Research Article

Double Pseudonym-Based Privacy Preservation Scheme for securing sensitive information in the SaaS cloud environment

V.Ganesan [a], Dr.N.Umadevi [b]

[a,b] Department of Computer Sciences, Sri Jayendra Saraswathy Maha Vidyalaya Collage of Arts& Science, Coimbatore, India

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 4 June 2021

Abstract: In the modern world, cloud computing is considered as the essential entity of diversified number of organization for assisting them towards the utilization of demand resources. In this context, cloud providers need to adhere to the privacy and security mechanisms in order to attain confident and secure exchange of user sensitive data in cloud environment. Thus, the data exchanged by the users in the cloud scenario need to be secured enough to resists the possible kinds of attacks that could be launched by the attackers. In this paper, Double Pseudonym-Based Privacy Preservation Scheme (DPBPPS) is proposed for securing sensitive data shared on the cloud. This DPBPPS includes a significant authentication scheme that inherited the benefits of the double pseudonym method for preventing the real identity of the cloud users by periodically updating the information (such as member secret, authentication key, internal pseudo-identity). This DPBPPS prevents the inclusion of bilinear pairing for yielding better performance in terms of computation overhead and communication overhead, and is more suitable to be applied independent to the number of users and sensitive data shared over the clouds.

Keywords: Cloud computing, Data mining, Security, authentication

1. Introduction

Security aspects in cloud computing is considered to be one of the important aspects of the cloud computing [1]. The scope of the security aspects projects of cloud computing is well examined by means of the describing about the Cloud Security Alliance (CSA) [2]. The CSA was created as a non-profit organization to promote the utility of best security practices in cloud computing environment. In the CSA domain it is possible to define the security related to application, cryptography and important aspects of management such as identity and access management [3]. Establishment of secured cloud environment necessitates the importance of implementing identity and access control management. The aspect of establishment of security and privacy in cloud computing is defined by means of Trusted Cloud Initiative (TCI). These cloud security alliance and initiatives also declares about the most common vulnerabilities in the cloud computing environment for which the mitigation process is considered to be most important [4]. The threats are listed as follows. i) Mistreatment and immoral Use of Cloud Computing, ii) Insecure Interfaces and Application Programming Interfaces (APIs), iii) Malicious Insiders, iv) Shared Technology Issues, v) Data Loss or Leakage, vi) Account or Service Hijacking, vii) Unknown Risk Profile [5]. Among these issues related to data leakage or loss and privacy related issues with respect to data is considered as the most significant things to be considered [6]. Since cloud provides services based on the establishment of the trust in the cloud computing environment, the privacy related problems are most significant problem.

Among the challenges in Cloud computing, security is considered to be one of the crucial factors to be made possible in this dynamic resource sharing and computing environment [7]. The security challenge is a crucial factor since computing approach is dynamic and data location is transparently maintained. Location transparency is one of the important elasticity for cloud computing, which is a security hazard at the same time without knowing the specific location of data storage, the stipulation of data protection act for a number of region might be severely affected and violated [18]. In cloud computing the users' personal data security is therefore a vital concern which needs high level of concentration. As far as the customer data or business data security is concerned the confinement of strategic policies plays a major role since technical security alone is not sufficient to handle the problem [19]. Trust establishment in cloud service is another problem which is also considered as most important concern in cloud. Trust establishment plays a major role which is directly related to the trustworthiness and legitimacy of the cloud service providers [20]. The booming success of cloud computing is that it lies in the establishment of trust. Hence the cloud computing environment requires the establishment of the trust model for the all stakeholders for any cloud computing environment. The factors like automation, management, processes and policies are the key factors to be considered for the establishment of the trust in the cloud computing environment. Establishment of the trust model in the cloud computing is not only the technical issue but it also considered as most important factor that are to be considered for the security issue in cloud computing. All the different types of vulnerabilities which are related to the computer network are also applicable for all types of cloud based services. Some of the threats for are man-in-the-middle attack, phishing, eavesdropping, sniffing and other similar attacks. Distributed Denial of Service (DDoS) attack is one common yet major attack for cloud computing infrastructure. The well-known DDoS attack can be a potential problem for cloud computing, though not with any exception of having no option to mitigate this.

In this paper, Double Pseudonym-Based Privacy Preservation Scheme (DPBPPS) is proposed for securing sensitive data shared on the cloud. This DPBPPS includes a significant authentication scheme that inherited the benefits of the double pseudonym method for preventing the real identity of the cloud users by periodically updating the information (such as member secret, authentication key, internal pseudo-identity). This DPBPPS prevents the inclusion of bilinear pairing for yielding better performance in terms of computation overhead and communication overhead, and is more suitable to be applied independent to the number of users and sensitive data shared over the clouds.

2. Related Work

A privacy scheme based on Verifiable Privacy-PreservingMulti-keyword Text Search (MTS) was proposed with ranking based on similarity [13]. The advantages are Multi-Dimensional (MD) algorithm provides improved search efficiency than linear search. Issues in security for two threat models are addressed i.e., known cipher-text model and known background model. Then, a privacy scheme based on searchable encryption construction, where anyone with public key can write to the data stored on server but only authorized users with private key can search [14]. Public key solutions are usually very computationally expensive however. Furthermore, the keyword privacy could not be protected in the public key setting since server could encrypt any keyword with public key and then use the received trapdoor to evaluate this cipher text. An LSA scheme which is used to reveal the relationship between terms and documents and they utilize k-Nearest Neighbour ($k - NN$) and returns the files containing the terms semantically related to the query keyword. It discussed batch attribute based encryption for multi cloud infrastructure. This concept leads to effective broadcast for the authentication and verification scheme. It was efficient to secure data to be shared to clouds. They utilized the information of the encrypted data and multiple parties computing in order to present an approach for identity management system without centralized agent.

Further, a hierarchy based encryption scheme in which encryption is based on the attributes of the data [15]. This scheme provides fine access control for the cloud infrastructure. They also recommended a weighted parameter based encryption scheme with cipher policy in order prevent the privacy and integrity in the data transformation. It included Pseudo random function families are a powerful cryptographic primitive, yielding, in particular, simple solutions for the main problems in private key cryptography. Their existence based on general assumptions (namely, the existence of one-way functions) has been established. A secure conjunctive keyword search schemes but incur significantly less storage overhead. It presented the algorithms of the corresponding OPE scheme can be obtained to eliminate state by using a length-flexible PRF as described in this paper. The security statement is the same as that of Theorem where the last term now corresponds to the error probability of the NHG algorithm.

An optimal fault-tolerance strategy was proposed for securing the significant cloud components [16]. The simulation results show that by tolerating faults of a small part of the most significant components, the reliability of cloud applications needs to be improved. It presented two protocols to protect the data leakage. The server learns the keyword fields that the capability enables the server to search. This alone may be enough to allow the server to infer unintended information about the documents. It would be interesting to explore solutions for the secure search problem that also protect keyword fields. Then, a have developed novel framework called as Big Cloud which provides faster retrieval of the data [17]. The security issues in the bank are solved based on the cloud space and load balancing of multiple queries among the various servers by applying existing encryption algorithms. It is time consuming approach. A ranking method to preserve the privacy of the keyword is proposed with the efficiency of the keyword search needs to be improved [18]. It also developed as an efficient ranked keyword search to achieve effective utilization of remotely stored encrypted data. But the proposed systems appropriately weaken the security guarantee. It explored a new approach to group key agreement and resultant protocol suite is very simple but more overhead due to more tree structure. It described theIdentity based and Attribute-based Encryption which will provide more security to user. It is required to check the integrity before upload the data in cloud. It is also related to the query keyword for fast index tree generation. The efficiency of the keyword search has to improve more for the dynamic cloud user.

