ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

Performance and Efficiency Analysis of Cipher-Text Policy Attribute Based Encryption

Jiji Sasidharan[1], Dipin Krishnan R[2]

M.Tech Scholar, Dept. of ECE, JECC, Thrissur, Kerala, India[1]

Asst. Professor, Dept. of ECE, JECC, Thrissur, Kerala, India [2]

ABSTRACT: Ciphertext policy attribute based encryption (CP-ABE) is a promising cryptographic technique which is being widely used in many cyber physical systems and IoTs for guaranteeing information security. In order to improve the efficiency and performance, this paper discuss on two techniques. One technique concentrates on key management, by proposing a collaborative key management protocol in CP-ABE. This protocol realizes distributed generation issue and storage of private keys without adding any extra infrastructure. The proposed system solves key escrow and key exposure problems effectively. In addition it provides a fine grained and immediate attribute revocation for key update. Other is based on making a change to the access structure and presents a new CP-ABE system based on the ordered binary decision diagram. In this system it reduces the size of the keys, fast encryption and decryption stages and also resists collision attacks.

KEYWORDS: Ciphertext, Attribute Based Encryption Ordered binary decision diagram, Key management, Key escrow, Access structure, Access policy.

I. INTRODUCTION

With the rapid exposure in the network technology and large-scale networks, data sharing has became a part of our daily routine. In these network scenarios, users and nodes are distributed in different regions. Thus a data owner often needs to maintain a one-to-many relationship and provide services to more than one unknown user. The data being shared should be secured in order to avoid the unwanted access from outsiders. For ensuring security we can encrypt the data before sharing. Encryption is the technique of converting the data into such a way that only authorized people can access the data. Now-a-days ensuring effective information security is a big challenge in the data sharing concept. Encryption can be either symmetric cryptography (Private Key) or asymmetric cryptography (Public key). Symmetric cryptography or private key encryption has been used since ancient Egyptian times. This technique uses a secret key to encrypt the data into unintelligible form. The recipient should have the secret key to decrypt the data [11]. Asymmetric cryptography or public key encryption is more sophisticated encryption technique that is being widely used. In this technique two keys are used, public key of the receiver is used to encrypt the data and secret key of the receiver is used to decrypt the data. Thus this technique ensures the secure communication between sender and receiver without any prior key exchange. But in systems like IoT there are multiple users, thus if public key encryption is used then the overhead in encryption, key generation, management and maintenance will be very large. Hence we move on to a more favorable system which overcomes these limitations that is Attribute Based Encryption (ABE) [19].

In ABE, a single key can decrypt different ciphertexts or different keys can decrypt the same ciphertext. ABE is a type of public key encryption in which the secret key and ciphertext are dependent on attributes and decryption is possible if and only if set of attributes of user key matches the ciphertext attributes. [11]. ABE is broadly divided into two 1) Key policy ABE (KP-ABE).2) Ciphertext policy ABE (CP-ABE) .In KP-ABE, user's secret keys are generated based on an access tree that defines the privileges scope of the concerned user, and data are encrypted over a set of attribute. In CP-ABE, encryption is done with the help of an access structure and decryption can be done if and only if

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

receiver's attribute set meets access structure requirements. An example for CP-ABE is given in Fig 1. [12].CP-ABE is well suited for encryption and decryption of shared messages in large scale networks. Thus it can be applied in network scenarios like IoT. However by modifying the representation of access policies, we can improve the efficiency of encryption and decryption. Several access structures have been proposed to represent access policy but still the efficiency and flexibility are not ideal. In this paper we will discuss about two techniques and compare its features to reach to a new technique with better performance and efficiency. Among that one technique is to generate the access structure based on an Ordered Binary Decision Diagram (OBDD). This structure supports both positive and negative attributes without increasing system overhead; it also supports multiple occurrences of attributes and supports all Boolean functions. Thus a new CP-ABE scheme based on this structure provides an improved efficiency in terms of encryption, key generation and decryption, resists collision attacks and is CPA secure under the decisional bilinear Diffie-Hellman (DBDH) assumption.

