International Journal of Computer Engineering & Technology (IJCET)
Volume 7, Issue 6, November–December 2016, pp. 55–63, Article ID: IJCET_07_06_007
Available online at
http://www.iaeme.com/ijcet/issues.asp?JType=IJCET&VType=7&IType=6
Journal Impact Factor (2016): 9.3590(Calculated by GISI) www.jifactor.com
ISSN Print: 0976-6367 and ISSN Online: 0976–6375

EFFICIENT SECURITY AND PRIVACY IN DECENTRALIZED AUTHORITY USING ATTRIBUTE-BASED ENCRYPTION

Dr. Koppula Srinivas Rao
Professor, Department of CSE, MLR Institute of Technology, Hyderabad, India

ABSTRACT

Property based encryption (ABE) [13] decides unscrambling capacity in light of a client's properties. In a multi-power ABE plot, numerous trait powers screen diverse arrangements of properties and issue comparing unscrambling keys to clients and encryptions can require that a client acquire keys for fitting qualities from every power before decoding a message. Pursue [5] gave a multi-power ABE conspire utilizing the ideas of a trusted focal power (CA) and worldwide identifiers (GID). Be that as it may, the CA in that development has the ability to decode each figure content, which appears to be some way or another opposing to the first objective of conveying control over numerous conceivably depended powers. In addition, in that development, the utilization of a steady GID permitted the powers to join their data to manufacture a full profile with the greater part of a client's traits, which pointlessly bargains the security of the client. In this paper, we propose an answer which evacuates the trusted focal power, and secures the clients' protection by keeping the powers from pooling their data on specific clients, along these lines making ABE more usable by and by.

Key words: property based encryption, mysterious certification, security, multi-power, evacuating trusted gathering.

Cite this Article: Dr. Koppula Srinivas Rao, Efficient Security and Privacy in Decentralized Authority using Attribute-Based Encryption. *International Journal of Computer Engineering and Technology,* 7(6), 2016, pp. 55–63.
http://www.iaeme.com/ijcet/issues.asp?JType=IJCET&VType=7&IType=6

1. INTRODUCTION

We frequently distinguish individuals by their characteristics. In 2005, Sahai and Waters [13] proposed a framework (portrayed in later phrasing as a key-strategy characteristic based encryption (ABE) framework for limit approaches) in which a sender can scramble a message determining a trait set and a number d, to such an extent that lone a beneficiary with at any rate d of the given properties can unscramble the message. Notwithstanding, the organization ramifications of their plan may not be altogether reasonable, in that it expect the presence of a solitary trusted gathering who screens all properties and issues all unscrambling keys. Rather, we frequently have distinctive substances in charge of checking diverse qualities of a man, e.g. the Department of Motor Vehicles tests whether you can drive, a college can affirm that you are an understudy, and so on. Therefore, Chase [5] gave a multi-power ABE conspire which

bolsters a wide range of powers working all the while, each distributing mystery keys for an alternate arrangement of characteristics. Be that as it may, this arrangement was still not perfect. There are two primary issues: one worry of security of the encryption, the other the protection of the clients.

1.1. Protecting the User's Privacy

Since every power is in charge of various properties, we need to permit them to issue unscrambling keys autonomously, without communicating with each other. As contended in [5], to counteract plot in such a setting, we require some predictable thought of personality. (Something else, a client could without much of a stretch acquires keys from one power and after that give them all to a companion.) The arrangement in that work is to require that every client have a one of a kind worldwide identifier (GID), which they should present to every power (and to require that the client demonstrate somehow that he is the proprietor of the GID he presents).1 Unfortunately, the insignificant presence of GID makes it hard for the clients to ensure any sort of protection. Since a client must present the same GID to every power, it is simple for plotting powers to pool their information and manufacture a "total profile" of the majority of the credits relating to each GID. Be that as it may, this may be undesirable, especially if the client utilizes the ABE framework as a part of a wide range of settings, and wishes to keep data about some of those settings private. This circumstance is by all accounts unavoidable if every one of one's characteristics are dictated by some sort of open personality like a name or SSN – all things considered clients should distinguish themselves regardless so as to get the decoding keys for a specific arrangement of qualities, so security is unavoidably com-guaranteed. In any case, there are numerous traits which don't have a place with this classification. The capacity to drive is a decent illustration. One ought to have the capacity to demonstrate the capacity to accomplish something in an examination and afterward get the comparing qualification, without showing any recognizing data. Then again, one may associate with an administration by means of a pen name. a login name) and wish to acquire credits identifying with this association without uncovering one's full personality. In any case, as the characteristic powers (AAs) are in charge of dealing with every client's traits, it appears to be inescapable that they will realize which subsets of its properties are held by various clients. Be that as it may, we could envision applications where a portion of the powers are diverse online administration suppliers giving credits identified with online exercises like blog/wiki commitments, access to online news destinations, interest in informal communication locales, or buys at an online store. For this situation, it would bode well for the client to have the capacity to keep up various, unlikable characteristic sets with every power.

