International Journal of Research in Advent Technology (IJRAT) Special Issue
E-ISSN: 2321-9637
Available online at www.ijrat.org
*International Conference "*INTELINC 18*", 12th & 13th October 2018*

Safe & Secure Ciphertext Policy Attribute Based Encryption To Avoid Suicidal Games nn Entering Whatsapp or Mobile Like Bluewhale Game or Momo Challenge

S.Porkodi, ME – Final Year
Department of Computer Science and Engineering
Dr.Sivanthi Aditanar College of Engineering
Tiruchendur
ishwaryaporkodi6296@gmail.com

D.Kesavaraja, Assistant Professor
Department of Computer Science and Engineering
Dr.Sivanthi Aditanar College of Engineering
Tiruchendur
dkesavraj@gmail.com

Abstract— Now-a-days there are lots of application are been used by the people. While using an application, a user's data is to be protected. So encryption is used in many applications when the data is transferred from one place to another. More over in order to register in an application either phone number or email id is used commonly and so a single user may have many accounts which cannot be identified. So some hackers use this as advantage and use some application as the medium to give threat and harm to the other users and the main problem is that we cannot find the real culprit as they use some fake information to create the account. In this paper, we propose an encryption algorithm based on user attributes, called ciphertext policy attribute based encryption. With this algorithm in use we can find the culprit who is misusing the application. Also we can add that person to the blacklist and all the accounts associated with that identity can also be blacklisted.

Keywords – Blacklist, Ciphertext policy attribute based encryption (cp-abe), Data transfer, Security, Whatsapp

1. INTRODUCTION

Many application uses encryption for the secure transfer of data from one place to another. End to end encryption is used in whatsapp, when using this photos, videos, voice messages, documents, status updates and calls are secured from falling into wrong hands. Even though now a days, there are lot of hackers using whatsapp as medium to spread malwares via whatsapp to be installed on to the mobile device which in turn sends data from our mobile to the hacker through whatsapp. Even some malware are used to hack the mobile's front camera to get a detailed information, photos and videos of the users. These hackers are hard to find since they use several different numbers and they does not have a unique user Id to be tracked. To avoid these types of hacking, usage of ciphertext policy attribute based encryption can be used. So that when a data is been encrypted and transferred from one user to another only they both can see the actual text and others cannot hack the data from the whatsapp. The same technique can be used in mobile too, which ensures that the data from the mobile can be only seen to the person to whom the data is transferred to. As the CP-ABE encryption uses the attributes of the user to encrypt data only that particular user will have the permission to access the data by matching their attribute. Whereas others who try to hack the datas will not have the attribute of that particular user and thus they cannot get the actual data and it is hard to hack. This algorithm can also be used to deduct the person who is illegally using the applications in a wrong way and we can also blacklist them. As unique Id is an attribute the different accounts using the same identity can also be blacklisted.

The main objective of the project is to encrypt user identity and to protect their data and privacy. Then to blacklist the user when the user is doubted to involve in illegal activities, regulators can reveal the identity of the user and blacklist them.

This project can also be used in other applications like bitcoin system, ATM system and other systems to protect user's privacy and to track

the culprit who is trying to steal the user's bitcoins or user's cash.

National and International needs

BlueWhale Game

The **Blue whale** was a game which was played across over a wide range of nations in 2016. One among those nations was India. It was a "game" reportedly consisting of a different series of tasks given by the admin to the users over a 50-day period of time, initially introducing the player to the elements of self-harm and then the final challenge is to make the player to commit suicide. Throughout 2017 the media in India reported several child suicide cases, self-harm and attempted suicide cases linked to be a result of Blue Whale and to the response, the Government of India's Ministry of Electronics and Information Technology requested several internet companies (including Google, Facebook, and Yahoo) to remove all the links which diverts the users to the game. Some commentators blamed the government of creating a moral panic. Indian internet watchdog, the Centre for Internet and Society blamed the coverage of effectively spreading and advertising a "game" for which there was only a little evidence. The Supreme Court requested the Indian Central government to ban the game. But following that the Central government responded that since Blue Whale wasn't an application, so it couldn't be banned. If our project is made possible, we can get the identities of the people who threaten like this and so the person who is responsible for all these issues can be found therefore crimes and criminals can be avoided easily.

