International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-5, March 2019

A Novel Single User Fingerprint Minutiae Based Integrity Verification and Encryption Algorithm for Cloud Data

Ruth Ramya Kalangi, M. V. P. Chandra Sekhara Rao

Abstract*: Data security and data privacy are considered as two major aspects of cloud computing. The main issues in traditional data security models include encrypting large data is difficult due to high computational time and lack of user integrity verification. To resolve these issues, A Novel Single User Fingerprint Minutiae based Integrity verification and Ciphertext-Policy Attribute-Based Encryption (SFM-CPABE) model is implemented on cloud data. This model includes a fingerprint extraction technique, policy integrity technique and ciphertext policy attribute-based encryption (CPABE). Experimental analysis over cloud data proved that the proposed algorithm has high efficiency and accuracy compared to the traditional cloud security models in terms of integrity, encryption time and computational time.

Index Terms*: Ciphertext Policy Attribute-based Encryption (CPABE), Fingerprint Biometry, Integrity Algorithm and Cloud Computing.

I. INTRODUCTION

Nowadays, with the rapid advancements in digital technology, the privacy of individuals, as well as enterprise data, has become a major concern. Various encryption and authentication techniques have been implemented in order to secure sensitive data. Compared to traditional cryptographic approaches, biometric techniques are considered to be the most secure and reliable techniques for the user authentication process. Most of the data is deployed in a cloud environment due to its advantages and rapid growth [11, 12]. If any unauthorized person access data stored in the cloud, then sensitive data will be compromised. Hence, there is a requirement of a strong security model to protect cloud data.

A. Attribute Based Encryption (ABE)

Sahaiand Waters proposed an Attribute-Based Encryption (ABE). It provides better security and access control mechanism. ABE can be stated as a type of public key encryption method in which encryption and decryption are based on user attributes. The classical attribute-based encryption schemes are classified into two: KP-ABE and CP-ABE.

Manuscript published on 30 March 2019.
***Correspondence Author(s)
Ruth Ramya Kalangi, Computer Science & Engineering, Acharya Nagarjuna University, Guntur, India.
Dr. M. V.P. Chndra Sekhara Rao, RVR & JC College of Engineering, Chowdavaram, India.

B. Key Policy Attribute Based Encryption (KP-ABE)

Every individual user is associated with an access tree structure. In access tree threshold gates represent the nodes attributes represent leaf nodes. Ciphertext includes an attribute set and secret keys that are merged with monotonic access structure in order to choose a particular ciphertext which is meant for that user to decrypt. The following are the four steps in the KP-ABE algorithm **Setup:** It accepts input K and produces a public key (PUK). A master secret key (MK) is generated by the algorithm. Encryption requires PUK. MK is responsible for the production of secret key (SK).

Encryption: This algorithm accepts plaintext M, generated PUK along with attribute set as input and produces ciphertext C.

Key Generation: Key generation algorithm includes an access structure T along with an input. The objective of key generation algorithm is to produce SK. SK is used to decrypt ciphertext. The process of encryption executes successfully when the set of attributes matches T.

Decryption: Inputs to decryption algorithm are user's secret key (SK) satisfying the access structure T and ciphertext C. Output is original plaintext message M when the attribute set satisfies T. In this paper, A Novel Single User Fingerprint Minutiae based Integrity Verification and the encryption algorithm (SFM-CPABE) is designed and implemented using the user's biometric details. Same biometric details are required in the process of decryption in order to decrypt the ciphertext successfully. If both the biometric samples don't match with each other, then the authentication process fails and that user cannot decrypt the cipher text.

II. RELATED WORK

A. Torres, et.al, proposed a more secure biometric authentication system using Fully Homomorphic Encryption (FHE) technique [1]. It is considered as most significant and useful in privacy preservation for small datasets. Biometric of an individual is permanent and it cannot be modified during data encryption and decryption. This model is tested using the AVISPA tool [2]. This model is inappropriate for large datasets due to high computational time.

W. K. Hassan, et.al. Proposed a new key-exchange scheme by using biometric Identity-based encryption (BIO-IBE) to share encrypted data [3]. This model is implemented in a cloud environment. An advanced protocol BIO-IBE is responsible for providing a more secure environment for both the sender and the receiver for key distribution.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

This approach integrates the traditional IBE scheme [4] with the biometric encryption. User's symmetric keys are accessed through the insecure channel using this model.