In the meantime, it additionally bodes well for every AA to assemble the insights of their framework use (e.g. the quantity of clients subscribed a specific administration as showed by the quantity of clients who asked for a decoding key for a specific property) without trading off individual's protection.

1.2. Removing the Trusted Authority

The arrangement introduced in [5] accepted the nearness of a solitary trusted "focal power" (CA) notwithstanding the characteristic powers. This CA did not deal with any qualities, but rather was in charge of issuing every client a novel key. To see why the CA is significant in [5], we first review the instinct. The thought was that, for every client, every AA would utilize his own mystery (not known by different AAs) to create a share of a framework wide ace mystery key. The powers should have been ready to create these shares freely (i.e. without speaking with whatever other power amid client key issuing). In the meantime, so as to avert plot it is important to utilize an alternate sharing for every client. This made it hard to ensure that all shares dependably signify a similar ace mystery. The arrangement was to have the CA issue every client an exceptional esteem to offset every one of these shares from the AAs and empower the client to "recoup" a component of the framework wide ace mystery key. Clearly, this calculation requires the CA to know the ace mystery of the framework, and the mystery data of every AA. This infers it should likewise have the ability to unscramble any figure content.

Notwithstanding, this decoding power appears to be some way or another opposing to the first inspiration of appropriating control of the traits over numerous possibly endowed powers. Along these lines, we asked whether it is conceivable to rather appropriate the usefulness of the CA over the greater part of the AAs, so that the length of some of them are straightforward, the plan will even now be secure.

1.3. Our Contributions

Here we display a multi-power ABE with client protection and without the trusted power. These prerequisites are non-unimportant to fulfill, due in both cases to the plot resistance necessity of ABE. Brent Waters proposed an approach for evacuating the CA prerequisite, in which every combine of property powers would share a mystery key. We formalize this thought, and demonstrate that it is secure the length of no less than two of the AAs are straightforward. The new arrangement utilizes systems for dispersed pseudorandom capacities (PRF) presented in [11].

Take note of that Lin et al. [10] as of late proposed an alternate approach for building a multi-power ABE plot without a focal power. Be that as it may, their development obliges architects to alter a steady m for the framework, which specifically decides productivity. The subsequent development is with the end goal that any gathering of m + 1 plotting clients will have the capacity to break security of the encryption. Our plan then again is secure regardless of what number of clients connives.

We additionally show a mysterious key issuing convention which permits multi-power ABE with improved client security – 1) we permit the clients to speak with AAs by means of nom de plumes of providing their GIDs free, and 2) we keep the AAs from pooling their information and connecting various credit sets having a place with a similar client. As a building square we develop a convention for a neglectful calculation of a key of the shape (SK • PRF (u)) where u is a client's GID, 2 SK speaks to some mystery data identified with the private key of a power, β is the mystery seed for the PRF claimed by a power and γ compares to some mystery identified with a trait controlled by a power. The key is created neglectfully, i.e. without either the power or the client uncovering any of their mystery data ((SK, β, γ) or u individually). We displayed the convention in this "nonexclusive" path (without coupling with a specific ABE plan) to represent its materialness. Our convention can be connected to Chase framework (with a little alteration) in a somewhat direct way (see full form for subtle elements). We additionally demonstrate to proficiently apply this convention to our plan which evacuates the CA. (For this situation the keys are more mind boggling, so we require to some degree more included strategies.

