ID BASED ADAPTIVE-KEY SIGNCRYPTION FOR DATA SECURITY IN CLOUD ENVIRONMENT

T. Sujithra
Research Scholar, Madurai Kamaraj University, Madurai, India

Dr. M. Sumathi
Associate Professor and Head, Department of Computer Science
Sri Meenakshi Govt. Arts College for women, Madurai, India

Dr. M. Ramakrishnan
Professor and Head, Department of Computer Applications
Madurai Kamaraj University, Madurai, India

S. M. Udhaya Sankar
Assistant Professor., Department of Information technology
Velammal Engineering College, Chennai, India

ABSTRACT

Towards assurance of the accuracy of public keys, the customary public-key cryptography (PKC) needs records to be retained through a certification authority (CA). Though in case important safety services, the accepted PKC agonizes since the organization of substructure associate records. An identity-based signcryption (IBS) scheme is a cryptographic technique which provides both confidentiality and authenticity. However, the IBS agonizes since the key contact difficult, that one of the unembellished refuge intimidations to authentic cryptographic methods above the days. Hence, in this paper we have designed a secure ID based Adaptive Key Signcryption (IBAKS) method for securing the confidential data to be stored on cloud computing. The important knowledge of future IBAKS deceits in apprising the private key adaptively based on the time period, although keeping the similar public key. Also, the encryption method utilizes the triple key DES for enabling higher security. The proposed methodology will be implemented in the working platform of JAVA and the performance outcomes were analyzed.

Keywords: DES-Data Encryption Standard, TDES-Triple Data Encryption Standard; IBAKS-ID based Adaptive Key Signcryption
INTRODUCTION

During the most recent decade, as one of the center advances in the present data time, distributed computing has been quickly applied to all enterprises. Clients are permitted to store huge measure of information on distributed storage for some time later. Distributed storage can make information clients store and access their documents whenever, from anywhere and with any gadget [1]. With the development in information age and utilize numerous associations will in general redistribute their information stockpiling and examination using cloud condition to diminish the heap on their neighborhood assets and to decrease the expenses of the administration and the upkeep. This is on the grounds that, distributed computing gives various preferences, for example, adaptability, less exertion of information the board, on interest get to, pay as you go. In any case, secrecy, honesty and protection of information are as yet the principle security worries for the two information proprietors, for example people and undertakings, and furthermore cloud specialist organizations [2]. In this way, it is essential to address the security issues and issues in cloud frameworks, and to discover an answer for the across the board acknowledgment of these arrangements [3].

The most effective method to guarantee the classification and approved access of information is the focal issue of information stockpiling in cloud condition. Information classification in the distributed computing is an extremely testing undertaking. Encryption is one of the most secure techniques guaranteeing this assignment. Be that as it may, regardless of this safe measure a few breaks may show up while recovering the information from cloud [4]. For instance, distributed computing supplies stockpiling administrations to clients. The clients can recover the information in wherever and whenever. The information likewise can be shared by different clients approved by the information proprietors. Since clients can't completely believe a cloud specialist co-op (CSP), the information ought to be put away in a scrambled structure. At the point when the information should be shared by approved clients, the scrambled information ought to be re-encoded without unscrambling. Just the approved clients can decode the re-encoded information to get unique information [5].

In this way cloud condition wants another working worldview for bringing such cloud administrations into Personality Based Encryption (IBE) plan to fix the issue of security depicted previously. IBE is an interesting decision in contrast to exposed key encryption, that is suggested to streamline key organization in a testament created Open Key Framework (PKI) by exploiting human -intelligible characters (e.g., remarkable name, Mail ID, Internet Protocol address, and so on) such as public keys [6]. Along these lines, transmitter using IBE doesn't consume to look into public key and authentication, however straightforwardly encrypts communication through beneficiary's personality. Besides, recipient receiving the private key related through the comparing character from Private Key Generator (PKG) be able to decrypt such figure content. So that, lone approved clients can acquire the first information put away in the cloud. Moreover a signcryption plan is to join the usefulness of an encryption with that of a mark conspires. What's more, it additionally gives security assurance and unforgeability [7].