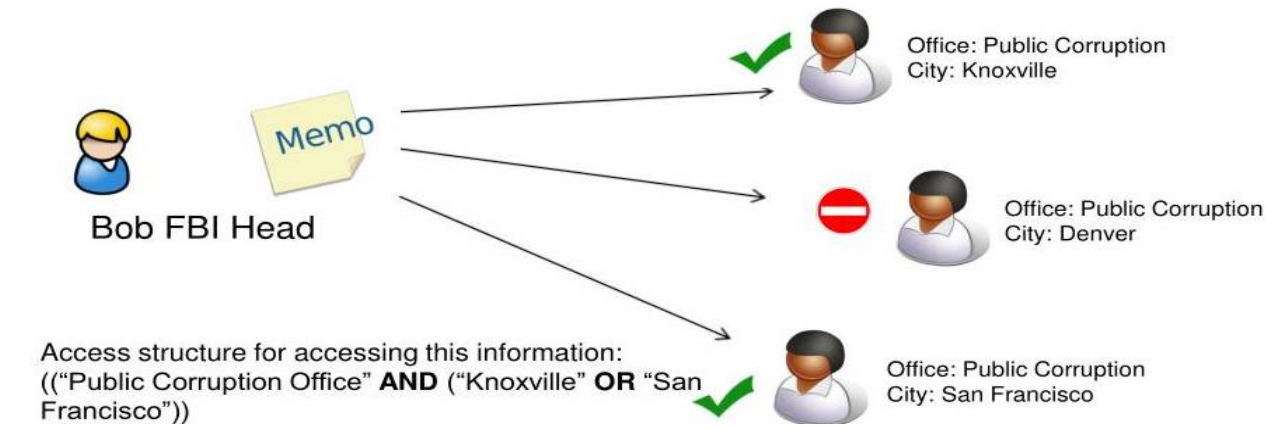

Fig 1 An example for Ciphertext policy Attribute Based Encryption

There are some limitations in ABE like the key authority must be completely trustworthy otherwise it can decrypt all the ciphertext without any permission from the data owner which is called as key escrow problem and this threatens user's privacy. With the growth of mobile applications, mobile front end devices such as smart phones are more vulnerable towards the privacy protection. The vulnerability in privacy protection leads to key exposure. Hence we propose another technique which is a novel collaborative key management protocol (CKM) in CP-ABE that aims at enhancing security and efficiency in key management. This model ensures security against key escrow, key exposure and provides data confidentiality and resists collision attack.

The rest of this paper is organized as follows. Two techniques are summarized in Section II. The performance analysis and results obtained are compared in section III. Conclusions and recommendations for future work are provided in section IV.

II. RELATED WORK

a) A COLLABORATIVE KEY MANAGEMENT PROTOCOL IN CIPHERTEXT POLICY ATTRIBUTE BASED ENCRYPTION FOR CLOUD DATA SHARING

In 2017 Lin, Guofeng, Hanshu Hong, and Zhixin Sun proposed a collaborative key management protocol [11]. In this they have concentrated on enhancing security and efficiency of key management in cloud data sharing system.

Model Of CKM-CP-ABE For Cloud Data-Sharing

The model of this system is shown in Fig. 2. As depicted, five entities are involved in cloud data sharing[11].There is an assumption that no collision of entities with each other in data sharing to access the data illegally, otherwise the scheme will be unavailable and meaningless. Authentication of attributes is done by the Key Authority (KA). The KA in collaboration with a Cloud Server (CS) generates a group of random elements included in public parameters which

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

represents all granted attributes. Let params be public parameters. When a Data Owner (DO) has an intention to share a data, it will encrypt the data using params and sent to form the initial ciphertext CTinit then it is uploaded to the KA. The initial ciphertext is being re-encrypted by the KA to form the ultimate ciphertext CTulti, which is sent to and stored in a CS. According to the Clients's (CL's) attribute set, three different components of the private key, namely, CPK_1, CPK_2 and CPK_3, each of which is kept by one of KA, CS or CL can be secretly generated with the help of the key management protocol simultaneously. When the data stored in the cloud is asked then the Decryption Server (DS) receives CPK_1 and CPK_2 to transform CT_{ulti} to CT ', finally the plaintext M from CT' is extracted using CL by its CPK_3. For CKM-CP-ABE in cloud data-sharing, plaintext can be extracted from the CTulti only if the all three private key components are known .It means a CL requires collaboration with the KA and CS for decrypting ciphertext.