At last, our outcomes might be of extra intrigue since they demonstrate new utilizations of the dispersed PRF of Nair, Pinkas, and Reingold [11], and a speculation of the neglectful PRF procedures of Jarecki and Liu [9].

2. RELATED WORK

2.1. ABE for Different Policies

ABE is really a speculation of IBE (character based encryption [14]): in an IBE framework, cipher texts are connected with one and only property (the personality). The ABE plan of Sahai-Waters [13] was proposed as a fluffy IBE plot, which took into consideration some blunder resistance around the picked character. In later wording, it would be depicted as a key-arrangement (KP) ABE conspire that takes into account limit approaches. Key-strategy implies that the encrypt or just gets the chance to name a figure content with an arrangement of properties. The power picks a strategy for every client that figures out which cipher texts he can unscramble. A limit arrangement framework would be one in which the power determines a characteristic set for the client, and the client is permitted to unscramble at whatever point the cover between this set and the set connected with specific figure content is over an edge. Goyal et al. [8] proposed a KP-ABE conspire which underpins any monotonic get to equation comprising of AND, OR, or limit entryways. A development for KP-ABE with no monotonic get to structures (which likewise incorporate NOT doors, i.e. negative requirements in a key's get to recipe) was star postured by Ostrovsky,

Sahai and Waters [12]. These plans are portrayed as key-arrangement ABE since the get to structure is indicated in the private key, while the credits are utilized to depict the cipher texts.

The parts of the cipher texts and keys are switched in the figure content strategy ABE (CP-ABE) presented by Bethencourt, Sahai and Waters [2], in that the figure content is scrambled with a get to approach picked by an encryptor yet a key is essentially made concerning a qualities set. The security of their plan is contended in the non specific gathering model. As of late, [15] proposed CP-ABE developments in view of a couple of various matching presumptions which work for any get to arrangement that can be communicated regarding a LSSS lattice. In this paper, we will take a gander at the KP-ABE setting. We will take a gander at both the straightforward edge, and the more muddled monotonic get to structure case, and will fabricate a development in light of an indistinguishable presumptions from Sahai and Waters [13] and Goyal et al.[8]. Both non-monotonic get to structures and the figure content approach plans require much more grounded suppositions, and altogether different methods, so we won't consider these cases in our work.

2.2. Multi-Authority ABE

The greater part of the earlier work depicted above considers the situation where the majority of the traits are observed by a solitary power. Nonetheless, as we said in Section 1, it appears to be regular that one might need to gap control of the different properties over a wide range of powers. The fundamental test here is to ensure that two intriguing clients can't each get keys from an alternate power, and afterward pool their keys to unscramble a message that they are not qualified for. Besides, in the multi-power case, we may wish to take into account a portion of the powers to be untrusted. The systems for single power ABE can't be effectively summed up for this situation – they depend on the way that the single power can produce the majority of a client's keys on the double, to guarantee that they must be utilized together, and can't be joined with whatever other client's keys.

The main multi-power ABE plans we know about are Chase's unique proposition [5] (which has as of now been examined in Section 1) and the exceptionally late Lin et al. augmentation [10]. Both plans are KP-ABE and work in a setting where different powers are in charge of separate arrangements of properties. The disservices of Chase's plan have as of now been talked about in Section 1. The plan of [10], similar to the plan we will show here, has the preferred standpoint that it doesn't depend on a focal power. In any case, their plan just accomplishes m-versatility, in that security is just ensured against a most extreme of m conspiring clients. (Conversely, the aftereffects of [5] and our new results consider a much more grounded model, which stays secure against any number of conspiring clients.) And this is not only an issue of formal security: Lin et al. shown an agreement assault of m+1 clients [10]. In their plan m is the quantity of mystery keys that every power acquires from an appropriated key era convention. (This additionally implies m must be resolved when the framework is introduced.) Clearly, for a largescale framework, m ought to set sensibly high with a specific end goal to ensure security (a free alluring lower bound ought to be N2, where N is the quantity of powers). This forces loads on the intelligent dispersed key era convention among every one of the powers, and on their safe stockpiling.