Signcryption is a public key in cryptography, encryption conspire that plays out the elements of advanced signature just as of encryption at the same time. The two principal cryptographic apparatuses are Encryption and Computerized signature which be able to confirm privacy, honesty, and non-revocation [8]. Up to the late mid-2000s, the two have been seen as
significant yet unique fundamental necessity of dissimilar cryptography outlines. In open key plans, a conventional method is mark then-encryption for example to prudently indicate a communication at that point pursued through an encryption. Yet, it can plan us to two issues: Low effectiveness and significant expense, then the situation that no personal strategy be able to safeguard the security [9]. Signcryption is a cryptographic method that satisfies the functionalities and properties of high-tech streak and encode in a private coherent advance for example both at a similar case and can diminish the computational costs viably and it likewise diminishes correspondence overheads when we contrast it and the customary mark then encryption plans. Signcryption is a plan that gives the properties and usefulness of both encryption and computerized marks plots in such a manner thus, that it turns out to be more proficient than marking and scrambling independently individually [10].

2. RELATED WORK

Qin-Long Huang et.al [11] have displayed a protected and security saving computerized rights the board (DRM) conspire utilizing homomorphic encryption in distributed computing. They introduced a productive computerized right the board system in distributed computing, which enables content supplier to redistribute scrambled substance to unified substance server and enables client to devour substance with the permit given by permit server. Further, they gave a protected substance key appropriation plan dependent on extra element homomorphic probabilistic open key encode and intermediate re-encode. They gave plan keeps noxious representatives of permit server from giving the permit to unapproved client. What's more, they accomplished protection saving through allowing consumers to continue secretive towards the key server and expert cooperative.

ThourayaBouabana-Tebibel and Abdellah Kaci [12] have built up the displayed technique to improve privacy of redistributed information. They are especially keen on fortifying the entrance control on the query output, when the pursuit was performed over scrambled information. The property behind this part of security was known as ACAS (Access Control Mindful Pursuit) rule. They introduced a hybridization of Accessible Encryption and Trait Based Encryption methods so as to fulfill the ACAS property. The exhibited model backings a customized and secure multi-client access to redistributed information, showing high search execution. It manages multi-watchwords look and was intended to accelerate the hunt time by exploiting Superior Processing, which was broadly utilized in Cloud computing.

Yong Yu et.al [13] has created ID-CDIC, a character-based cloud information trustworthiness checking convention which could wipe out the mind-boggling authentication the board in customary cloud information respectability checking conventions. Besides they gave the development RSA mark could bolster variable-sized record squares and open examining. Moreover, they gave a proper security model to ID-CDIC and demonstrate the security of the executed development under the RSA suspicion with enormous open types in the irregular prophet model. They showed the presentation of the exhibited technique by building up a model of the convention.

Cheng Guo et.al [14] has displayed a key-total validation cryptosystem that could produce a steady size key that supports adaptable assignment of decoding rights for any arrangement of figure writings. The size of the key was autonomous of the quantity of most extreme figure writings, implying that the cost of the introduced plan was steady regardless of how much of the time clients transfer documents to the cloud server. Furthermore, the confirmation procedure in the game plan takes care of the key-spillage issue of information sharing. The information proprietor could remove a totaled key that incorporates lists of the figure messages, the character of the representative, and the termination date of the key. The key with the open parameters was utilized by the cloud server to recognize the individual or element mentioning
a download, enabling the cloud server to control the privilege to download. Strikingly, they demonstrated that the confirmation key couldn't be fashioned, and the message in this key couldn't be denied. The technique that was utilized to accomplish effective and secure information partaking in powerful distributed storage must be steady in cost and spillage flexible.

Meng Shen et.al [15] has displayed a safe CBIR plot that supports Different Picture proprietors with Security Insurance (MIPP). They encode picture highlights with a protected multi-party calculation system, which permits picture proprietors to scramble picture highlights with their very own keys. This empowers effective picture recovery over pictures assembled from different sources, while ensuring that picture protection of an individual picture proprietor would not be spilled to other picture proprietors. They likewise gave a technique to closeness estimation of pictures that could abstain from uncovering picture likeness data to the cloud.