Momo Challenge

The **Momo Challenge** is a form of digital tormenting or cyber bullying that spreads through online social media and mobile phones. After the victims are subjected to contact a Momo account through social media network such as WhatsApp, they get realistic threats in forms of image, text and they are threatened to perform a series of dangerous tasks. This may also include hacking the victim's phone. The Momo Challenge relies entirely on threats just to get the victims to perform deadly tasks. Focusing on young people, Momo relies on Whatsapp messages to convince common young people as victims to use their mobile phone to contact one of different Momo account phone numbers. Whoever has set up the account then repeatedly threatens the victim to make personal and private information public, or threaten to harm on their family members, unless a series of tasks is completed. Some victims are even threatened with supernatural harm such as magical curses. These threats and the corresponding communications are often done with the help of disturbing, scary or aggravating images. If our project is made possible, we can get the identities of the people who threaten like this and so crimes can be easily avoided.

2. RELATED WORKS

In this session, we can see about the attribute based encryption and a brief overview on existing ciphertext policy attribute based encryption with access control schemes.

Attribute Based Encryption

Attribute Based Encryption is a type of encryption where the key values and the ciphertext depend on the attributes of the user which was first proposed by Goyal, Sahai and Waters[1]. Many applications use encryption to protect data where the data is protected but the identity of the illegal or problematic user cannot be deducted since the accounts in the application or registered mostly with mobile numbers or email ids. These details are not unique identities of the users and thus the culprits cannot be found. The challenges faced in attribute based encryption are key coordination, key escrow and key revocation and thus different types of attribute based encryptions were proposed. There are two types of attribute based encryptions they are Key-policy attribute based encryption and cipher text policy attribute based encryption.

Key Policy Attribute Based Encryption and Ciphertext Policy Attribute Based Encryption

In 2006, sahai and waters introduced attribute based encryption. Then it was classified into two where in KP-ABE[2], the encrypted data is based on the set of attributes and access rules which supports mono access tree where in cipertext policy attribute based encryption[3] (CP-ABE) the plain text is encrypted with access policy written by the encryptors and the user's private key is based on the set of attributes. The decryption is only done when the user attributes satisfies the access control policy of the ciphertext. The ciphertext policy attribute based encryption is used in this project since the access policy of a user can be determined by the data owner.

In 2011, for the flexible and scalable access zhiguo wan, jun'e Liu and Robert H. Deng proposed a system [4] with access control scheme which supports disjunction normal form (DNF) and conjuctive normal form (CNF) access control policy. But this system can't provide flexible access.

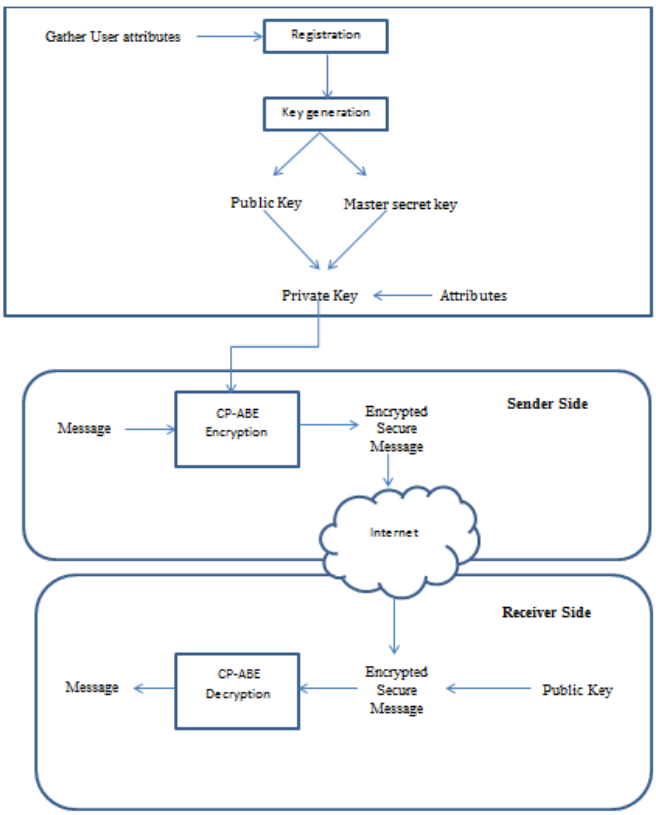
In 2011, an expressive, efficient and secure realization of cipher text policy attribute based encryption system [5] was proposed by Brent waters.