Those Users chosen by data owner are required to provide a sample of their biometric identity for the decryption process. G. Mehta, et.al, introduced an edge-based selective encryption technique for secure biometric authentication [5]. Due to the vast usage of biometric-based applications, it became essential to maintain the security of biometrics. The prime objective of this process is to localize iris out of the whole image so that features can be easily retrieved in order to produce a biometric template. Selective encryption technique is responsible for the encryption of ROI. This technique also decreased overall computational overhead as well as processing time.

I. Nakouri, et.al, Biometric-based cryptographic keys play an important role in the process of authentication, encryption and biometric template protection [6]. Fuzzy extractors can be used to identify the problems through processing of noisy biometric data. The random cipher key is generated with the help of fuzzy extractors. This technique basically depends on chaotic maps to improve the overall sensitivity of the key generation process.

M. N. Omar, et.al, tried to improve the confidentiality of cloud computing by developing a more secure biometric encryption technique [7]. It ensures confidentiality of biometric data stored in the cloud. The security of cloud data is extended by implementing the proposed scheme. The above biometric-based encryption technique is incapable to overcome all security related problems of cloud computing.

M. A. Murillo-Escobar, et.al presented a secure embedded biometric authentication technique [8] that is based on fingerprint and chaotic encryption. This technique is applied to the embedded authentication system having a 32-bit microcontroller. The overall security of this model is evaluated by analyzing security details at a statistical level. The only limitation of this model is its irrevocability. It also has significant applications in the fields of control access of banks, hospitals, e-commerce, etc.

C. Chae, et.al, developed an improved biometric encryption technique for private key protection in Biometric Public key infrastructure (BioPKI) [9]. In case of PKI system, protection of private key is the most complicated task. This technique is completely based on the confidentiality of private key. The threat of password identification is considered one of the vulnerabilities of the PKI system. Currently, all BioPKI systems are using biometric details in order to verify the authenticity of the user instead of traditional passwords. Biometric details that are applied to provide security to private key can't be reused if those details are compromised. This technique improves the reusability of biometric details. Further research works can be performed to implement private key protection through secret distribution scheme [10].

III. PROPOSED MODEL

The proposed Single User Novel Fingerprint Minutiae based Integrity Verification and Encryption (SFM-CPABE) model is implemented on cloud data. The overall framework is shown in Figure 1. Initially, the fingerprint of a user acts as an input for policy extraction. Binarization, thinning and pattern extraction procedures are used to extract Fingerprint policy patterns. Iintegrity value computation is done by using CP-ABE encryption model.

The overall framework is divided into 3 phases:

A. Fingerprint Pattern Extraction

B. Biometric Integrity Algorithm

C. Integrity based CP-ABE for Biometrics

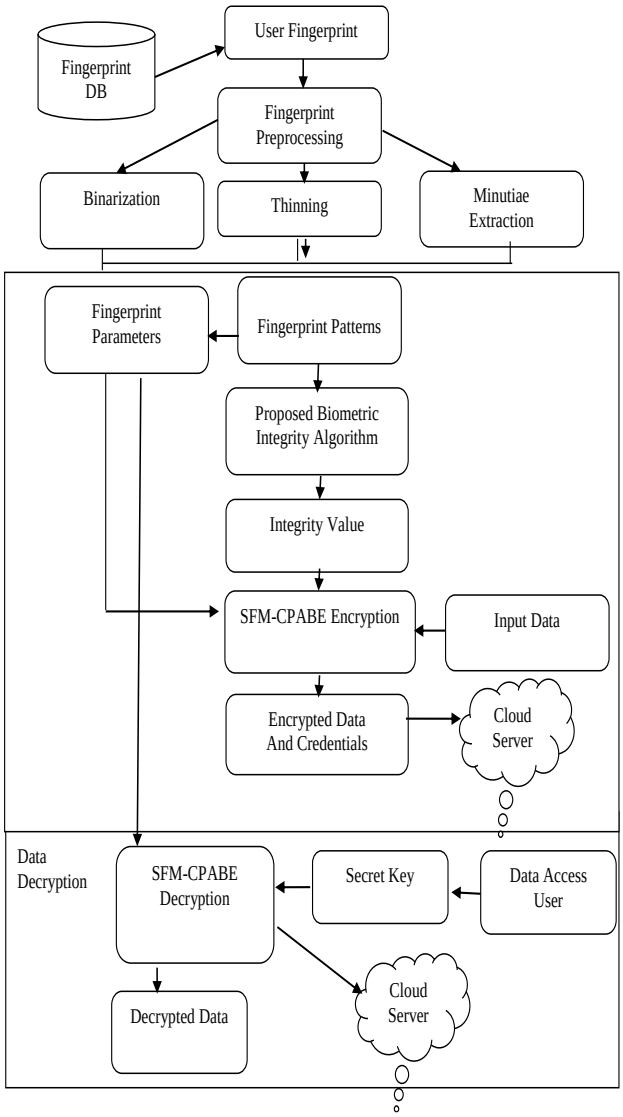

Fig 1. Single User Fingerprint Minutiae based Integrity Verification and Encryption Model (SFM-CPABE)

A. Fingerprint Pattern Extraction

In this phase, each user fingerprint image from the database is pre-processed using three steps such as Binarization, Thinning and minutiae extraction. The output of binarization step is to convert given fingerprint image into binary. In the binary image white points represents value one and black points value zero. To eliminate noise and to find skeleton of the image Thinning is used. SFM-CPABE model optimized the minutiae extraction process for pattern evaluation by using Equation 1.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

$$N_a(s,t) = \sum_{s=1}^{k} (| As - A_{s+1} | \quad (1)$$

Where
$N_a(s,t) = 0$; Isolated Point
$N_a(s,t) = 1$; Ending Point
$N_a(s,t) = 2$; Connection Point
$N_a(s,t) = 3$; Bifurcation Point

The above-mentioned equation is used to find four different types of fingerprint patterns such as isolated pattern point, ending point, connection pattern point and bifurcation pattern point based on the computational values of M. Basic 8 bit block of the fingerprint image is shown in Figure 2 that illustrates an 8-bit block with central pixel A(c) and its neighbours.

A(s+3)	A(s+2)	A(s+1)
A(s+4)	A(c)	A(s)
A(s+5)	A(s+6)	A(s+7)

Fig 2. Block of Fingerprint Image after Binarization

Equations 2 to 5 represent the four fingerprint patterns that are uniquely identified for data security.

Isolated Point (IP) = {U (s,t) x U (s,t),y}; ∀ i, j ϵ N_a (s,t) =0 (2)

Ending Point (EP) = {U (s,t) x U (s,t),y}; ∀i, j ϵ N_a (s,t)=1 (3)

Connective Point (CP)={ U (s,t).x U (s,t),y}; ∀ i, j ϵ N_a (s,t)=2 (4)

Bifurcation Point (BP) = { U (s,t).x U (s,t),y}; ∀ i, j ϵ N_a (s,t)=3 (5)

B. Biometric Integrity Algorithm

In SFM-CPABE model, fingerprint patterns and their respective integrity values are used as attributes and policies in the CP-ABE algorithm. Integrity value generated from the fingerprint pattern is used as an access policy for data encryption and decryption. SFM-CPABE model uses proposed Single User Novel Biometric Integrity Algorithm. Steps used in the biometric integrity algorithm for computing integrity value are shown below in algorithm 1. In this algorithm, a unique integrity value is extracted from the fingerprint.

Input: Initialization parameters, block size B, Number of rounds R, block bits m, Block length L, h[ ] round hash vector, Data size S, input data D, y, and L are permutation matrices.

Output: Integrity value.

Algorithm 1. Biometric Integrity Algorithm

1. Hash vector Initialization
   h[m/8]← 0
2. for each data size
3. Check the condition (S>m/8)
4. Compute
   BD←D(0,L)
   RD←D(L, S-L)
5. Divide block data into sub-blocks (BBlock) of 4 bytes each or 32 bits each
   B← First 4 bytes of sub block
   C← Last 4 bytes of sub block
6. for each partition in the BBlock
7. for each round in the R
8. Compute
   $Y1=(L^T.y) \bmod 1$
   z=l..Lnonproduct(y1).scale(256)
   $E_i = P[i]+e[\max(0,i-1)]$
   $E_i = E_i \oplus z_i$
   $E_{sum} = \sum E_i$
   NR= Max (R) – Min(R)+1
   $E_{sum} = \text{Min}(R)+(E_{sum}\%NR)$
9. Consider the block F and Reverse the order and left shift 3 positions
   F← CyclicReverse(F[i])
   F← LeftShift(F[i],3)
   If(r+1< R)
   F[i]←RightShift(F[i],3)
   F[i]← Reverse(F[i])
10. $H = h_0 + h_1 ..... h_{NR}$

C. Biometric Integrity based CP-ABE

In Ciphertext-Policy Attribute-Based Encryption (CP-ABE), public key is used for encryption and decryption would be successful if receiver attributes meet the access tree structure. Algorithm 2 is used to encrypt the cloud user's data before deploying to the remote cloud server. There are four phases in the CP-ABE algorithm as in Algorithm 2. They are:

Setup Phase
Encrypt Phase
Key Generation Phase (KEYGEN)
Decrypt Phase.