Shahzaib Tahir et.al [16] have displayed a positioned Accessible Encryption conspire that tends to different plans don't take the practically certain nearness of typographical mistakes in the records viable issue by supporting fluffy catchphrases. The exhibited development depended on probabilistic trapdoors that help oppose recognize capacity assaults. They built up an Accessible Encryption as an Assistance (SEaaS) which was sent on the English Media transmission's open Cloud design and assessed over a genuine discourse corpus. This security examination yields that the development fulfills solid security ensures and was likewise calm lightweight, by breaking down its presentation over the discourse corpus.

Priyanka Singh et.al [17] have exhibited a protected information deduplication plot that officially addresses the issues of adaptation to internal failure, productive and dependable key administration, information secrecy by obscurity of re-appropriated data and honesty check at the client's end preceding downloading through calculation of verification codes. Information was appropriated into irregular looking offers dependent on Stage requested twofold (POB) number framework at various servers and was additionally made secure by means of the idea of evidence of possession (PoW) idea. Likewise, key overhead was limited utilizing Chinese Leftover portion Hypothesis (CRT) based mystery sharing. The viability of the displayed plan has been exhibited where the security examination approves its appropriateness as for different assaults continuously situations.

3. MOTIVATION OF THE CURRENT RESEARCH

The advantages of distributed computing are being acknowledged by more organizations and associations consistently. Distributed computing gives customer a virtual registering framework on which they can store information and run applications. Be that as it may, distributed computing has presented security challenges since cloud administrators store and handle customer information outside of the span of customers' current safety efforts. Different organizations are structuring cryptographic conventions custom fitted to distributed computing trying to adequately adjust security and execution. In customary cryptographic frameworks, at least one keys are utilized to change over the plain content into figure content at the sending side, and the plain content will be recovered back at the accepting side by utilizing proper unscrambling keys. Without the learning of the right decoding keys the change is infeasible thinking about both in time and cost. The primary huge downside of data secure plan dependent on conventional cryptography is unlawful sharing of key among sender and collector, for example key dispersion issue. Some ongoing techniques have attempted to correct the above issue by determining the cryptographic keys by utilizing the biometric highlights of a genuine client. Presenting the keys got from the biometric highlights and other data of an authentic client into encryption and unscrambling procedure can build the data security and lessening the probability of its unlawful usage.
ID-based encryption (IBE) is a significant crude of ID-based cryptography. In that volume it is a sort of open key encryption where the open key of a consumer is approximately one of a caring data almost the appeal of the consumer (for example a client's email address). This suggests a transmitter who methods the open constraints of the outline can ascent a message for example the gratified approximation of the collector's name or mail ID as a key. The recipient becomes that one decodes the key from a focal position, which should be trusted as it creates mystery keys on behalf of respectively consumer. In any case, there are two issues that make the plan of IBE incredibly hard: the necessity that the open key can be a discretionary string and the likelihood to remove decoding keys from the open keys. In light of these natural issues ID-based cryptography is viewed as reasonable just for little private system with lower security necessities. In this manner giving a protected key giving system in ID-based cryptography is a significant issue to make the ID-based cryptography progressively relevant to this present reality. Away after these viewpoints, IBE proposals fascinating best part exuding after the probability to encrypt additional data into the identifier. The initial motivation for character-based encode is to support the sending of an open key foundation. Entire the additional for the most part, IBE can rearrange outlines that contract through an enormous number of open keys. Instead of pushing gone a foremost database of open keys the outline be able to moreover become these open keys since usernames, or fair exploit the entire numbers as particular open keys. In any case, the absence of answers for the above issue spurred me to do investigate around there.