At long last, O (m) online particular operations are required by every power to issue mystery keys to a client. We assist take note of that this weaker thought of security appears to be undesirable. It might be of business enthusiasm to have whatever number clients as could reasonably be expected, yet it at the same time builds the danger of being bargained. (Regardless of the possibility that clients themselves are not malevolent, one may stress over malware on a client's machine, or data spilled accidentally through side channels.) Thus, we contend that it is still a critical open issue to outline a proficient and secure multi-power ABE plot without a trusted CA, and this is one of the issues we will endeavor to unravel here.

2.3. Anonymous Credentials

As of not long ago, there has been little relationship between mysterious qualifications and ABE (with the exception of a late work in [6] which acquires a few procedures from unknown accreditation to address the key-escrow issue of IBE). In our new plans we will make utilization of some fundamental strategies in unknown certification frameworks to secure the protection of ABE clients. In an unknown qualification framework (see [3, 4]), clients wish to get and demonstrate ownership of certifications while staying mysterious. In such work it is expected that every client has a one of a kind mystery key (and there are diverse proposition for how to demonstrate that a given key is legitimate and to keep clients from crediting out their keys). At that point the client can connect with every power under an alternate nom de plume such a route, to the point that it is difficult to interface numerous aliases to a similar client. In the meantime, the majority of a client's pen names, the subsequent certifications, are fixing to a similar mystery key so that the client can demonstrate that he has both characteristic set A from one power and set B from another. We will utilize procedures from unknown certifications to permit the clients to get unscrambling keys from the powers without uncovering their GID's.

The essential thought is to let the GID assume the part of the unknown certification mystery key. We will now expect that every client has a special and mystery GID esteem. He collaborates with powers utilizing nom de plumes on this esteem, and along these lines gets decoding keys.3 Thus, we will supplant the GID with the supposition that every client has interesting mystery enter as in an unknown accreditation framework. Ensuring that this mystery key is remarkable includes various unobtrusive issues. Standard systems can be found from the unknown accreditation writing. Note, nonetheless, that unknown accreditations don't promptly unravel the security issue in an ABE setting. Consider the accompanying proposition: The client interfaces with the power by means of a nom de plume. At the point when the client needs to get unscrambling keys relating to an arrangement of characteristics, he demonstrates (through the unknown qualification framework) that he is the proprietor of a certification for these properties. At that point he utilizes the ABE framework to get unscrambling keys. This thought appears to be direct, yet in truth it is indistinct how to fulfill our security and protection necessities. To begin with, the current developments for multi-power ABE plans (by Chase [5] and Lin et al. [10]) require that the client shows the GID free to every power. The power then uses this GID to create the client's unscrambling keys, keeping in mind the end goal to guarantee intrigue resistance. This clearly does not give any client security. Then again, if the client was permitted 3Another choice is permit the client to uncover the GID to choose powers, yet to require that there be some extra mystery data that was known just to the client, to avoid pantomime. to introduce an alternate anonymized esteem to every power, then we would never again have the capacity to ensure the security of the multi-power ABE against intriguing clients.

Rather, we will take care of the security issue by outlining a convention by which a client can get an arrangement of unscrambling keys for his mystery GID without uncovering any data about that GID to the power. In the meantime, the power is ensured that the settled upon unscrambling keys are the main thing that the client gains from the exchange. At long last, we push that, in spite of the fact that we utilize a few components of unknown certification frameworks, our answer does not scramble as for a client's mystery key. This is still entirely a quality based encryption framework, in which decoding capacity is resolved just by a client's traits. The mystery key/GID is just utilized as a part of speaking with the different powers, and in deciding the fitting decoding keys.