Algorithm 2. Ciphertext Policy Attribute Based Encryption (CP-ABE)

Setup Phase: It generates the master key (MK), Q shared key and public key parameters (PUK). Let O1, O2 are the bilinear groups with prime order p, which satisfies bilinear property and non-degeneracy property such that $\theta_1, \theta_2 \epsilon O_p$ and generated from the hash key generator. Similarly, Z_r is the cyclic group generator using the hash key generator. Public Key and master key can be generated as

PublicKey(PUK) = {(o ϵ O_1, o_p ϵ O_1) ϵ Hash(SecretKey(patterns)),$e(o,o_p)^{\theta}1$,h ϵZ_r , o=e (o,o_p)}

MasterKey(MK) ={α ϵ PUK(o_p), β ϵ Hash(secretkey(patterns)) ∪ Z_r, e (α, β) $^{\theta}2$} (6)

Encrypt Phase (PUK, Attributes, and Policies): Input to the algorithm is plaintext message (M) and output is ciphertext. Select a random number r in p–integer modulo Z with the polynomial function and sets q(R,0)=r. q(x,0)=q(parentnode(x,index)) for intermediate nodes. Let L be the set of leaf nodes in access tree structure, then the ciphertext is generated based on the given access tree structure T as:

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Ciphertext (C) = {Fill_AccessTree(Policies, s Є Z_r ,PUK), for all x Є X:$C_x = k^{q(x,0)}$, $C^1_x = H(A(x))^{q(x,0)}$, m.o,h Є PUK} (7)

KeyGen Phase (Attributes, Public Key, Master Key): Output of this algorithm is a private key (PrK) using the attributes' set (A).

Input is set of attributes A, H (sharedkey) and output. This algorithm selects a random number r and $rand_j$ for each attribute A_j and these random numbers are selected as the factor of H (sharedkey) and holds in Z_p.

SecretKey (SK) = {r_j ϵ Zr, hs ϵ hash(attributes), hs. $r_{j,D=} g_P$ ϵ PK} (8)

Decrypt Phase: It accepts private key (SK), attributes set (A)), cipher-text (C, embedded with the access structure (T)), and public key (PUK) as input. A recursive procedure is executed with three parameters ciphertext, secret key, attributes set and the node x from access tree T.

IV. RESULTS

Access control mechanisms is to restrict the actions of users or programs. Reference Monitor enforces Access policies. In the cloud server, each instance communicates with the centralized database to detect whether the user accessing data is authorized or not. Public-key approaches are computationally easy for user's in order to construct their own cryptographic keys. These keys are generally used in the process of encryption and decryption. It is quite infeasible to disclose the secret key by knowing the public key. SFM-CPABE model is executed using real-time Amazon Ec2 cloud server with multiple cloud instances. Figure 3 describes the pattern evaluation process of the grayscale fingerprint image. Different levels of patterns are visualized. Input fingerprint image is binarized and thinned for pattern extraction.

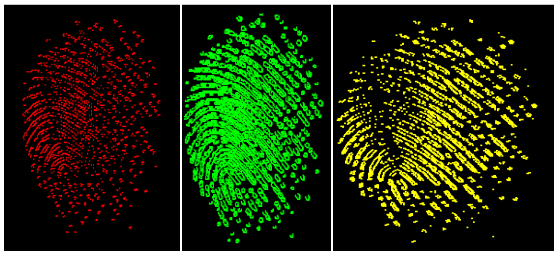

Fig 3. Fingerprint Pattern Evaluation Results

Figure 4 illustrates the fingerprint minutiae extraction process to find the essential patterns for generating access policy. Outlier points are eliminated using the pattern extraction method.

Fig 4. Final Fingerprint Minutiae Extraction

Table 1 Illustrates the performance of SFM-CPABE model to the traditional Attribute-Based Encryption (ABE) algorithms. SFM-CPABE model has less computational time compared to the traditional models.

