Volume No:3, Issue No:3 (August-2017)
ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

A Method IBE Interfaced With Private Key Generation and Public Key Infrastructure to Achieve High Data Security

Alaa Sahl Jaafer
Department of M. S.C.IS
Osmania University, Hyderabad, India
Foundation of Technical Education, Iraq

Abdali Abdulkareem Abdali
Department of M. S.C.IS
Osmania University, Hyderabad, India
Foundation of Technical Education, Iraq

ABSTRACT

Identity based Public key encryption empowers straightforward introduction of open key cryptography by allowing a component's open key to be gotten from a discretionary distinguishing proof worth, for example, name or email address. The fundamental down to earth advantage of character based cryptography is in enormously lessening the requirement for, and dependence on, open key authentications. Albeit some intriguing character based systems have been created previously, none are good with prominent open key encryption calculations. Besides, it is in a general sense hard to accommodate fine-grained denial with character based cryptography. Interceded RSA (mRSA) is a basic and down to earth technique for part a RSA private key between the client and a Security Mediator (SEM).

Neither the customer nor the SEM can cheat each other since each crypto-practical operation (mark or unscrambling) incorporates the two sides. mRSA allows brisk and fine-grained control of customers' security benefits. Be that as it may, mRSA still depends on traditional open key declarations to store and impart open keys.

In this paper, we show IB-mRSA, a fundamental variety of mRSA that joins identity based and interceded cryptography. Under the discretionary prophet display, IB-mRSA with OAEP is showed up as secure (against adaptable picked ciphertext strike) as standard RSA with OAEP. Also, IB-mRSA is clear, feasible, and idealize with current open key establishments.

Keywords: ***Ciphertext, Encryption algorithms, Identity-based mRSA, public key encryption, private key encryption, SEM.***

INTRODUCTION

A protected server despite giving an ensured establishment to empowering your Web applications, and Web server design expect a basic character in your Web application's security. Gravely sorted out server can affect unapproved get to. A disregarded offer can make a steady discretionary segment, while an overlooked port can be an aggressor's front entryway. Disregarded client records can allow an attacker to sneak past your obstacles unnoticed. Understanding the threats to your Web server and having the capacity to recognize appropriate countermeasures licenses you to suspect various attacks and miracle the routinely creating amounts of aggressors. This system gives bidirectional encryption of correspondences between a customer and server, which guarantees against listening stealthily and upsetting and/or fabricating the substance of the correspondence [1].

Much talking, this applies a sense surety that one is relating with definitively. The site that I proposed to talk with furthermore protecting that the substance of correspondences between the client and the site can't be scrutinized or made by any outsider. Secure Server Plus application has principally twofold login security. That is, in the wake of marking into the application customer gets a mystery key on his selected gmail id. This mystery key must be embedded in the pop-up box appeared in the wake of marking into SSP Application.

This application has two functionalities, Encryption and Decryption. Encoding is the handiness in which the record to be systematized over the mail in right off the bat disconnected in 4 an adjustment of in byte course of action and a while later encoded utilizing unmistakable encryption calculations [2]. After Encryption records would be sent to the recipient through Gmail At the recipient end, He will download the archives and using SSP Application data as a piece of reports would be unscrambled and mixed.

Client security is likewise required in cloud. By using assurance the cloud or distinctive customers don't have the foggiest thought regarding the identity of the other hub. The cloud can contain the hub introduces the information in the cloud, and in like way, to give advantages the cloud itself is mindful. The genuineness of the customer who stores the data is likewise bolstered.

There is likewise a necessity for law approval isolated from the specific responses for surety security and safe house. Various encryption frameworks have been utilized to secure data on cloud to examine the data while doing computations on the information. By utilizing Attribute based encryption plot, the cloud gets figure substance of the information and performs calculations on the figure substance and gives the encoded estimation of the last outcome to the center point then the client can translate the result, regardless of the way that the cloud does not comprehend what information it has worn down [3].

Distinctive strategies have been recommended to safeguard the data substance assurance by method for affirmation control. Identity based encryption (IBE) was at first presented by Shamir, in which the sender of a message can exhibit a character to such an extent that restrictive a beneficiary with sorting out identity can unscramble it. A couple of years at some point later, Fuzzy Identity-Based Encryption is proposed, which is for the most part called Attribute-Based Encryption (ABE).