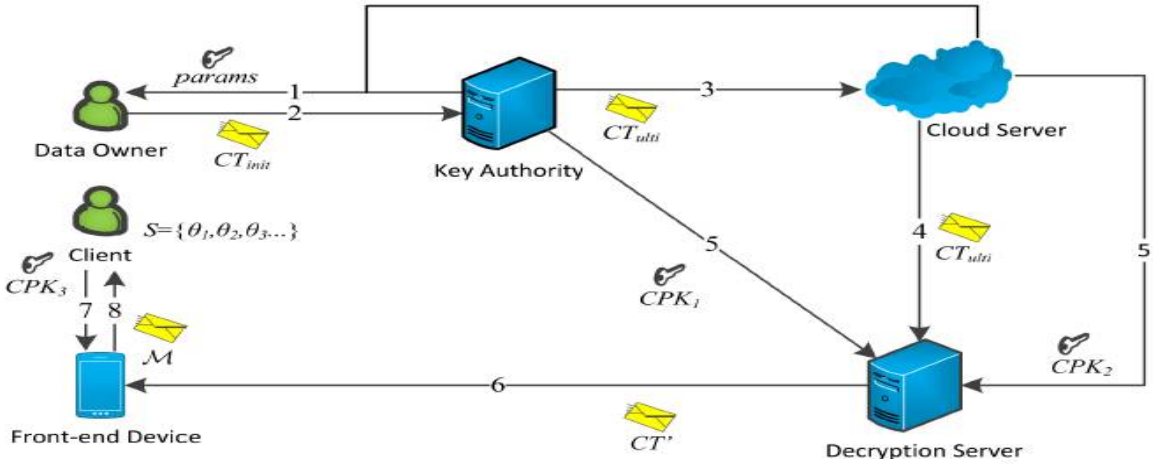

Fig 2.The model of CKM CP-ABE for cloud data sharing

Security Requirements:

- Data Confidentiality
- Backward And Forward Secrecy
- Collusion Resistance
- Key Escrow Free
- Key Exposure Free

b) A CIPHERTEXT – POLICY ATTRIBUTE BASED ENCRYPTION BASED ON AN ORDERED BINARY DECISION DIAGRAM

In 2017 Li, Long, et al propose the CP-ABE based on Ordered Binary Decision Diagram (OBDD) [12]; in this approach the access structure is based on an OBDD. This paper proposes a non-monotonic, expressive and flexible access structure. Without increasing system overhead, this structure supports both positive attributes and negative attributes; it also supports multiple occurrences of attributes and all Boolean operations such as AND, OR and NOT between attributes. Based on the above access structure, a new CP-ABE scheme is proposed which offers better performance in terms of encryption, key generation and decryption, resists collusion attacks and is CPA secure under the decisional bilinear Diffie-Hellman (DBDH) assumption.

Access Structure:

The essence of an access policy is a rule R that returns 1 or 0 according to the state of an attribute set S. The rule R will return 1 if and only if S satisfies R, written as $S \vDash R$, and 0 is returned by R when S does not satisfy R, written as $S \nvDash R$. [Access structures are intuitive expressions of access policies and have several mathematical forms, such as Boolean expressions and threshold gates [4], [14], [18]. Threshold gates are the most common form of access structures, by

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

which the access policies can be described as element matches between two attribute sets. AND gates [5], [10] are another frequently used form of access structure.

CP-ABE Framework:
A common framework of CP-ABE contains four algorithms:
Setup, the algorithm is executed by the authority in charge of the generation of the public key PK and master key MK.
Encrypt, the algorithm is executed by the data owner to encrypt plaintext M.
Keygen, the algorithm is executed by the authority and generates a secret key SK according to the attribute set S provided by a user.
Decrypt, the algorithm is executed by the data user to decrypt a ciphertext CT with a pre-generated secret key.

DBDH Assumption:
Let e be a bilinear map e: G0×G0→G1. Let a, b, c, z be chosen randomly from Z_p and g be a generator of G_0. The DBDH assumption can be described as follows: no probabilistic polynomial-time adversary can distinguish the tuple $(g^a, g^b, g^c, e(g, g)^{abc})$ from the tuple $(g^a, g^b, g^c, e(g, g)^z)$.
For any probabilistic polynomial-time adversary A, the advantage in solving the DBDH problem is defined as follows:

$$Adv^{G_0}_{DBDH}(A) = |\Pr[A(g, g^a, g^b, g^c, e(g, g)^{abc})=1] - \Pr[A(g, g^a, g^b, g^c, e(g, g)^z)=1]|.$$

The DBDH assumption holds if $Adv^{G_0}_{DBDH}(A)$ is negligible.