In 2014, for more flexible access, Hua Deng and team proposed a system [6] which is based on LSSS which enriches the expression of access control policy but this system has low efficiency in decryption phase.

In our paper we propose a Cipher text policy attribute based encryption to encrypt with the user's real identities with which fine grained access control can be achieved. If a user is reported to involve in cyber bulling or cybercrime then the account of that user and the accounts with same identity can also be blacklisted. Since same user can have different accounts but their identity will be same so it is easy to blacklist them by avoiding threats to the common people. As well as if any action is to be taken then that can also be done as now the identity of the user can be found if needed.

3. METHODOLOGY

Flow Chart



The purpose of our system is to make it possible to find the illegal user in the system. The main idea is to encrypt the users' identities using CP-HABE (Ciphertext Policy – Hierarchical Attribute based Encryption). Only the authorized regulation nodes have the correct key to the decrypted identities.

User Registration

The necessary attributes alone with a unique attribute is gathered from the users who are then registered into the application. As a user is registered, a key pair along with the account address is distributed to the user.

Key Pair Generation

The key pair of public key and master secret key (pk, msk) is generated with the attributes of the registered users. The public key is related with the user identity. This relationship is known only to the user and the server. When the identity of the user is identified to be valid then the key pair is distributed to the user. If a user is identified with fake identity then no key pair is generated. Some attributes are hashed with the key pair to produce a private key.

CP-ABE Encryption

When a user A sends message to another user B, the message gets encrypted with CP-ABE algorithm along with the access control policy and private key to produce an encrypted secured message as output. The encrypted message is passed through the internet to reach the receiver side from the sender side.

CP-ABE Decryption

When the user B receives the encrypted message, the public key which is based on the user attributes is used to decrypt the message and thus original text is obtained. The hackers who try to hack the message will not have the real attribute of that particular user and thus they cannot get the original message and it is hard to hack. This algorithm can also be used to deduct the person who is illegally using the applications in a wrong way and we can also blacklist them. As one unique Id is used as an attribute the different accounts using the same identity can also be blacklisted.

4. SAFE AND SECURE CP-ABE ENCRYPTION SYSTEM

The proposed CP-ABE Scheme

G and GT are two multiplicative cyclic groups of prime order p and e_2: G*G -> G_t be a bilinear map g is defined as generator of group G.

CP-ABE – Setup

The attributes are S = {w_1, w_2,.. w_N) where w_1, w_2,... $w_N \in Z_p$. The subscript N is the number of attributes in S which is divided into n trees according to the relationship. The depth of i^{th} tree is l_i and l = max $\{l_i\}_{i\in[1,n]}$ for i=1…n. Then choose a random element $u'_i \in G$ and random vector $U_i = (u_{i1}, u_{i2}, ... u_{li}) \in G^{li}$. Choose two random value α , a $\in Z_p$. The key pair is PK_{abe} (Public Key) and MK_{abe} (Master Secret Key).