In such encryption imagine, an identity is seen as an arrangement of clear traits, and interpreting is conceivable if a decrypter's character has two or three spreads with the one demonstrated in the ciphertext.

Ahead long, more wide tree-based ABE organizes [4], Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE), are familiar with express more broad condition than coordinate 'cover'. They are assistants to each unique as in the option of encryption method (who can or can't decipher the message) is settled by various get-togethers [5].

In the KP-ABE, a ciphertext is associated with a course of action of qualities, and a private key is related with a monotonic get to structure like a tree, which depicts this present customer's identity (e.g. IIT AND (Ph.D OR Master)). A customer can unscramble the ciphertext if and just if the way tree in his private key is satisfied by the characters in the ciphertext. In whatever claim, the encoding structure is depicted in the keys, so the Encrypter does not have full control over the encoding access. He needs to trust that the key generators issue keys with the right structures to the privilege customers[5]. Besides, when a re-encryption happens, a large portion of the customers in the same framework must bear their private keys, re-issued remembering the final objective to go to the re-encoded circles, and this procedure causes immense issues in the usage.

Of way, those occasions and working cost are all esteemed in the CP-ABE. In the CP-ABE, ciphertexts are made with an entry structure, which shows the encryption approach, and private keys are made by qualitiesA customer can disentangle the ciphertext if and just if his qualities in the private key satisfy the area tree displayed in the ciphertext. Thusly, the Encrypter holds a total power about the encoding structure. In addition, the starting now issued private keys will never be balanced unless the whole structure reboots.

RELATED WORK:

Bitar, N., Gringeri, S., and Xia, T. J. (2013), explore says cloud today face a couple of troubles while encouraging line-of-business applications in the cloud. Major to countless troubles is the confined support for control over cloud framework limits, for example, the ability to ensure security, execution sureties or partition, and to adaptably mediate middleboxes in application associations. In this paper, we demonstrate the setup and use of a novel cloud arranging system called CloudNaaS.

Customers can impact CloudNaaS to pass on applications extended with a rich and extensible game plan of framework limits, for example, virtual framework disengagement, custom keeping an eye on, organization partition, and versatile mediation of various middleboxes. CloudNaaS primitives are particularly executed inside the cloud structure itself using quick programmable framework segments, making CloudNaaS extremely gainful. We evaluate an OpenFlow-based model of CloudNaaS and watch that it can be used to instantiate a blended sack of framework limits in the cloud, and that its execution is healthy even in spite of tremendous amounts of provisioned organizations and association/device disillusionments.

Ramgovind, S., Eloff, M. M., and Smith, E. (2010, August), distributed computing has raised IT beyond what many would consider possible by offering the business condition data storing and confine with versatile adaptable figuring planning vitality to coordinate adaptable demand and supply, while diminishing capital utilize. However the open entryway cost of the productive execution of Cloud enlisting is to effectively manage the security in the cloud applications. Security discernment and concerns develop when one begins to run applications past the appointed firewall and draw nearer towards the all inclusive community space.

The inspiration driving the paper is to give a general security perspective of Cloud handling with the hope to feature the security stresses that should be fittingly tended to and made sense of how to comprehend the most extreme limit of Cloud enlisting. Gartner's once-over on cloud security issues, additionally the revelations from the International Data Corporation wander board consider in perspective of cloud threats, will be inspected in this paper.

Oberheide, J., Veeraraghavan, K., Cooke, E., Flinn, J., and Jahanian, F. (2008, June) look into says cell phones continue moving toward the limits and extensibility of standard desktop PCs. Shockingly, these contraptions are in like manner beginning to confront a substantial number of an indistinguishable security threats from desktops. Starting at now, compact security game plans mirror the traditional desktop show in which they run distinguishing proof advantages on the contraption. This system is intricate and resource packed in both preparing and constrain.

This paper proposes another model whereby adaptable antivirus convenience is moved to an off-device framework organization using different virtualized malware area engines. Our conflict is that it is possible to spend information exchange limit resources for basically diminish on-contraption CPU, memory, and compel resources. We demonstrate how our in-cloud show enhances compact security and abatements on-contraption programming unusualness, while contemplating new organizations, for example, arrange specific behavioral examination engines.