3. Proposed Double Pseudonym-Based Privacy Preservation Scheme (DPBPPS)

This proposed Double Pseudonym-Based Privacy Preservation Scheme (DPBPPS) is proposed for sustaining privacy strength for securing sensitive data shared on the cloud. The system model diagram used for the implementation of the proposed DPBPPS scheme is portrayed in Figure 1.

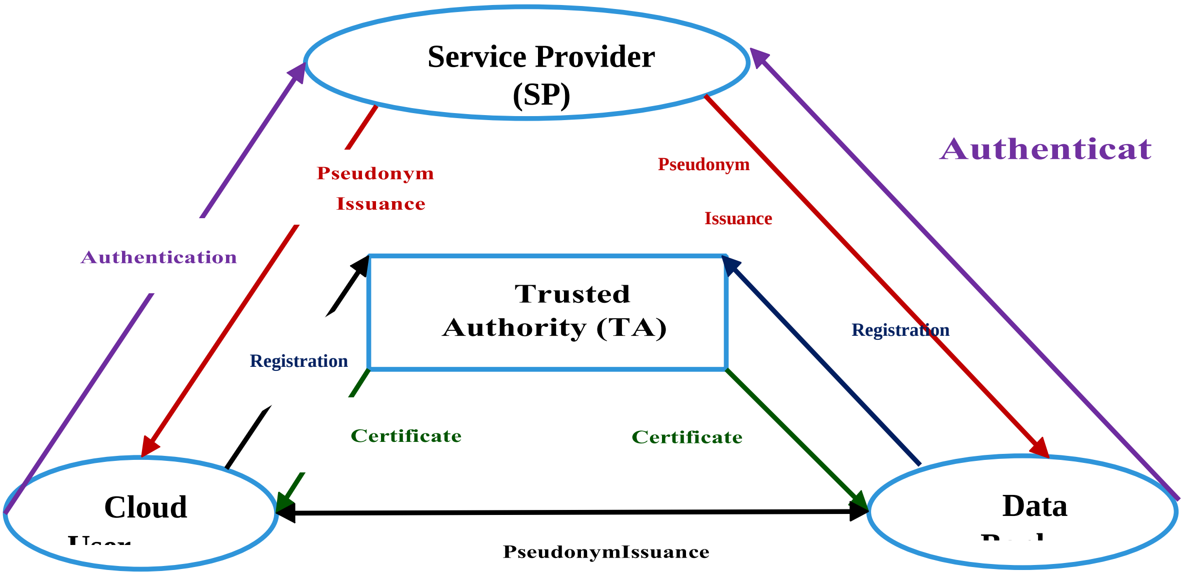

Figure 1: System model used for implementation of the proposed DPBPPS

This proposed DPBPPS utilized the dual pseudonym method for improving the strength of the location privacy since the need for bilinear pairing [19] in the process of generation and verification of the single and batched signature [20].

3.1 Adversary Model used in the implemented DPBPPS scheme

The open and error-prone nature of cloud architecture introduces the option of vulnerabilities into the network such as a) eavesdropping, b) interception and c) modification in messages exchanged. The core objective of this proposed DPBPPS mechanism is to provide security against the threats to anonymity and threats to the generation of the incentive certificates.

Initial System Setup Phase

In this initial system setup phase, a list of predefined factors that are essential for the implementation of the proposed DPBPPS approach which is initialized by the trusted authority are incorporated into the SERVICE PROVIDERs and users is established through the following phases. This phase of initializing the predefined factors, by the trusted authority is facilitated until the attacker compromises the private key of the system. In specific, this process of initializing the parameters of the system needs to be periodically updated for improving the security degree of the system. In this step, initially the TA chooses two different prime numbers ‘$_a$’ and ‘$_b$’ with a non-singular elliptic curve ‘$_E$’ as defined by $_z{}^2 = ({}_y{}^3 + {}_{py} + {}_q)_{modm}$with $_{p,q} \in G_a$. Further, a Group ‘$_G$’ that satisfies the property of cyclic addition is selected by the TA with ‘$_a$’ and ‘$_b$’ considered as the generator and order of the group. Furthermore, a random number is considered as the secret key $S_{KEY} \in R_b{}^*$by the TA for calculating $P_{KEY} = a * S_{KEY}$ as the determined public key. In addition, an encryption key$_{Ep}(.)$, a decryption key $_{Dp}(.)$ and hash functions h_{f1}, h_{f2}, $H_{f1(key)}(\bullet)$, $H_{f2}(\bullet)$ and $H_{f3}(\bullet)$ are selected by the TA with $H_{f1(key)}(\bullet)$ representing the hash key function. In this context, $h_{f1} : G \rightarrow R_b$, $h_{f2} : \{0,1\} \rightarrow R_b$, $H_{f1(key)}(\bullet) : \{0,1\}^* \rightarrow \{0,1\}^h$, $H_{f2}(\bullet) : \{0,1\}^* \rightarrow \beta$ and $H_{f3}(\bullet) : \{0,1\}^* \rightarrow \{0,1\}^{h1}$ are defined. Finally, the system parameters designated as $\alpha = \{a,b,p,q,E_p(\bullet),D_p(\bullet),h_{f1},h_{f2},H_{f1(key)}(\bullet),H_{f2}(\bullet),H_{f3}(\bullet)\}$ are incorporated into the service providers and users in the network.

Setup phase of Service Provider

In this setup phase, the service provider is responsible for generating its own Fuzzy Trust-basedCertificate ($_{FTcert(i)}$) derived from TA with its public and private key pairs. In specific, this generation of fuzzy trust-based certificate is useful only for a short period of time. This process needs to be iterated for periodic intervals of time in order to enhance the security. Then, service provider selects two numbers $_{c_i,d_i \in R_b}{}^*$randomly for determining$KP_{O(i1)} = c_i * S_{KEY}$ and $KP_{O(i2)} = d_i * S_{KEY}$, in order to generate its own public and private key pairs. Thus, the pairs (c_i,d_i) and $(KP_{O(i1)},KP_{O(i2)})$ are the private and public keys with $_{ci}$ and $_{di}$ used for establishing users sharing and maintaining the channel between the users and the service providers. Once this generation of public and private key pairs is completed, the public key $({}_{KPO(i1)},KP_{O(i2)})$ with its own identity is forwarded to the TA through the established secure channel. In this juncture, the service provider broadcasts the Fuzzy Trust-based

Certificate (${}_{FTcert(i)}$) to the users of their own range of communication, when the TA receives the public and private key pairs and generates the service provider certification.

Setup phase of Users

In this phase, the information stored in the Tamper Resistant Equipment (TRE) needs to be initialized whenever the users enter into the region of communication with the service providers and other users. Then TA determines an Inter-Pseudonym Identity (IPI) $IPI_{V\ (i)} = H_N(ID_{(R)}||V\ T_{P(i)})$ with $V\ T_{P(i)}$ as the valid time period. Further, an authentication key ${}_{\eta i}$is selected by the users and stores $({}_{\alpha,\eta i},IPI_{V\ (i)})$ into theTRE. Finally, the set $(ID_{(R)},V\ T_{P(i)},\eta_i,IPI_{V\ (i)})$ is stored and updated in the Potent Membership List (PML) of the TA.