$$PK_{abe} = (g, g^a, Y=e_2 (g, g)^{\alpha}, u'_1 \ldots u'_n, U_1 \ldots U_n)$$

$$MK_{abe} = g^{\alpha}$$

CP-ABE – KeyGen

The inputs of this algorithm are User's set of attributes ($S_u \subseteq S$) and Master Secret Key (MK_{abe}). The output of this algorithm would be the Private Key (SK_u). The key server takes the random number $r \in Z_p$ and computes $D = g^{\alpha + ar}$. Suppose if $w \subseteq S_u$ is an attribute in the i^{th} tree with depth k and path R(w) = (w_{i0},w_{i1},…w_{ik}) for every $w \subseteq S_u$, it computes $d_i = (u'_I \Pi^k_{\delta=1} u^{wi\delta}_{i\delta})^r$

$$SK_u = D = (g^{\alpha+ar}, D' = g^r, \{D_w\}_{\forall w\varepsilon Su})$$

Where,

$$D_w = \{d_i , d_{i,..k+1}\ldots., d_{ili}\}$$

$$d_{i\delta} = u^r_{i\delta} \text{ for } k+1 \le \delta \le l_i$$

CP-ABE Encryption

The input for performing encryption would be Public parameters (PK_{abe}), Message to be sent (m), Access structure (M,ρ), access policy (AP). Where, M is the matrix of d rows and e columns. P maps the σ^{th} row M_σ of matrix M to a certain attribute ρ(σ). The output will be cipher text (CT). Only users who have a set of attributes that satisfies the access structure can decrypt the message.

$$CT = (\check{C}, C, \{C_{\sigma1}, C_{\sigma2}\}_{\forall\sigma\varepsilon[1,d]})$$

$$C_{\sigma1} = g^{as\sigma} (u'_j \Pi^k_{\delta=1} u_{j\delta}^{w1/j\delta})^{-r\sigma}$$

$$C_{\sigma2} = g^{r\sigma}$$

$$\check{C} = mY^s$$

$$C = g^{-s}$$

Choose a secret value S $\in Z_p$ and some random elements $v_2 \ldots v_e$. Let $v = (s, v_2 \ldots v_e)^T$ be the column vector for σ = 1,2…d. $s_\sigma = M_\sigma . v$ where s_σ is the σ^{th} share of secret s. ρ(σ) = w' where attribute w' is in the j^{th} tree with depth k' and path of R(w') = (w'_{j0}, w'_{j1},… $w'_{jk'}$) then s_σ belongs to w' according to the map ρ. To encrypt message m, choose $r_\sigma \in Z_p$ for all σ = 1,2…d.

CP-ABE – Decryption

When a user attribute set matches the access policy of the cipher text then the user is the authorized user. If the authorized user with the secret key wants to decrypt the cipher text then the user should match

their attributes to find the minimum set S_u, which satisfies the access policy. The original message can be recovered by,

$$\frac{\check{C} \cdot e_2(C, D)}{e_2(D\ \Pi_{\sigma\varepsilon 1} C_{\sigma 1}^{\lambda\sigma} \Pi_{\sigma\varepsilon 1} e_2(d_i', g^{r\sigma})^{\lambda\sigma}}$$

$$= \frac{\check{C} \cdot e_2(C, D)}{\Pi_{\sigma\varepsilon 1}(e_2(D',\ C_{\sigma 1}) \cdot e_2(d_i', C_{\sigma 2})^{\lambda\sigma}}$$

$$= \frac{me(g,g)^{\alpha s} \cdot e_2(g^{-g}, g^{\alpha + ar})}{\Pi_{\sigma\varepsilon 1}(e_2\left(g^r, h^{s\sigma}\left(U_j' \Pi_{\delta=1}^{k} u_{j\delta}^{w'j\delta}\right)^{r\sigma}\right) \cdot e_2(d_i', g^{r\sigma}))^{\lambda\sigma}}$$

$$= \frac{m \cdot e_2(g,g)^{-ars}}{\Pi_{\sigma\varepsilon 1} e_2(g^r, h^{s\sigma})^{\lambda\sigma}}$$

$$= \frac{m \cdot e_2(g,g)^{-ars}}{\Pi_{\sigma\varepsilon 1} e_2(g^r, g)^{ars\sigma\lambda\sigma}}$$

$$= \frac{m \cdot e_2(g,g)^{-ars}}{(g^r, g)^{ars}}$$

$$= m$$

5. TECHNIQUES

Prevent Unauthorized Users with Unique ID

All the users should register the account with their unique user Id in order to prevent the unauthorized user access. For the unique user Id finger prints or iris scan or verified aadhar number can be used