4. PROPOSED DATA SECURITY MODEL USING ID-BASED ADAPTIVE-KEY SIGNCRYPTION METHOD

The enormous development of the distributed computing conditions requires new engineering for security administrations, since information security is one of the most basic worries of distributed computing. Through affecting information interested in the cloud a suggestion remains giving up authority of which information to the cloud supplier. Protection issues are the principle worry of cloud clients (over 85%) in re-appropriated information stockpiling. Information Encryption is a widespread method to ensure private information. After encryption, information in the cloud is put away in figure structure. The Approved Clients who gets the key can access to the figure message and decode it to get the plaintext. For associations with an enormous gathering of clients, it is hard to deal with the keys.

Be that as it may, the key administration can be improved with the assistance of personality-based encryption, which when utilized for the sending of a public key substance. All the extra for the greatest part, IBE be able to improve structures that pact with uncountable open keys. Then again, the capacity of huge database of open keys with client name likewise takes more memory.

In this way, by way of different to pushing gone a foremost database of public keys, the framework is permitted to store either the public keys got from usernames, or essentially exploit the sums as unique open keys. Also, by and large, the key presentation issue is one of the unadorned refuge dangers to real cryptographic plans completed the days.

Near moderate the injury because of the overview of mystery key data, single route remains to develop key-advancing various leveled ID-based cryptographic plans that enable every client in the pecking order to invigorate their private keys occasionally while keeping up a similar open key. Key development was for the most part proposed to set up the safe encryption model.

Consequently, in this paper we have set up the personality based versatile Key cryptography utilizing signcryption calculation to give both privacy and legitimacy. The proposed character based versatile Key signcryption calculation is additionally expected to alleviate the harm if there should arise an occurrence of a mystery key trade off, any of the unadorned refuge dangers
near real cryptography plans. That the open key framework, the fundamental thought of versatile key age deceits in refreshing the reserved key through period, although keeping up a similar open key. Besides, the proposed signcryption based encryption system utilizes the Triple DES encryption technique for improving the ordinary Signcryption based encryption strategy.

Further, in the proposed Signcryption calculation, the private key is determined utilizing the sender's close to home information and it is adaptively changed with time so as to guarantee security. The open key will be same with change in time. In this way, during the recovery of unique information, the collector needs to know the key of the comparing timeframe. Alongside the versatile key age, the client id-based validation will be made for the beneficiary on the cloud specialist co-op to improve the security. The sender sends the mystery keys, just to the validated clients. After validation, the beneficiary can decide the key of the comparing timespan.

Priyanka Singh et.al [17] have exhibited a protected information deduplication plot that officially addresses the issues of adaptation to internal failure, productive and dependable key administration, information secrecy by obscurity of re-appropriated data and honesty check at the client's end preceding downloading through calculation of verification codes. Information was appropriated into irregular looking offers dependent on Stage requested twofold (POB) number framework at various servers and was additionally made secure by means of the idea of evidence of possession (PoW) idea. Likewise, key overhead was limited utilizing Chinese Leftover portion Hypothesis (CRT) based mystery sharing. The viability of the displayed plan has been exhibited where the security examination approves its appropriateness as for different assaults continuously situations.

The overall block diagram of the planned secure cryptography scheme is given in the below figure 1.
4.1. ID-based Adaptive-Key Signcryption

Signcryption is an original worldview in open key cryptography that concurrently fulfils together the elements of computerized signature and open key encode in a wisely one stage, and through a cost which is significantly lesser than the expense of normal mark then encryption draws near. During the advanced signature, key age procedure is pursued. Additionally, the open key encryption can be made utilizing DES, 3DES and so on. Contrasting with DES, the 3DES guarantees greater security through the three-stage key confirmation.

Despite the fact that, the Signcryption calculation has numerous points of interest, it experiences couple of issues given as pursues:

- In Signcryption calculation, the Sender needs to utilize the Recipient's open key to signcrypt a communication. Signcryption has a drawback while the sender needs to communicate a Signcrypted content to various Collectors; since, it wants toward signcrypt the communication through every one of its proposed beneficiary's open keys and direct them independently to every last one of them.
- This method is repetitive regarding transfer speed utilization and computational asset use.
- Further, the utilization of keys from the arbitrary Key Generator in the key age procedure of signcryption likewise leads in the trouble of dealing with the keys for the association with more clients.
- Moreover, the key introduction issue emerges in the ordinary Signcryption approach over the lifetime.