Generation Phase of Member Key

In this Generation Phase of Member Key, the users in the network determine the member secrets and its related timestamp from the closest proximity service provider. This processes of member key generation phase needs confidentiality among the TA, service provider, and users. As mentioned earlier, the users receive the Fuzzy Trust-based Certificate (${}_{FTcert(i)}$) from the service provider whenever the users enter into the service providers communication range. Further, the users are keen on identifying the secrets of the member entities participating in the cloud with the active valid timestamp in which the service provider will be active. Thus, the steps included in the Generation Phase of Member Key are discussed below.

Step 1: The users receive the Fuzzy Trust-based Certificate (${}_{FTcert(i)}$) from the interacting service provider whenever they enter into the range of communication. The receivedFuzzy Trust-based Certificate ($FT_{cert(i)}$) of the form $(ID_{(R)},KP_{O(i1)},KP_{O(i2)},Sig_{O(i)})$ is validated with ${}_{SigO(i)}$corresponding to the signature applied over the TA issued $(ID_{(R)},KP_{O(i1)},KP_{O(i2)})$ parameters. If the validation of the certificate is identified as valid according to the public key system, then extract the identity and public key of service provider from the Fuzzy Trust-based Certificate (${}_{FTcert(i)}$).

Step 2: Then, a random number$r_a \in R_b{}^*$is selected for computing $f_1 = r_a * S_{KEY}$, $\gamma_{(i1)}$ =(f1,KPO(i2),ra∗KPO(i2),ID(R),TP) and γ(i2) = (f1,KPO(i1),ra∗KPO(i1),ID(R),TP). Where ${}_{\gamma(i1)}$, ${}_{\gamma(i2)}$and ${}_{TP}$ refers to the symmetric encryption keys and Time Period of the system corresponding to encryption and decryption ${}_{Ep}(.)$and ${}_{Dp}(.)$ functions respectively. In addition, $({}_{qj}= {}_{E\gamma(i2)}({}_{\eta i},T_P)$ is computed by the user and ${}_a = (f_1,ID_{(R)},q_j,T_P)$ is transmitted to service provider.

Step 3: Service Provider sends '${}_a$' to the TA after being received from the users, if it is determined to be valid. If the value of '${}_a$' is invalid, then the process gets aborted. Then, TA computes $\gamma_{(i2)} = H_{f2}(f_1,KP_{O(i1)},af_1,ID_{(R)},T_P)$ and $D_{\gamma(i2)}(q_j)$ after receiving 'a' from SERVICE PROVIDER in order to determine $({}_{\eta j}{}^1{}_{,TP}{}^1)$. If the constraint ${}_{\eta j}$, $\eta_j{}^1$ is absent in the member list of the TA $(ID_{(R)},V\ T_{P(i)},\eta_i,IPI_{V\ (i)})$ and the condition T_P , $T_P{}^1$ is invalid, then the process is aborted. Otherwise, TA sends the authentication message to the users and service provider which has sent the value of 'a' during member key generation phase. In this context, the user is legitimate, since it has received the service provider the authentication message from TA.

Signature generation phase of the Users

In this user signature generation phase, the users generate the explicit pseudonym identity and a digital signature of the messages when it receives the secret of the membership (${}_{\lambda i,\beta i}$) from the service provider with the value of membership time is well within the value of the authorized period. Then, the users broadcast the generated explicit pseudonym identity and digital signature of the messages to other cooperating (determined through Fuzzy Trust Value) users and service providers. The detailed steps incorporated into the users signature generation phase are described below.

Step 1: The users estimate the explicit pseudonym identity $P_{iden(i)} = H_{f3}(V\ T_{P(i)},T_P)$ and one-time signature key OTKEY (Sig(i) = (λi,βi)∗hf1(Piden(i)) mod m .

Step 2: A random number ${}_{ra}\in{}_{Rb}{}^*$is selected by the users in order to compute RK(i) =rb∗SKEY and λi =hf2(Piden(i)||RK(i)||MK(i)) and SK(i) =sk(i)+λi∗rb. Further, the users forward the tuples $(M_{K(i)},P_{iden(i)},R_{K(i)},S_{K(i)})$ to the nearby service providers and users.

Step 3: The secret related to the membership (${}_{\lambda i,\beta i}$) stored in the TRE should be periodically updated. In addition, select ${}_{\lambda i}$= ${}_{a\lambda i}$and ${}_{\beta i}$= ${}_{a\beta i}$ as the current member secret value.

Message Verification Phase of the users generated signature

In this phase, the validity of the disseminated message is facilitated without the utilization of bilinear pairing in order to phenomenally reduce the overhead in computation. This phase of the proposed DPBPPS technique also possesses the potential of validating single and batch messages. In the case of single message validation, TA verifies the validity of the tuples $(M_{K(i)},P_{iden(i)},R_{K(i)},S_{K(i)})$ received from the users-based on the values of the system parameter ‘$_{\alpha}$’. The verifier TA checks whether $SK(i)*SKEY\ (i) = hf1((Piden(i)*KPO(i1))+\lambda i*PK(i))$ is satisfied and receives the validated message with the timestamp. In case of the batched message verification process, the proposed DPBPPS technique uses the method of small index test for investigating the vector which consists of randomly selected small integers for facilitating modification detection in the stored signature.