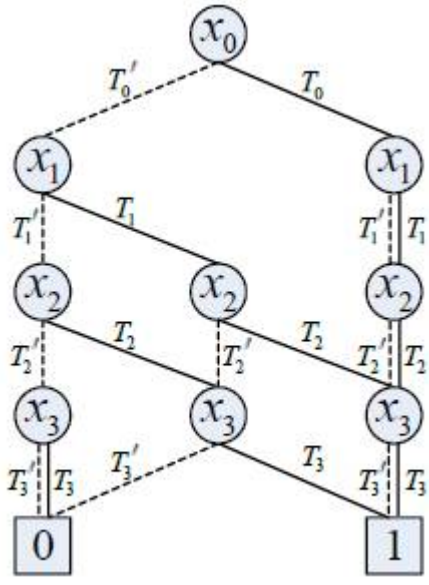

Fig 3. OBDD representation of $f_1(x_0,x_1,x_2,x_3)$

OBDD based access structure:
First, obtain the Boolean function of an access policy. We assume that all of the attributes appearing in the access policy are numbered as i ($0 \le i \le n-1$) in a pre-defined sequence and represented by x_i ($0 \le i \le n-1$), in which n is the total number of attributes. Then, the access policy can be converted into a Boolean function $f(x_0, x_1, x_{n-1})$. All Boolean functions can be transferred to basic logical operations between variables (i.e., AND, OR and NOT). The construction of *OBDDs* used to represent Boolean functions is completed by applying a simple recursive process. As Shannon's expansion theorem shows, $f(x_0, x_1, \ldots, xn\text{-}1) = xi \cdot f|xi=1 + xi' \cdot f|xi=0$ ($0 \le i \le n-1$). After the construction, all of the nodes contained in OBDD should be numbered to obtain the final expression: OBDD={ $Node^i_{id}$ | id ϵ ID, I ϵ I}, in which ID

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

is a set that contains all of the serial numbers of non-terminal nodes and I is a set formed by all of the attributes appearing in the access structure. $Node_{id}^{i}$ is a tuple <id, i, high, low>, in which id is the serial number of current node, i is the serial number of the attribute contained in current node, high is the serial number of the 1-branch node, and low is the serial number of the 0-branch node. The parameters high and low are used to maintain the relationships between parent nodes and child nodes. The nodes with serial numbers 0 (i.e., 0) and 1 (i.e., 1) have fixed meanings and the i, high and low domains of these two special nodes are meaningless, so these nodes are deleted in OBDD-based access structures to reduce the storage cost.

Let OBDD be an access structure and S be an attributes set. Starting from the root, a comparison based on the values of attributes is made as follows: for a non-terminal node with attribute i, if the attribute valued 1 is contained in S, the comparison will be delivered to the 1-branch node; otherwise, the comparison must be delivered to the 0-branch node. The above process is executed repeatedly until one of the terminal nodes is reached. If the terminal node 1 is finally reached, the set S satisfies the OBDD, denoted by S⊨OBDD. On the contrary, the set S does not satisfy the OBDD, denoted by S⊭OBDD.

Example: *Access policy 1: Users who own attribute x*0 *or any two attributes among* {*x*1, *x*2, *x*3} *can finish the decryption successfully.*

Access policy 1 contains a threshold gate T (2, 3). According to access policy 1 and the above method used to obtain the Boolean function of an access policy, the corresponding Boolean function obtained is f1(x0, x1, x2, x3) =x0+x1x2+x1x3+x2x3. Let the variable ordering be π: x0<x1<x2<x3; then, the OBDD of the Boolean function f1(x0, x1, x2, x3) =x0+x1x2+x1x3+x2x3 is constructed according to Shannon's expansion theorem. Secondly, all of the nodes should be renumbered from top to bottom and left to right to obtain the final expression as OBDD = { $Node_{id}^{i}$ | id ϵ ID, I ϵ I}.The access structure is finally described as OBDD= {Node20, Node31, Node41, Node52, Node62, Node72, Node83, Node93, Node10 3}. A valid path: In OBDD, each path derived from root and ended at terminal node 1 is called a valid path, denoted by root→1. For example, in Fig. 4, the path (x0→x1→x2'→x3'→1) is a valid path, but the path (x0'→x1'→x2'→x3→0) is not a valid path.