Methodology for I*rrelevant Message Detection*

The application can maintain an ABE dictionary which consists of all malicious or irrelevant words to be muted. When a word is added to the muted list, the message consist of those words can generate an alert message for the user. Eg. If the word blue whale is added to the dictionary of muted list, a message with the word blue whale to the mobile generates alert message to the user.

Regular Communication Monitoring with SVM

The communication between the users is regularly monitored. To do this SVM classification in the data mining is used. This is done only to protect the users from the persons who try to harm large amount of users.

User's Data Access Permissions with Sessions

The user's profile picture, status and last seen are to be protected as the user need privacy. So sessions can be maintained for not giving other users access to the data of the user who updates the data.

6. CONCLUSION

For the secure transfer of data in the modern world encryption is used. In this paper we use ciphertext policy attribute based encryption in order to protect data privacy and also to find the people who are misleading other peoples or harassing and causing harm to other people in the name of game and challenge which sometime even lead the victim to suicide. As these criminals are not found till date, since their identities can't be recognized our society will soon be in danger. To avoid such conditions in future, ciphertext attribute based encryption can be used.

In order to obtain the security certain techniques has been implemented, such as to prevent unauthorized user we use unique ID such a finger prints or face recognition which are now commonly used in most of the mobile phones to unlock the mobile screen. To deduct the irrelevant or inappropriate messages we can use mute the words or block the words in order to avoid panic among public. As when a word is been added to the block list then if those words occur in the chat of the user or from a new number there will be an alert will be raised which will can be used to create alert and awareness among common people. Regular communication monitoring is also used to find if anyone is trying to harass people. The data which are shared among other people should have privacy as like one should not have access to download the display picture or status without the knowledge of the owner of the data.

In this paper, we propose the ABE encryption with access policy rights. In this system, the identity of the culprit or who cause harm to people can be found very easily with the help of their own verified attributes. Even if a person opens different accounts with the same attribute and that particular attribute is in the harm list then this new account will be in suspect list and this new account is also causing harm to the users them that account will also be blocked. If there involves any blackmails or threats

then necessary action can also be taken like arresting the criminal, etc. we can blacklist or block the user with their wallet address that is generated at the time of creating a new account. In future, this system can be used in applications like bitcoin system and ATM systems to avoid money being stolen from the account. If money or bitcoins are stolen the user who did this can be traced with the help of wallet address and punished accordingly.

REFERENCES

[1] V. Goyal, O. Pandey, A. Sahai and B.Waters, "Fuzzy identity-based encryption," in EUROCRYPT'05, Springer, 2005, pp. 457–473.

[2] V. Goyal, O. Pandey, A. Sahai and B.Waters, "Attribute based encryption for fine-grained access control of encrypted data," ACM conference on computer and communication safty, 2006 pp. 89–98.

[3] J.Bethencourt, A. Sahai and B.Waters, "Ciphertext-policy attribute-based encryption," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] Zhiguo Wan, Jun'e Liu and Robert H.Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in cloud computing," in IEEE Transactions on Information Forensics and Security, vol.7,No.2, April 2012.

[5] Brent Waters, "Ciphertext-policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," in International Association for Crytologic Research, PKC 2011, LNCS 6571, pp. 53-70, 2011.

[6] Hua Deng, Qianhong Wu, Bo Qin, Josep Domingo-Ferrer, Lei Zhang, Jianwei Liu and Wenchang Shi, "Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts," in International Science 275, pp. 370-384, 2014.