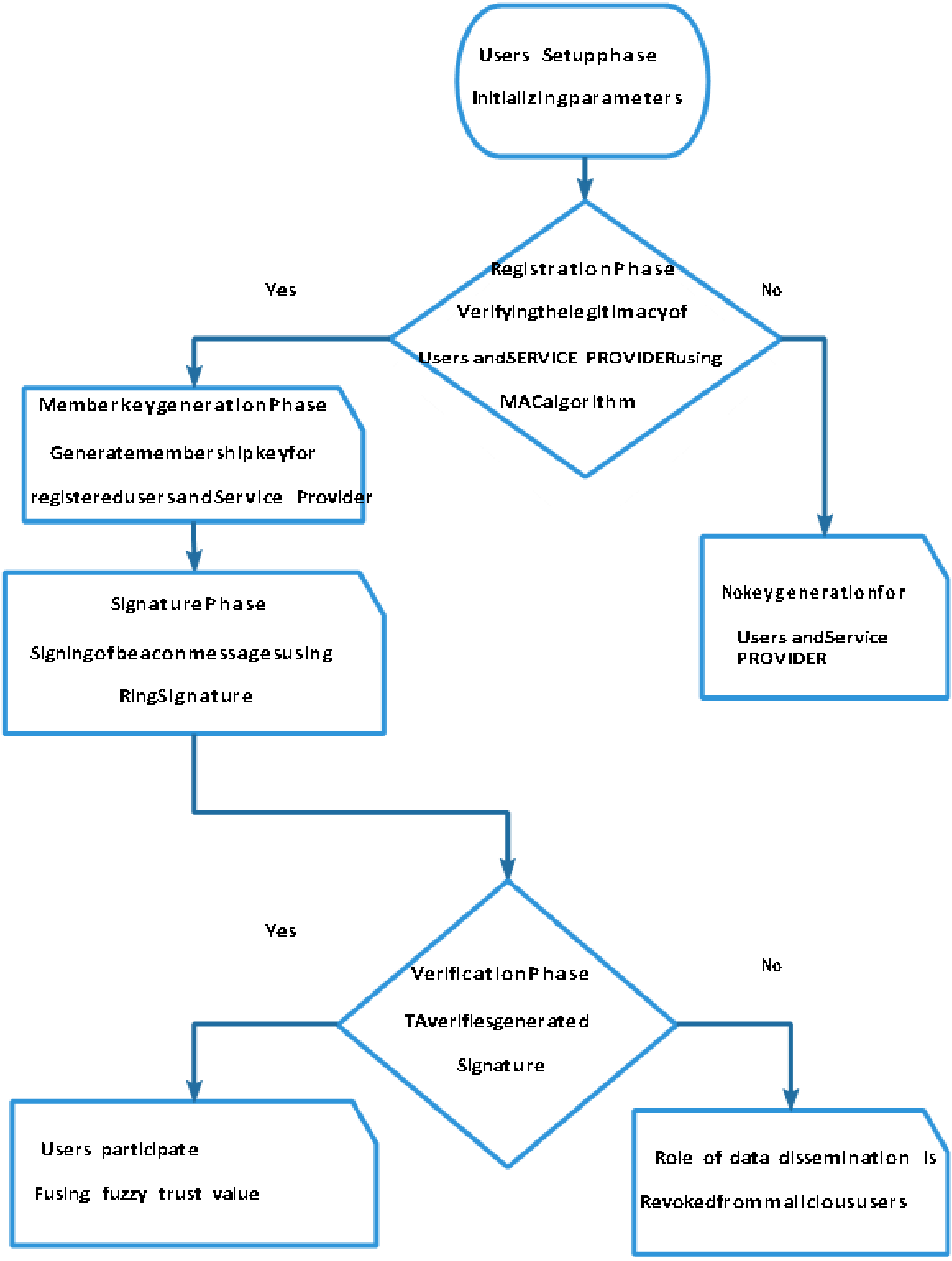

Figure 2: Flowchart of the proposed DPBPPS mechanism

Algorithm of the proposed DPBPPS scheme

Step 1: Initial System Setup Phase

Step 1.1: Initially the TA chooses two different prime numbers ‘a’ and ‘b’ with a non-singular elliptic curve ‘E’ as defined by $Z^2 = (y^3+py+q)\mathrm{modm}$ with $p,q \in G_a$.

Step1.2: Further, a Group ‘G’ that satisfies the property of cyclic addition is selected by the TA with ‘a’ and ‘b’ considered as the generator and order of the group.

Step1.3: A random number is considered as the secret key $S_{KEY} \in R_b{}^*$by the TA for calculating $P_{KEY} = a*S_{KEY}$ as the determined public key.

Step1.4: An encryption key$E_p(\bullet)$, a decryption key and hash functions h_{f1}, h_{f2}, , $H_{f2}(\bullet)$ and $H_{f3}(\bullet)$ is selected by the TA with $H_{f1(key)}(\bullet)$ representing the hash key function. In this context, $h_{f1}: G \rightarrow R_b$, $h_{f2}: \{0,1\} \rightarrow R_b$, $H_{f1(key)}(\bullet): \{0,1\}^* \rightarrow \{0,1\}^h$, $H_{f2}(\bullet) : \{0,1\}^* \rightarrow \beta$and $H_{f3}(\bullet) : \{0,1\}^* \rightarrow \{0,1\}^{h1}$are defined.

Step1.5: Thesystem parameters designated as$\alpha = {}^n a,b,p,q,E_p(.),D_p(.),h_{f1},h_{f2},h_{f1key}(.),H_{f2}(.),H_{f3}(.)^o$ is incorporated into the service providers and users in the network.

Step 2: Setup phase of service provider

Step2.1: Service Provider selects two numbers $c_i,d_i \in R_b{}^*$randomly for determining $KP_{O(i1)} = c_i * S_{KEY}$ and $KP_{O(i2)} = d_i * S_{KEY}$ in order to generate its own public and private key pairs. The pairs (c_i,d_i) and ($KP_{O(i1)},KP_{O(i2)}$) is the private and public key with $c_i$and d_i used for establishing users sharing and maintaining the channel between the users and the service providers.

Step2.2: The public key ($KP_{O(i1)},KP_{O(i2)}$) with its own identity is forwarded to the TA through the established secure channel.

Step2.3: The service provider broadcasts the Fuzzy Trust-based Certificate ($FT_{cert(i)}$) to the users of their own range of communication when the TA receives the public and private keypairs and generates the service provider certification.

Step 3: Setup phase of Users

Step3.1: The information stored in the Tamper Resistant Equipment (TRE) needs to be initialized whenever the users enter into the region of communication with the service providers and other users.

Step3.2: TA determines an Inter-Pseudonym Identity (IPI) $IPI_{v(i)} = H_N(ID_R \| V\ T_{p(i)})$ with $V\ T_{P(i)}$ as the valid time period.

Step3.3: An authentication key $\eta_i$is selected by the users and stores $(\alpha,\eta_i,IPI_{V\ (i)})$ into the TRE.

Step 3.4: The set $(ID_{(R)},V\ T_{P(i)},\eta_i,IPI_{V\ (i)})$ is stored and updated in the Potent Membership List (PML) of the TA.

Step 4: Generation Phase of Member Key

Step 4.1: The users receive the Fuzzy Trust-based Certificate ($FT_{cert(i)}$) from the interacting SERVICE PROVIDER whenever they enter into the range of communication. The received Fuzzy Trust-based Certificate (FTcert(i)) of the form (ID(R),KPO(i1),KPO(i2),SigO(i)) is validated with $Sig_{O(i)}$ corresponding to the signature applied over the TA issued $(ID_{(R)},KP_{O(i1)},KP_{O(i2)})$ parameters. If the validation of the certificate is identified as valid according to the public key system, then extract the identity and public key of Service Provider from the Fuzzy Trust-based Certificate ($FT_{cert(i)}$).

Step 4.2: Then, a random number$r_a \in R_b{}^*$is selected for computing $f_1 = r_a * S_{KEY}$, and γ(i2) = (f1,KPO(i1),ra∗KPO(i1),ID(R),TP). Where γ(i1), γ(i2) and TP refers to the symmetric encryption keys and Time Period of the system corresponding to encryption and decryption $E_p(\bullet)$and $D_p(\bullet)$ functions respectively. In addition, ($q_j = E_{\gamma(i2)}(\eta_i,T_P)$ is computed by the users and $a = (f_1,ID_{(R)},q_j,T_P)$ is transmitted to Service Provider.

Step 4.3: Service Provider sends ‘a’ to the TA after being received from the userss if it is determined to be valid. If the value of ‘a’ is invalid, then the process gets aborted. Then, TA computes $\gamma_{(i2)} = H_{f2}(f_1,KP_{O(i1)},af_1,ID_{(R)},T_P)$ and $D_{\gamma(i2)}(q_j)$ after receiving ‘a’ from Service Provider in order to determine $(\eta_j{}^1,T_P{}^1)$. If the constraint η_j, $\eta_j{}^1$ is absent in the member list of the TA $(ID_{(R)},V\ T_{P(i)},\eta_i,IPI_{V\ (i)})$ and the condition T_P , $T_P{}^1$ is invalid, then the process is aborted. Otherwise, TA sends the authentication message to the users and service provider which has sent the value of ‘a’ during member key generation phase. in this context, the users are legitimate since it has received the service provider the authentication message from TA.

Step 5: Signature generation phase of the Users

Step 5.1: The users estimate the explicit pseudonym identity $P_{iden(i)}$ =H_{f3}(V $T_{P(i)}$,T_P) and one-time signature key OTKEY (Sig(i) = (λi,βi)∗hf1(Piden(i)) mod m .