3. POWER UNLINKABLE ABE

As specified some time recently, a multi-power ABE framework which requires a client to present his novel identifier to each power would have extreme protection inadequacies. Specifically, it will be unimportant for the different powers to join their information and amass an entire photo of the majority of a client's properties in all spaces. To evade this we hope to related work on unknown certifications [3, 4]. We will regard the GID as the client's mystery key. At that point the client can shape distinctive nom de plumes on this GID to utilize when communicating with various powers. At the point when the client

wishes to get unscrambling keys for specific properties connected with this power, he plays out an intuitive convention with the power. As a consequence of this convention, he gets unscrambling keys attached to the GID that compares to his nom de plume. These can then be joined with unscrambling keys got from different powers utilizing different pen names the same GID. In any case, from the powers' perspective the GID is totally covered up. Indeed it is even infeasible for two powers to advise that they are conversing with a similar client. 4As in all ABE plans to date, clients are not permitted to just add ascribes to their unscrambling key set. Rather, a client who needs to upgrade his quality set must get a completely new arrangement of keys. In the multi-power case (see e.g. [5]), this implies a client can't just come back to a power with the same GID – he should acquire new keys from all powers.

3.1. Framework and Security Requirements

Our meaning of a power unlinkable ABE conspire develops the definition in Section 2.2 by adding an intelligent convention to permit the client to get an unscrambling key from the power without uncovering his GID. Definition 8. A N-power unlinkable ABE plan is a N-power ABE plot with three additional calculations (params and {apkk}k∈{1,...N} are discarded from the information):

1. (nym, aux) $← Form Nym(GID) probabilistically yields an alias personality GID, and some helper data aux.

2. Obtain (apkk, GID, Ak, nym, aux) ↔ Issue (askk, Ak, nym) are two intelligent calculations which execute a client mystery key issuing convention between a client and the characteristic power k.

The client takes as info people in general key apkk of the property power k, a quality set Ak, a character GID, and the comparing pseudo nymnym with helper data aux, and gets what AKeyGen (askk,GID,Ak) yields, i.e. an unscrambling key for personality GID relating to the trait set Ak. The characteristic power gets the mystery key askk, the arrangement of qualities Ak and the nom de plume as info, and gets nothing as yield. With the accompanying properties

1. (nym, aux) $← Form Nym(GID) produces a promise nym to the client's GID with irregularity aux,

2. Get ↔ Issue shape a protected two gathering calculation (2PC) convention for the accompanying usefulness F, where ({(apkk, askk)}k∈{1,...N}) is as yield by Setup(1 ,N): F takes as open info the power's open key apkk, the client's alias, and the characteristic set Ak. It additionally gets as mystery info the client's character GID and the comparing aux, and the power's mystery key askk. It yields the consequence of AKeyGen (askk, GID, Ak) to the client.

3.2. Generic Anonymous Key Issuing Protocol

Here we exhibit a "non specific" convention to such an extent that a client with a private esteem u ∈ Zq and a power with private keys α, β, γ ∈ Zq can together figure the esteem (hg1/(+u)) for regularly known g, h ∈ G5. Just the client gets this yield, and all other data is covered up. The parts of every private esteem will be evident when this convention is utilized as the mysterious key issuing convention for the ABE framework to be displayed in Section 5. The fundamental instinct is that the structure of the last esteem looks like a result of h , which compares to something identified with the private key of a power, and a randomizer processed as PRF(u), where β is the mystery seed for Dodis-Yampolskiy PRF [7], and u is the GID of the client. 6 γ compares to some mystery identified with a trait. 5We additionally require that the discrete logarithm amongst g and h be obscure to any degenerate client. 6 all together for this to be a legitimate PRF, we require u to be looked over some predefined polynomial-sized space. Then again, we can pick u = H(GID) for hash work H, and the outcome will be secure in the arbitrary prophet show.

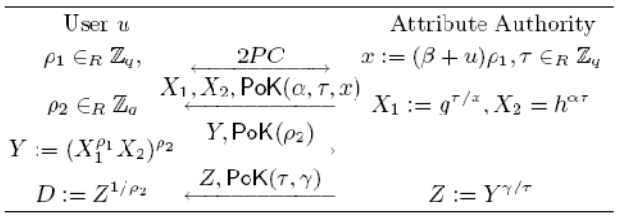

Figure 1: Our anonymous ABE key issuing protocol

Figure 1 demonstrates our convention for mysterious key issuing. In every progression, PoK speaks to a proof of information of the mystery values utilized as a part of the calculation. For straightforwardness we have overlooked the announcement being demonstrated. Here the initial step indicates a 2PC convention which takes (u, ρ1) from the client and β from the power and returns x := (β + u)ρ1 mod q to the power. This should be possible by means of a general 2PC convention for a straightforward number juggling calculation. Then again, we can do this all the more effectively utilizing the development as a part of [1]. The important confirmations of learning (PoK) for the above proclamations can be productively acknowledged, e.g. through a Schnorr convention.

