- [6] A. Saboor, A. K. Mahmood, M. F. Hassan, S. N. M. Shah, F. Hassan, and M. A. Siddiqui, "Design pattern-based distribution of microservices in cloud computing environment," in *Proceedings-International Conference on Computer and Information Sciences: Sustaining Tomorrow with Digital Innovation, ICCOINS 2021*, Jul. 2021, pp. 396–400, doi: 10.1109/ICCOINS49721.2021.9497188.







- [7] H. Jin, Z. Li, D. Zou, and B. Yuan, "DSEOM: A framework for dynamic security evaluation and optimization of MTD in container-based cloud," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 3, pp. 1125–1136, 2021, doi: 10.1109/TDSC.2019.2916666.
- [8] C. Lan, C. Wang, H. Li, and L. Liu, "Comments on 'attribute-based data sharing scheme revisited in cloud computing,'" *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2579–2580, 2021, doi: 10.1109/TIFS.2021.3058758.
- [9] M. Shabbir *et al.*, "Enhancing security of health information using modular encryption standard in mobile cloud computing," *IEEE Access*, vol. 9, pp. 8820–8834, 2021, doi: 10.1109/ACCESS.2021.3049564.
- [10] F. M. Awaysheh, M. N. Aladwan, M. Alazab, S. Alawadi, J. C. Cabaleiro, and T. F. Pena, "Security by design for big data frameworks over cloud computing," *IEEE Transactions on Engineering Management*, vol. 69, no. 6, pp. 3676–3693, Dec. 2022, doi: 10.1109/TEM.2020.3045661.
- [11] D. Samanta *et al.*, "Cipher block chaining support vector machine for secured decentralized cloud enabled intelligent iot architecture," *IEEE Access*, vol. 9, pp. 98013–98025, 2021, doi: 10.1109/ACCESS.2021.3095297.
- [12] J. Shen, C. Wang, A. Wang, S. Ji, and Y. Zhang, "A searchable and verifiable data protection scheme for scholarly big data," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 1, pp. 216–225, Jan. 2021, doi: 10.1109/TETC.2018.2830368.
- [13] Y. Bao, W. Qiu, and X. Cheng, "Secure and lightweight fine-grained searchable data sharing for IoT-oriented and cloud-assisted smart healthcare system," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2513–2526, Feb. 2022, doi: 10.1109/JIOT.2021.3063846.
- [14] J. S. Fu, Y. Liu, H. C. Chao, B. K. Bhargava, and Z. J. Zhang, "Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 10, pp. 4519–4528, Oct. 2018, doi: 10.1109/TII.2018.2793350.
- [15] J. Yuan and X. Li, "A reliable and lightweight trust computing mechanism for IoT edge devices based on multi-source feedback information fusion," *IEEE Access*, vol. 6, pp. 23626–23638, 2018, doi: 10.1109/ACCESS.2018.2831898.
- [16] K. Lee, "Comments on 'secure data sharing in cloud computing using revocable-storage identity-based encryption,'" *IEEE Transactions on Cloud Computing*, vol. 8, no. 4, pp. 1299–1300, Oct. 2020, doi: 10.1109/TCC.2020.2973623.
- [17] Y. Tao, P. Xu, and H. Jin, "Secure data sharing and search for cloud-edge-collaborative storage," *IEEE Access*, vol. 8, pp. 15963–15972, 2020, doi: 10.1109/ACCESS.2019.2962600.
- [18] X. J. Lin, L. Sun, and H. Qu, "Cryptanalysis of an anonymous and traceable group data sharing in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2773–2775, 2021, doi: 10.1109/TIFS.2021.3065505.
- [19] S. Han, K. Han, and S. Zhang, "A Data Sharing Protocol to Minimize Security and Privacy Risks of Cloud Storage in Big Data Era," *IEEE Access*, vol. 7, pp. 60290–60298, 2019, doi: 10.1109/ACCESS.2019.2914862.
- [20] X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang, and D. Chen, "Enhancing cloud-based IoT security through trustworthy cloud service: An integration of security and reputation approach," *IEEE Access*, vol. 7, pp. 9368–9383, 2019, doi: 10.1109/ACCESS.2018.2890432.
- [21] S. Di Bao, M. Chen, and G. Z. Yang, "A method of signal scrambling to secure data storage for healthcare applications," *IEEE Journal of Biomedical and Health Informatics*, vol. 21, no. 6, pp. 1487–1494, Nov. 2017, doi: 10.1109/JBHI.2017.2679979.
- [22] I. Masood, Y. Wang, A. Daud, N. R. Aljohani, and H. Dawood, "Towards smart healthcare: Patient data privacy and security in sensor-cloud infrastructure," *Wireless Communications and Mobile Computing*, vol. 2018, pp. 1–23, Nov. 2018, doi: 10.1155/2018/2143897.
- [23] J. Shen, A. Wang, C. Wang, J. Li, and Y. Zhang, "Content-centric group user authentication for secure social networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 8, no. 3, pp. 833–844, Jul. 2020, doi: 10.1109/TETC.2017.2779163.
- [24] S. Benabbas, R. Gennaro, and Y. Vahlis, "Verifiable delegation of computation over large datasets," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6841 LNCS, Springer Berlin Heidelberg, 2011, pp. 111–131.
- [25] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, "New publicly verifiable databases with efficient updates," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 5, pp. 546–556, Sep. 2015, doi: 10.1109/TDSC.2014.2366471.

## BIOGRAPHIES OF AUTHORS



**Jayalakshmi Karemallaiah**     is currently working as a Assistant Professor in the Department of Computer Science and Engineering, Dr. Ambedkar Institute of Technology, Bangalore, India. She has *obtained* Bachelor's of Engineering BE degree in Computer Science and Engineering from Mysore University, Master's Degree M.Tech. Computer Network Engineering from VTU in 2009. And currently she is a research scholar at Dr. Ambedkar Institute of Technology doing her Ph.D. in Computer Science and Engineering. She has attended many workshops and induction programs conducted by various universities. Her areas of interest are Cloud Computing and Computer Networks. She can be contacted at this email: jayalakshmi\_112@rediffmail.com.



**Dr. Prabha Revaiah**     is currently working as a Professor in the Department of Computer Science and Engineering, Dr. Ambedkar Institute of Technology, Bangalore, India. She obtained her Bachelor of Engineering degree in Computer Science and Engineering branch from Mysore University, M.E in Computer Science and Engineering from Computer Science Department, UVCE, Bangalore University in the year 2003. She has 30 years of teaching experience. She was awarded Ph. D in Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. Her research interest is in the area of Wireless Sensor Networks and IOT. She can be contacted at this email: prabha.cs@drait.edu.in.