III. RESULTS OBTAINED

In terms of efficiency, we compare the proposed CKM-CP-ABE with OBDD based CP-ABE .We summarize the efficiency comparison with respect to public key, ciphertext, and private key size in Table. 1. For CKM-CP-ABE, the public key size is $(\phi+1)|G_0|+|G_1|$, which is larger than OBDD scheme. CKM CP-ABE key requires a tuple of random elements h_1, h_2, hm respectively associated with each authorized attribute. The CKM-CP-ABE ciphertext size is $(\phi+1)|G_0|+|G_1|+|G_2|$ which is also larger than OBDD scheme. The private key size of CKM-CP-ABE is $|Z_{ap}|+(|S|+2)|G_0|$ whereas private key size of OBDD based scheme is only $2|G_0|$.Thus OBDD produces an efficient key size as compared to CKM technique. The total decryption overhead CKM-CP-ABE has heavy total decryption overhead. Introducing the attribute group mechanism adds more exponentiation and multiplication calculation to scheme. Due to the collaborative mechanism, however, we decrease client decryption overhead dramatically. Authorized CLs in our scheme require only one exponentiation calculation and one division calculation because the DS undertakes enormous computation without any knowledge leakage.

Differed from [5], CKM-CP-ABE not only outsources decryption but also provides a collaborative mechanism with reliable security. To explain the capacities and efficiency of our scheme in the representation of access policies, the most frequently used access structures, threshold gates [2], [9] and AND gates [5] will be analysed along with our scheme in the following example. The AND gates do not possess the skills to describe the *f*2(*x*0, *x*1, *x*2), so it will not be discussed in this aspect. The threshold gates are relatively simple, which means more variables and nodes must be employed to describe Boolean functions. For example, *f*2(*x*0, *x*1, *x*2) is described in disjunctive form, in which two different values (*xi*, *xi'*) (*i*=0, 1, 2) of each variable are located in multi parts of the given disjunction. Since the two values cannot be represented by a single variable of threshold gates, the number of variables and nodes used to

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

construct the structure must be multiplied. Besides, since the reciprocal relationship between *xi* and *xi'* is broken, *xi* and *xi'* are two entirely independent variables, which means the NOT operation cannot be supported by threshold gates.

Since the nodes numbered 0 and 1 are deleted to reduce the storage cost, the number of nodes in OBDD representation is less than that of threshold gates representation. More importantly, only three variables are needed, only half of that in threshold gates representation. To give a more intuitive comparison, the Table 2 is listed below, which indicates that our scheme can not only support all kinds of Boolean operations but also achieves a much better overall performance.

System	Public key size	Ciphertext size	Private key size
CKM-CP-ABE	$(\Phi+1)$ $\|G0\|+\|G1\|$	$(\Phi+1)\|G0\|+\|G1\|+\|G2\|$	$\|Zp\|+(\|S\|+2)\|G0\|$
OBDD	$\|G0\|+\|G1\|$	$(T+1)\|G0\|+\|G1\|$	$2\|G0\|$

Table 1 Key size comparison between CKM CP-ABE and OBDD CP-ABE

In terms of further measuring the performance in encryption and decryption of CP-ABE, the following indicators are used: complexity of key generation, encryption and decryption, ciphertext size and secret key size. In the measurement of complexity, the number of exponentiation steps in $G0/G1$ and the number of bilinear pairings have more significance, since these operations require much more time than other operations in both encryption and decryption. The meaning of each symbol is as follows: Φ is the number of attributes contained in the access structure, l is the number of attributes used to generate private user keys, T is the number of valid paths contained in our OBDD access structure, σ is the least number of attributes used to decrypt successfully, and B_{G0} and B_{G1} represent the size of each element contained in group $G0$ and group $G1$, respectively.

Indicator/scheme	AS	AND	OR	Threshold	NOT	Var No.	Nodes No.
LN[3]	AND gate	√	×	×	×	\	\
BSW[4], RD[6]	Thresh-old gates	√	√	√	×	6	10
Our scheme	OBDD	√	√	√	√	3	6

Table 2 Capacities Analysis and Comparison of OBDD technique

Both the time complexity of the ***KeyGen*** algorithm and the ***Decrypt*** algorithm are O(1); in particular, the ***KeyGen*** algorithm only needs two exponentiations in $G0$, and the ***Decrypt*** algorithm only needs two exponentiations in $G1$ and two bilinear pairings computations. Besides, the size of a secret key is a constant, rather than a function of the number of attributes. These features will greatly reduce the burden of authority in generating secret keys, reduce the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

communication traffic between authority and decryptor, and realize fast decryption. Besides, the complexity of the ***Encrypt*** algorithm and the size of ciphertext relate to the number of valid paths contained in *OBDD*, rather than the number of attributes; these factors will improve the efficiency in encryption and sharing of ciphertext, especially when *T* is small.