4. PROPOSED MULTI-AUTHORITY ABE

4.1. Removing the Trusted Authority

We audit the inspiration driving the utilization of the CA, and demonstrate to keep away from it. To have a solid examination, we accept the accompanying subtle elements of an ABE framework. The ace open key is ˆe (g1, g2) msk and the message m is encoded by ˆe (g1, g2) s•msk•m where s is the irregularity of the figure content. Basic Secret Sharing Allows Collusion. To take into consideration numerous trait powers, the initial step is to disperse the ace mystery key msk over the diverse quality powers. In any case, mind must be taken to avoid intrigue assaults so that clients An and B who each have the proper qualities from one of two unique powers can't join their insight to decode something neither of them is qualified for. Presently we should take a gander at what happens when we need to partition this msk among the powers. Consider the two-power case. Assume we utilize a paltry added substance sharing of the ace mystery key y1 + y2 = msk where one power utilizes y1 and alternate uses y2, and a plan where a legitimate client gets a decoding key in light of gy1 and gy2 from the separate powers. At that point a client A with enough characteristics from the main power can recoup ˆe(g1, g2)y1s, and likewise, client B with enough qualities from the second power can recuperate ˆe (g1, g2) y2s.

Regardless of the possibility that neither alone has adequate traits from both powers, together they will be capable recuperate ˆe (g1, g2) s•msk and consequently the message m. Consequently we can't utilize a direct sharing of the ace mystery key between the powers. The essential thought is to utilize an alternate sharing for every client. In any case, since we don't need these powers to impart among them for each mystery key demand, in what manner would they be able to guarantee that the qualities utilized for every client dependably total to msk? Utilizing PRFs to make the Key "Client Specific". The reply in [5] was to require that powers process offers deterministically, every utilizing their own PRF, and after that to have a different CA, whose employment was to guarantee that the sharing would include: it would know every power's PRF seed and in addition the msk, it would utilize this data produce the shares utilized for every client, and it would create the fitting last share. In particular, for client GID, every power k utilizes share gPRFk (GID), and the CA provides for client GID the esteem gmsk−PN k=1(PRFk (GID)), where PRFk (•) indicates a pseudorandom work utilizing power k's mystery seed. A client GID with enough properties from power k can recuperate ˆe (g1, g2) s•PRFk (GID) from the figure content. At that point this can be joined with the "coordinating" esteem acquired from the CA and some part in the figure content to recoup the session key ˆe (g1, g2) s•msk.

The excellence of a PRF family is that no polynomial-time enemy can recognize (with huge favorable position) between an arbitrarily picked work and a really irregular capacity (conversely with a degree m polynomial utilized as a part of [10]). The thought here (proposed by Waters) thought is to dispose of the requirement for the CA by utilizing an arrangement of PRFs whose yield values on a specific info dependably entirety to zero. Every combine of powers (j, k) shares a mystery PRF seed seedjk (once more, this sharing is done unequivocally at the underlying setup organize). This implies there are O(N2) PRFs to be utilized as a part of aggregate. The last "arbitrary looking" Fk(GID) utilized by every power is a straight mix of N − 1 fundamental PRFs. All the more particularly, it is the summation of these PRFs, each weighted by either 1 or −1. A proper decision of summation and subtraction makes all these PRF values cross out each other when Fk(GID) for various k are included. Casually, such an "entirety of-PRF" development still looks pseudorandom to any foe who knows not as much as N − 2 of a specific power k's mystery seeds seedkj (i.e. to any enemy controlling not as much as N – 2 different powers). The last composite PRF is figured as Fk (GID) = Pj<k PRFjk (GID) − Pj>k PRFjk (GID). This PRF development is like the least complex development in [11], where it is utilized to assemble a disseminated key circulation focus.