Table 1. Computation Time of Various Attribute Based Algorithms compared with Proposed SFM-CPABE

KPABE (ms)	FHABE (ms)	Hash based KPABE(ms)	SFM-CPABE (ms)
766.614	692.356	591.051	356.923
725.743	768.307	633.099	326.105
849.538	727.958	559.974	360.164
750.876	751.237	423.07	366.863
719.108	829.709	425.777	330.759
774.168	768.612	668.534	336.591
754.32	716.689	648.873	367.981
708.655	752.422	474.115	330.519
768.952	690.069	401.31	338.341
813.004	768.258	556.947	376.516
700.798	799.551	481.05	338.489
853.635	700.205	508.461	344.768
831.898	778.367	572.965	356.173
826.784	720.62	450.971	348.144
719.751	684.12	477.005	327.792
788.252	819.767	412.16	377.487
879.406	705.091	645.005	389.681
808.638	804.47	656.607	323.396
709.872	704.185	586.741	389.602
740.515	731.056	403.438	371.554
777.297	696.665	619.014	389.008
810.077	769.518	651.31	353.016
749.003	704.939	424.865	376.911
866.095	723.124	602.137	345.49
804.379	788.075	462.737	328.835

Figure 5 illustrates the performance of SFM-CPABE model to the traditional ABE algorithms. From the figure, computational time of proposed model is less when compared to traditional models. Using statistical P value and test statistics, the null hypothesis is rejected and the alternative hypothesis is accepted in all the cases. So, can conclude that SFM-CPABE model is better than traditional ABE models in terms of time taken to encrypt and decrypt.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

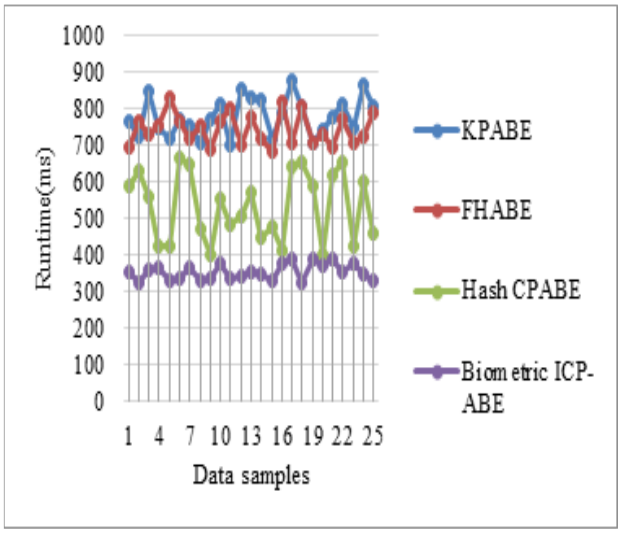

Fig 5. Performance Analysis

Table 2 describes the comparison of SFM-CPABE model to the existing integrity algorithms. Compared to traditional algorithms SFM-CPABE model has better integrity value

Table 2. Comparison of Several Integrity Algorithms with Proposed SFM-CPABE model for various sizes of Data

DataSize	MD5	SHA-256	SHA512	SHA-1024	Whirlpool	SFM-CPABE
10KB	113	102	111	109	118	128
20KB	109	96	107	118	123	135
30KB	115	104	119	127	129	137
40KB	114	106	121	124	118	143
50KB	117	99	123	117	126	132

Table 3 describes the communication time of SFM-CPABE model to the existing models in terms of time taken to communicate with the cloud server for data storage.

Table 3. Performance analysis of SFM-CPABE Model to the Traditional Models in Terms of Time taken to Communicate with the Cloud Server

Data size(KB)	CP-ABE(ms)	KPABE(ms)	Homomorphic CP-ABE(ms)	Biometric Based ICP-ABE(ms)
50	435	385	367	353
100	963	734	715	708
150	1483	1286	1183	1059
200	1963	1796	1693	1606
250	2535	2386	2304	2259
300	2856	2719	2704	2678
500	3363	3145	3109	3003

The accuracy of the proposed model is defined as the ratio of a number of bytes that are encrypted in the encryption process to the number of bytes that are decrypted from the cloud server.

V. CONCLUSION

In this paper, the Novel SFM-CPABE model is implemented on cloud data to enhance security against third-party attacks. In this model, the Fingerprint extraction technique, Biometric integrity algorithm, and Biometric Integrity based cipher-text policy attribute-based encryption (CPABE) are implemented on the cloud data. Experimental results on different sizes of cloud data show that SFM-CPABE model has low computational time, high efficiency and accuracy compared to the traditional cloud security models.