Step 5.2: A random number r_a∈$R_b^*$is selected by the users in order to compute RK(i) = rb∗SKEY and λi = hf2(Piden(i)||RK(i)||MK(i)) and Sk(i) +λi∗rb. Further, the users forward the tuples (MK(i),Piden(i),RK(i),SK(i)) to the nearby service providers and users.

Step 5.3: The secret related to the membership (λ_i,β_i) stored in the TRE should be periodically updated. In addition, select λ_i= a$\lambda_i$and β_i= aβ_i as the current membersecret value.

Step 6: Message Verification Phase of the users generated signature

Step6.1: TA verifies the validity of the tuples (Mk(i),Piden(i),Rk(i),Sk(i)) received from the users based on the values of the system parameter ‘α’.

Step6.2: The verifier TA checks whether Sk(i)∗SKEY (i) = hf1((Piden(i)∗KPo(i1))+λi∗$P_{k(i)}$) is satisfied and receives the validated message with the timestamp T_P.

4. Simulation Results and Discussion

The potential of the proposed DPBPPS scheme is explored using Cloudsim based on communication overhead, computation overhead, privacy preservation degree and time incurred in security key generation under different number of users and key lengths utilized during privacy preservation.

In the first part of analysis, Figure 2 and 3 presents the communication overhead and computation overhead of the proposed DPBPPS scheme evaluated with different number of users. The proposed DPBPPS schemewas identified to betterthan the benchmarked FGTFAC, PPDFAC and FAACAS approaches independent to the number of users in the cloud environment, since the verification methodology included in the proposed privacy preservation scheme reduced the complexity of computation to be imposed over the keys. The percentage increase in Privacy Preservation Degree achieved by the proposed DPBPPS scheme with different users is confirmed to be improved by 5.12%, 6.83% and 7.64%, compared to the benchmarked FGTFAC, PPDFAC and FAACAS approaches. The percentage decrease in time for security key generation attained by the proposed DPBPPS scheme is proved enhanced by 4.98%, 5.68% and 6.84%, compared to the benchmarked FGTFAC, PPDFAC and FAACAS approaches.