Henceforth to guarantee the security and to beat the issues of the customary Signcryption based cryptography strategy, we have utilized the ID based versatile key signcryption calculation to scramble the mystery message. The ID based versatile key signcryption produces the key adaptively dependent on the timespan and scrambles the mystery information dependent on 3DES methodology. The proposed cryptography strategy builds the protection as well as uses the upside of ID based encryption techniques. In addition, the proposed cryptography technique takes care of the key presentation issue by the age of gathering of time-based changing keys between the sender and the beneficiaries.

The Block Diagram of 3DES based Encryption standard is given in the following figure 2.

![Figure 2 3DES based Encryption standard- Block Diagram](image-url)
The proposed ID based adaptive key Signcryption algorithm contains four phases. The first two phases are carried out in the sender side and the other two phases are done at the receiver side.

In the sender side, the proposed secure cryptography method involves,

- key generation phase (Time period based)
- Encryption phase (3DES algorithm)

Similarly, in the receiver side, the proposed secure cryptography method involves,

- Authentication by CSP
- Decryption phase (Reverse 3DES operation)

In key generation phase, the private keys for sender and receiver are produced. Before key will go for the encryption stage, the secret data is encoded through the support of 3DES encryption algorithm using another three set of keys. Finally, to retrieve the original secret data from the encrypted cipher text, the receiver is subjected for the two step verification. In the first step of verification, the CSP (Cloud Service Provider) verifies the receiver before providing the private keys. Once authenticated, the Reverse 3DES operation is done; The sender gives the encrypted and decrypted data.

4.1.1. Key Generation Phase

Signcryption is an open-key original that simultaneously performs the roles of together digital signature and encryption. In the digital signature phase of the proposed adaptive key Signcryption algorithm, the adaptively varying private keys for the sender and the receiver are derived. The proposed adaptive key generation strategy is developed from the Key-derived cryptographic, which is proposed to moderate the harm if the secret key cooperation, which is any of the unadorned refuge threats to real cryptography methods. Now the open-key setting, the important indication of key-derived deceits in apprising the secluded key through time, although keeping the similar open key. Therefore, the attackers, who have no knowledge about the adaptive keys, cannot be able to steal the personal data of the sender.

Here, the $K_{T,P}$ is the adaptively varying keys calculated for different time-period $(T,P)$ based on the following representation as,

$$K_{T,P} = \left( T \times A_i \times S_{priv}(A) + A_i \right) + \left( T \times B_i \times S_{priv}(B) + B_i \right)$$

Where, $A_i$ and $B_i$ represents the sender and the receiver identity length. Here, $S_{priv}(A)$ and $S_{priv}(B)$, are the secret keys of the sender and the receiver generated by the prime field operation. The prime field operation is done to select those keys from a large range of prime numbers, $[1, \Lambda, p-1]$. Based on the prime field operation, we get the private key for both the sender and receiver from a large range of prime numbers, $[1, \Lambda, p-1]$.

The secret keys, $S_{priv}(A)$ and $S_{priv}(B)$ are generated the unique prime number values selected randomly for distinct identity of the sender and the receiver using the prime field operation.

Therefore, the Sender has the set of keys, $(S_{priv}(A), K_{T,P}, S_{pub}(A))$. where, $S_{priv}(A)$ denotes the Sender’s private key, $K_{T,P}$ defines the adaptively varying private keys based on time period and $S_{pub}(A)$ represents the Sender’s public key.
Similarly, the Sender has the set of keys, \( (S_{pr}(B), K_{T_p}, S_{pub}(B)) \). where, \( S_{pr}(A) \) denotes the Sender’s private key, \( K_{T_p} \) defines the adaptively varying keys based on time period and \( S_{pub}(A) \) represents the Sender’s public key.