5. CONCLUSION

It is unlikely to expect there is a solitary power which can screen each and every trait of all clients. Multi-power characteristic based encryption empowers a more sensible organization of trait based get to control, with the end goal that distinctive powers are in charge of issuing diverse arrangements of qualities. The first arrangement by Chase utilizes a trusted focal power and the utilization of a worldwide identifier for every client, which implies the secrecy, depends fundamentally on the security of the focal power and the client protection relies on upon the genuine conduct of the trait powers. We propose a quality based encryption conspire without the trusted power, and an unknown key issuing convention which works for both existing plans and for our new development. We trust that our work gives a more practice oriented characteristic based encryption framework. Affirmation. We say thanks to Brent Waters for recommending the aggregate of PRFs development. 7In complexity to a typical limit cryptosystem, here the edge might be lessened if the encryptor does as such (by incorporating sham properties in the figure content characteristic set). Therefore, every figure content may have an alternate limit.

REFERENCE

[1] Mira Belenkiy, Jan Camenisch, Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Hovav Shacham. Randomizable Proofs and Delegatable Anonymous Credentials. In CRYPTO, LNCS. Springer, 2009. To appear.

[2] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-Policy Attribute-Based Encryption. In IEEE Symposium on Security and Privacy, pages 321–334. IEEE Computer Society, 2007.

[3] Stefan Brands. Rethinking Public Key Infrastructure and Digital Certificates – Building in Privacy. PhD thesis, Eindhoven Inst. of Tech. 1999.

[4] Jan Camenisch and Anna Lysyanskaya. Efficient Non-transferable Anonymous Multi-show Credential System with Optional Anonymity Revocation. In EUROCRYPT 2001, volume 2045 of LNCS, pages 93–118. Springer Verlag, 2001.

[5] Melissa Chase. Multi-authority Attribute Based Encryption. In TCC, volume 4392 of LNCS, pages515–534. Springer, 2007.

[6] Sherman S.M. Chow. Removing Escrow from Identity-Based Encryption. In Public Key Cryptography, volume 5443 of LNCS, pages 256–276. Springer, 2009.

[7] Yevgeniy Dodis and Aleksandr Yampolskiy. A Verifiable Random Function with Short Proofs and Keys. In Public Key Cryptography, volume 3386 of LNCS, pages 416–431. Springer, 2005.

[8] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. In Computer and Communications Security, pages 89–98. ACM, 2006.

[9] Stanislaw Jarecki and Xiaomin Liu. Efficient Oblivious Pseudorandom Function with Applications to Adaptive OT and Secure Computation of Set Intersection. In TCC, pages 577–594. Springer, 2009.

[10] Huang Lin, Zhenfu Cao, Xiaohui Liang, and Jun Shao. Secure Threshold Multi Authority Attribute Based Encryption without a Central Authority. In INDOCRYPT, volume 5365 of LNCS, pages 426–436. Springer, 2008.

[11] Moni Naor, Benny Pinkas, and Omer Reingold. Distributed Pseudo-random Functions and KDCs. In EUROCRYPT, volume 1592 of LNCS, pages 327–346. Springer, 1999.

[12] Rafail Ostrovsky, Amit Sahai, and Brent Waters. Attribute-Based Encryption with Non-Monotonic Access Structures. In Computer and Communications Security, pages 195–203, 2007.

[13] Amit Sahai and Brent Waters. Fuzzy Identity-Based Encryption. In EUROCRYPT, volume 3494 of LNCS, pages 457–473. Springer, 2005.

[14] Adi Shamir. Identity-Based Cryptosystems and Signature Schemes. In CRYPTO, pages 47–53. Springer, 1984.

[15] Brent Waters. Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization. Cryptology ePrint 2008/290.

[16] Dr. V. Goutham, Lalbahadur Kethavath and K.Swetha, Key Aggregate Searchable Encryption with Secure and Efficient Data Sharing in Cloud. *International Journal of Computer Engineering and Technology (IJCET),* 7(4), 2016, pp. 41–47.

[17] Dr. R. Mala and K. Karthikeyan. Artificial Neural Cryptography Datagram Hiding Techniques For Computer Security Objects Register , *International Journal of Computer Engineering and Technology (IJCET)*, 7(2), 2016, pp. 36 – 43 .