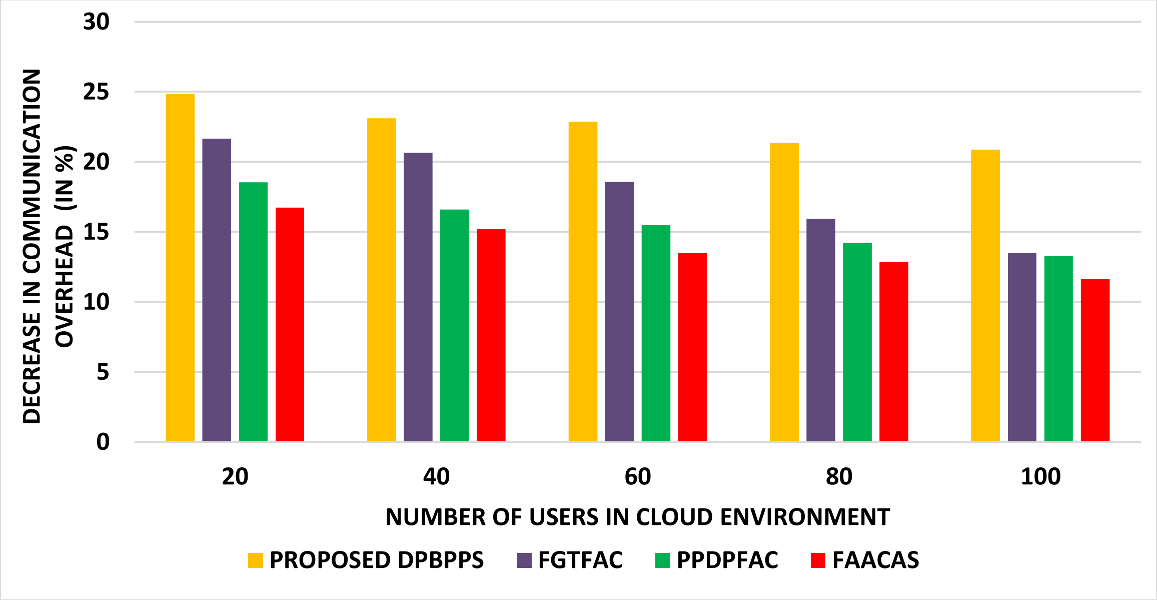

Figure 2: Proposed DPBPPS-Communication overhead with number of users

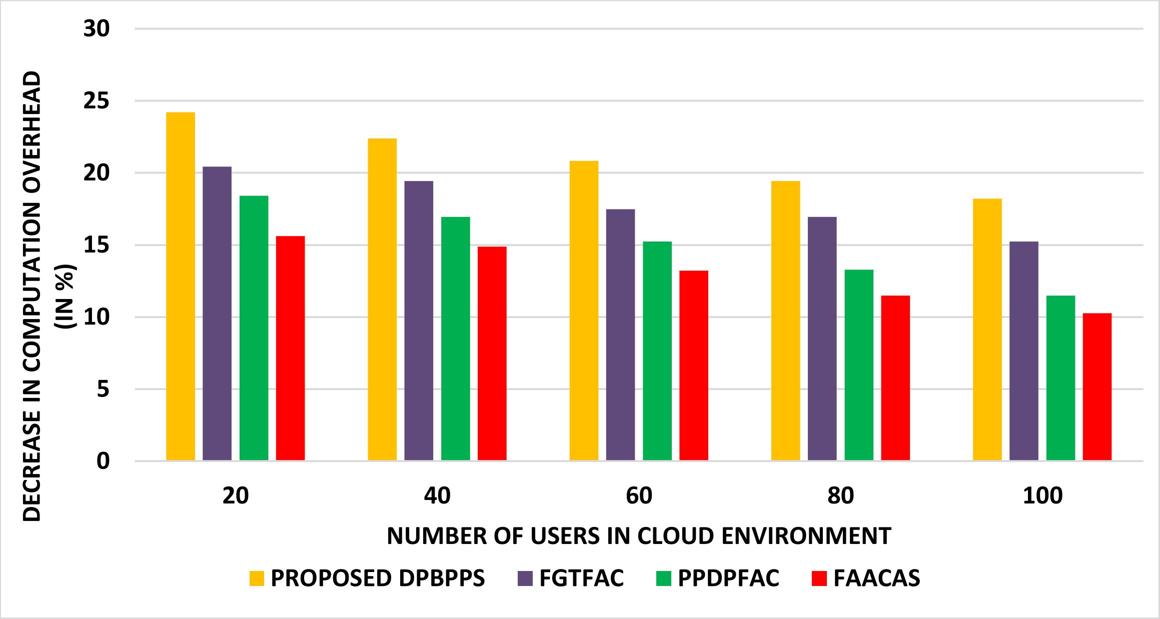

Figure 3: Proposed DPBPPS-Computation overhead with number of users

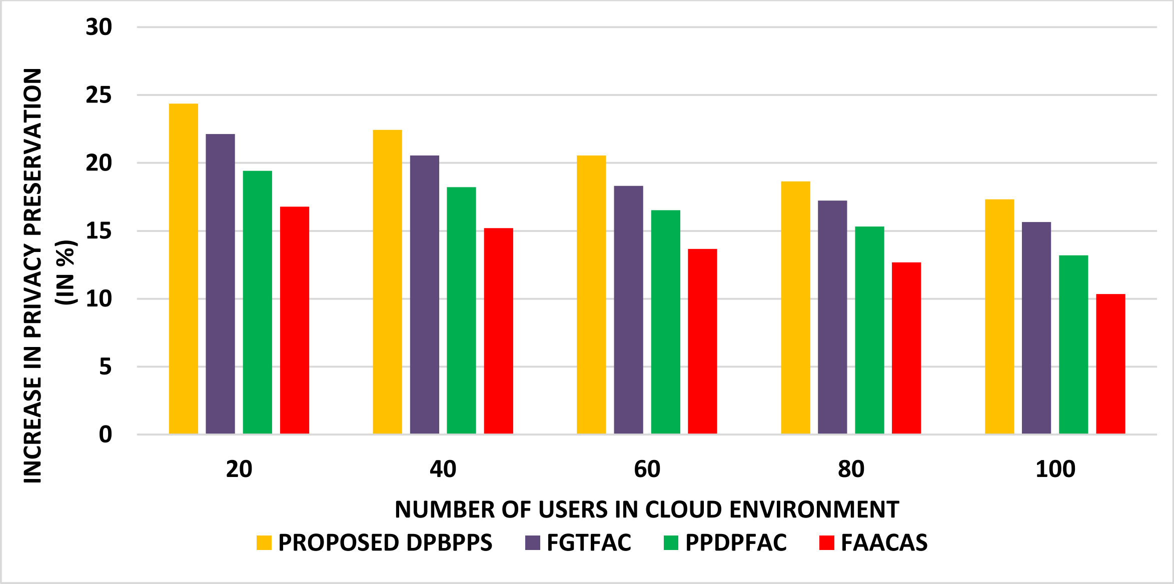

Figure 4: Proposed DPBPPS-Privacy Preservation Degreewith number of users

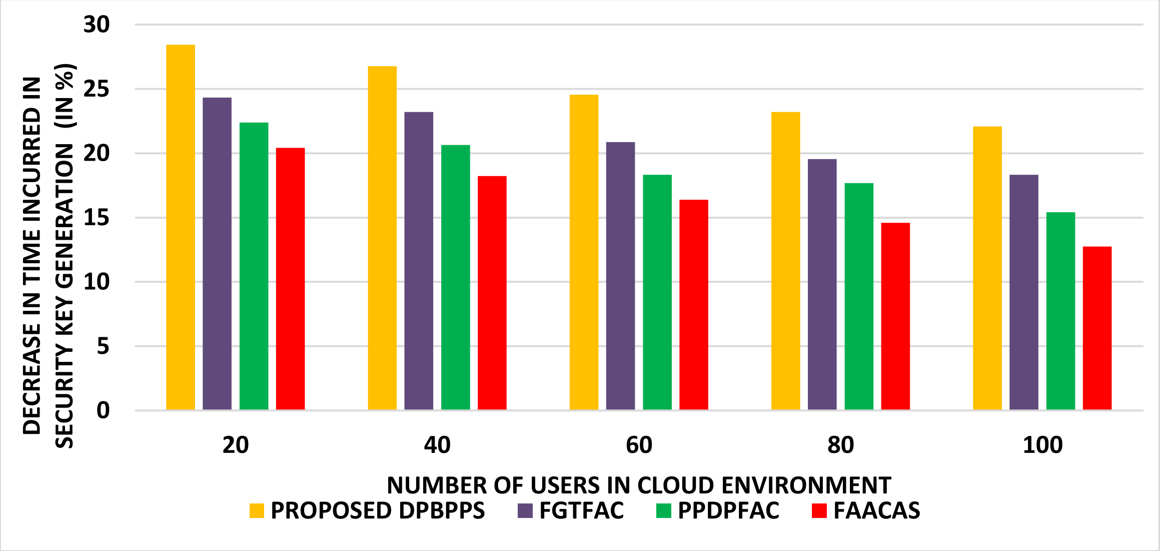

Figure 5: Proposed DPBPPS- Time for security key generation with number of users

Figure 4 and 5 demonstrates the percentage increase in Privacy Preservation Degree and percentage decrease in time for security key generation achieved by the proposed DPBPPS with different number of users in the cloud scenario. The proposed DPBPPS schemewas identified to betterthan the benchmarked FGTFAC, PPDFAC and FAACAS approaches independent to the number of users in the cloud environment, since the verification methodology included in the proposed privacy preservation scheme reduced the complexity of computation to be imposed over the keys. The percentage increase in Privacy Preservation Degree achieved by the proposed DPBPPS scheme with different users is confirmed to be improved by 5.12%, 6.83% and 7.64%, compared to the benchmarked FGTFAC, PPDFAC and FAACAS approaches. The percentage decrease in time for security key generation attained by the proposed DPBPPS scheme is proved enhanced by 4.98%, 5.68% and 6.84%, compared to the benchmarked FGTFAC, PPDFAC and FAACAS approaches.

In the second part of analysis, Figure 6 and 7 depicts the communication overhead and computation overhead of the proposed DPBPPS scheme evaluated with different key lengths. The proposed DPBPPS schemewas identified to betterthan the benchmarked FGTFAC, PPDFAC and FAACAS approaches independent to the size of keys utilized for privacy preservation in the cloud, since it is a lightweight approach with reduced complexity and time in key generation and verification of the keys. The percentage increase in Privacy Preservation Degree achieved by the proposed DPBPPS scheme with different key sizes is confirmed to be improved by 5.04%, 6.94% and 7.92%, compared to the benchmarked FGTFAC, PPDFAC and FAACAS approaches. The percentage decrease in time for security key generation attained by the proposed DPBPPS scheme with different key sizes is confirmed to be enhanced by 5.92%, 6, 82% and 8.46%, compared to the benchmarked FGTFAC, PPDFAC and FAACAS approaches.