IV. CONCLUSION

CKM CP-ABE is a protocol to enhance both security and efficiency of key management in CP-ABE for cloud data sharing system. But still high ciphertext size, encryption cost and decryption cost. **CP-ABE based on OBDD improves** efficiency & capacity, reduces computation of the KeyGen algorithm, the size of secret key and computation of the Decrypt algorithm to constants. The efficiency of the Encrypt algorithm and the size of ciphertext can also be improved**.** As a future scope we can make full use of the access structure based on OBDD and apply it to CKM –CP ABE, a more efficient encryption technique with assured security can be realized with lots of follow-up such as

- Attribute management
- User revocation
- Reduced keygen ,encryption, decryption and key size
- Key escrow free
- Key exposure free
- Data confidentiality

REFERENCES

[1]. A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in EUROCRYPT 2005, Aarhus, DK, 2005, pp. 457-473, 2005.
[2]. V. Goyal, O. Pandey, A. Sahai, et al., “Attribute-based encryption for fine-grained access control of encrypted data,” in ACM CCS 2006, New York, USA, 2006, pp. 89-98, 2006.
[3]. C. Ling and C. Newport, “Provably secure ciphertext policy ABE,” in ACM CCS, New York, USA, 2007, pp. 456-465, 2007.
[4]. J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext- policy attribute-based encryption,” in IEEE SP 2007, Oakland, CA, USA, 2007, pp. 321–334, 2007.
[5]. C. Ling and C. Newport, “Provably secure ciphertext policy ABE,” in ACM CCS, New York, USA, 2007, pp. 456-465, 2007.
[6]. Y. S. Rao and R. Dutta, “Dynamic Cipher text-Policy Attribute-Based Encryption for Expressive Access Policy,” in ICDCIT 2014, Bhubaneswar, India, 2014, pp.275-286, 2014.
[7]. S. B. Akers, “Binary Decision Diagrams,” IEEE Trans. Comput.ers, vol. 27, no. 6, pp. 509-516, Jun. 1978.
[8]. R Drechsler and D Sieling, “Binary decision diagrams in theory and practice,” Int. J. Software Tools Technol. Transfer, vol.3, no. 2, pp. 112-136, May. 2001.
[9]. Y. S. Rao and R. Dutta, “Dynamic Ciphertext-Policy Attribute-Based Encryption for Expressive Access Policy,” in ICDCIT 2014, Bhubaneswar, India, 2014, pp.275-286, 2014.
[10]. Z. Zhou, D. Huang and Z. Wang, “Efficient privacy- preserving cipher text-policy attribute based-encryption and broadcast encryption,” IEEE Trans. Comput.ers, vol. 64, no. 1, pp. 126-138, Oct. 2013.
[11]. Lin, Guofeng, Hanshu Hong, and Zhixin Sun. "A Collaborative Key Management Protocol in Ciphertext Policy Attribute-Based Encryption for Cloud Data Sharing." *IEEE Access* (2017).
[12]. Li, Long, et al. "A Ciphertext-Policy Attribute-Based Encryption Based on an Ordered Binary Decision Diagram." *IEEE Access* 5 (2017): 1137-1145.
[13]. M. S. Ahmad, N. E. Musa, R. Nadarajah, R. Hassan, and N. E. Othman,``Comparison between Android and iOS operating system in terms of security," in *Proc. CITA*, Jul. 2013, pp. 1_4.
[14]. V. Goyal, O. Pandey, A. Sahai, and B.Waters, ``Attribute-based encryption for _ne-grained access control of encrypted data," in *Proc. ACM CCS*, 2006, pp. 89_98.
[15]. H. T. Dinh, C. Lee, D. Niyato, and P. Wang, ``A survey of mobile cloud computing: Architecture, applications, and approaches," *Wireless Commun. Mobile Comput.*, vol. 13, no. 18, pp. 1587_1611,Dec. 2013.
[16]. X. Yao, Z. Chen, and Y. Tian, ``A lightweight attribute-based encryption scheme for the Internet of Things," *Future Generat. Comput. Syst.*, vol. 49, pp. 104_112, Aug. 2015.
[17]. B.Waters, “Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization,” in PKC 2011, Berlin, Germany, 2011, pp. 53-70, 2011.
[18]. A. Balu and K. Kuppusamy, “An expressive and provably secure Ciphertext-Policy Attribute-Based Encryption,” Inf. Sci., vol. 326, no. 4, pp. 354-362, Aug. 2014.