Here, the public keys \( S_{pub}(A) \) and \( S_{pub}(B) \) represents the identity (i.e. mail id or username) of the sender and receiver respectively. Using the public keys, the private keys are generated by the Cloud server through the prime field operation. Moreover, a set of adaptive keys are also created from the data driven from open and isolated keys of the sender and the receivers. The receiver with knowledge about the key of corresponding time period can only be able to retrieve the data.

4.1.2. Encryption Phase

During this phase, the secret data is encrypted based on distinct set of keys generated by the 3DES encryption algorithm. The Triple DES is worthwhile since it takes a significantly valued key distance, which is lengthier than greatest key distances combined through additional encryption manners. Since, the TDES uses three set of keys for the encryption process. So, the key exposure problem can be more reduced. In the Triple DES, there are three possible keying options.

Keying option 1: In the first option, the three keys \( S = (s_p, s_q, s_r) \) are identical (i.e. \( s_p = s_q = s_r \)). This is backward compatible to single DES.

Keying option 2: In the second option, the three keys \( (s_p, s_q, s_r) \) are chosen such that the first two keys are independent to each other \( s_p \neq s_q \) and at the same time the encryption keys are similar \( s_p = s_r \).

Keying option 3: In this option, all the three keys are different, \( s_p \neq s_q \neq s_r \). This is also termed as the triple key DES.

The three key 3DES algorithm is emerged to strengthen the DES algorithm. The three-key triple-DES is a popular technique on behalf of establishment DES with a 168-bit key. This method can remain well-thought-out a 3-round cipher through liberated 56-bit round subkeys, understanding that separately sequence is exact tough. Honestly, one strength custom turning related-key cryptanalysis; though, such a method would need several identified plaintexts.

In 3DES, the algorithm generates a set of three unique keys, \( S = (s_p, s_q, s_r) \) to perform three step encrypt-decrypt process of single DES. The 3DES uses both the combination of encryption and decryption strategies for encryptingthe secret data.

The phases complicated in the 3DES algorithm are of,

Step 1: Encryption (\( s_p \))

In this step, the data is encrypted through the single DES Algorithm with the help of the first key (say, \( s_p \)). Therefore, the initial cipher text is obtained as, \( z_1 = (Enc(s_p, M_{plain}) \)

SingleDES based encryption (\( z_1(s_p) \))

In this section, the single DES Algorithm used for the encryption step of TDES is provided. DES is a kind of symmetric key encryption procedure. This procedure encrypts information in the blocks and the scope of respectively block is 64 bits. That is the DES algorithm takings the input of 64 bits simple script and transforms that input into 64 bits ciphertext. The key extent
of this algorithm is 56 bits. DES is established on dual essential characteristics of cryptography: Substitution (confusion) and transposition (Diffusion). Now the initial stage of encryption, the information in the block of 64 bit goes over early permutation stage. Afterward that, 16 rounds of permutation and substitution are executed. The DES consists of 16 round. The last round of 16, the DES gives the outcome of 64-bit ciphertext.

The steps involved in the DES algorithm so as to obtain the cipher text \( z_1 \) with key \((s_p)\) are explained below;

- At first, the 64-bit plaintext block is given to the initial permutation (IP) function.
- After the permutation, we obtained dual splits of permuted blocks such as Left Plain text (LPT) and Right Plain Test (RPT).
- Then, each LPT and RPT is given to the 16 round encryption process. Here, the utilized key size is 56 bit, which is derived from \((s_p)\). In the 16 rounds, each round has own key derived through the permutation step over the key, \((s_p)\).
- Then, each round we use a 48-bit sub-key which is generated from the 56-bit key.
- After that, RPT is expended from 32 bits to 48 bits using expansion permutation.
- Then, the 48-bit key is XOR with 48-bit RBT then the obtained value remains assumed to the following stage.
- Then, consuming the S-box substitution 32-bits are formed from 48-bits.
- After that, 32 bits are permuted using P-Box Permutation.
- Then, the output of P-Box is XOR with LPT which is of 32 bits.
- Then, the 32-bit LPT and 32-bit RBT output sizes are exchanged to make a pre-output. The obtained production is extracted converse of the early permutation.
- The output of the final permutation is the 64-bit ciphertext.