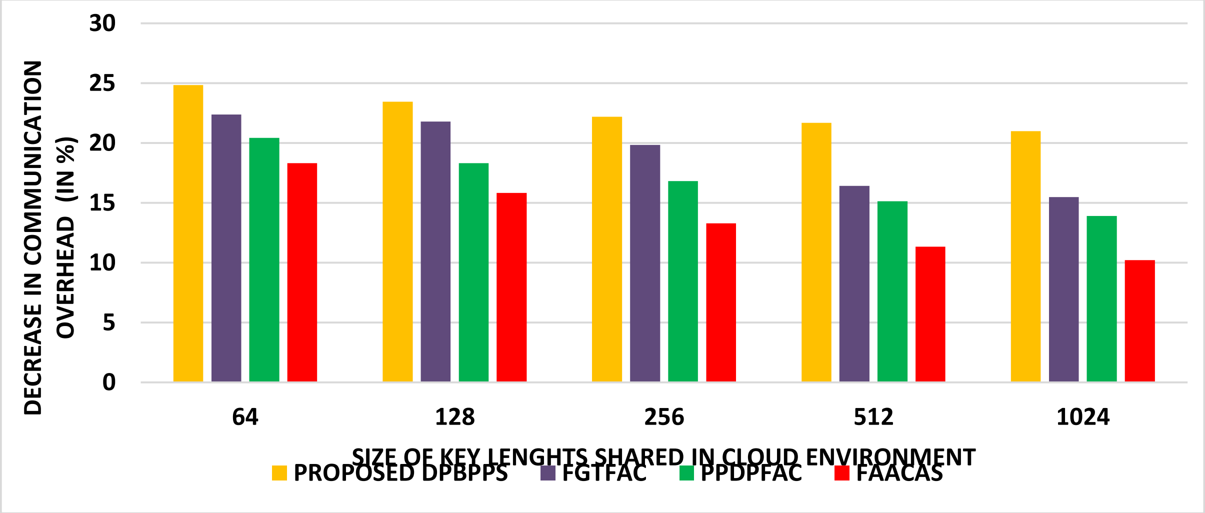

Figure 6: Proposed DPBPPS-Communication Overhead withdifferent key lengths

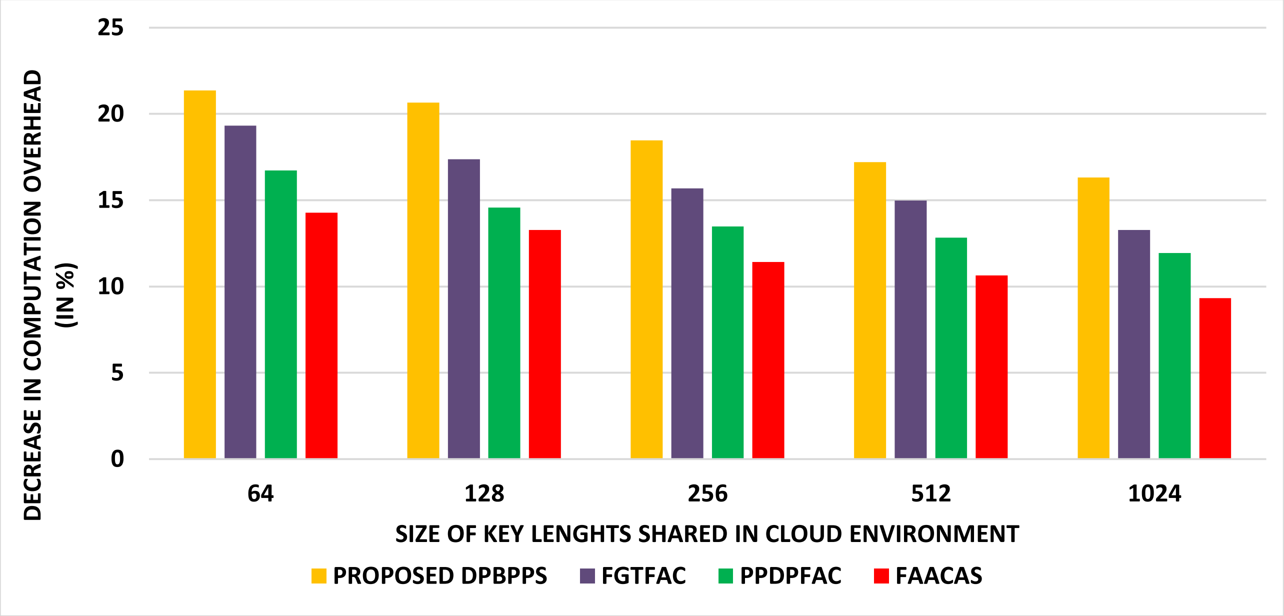

Figure 7: Proposed DPBPPS-Computation Overhead with different key lengths

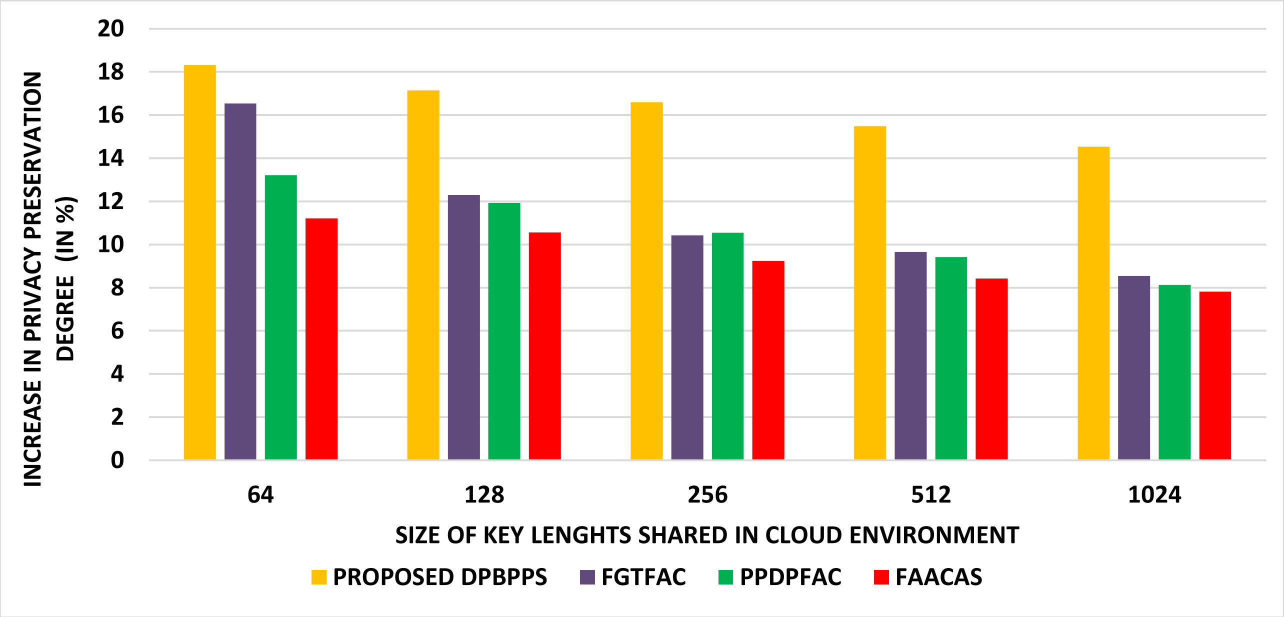

Figure 8: Proposed DPBPPS- Privacy Preservation Degree with different key lengths

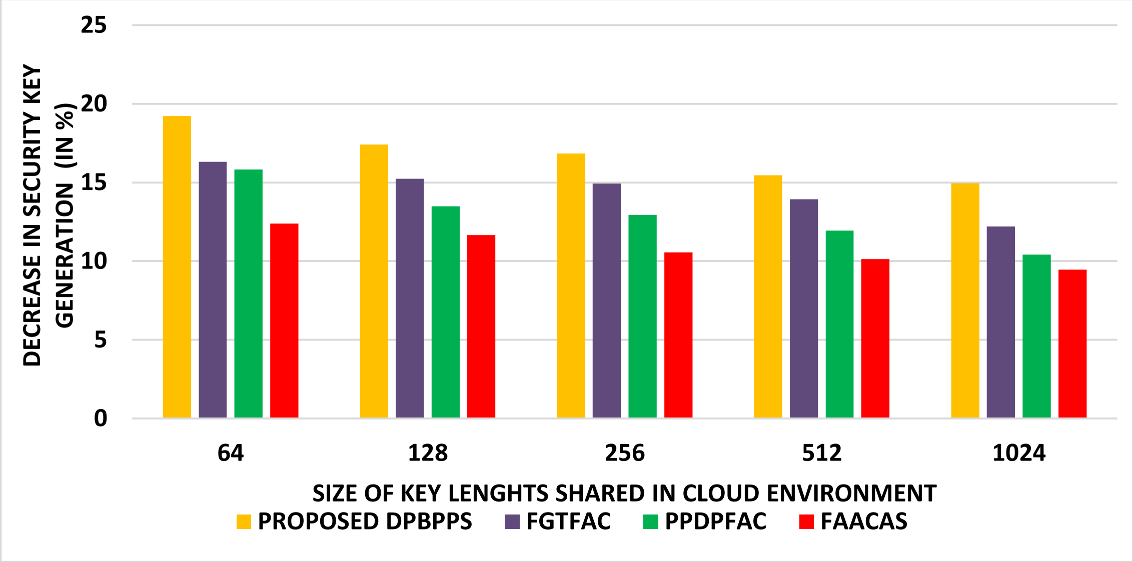

Figure 9: Proposed DPBPPS- Time for security key generation with different key lengths