REFERENCES

1. N. Kaaniche and M Laurent, "Data Security and Privacy preservation in Cloud Storage Environments based on Cryptographic Mechanisms", Preprint submitted to Computer Communications, Vol. 111, no. 1, **(2017)**, pp. 1-70.
2. C. Guo, N. Luo, Md. Z. Bhuiyan, Y. Jie, Y. Chen, B. Feng and M. Alam, "Key-Aggregate Authentication Cryptosystem for Data Sharing in Dynamic Cloud Storage ", Future Generation Computer Systems, Vol. 86, no. 1, **(2017)**, pp. 1-29.
3. A. Alabdulatif, H. Kumarage, I. Khalil and X. Yi, "Privacy-Preserving Anomaly Detection in Cloud with a lightweight Homomorphic Approach", Preprint submitted to Journal of Computer and System Sciences, Vo. 90, no. 1, **(2017)**, pp. 1-41.
4. Q. Huang, Y. Yang and M. Shenc, "Secure and efficient data collaboration with hierarchical attributebased encryption in cloud computing ", Future Generation Computer Systems, Vol. 72, no.1, **(2016)**, pp. 1-28.
5. X. Liu, Q. Liu, T. Peng and J. Wu, "Dynamic Access Policy in Cloud-Based Personal Health Record (PHR) Systems", Preprint submitted to Information Sciences, Vol. 379, no. 1, **(2016)**, pp. 1-39.
6. V. Odelu, A. K. Das, Y. S. Rao, S. Kumari, M. K. Khan, K. R. Choo, "Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment ", Preprint submitted to Elsevier, Vol. 54, no. 1, (2016).
7. M. Sookhak, F. R. Yu, M. K. Khan, Y. Xiang and R. Buyya, "Attribute-based data access control in mobile cloud computing: Taxonomy and open issues", Future Generation Computer Systems, Vol. 72, no. 2, **(2016)**, pp. 1-14.
8. S. Souza and R. S. Puttini, "Client-side encryption for privacy-sensitive applications on the cloud ", Procedia Computer Science 97, Vol. 97, no. 1, (2016), pp. 126-130.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

9. X. A. Wang, F. Xhaf, W. Cai, J. Ma and F. Wei, "Efficient privacy preserving predicate encryption with fine-grained searchable capability for Cloud storage", Computers and Electrical Engineering, Vol. 56, no. 1, **(2016)**, pp. 1-13, V 56(1).
10. G. Kalpana, P. V. Kumar, S. Aljawarneh and R. V. Krishnaiah, "Shifted Adaption Homomorphism Encryption for Mobile and Cloud Learning", Computers and Electrical Engineering, Vol. 65, no. 1, **(2017)**, pp. 1-18.
11. B.Tirapathi Reddy, Dr.M.V.P.Chandra Sekhara Rao, Performance evaluation of various data deduplication schemes in cloud storage, IJPAM, Vol. 116, no.5, 2016, pp. 175-180.
12. B.Tirapathi Reddy, Dr.M.V.P. Chandra Sekhara Rao, "Data deduplication in cloud storage using dynamic perfect hash functions", Journal of Advanced Research in Dynamical and Control Systems, Vol. 9, no. 12, **(2017)**, pp. 2121-2132.

AUTHORS PROFILE

Mrs. Ruth Ramya Kalangi is a Research Scholar in the department of Computer Science and Engineering, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India. She is currently Assistant Professor in the department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India. Her research interests are Biometrics, Network Security and Wireless Sensor Networks.

Dr. M.V.P. ChandraSekhara Rao received his Ph.D. degree in Computer Science and Engineering from the Jawaharlal Nehru Technological University, Hyderabad. He is currently Professor in the Department of Computer Science and Engineering, RVR & JC College of Engineering, Guntur, Andhra Pradesh, India. His research interests are Data Mining, Big Data Analytics and Privacy Preserving in Data Mining..

A. Equations

Number equations consecutively with equation numbers in parentheses flush with the right margin, as in (1). First use the equation editor to create the equation. Then select the "Equation" markup style. Press the tab key and write the equation number in parentheses. To make your equations more compact, you may use the solidus (/), the exp function, or appropriate exponents. Use parentheses to avoid ambiguities in denominators. Punctuate equations when they are part of a sentence, as in

(1)

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)