In this section, the secret data is first encrypted using the key, \((s_p)\). This encrypted data is then passed to the second level security step.

**Step 2: Decryption \((s_q)\)**

In the second step, the output created since the initial stage is decrypted by single DES Algorithm through the benefit of the second key (say, \(s_q\)). In the decryption step, the inverse process of the encryption will be done, but with different keys to ensure the data security.

The second level security step to generate the cipher text \( z_2 \) with key \((s_q)\) is represented as,

\[
 z_2 = Dec(s_q, Enc(s_p, M_{plain}))
\]  

(2)

**Step 3: Encryption \((s_r)\)**

Finally, in the third step, the decrypted output of second step is again encrypted using the same single DES Algorithm through the support of the third key (say, \(s_r\)) to the cipher text \( z_1 \) with key \((s_p)\).

Therefore, the 3DES encryption algorithm can be simply represented using the following representation:

\[
 Z = Enc(s_r, (Dec(s_q, Enc(s_p, M_{plain}))))
\]

(3)
Here $Z$ denotes the Cipher data; $(Enc(s_p, M_{plain})$ is the encrypted data using key, $s_p$; $(Dec(s_q, (Enc(s_p, M_{plain})))$ is the decrypted data using key, $s_q$ performed over the cipher text $z$, and $M_{plain}$ represents the original plaintext.

Once, the data is secured, it is stored in the cloud storage database handled by the Cloud Service Provider. In the data retrieval process, the receiver has to go for the two-step verification which is given in the following section.

### 4.1.3. Receiver Authentication

The first step verification taken place in the data retrieval process is the authentication. In this stage, the identity based Authentication is followed before entering to the decryption phase by the receiver. The proposed system is designed in such a manner that, if and only if the receiver enters the correct password, he will get the suitable required keys for decrypting the cipher text. The user identity is the username or mail id and the password can be in the form of numbers or characters. The authentication is verified by the cloud server. If the provided credentials are not matched, the cloud server rejects the request; otherwise accepts and provides the necessary keys. The keys include the sender’s private key $(S_{p\_pvt}(A))$ and the sender’s identity. So, that the receiver can calculate the keys of the corresponding time period, with which he can decrypt the original data.

### 4.1.4. Decryption Phase

Once the receiver is authenticated and verified by the server, he gets the keys and then he calculates the adaptively varying time period key. On providing the suitable time period key, the service provider works out the decryption phase. At the end of decryption, the original plaintext can be retrieved from the encrypted message.

The steps involved in the decryption by the 3DES algorithm are of,

**Decryption $(s_r)$**

In this step, the data is decrypted first through the single DES Algorithm through the support of the third key, $s_r$.

**Encryption $(s_q)$**

In the second step, the output made after the initial stage is encrypted by single DES Algorithm through the support of the second key, $s_q$.

**Decryption $(s_p)$**

Finally, in the third step, the encrypted output of second step is decrypted using the same single DES Algorithm through the support of the first key, $s_p$.

Hence, the 3DES decryption algorithm can also be simply represented using the following representation:

$$M_{plain} = Dec(s_r, (Enc(s_q, (Dec(s_p)))))$$

(4)

Once the decryption process is done, the receiver can extract the secret data. As the proposed cloud data security model undergoes a series of verification procedures, it can be thus applied in organizations that require higher level security.
4.2. Outcome and Discussion

Now this segment, we have examined the result found after the future cloud data security model utilizing ID-based Adaptive-Key Signcryption-based encryption (IBAKS) technique. We have actualized our proposed cloud data security procedure spending Java (jdk 1.6) with cloudSim strategies and a development of tests remained made on a PC with Windows 7 Operating framework at 2 GHz dual core computer with 4 GB RAM running a 64-bit version of Windows 2007.