In addition, Figure 8 and 9 presents the percentage increase in Privacy Preservation Degree and percentage decrease in time for security key generation achieved by the proposed DPBPPS with different key lengths. The proposed DPBPPS scheme was identified to better than the benchmarked FGTFAC, PPDFAC and FAACAS approaches independent to the size of keys shared in the cloud environment, since the use of double pseudonym played a significant role in reducing the time in generating keys and increasing the degree of privacy preservation. The percentage increase in Privacy Preservation Degree achieved by the proposed DPBPPS scheme with different key sizes is confirmed to be improved by 4.21%, 5.98% and 7.42%, compared to the benchmarked FGTFAC, PPDFAC and FAACAS approaches. The percentage decrease in time for security key generation attained by the proposed DPBPPS scheme is proved to be enhanced by 5.68%, 6.89% and 7.64%, compared to the benchmarked FGTFAC, PPDFAC and FAACAS approaches.

5.Conclusion

In this paper, DPBPPS was proposed for securing sensitive data shared on the cloud. This DPBPPS includes a significant authentication scheme that inherited the benefits of the double pseudonym method for preventing the real identity of the cloud users by periodically updating the information (such as member secret, authentication key, internal pseudo-identity). This DPBPPS prevents the inclusion of bilinear pairing for yielding better performance in terms of computation overhead and communication overhead, and is more suitable to be applied independent to the number of users and sensitive data shared over the clouds.The experimental results confirmed that the percentage increase in Privacy Preservation Degree achieved by the proposed DPBPPS scheme with different users is confirmed to be improved by 5.12%, 6.83% and 7.64%, compared to the benchmarked FGTFAC, PPDFAC and FAACAS approaches. The percentage decrease in time for security key generation attained by the proposed DPBPPS scheme is proved enhanced by 4.98%, 5.68% and 6.84%, compared to the benchmarked FGTFAC, PPDFAC and FAACAS approaches. The results confirmed that the percentage decrease in time for security key generation attained by the proposed DPBPPS scheme with different key sizes is proved to be enhanced by 5.68%, 6.89% and 7.64%, compared to the benchmarked FGTFAC, PPDFAC and FAACAS approaches. The percentage increase in Privacy Preservation Degree achieved by the proposed DPBPPS scheme with different key sizes is confirmed to be improved by 4.21%, 5.98% and 7.42%, compared to the baseline approaches.

References

1. X. Zhang, C. Liu, S. Nepal, S. Pandey and J. Chen, "A Privacy Leakage Upper Bound Constraint-Based Approach for Cost-Effective Privacy Preserving of Intermediate Data Sets in Cloud," in IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1192-1202, June 2013.
2. Z. Liu, L. Wu, J. Ke, W. Qu, W. Wang and H. Wang, "Accountable Outsourcing Location-Based Services With Privacy Preservation," in IEEE Access, vol. 7, pp. 117258-117273, 2019.
3. H. Liu, H. Ning, Q. Xiong and L. T. Yang, "Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing," in IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 1, pp. 241-251, Jan. 2015.

4. L. Liu, R. Chen, X. Liu, J. Su and L. Qiao, "Towards Practical Privacy-Preserving Decision Tree Training and Evaluation in the Cloud," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2914-2929, 2020,
5. X. Liu, Y. Zhang, B. Wang and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," in IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, June 2013.
6. X. Zhang, L. T. Yang, C. Liu and J. Chen, "A Scalable Two-Phase Top-Down Specialization Approach for Data Anonymization Using MapReduce on Cloud," in IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp. 363-373, Feb. 2014.
7. J. Li, D. Lin, A. C. Squicciarini, J. Li and C. Jia, "Towards Privacy-Preserving Storage and Retrieval in Multiple Clouds," in IEEE Transactions on Cloud Computing, vol. 5, no. 3, pp. 499-509, 1 July-Sept. 2017.
8. X. Wang, J. He, P. Cheng and J. Chen, "Privacy Preserving Collaborative Computing: Heterogeneous Privacy Guarantee and Efficient Incentive Mechanism," in IEEE Transactions on Signal Processing, vol. 67, no. 1, pp. 221-233, 1 Jan.1, 2019.
9. X. Ye, "Privacy preserving and delegated access control for cloud applications," in Tsinghua Science and Technology, vol. 21, no. 1, pp. 40-54, Feb. 2016.
10. K. Zhang, X. Liang, J. Ni, K. Yang and X. Shen, "Exploiting Social Network to Enhance Human-to-Human Infection Analysis without Privacy Leakage," in IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 4, pp. 607-620, 1 July-Aug. 2018,
11. S. Hu, Q. Wang, J. Wang, Z. Qin and K. Ren, "Securing SIFT: Privacy-Preserving Outsourcing Computation of Feature Extractions Over Encrypted Image Data," in IEEE Transactions on Image Processing, vol. 25, no. 7, pp. 3411-3425, July 2016.
12. W. Guo, J. Shao, R. Lu, Y. Liu and A. A. Ghorbani, "A Privacy-Preserving Online Medical Prediagnosis Scheme for Cloud Environment," in IEEE Access, vol. 6, pp. 48946-48957, 2018.
13. H. Zhu, R. Lu, C. Huang, L. Chen and H. Li, "An Efficient Privacy-Preserving Location-Based Services Query Scheme in Outsourced Cloud," in IEEE Transactions on Vehicular Technology, vol. 65, no. 9, pp. 7729-7739, Sept. 2016.
14. O. Kwabena, Z. Qin, T. Zhuang and Z. Qin, "MSCryptoNet: Multi-Scheme Privacy-Preserving Deep Learning in Cloud Computing," in IEEE Access, vol. 7, pp. 29344-29354, 2019.
15. W. Ding, Z. Yan and R. H. Deng, "Privacy-Preserving Data Processing with Flexible Access Control," in IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 2, pp. 363-376, 1 March-April 2020.
16. J. Hao, J. Liu, H. Wang, L. Liu, M. Xian and X. Shen, "Efficient Attribute-Based Access Control With Authorized Search in Cloud Storage," in IEEE Access, vol. 7, pp. 182772-182783, 2019.
17. H. Xu, S. Guo and K. Chen, "Building Confidential and Efficient Query Services in the Cloud with RASP Data Perturbation," in IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 2, pp. 322-335, Feb. 2014.
18. J. K. Liu, M. H. Au, X. Huang, R. Lu and J. Li, "Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 3, pp. 484-497, March 2016.
19. X. Ding, P. Liu and H. Jin, "Privacy-Preserving Multi-Keyword Top-k k Similarity Search Over Encrypted Data," in IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 2, pp. 344-357, 1 March-April 2019.
20. S. Tahir, S. Ruj, Y. Rahulamathavan, M. Rajarajan and C. Glackin, "A New Secure and Lightweight Searchable Encryption Scheme over Encrypted Cloud Data," in IEEE Transactions on Emerging Topics in Computing, vol. 7, no. 4, pp. 530-544, 1 Oct.-Dec. 2019.