4.3. Performance Analysis

The performance of the future cloud data security approach is analyzed in this section. The analysis is carried out by contrasting the performance outcomes of proposed ID-AKS technique with ID based Signcryption method and ID based Homomorphic encryption technique. The measures like time and memory consumed for the encryption and decryption procedures are considered for evaluating the performance of the proposed IBAKS encryption technique with the existing encryption standards. Here, the time measure is measured in terms of milliseconds and the memory is measured in terms of bytes. Moreover, the comparison is made by varying the size of the confidential data uploaded on cloud.

The time taken for the Encryption and Decryption procedure for the proposed ID-AKS technique and the existing ID based Signcryption method and ID based Homomorphic encryption technique is given in the below table 1.

<table>
<thead>
<tr>
<th>Data Size (KB)</th>
<th>Encryption time (ms)</th>
<th>Decryption time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IBAKS</td>
<td>IBAKS</td>
</tr>
<tr>
<td>10</td>
<td>11024</td>
<td>11024</td>
</tr>
<tr>
<td>20</td>
<td>15625</td>
<td>15625</td>
</tr>
<tr>
<td>30</td>
<td>21548</td>
<td>21548</td>
</tr>
<tr>
<td>40</td>
<td>25468</td>
<td>28948</td>
</tr>
</tbody>
</table>

From the above table, it is noted that the period occupied for the decryption is fewer than the interval occupied for the encryption and it is increased when the size of data is raised from 10 kb to 40 kb. On comparing to the existing methods, the encryption and decryption time is also reduced for the proposed IBAKS method.

Moreover, the memory consumed for the Encryption and Decryption procedure for the proposed IBAKS technique and the existing ID based Signcryption method and ID based Homomorphic encryption technique is given in the below table 2.

<table>
<thead>
<tr>
<th>Data Size (KB)</th>
<th>Encryption Memory (Bytes)</th>
<th>Decryption Memory (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IBAKS</td>
<td>IBAKS</td>
</tr>
<tr>
<td>10</td>
<td>1124412</td>
<td>1138628</td>
</tr>
<tr>
<td>20</td>
<td>1354584</td>
<td>1369183</td>
</tr>
<tr>
<td>30</td>
<td>1658744</td>
<td>1670048</td>
</tr>
<tr>
<td>40</td>
<td>1985475</td>
<td>1993110</td>
</tr>
</tbody>
</table>

Table 2 represents that the memory consumed for encrypting the data is more when compared to the decryption memory. However, the memory consumed by the proposed IBAKS is less than the existing methods. This shows the efficiency of the proposed security model.
Finally, the graph is drawn for showing the variations between the encryption-decryption time and memory of the proposed and the existing methods by the following figures 3 to 6.

**Figure 3** Encryption Time of proposed and existing methods

**Figure 4** Decryption Time of proposed and existing methods

The beyond diagram clearly demonstrations that the encrypted and decrypted time taken for the proposed IBAKS method is very much less than the existing IBS and IBHE methods.
The above figures 5 and 6 shows that the encryption memory is not that much reduced than the existing methods. However, the decryption of secret data by the proposed IBAKS is very much reduced than the existing methods. This shows the less complexity on data decryption than the existing methods. By the same time, the proposed IBAKS also ensures more security than the existing methods.

5. CONCLUSION

In this paper, we have introduced the secure ID based Adaptive Key Signcryption (IBAKS) method for securing the confidential data to be stored on cloud computing. The proposed IBAKS avoids the key exposure problem and at the same time ensures the confidentiality and authenticity. The key exposure problem is solved here by the adaptively varying private keys based on the time period, and the security is further enhanced by the triple key TDES. The
ID based Adaptive-Key Signcryption for data security in cloud environment

performance efficiency of the proposed IBAKS is analyzed with the existing ID based Signcryption method and ID based Homomorphic encryption technique in terms of time and memory. The results show that the time and memory requirement of the proposed IBAKS is very less than the existing methods. Thus, the proposed security model enables higher level of security and can be applied in the organizations that will handle more confidential data.

REFERENCE