Our benchmarks on Nokia's N800 and N95 mobile phones exhibit that our versatile masters eats up a demand of enormity less CPU and memory while in like manner consuming less power in like way circumstances stood out from existing on-contraption antivirus programming.

As demonstrated by Schoo, P., Fusenig, V., Souza, V., Melo, M., Murray, P., Debar, H., ... what's more, Zeghlache, D. (2011), Cloud handling is generally considered as a drawing in association exhibit following the clients commitments in regards to attempt and operations are restricted, and costs are in snappy relationship with utilization and interest. In any case, while sorting out plots for circled fogs are considered, there is small sponsorship and the effort is as often as possible demonized. The wander SAIL is tending to cloud sorting out as the mix of organization for circulated figuring and fundamental frameworks organization limits between spread cloud resources included to improve the organization of both.

This position paper shows new security challenges as considered in SAIL for ensuring honest to goodness usage of cloud frameworks organization resources and for turning away mishandle.

As indicated by Bitar, N., Gringeri, S., and Xia, T. J. (2013), Server homestead and cloud models continue progressing to address the necessities of broad scale multi-tenant server ranches and fogs. These requirements are based on seven estimations: flexibility in figuring, storing, and information exchange limit, adaptability in framework organizations, adequacy in resource utilization, deftness in organization creation, cost profitability, organization relentless quality, and security.

This article focuses on the underlying five estimations as they identify with frameworks organization. Immense server ranches are concentrating on support for countless, exabytes of limit, terabits each second of movement, and endless tenants. In a server ranch, server and limit resources are interconnected with distribute and switches that suit the information transmission and multi-inhabitant virtual frameworks organization needs.

Server ranches are interconnected over the wide zone framework through guiding and transport advances to give a pool of benefits, known as the cloud. Quick optical interfaces and thick wavelength-division multiplexing optical transport are used to suit high-confine transport intra-and between datacenter. This article reviews diverse trading, coordinating, and optical transport developments, and their suitability in keeping an eye on the frameworks organization needs of huge scale multi-tenant server ranches.

As per Zissis, D., and Lekkas, D. (2012), the late advancement of appropriated figuring has unquestionably altered everyone's perspective of base designs, programming movement and change models. Envisioning as a transformative wander, taking after the move from brought together PC PCs to client/server game plan models, conveyed processing incorporates segments from arrange enrolling, utility figuring and autonomic preparing, into an imaginative association development demonstrating.

This quick move towards the fogs, has fuelled worries on a segregating issue for the achievement of information systems, correspondence and information security. From a security perspective, different unchartered risks and troubles have been familiar from this movement with the fogs, going to pieces an extraordinary piece of the reasonability of standard confirmation frameworks.

In this way the purpose of this paper is twofold; right off the bat to evaluate cloud security by distinguishing extraordinary security essentials and furthermore to attempt to show a reasonable course of action that takes out these potential threats.

This paper proposes introducing a Trusted Third Party, entrusted with ensuring specific security qualities inside a cloud circumstance. The proposed course of action calls upon cryptography, especially Public Key Infrastructure cooperating with SSO and LDAP, to ensure the approval, respectability and mystery of included data and correspondences. The game plan, demonstrates a level of organization, open to every single included component, that comprehends a security arrange, inside which major trust is kept up.

Volume No:3, Issue No:3 (August-2017) ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

PROPOSED SYSTEM:

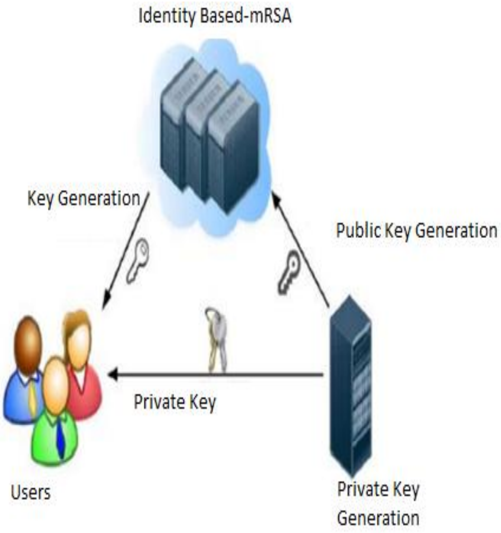

Figure 1: System Architecture

The need to make accessible bona fide duplicates of substances 'open keys is a noteworthy downside to the utilization of open key cryptography. The customary methodology for doing this is to utilize the general population key frameworks, in which an affirmation power (CA) issues a testament which ties a client's personality with his/her open key. With ID-based cryptosystems, this coupling is redundant as the character of the element would be his/her open key (If not straightforwardly, the general population key is gotten from the personality). In ID-based PKC, everybody's open Keys are foreordained by data that interestingly distinguishes them, for example, their email address.

This idea unique inspiration for ID-based encryption was to disentangle endorsement administration in email frameworks. Every substance in the framework sends his/her personality to a trusted outsider called the Key Generation Center (KGC), to get the private key. The private key is figured utilizing the private key of the KGC and the personality of the client. Key escrow is inborn in ID-based frameworks since the KGC knows all the private keys. For different reasons, this makes execution of the innovation much less demanding, and conveys some additional data security advantages. ID-based PKC (ID-PKC) remained a hypothetical idea until were proposed. A portion of the issues to be tended to contrast the ID-based frameworks and the customary PKI upheld open key cryptography.

RESEARCH METHOD

Setup→ The setup estimation takes no information other than the specific security parameter. It renders individuals as a rule parameters PK and a specialist key MK.

Encode (PK, M, A) → The encryption calculation takes as information people all around parameters PK, a message M, and an entry structure An over the universe of attributes.The number will encode M and deliver a ciphertext CT with the end goal that exclusive a client that holds a course of action of qualities that fulfills the way structure will hold the capacity to interpret the message.We will expect that the ciphertext obvious contains A.

Key Generation (MK, S) → The key time figuring takes as information the ace key MK and a course of action of qualities S that depict the key.It bears a private key SK.

Decode (PK, CT, SK) →The unscrambling count takes as information the all inclusive community parameters PK, a ciphertext CT, which contains a passage system An, and a private key SK, which is a private key for a set S of qualities. For the situation that the set S of qualities satisfies the passageway structure A then the computation will translate the ciphertext and return a message M.

Delegate (SK, $\tilde{S}$) →The representative count takes as data a puzzle key SK for some arrangement of properties S and a set $\tilde{S} \subseteq S$. It moves over a secret key SK for the game plan of $\tilde{S}$ qualities S [13].

Particularly we set emerge the advantage of the record access, and we evaluated a perfect chance to touch base at one advantage tree and depend on its affirmation parameter. When all is said in done, the computation overhead of Li is much higher than others in light of the way that their outline incorporates various more exponentiations and bilinear mappings in light of the commitment.

The encryption/unscrambling under different archive sizes did not demonstrate colossal differences when record sizes are significant (≥20MB), in light of the way that the run times are controlled by the symmetric encryption (AES-256). At last, however our run times are plotted in light of the fact that the advantage creation is the additional routine in our outline.

The need to make accessible bona fide duplicates of substances 'open keys is a noteworthy downside to the utilization of open key cryptography. The customary methodology for doing this is to utilize the general population key frameworks, in which an affirmation power (CA) issues a testament which ties a client's personality with his/her open key. With ID-based cryptosystems, this coupling is redundant as the character of the element would be his/her open key (If not straightforwardly, the general population key is gotten from the personality). In ID-based PKC, everybody's open Keys are foreordained by data that interestingly distinguishes them, for example, their email address[14].

This idea unique inspiration for ID-based encryption was to disentangle endorsement administration in email frameworks. Every substance in the framework sends his/her personality to a trusted outsider called the Key Generation Center (KGC), to get the private key. The private key is figured utilizing the private key of the KGC and the personality of the client. Key escrow is inborn in ID-based frameworks since the KGC knows all the private keys. For different reasons, this makes execution of the innovation much less demanding, and conveys some additional data security advantages.

ID-based PKC (ID-PKC) remained a hypothetical idea until were proposed. A portion of the issues to be tended to contrast the ID-based frameworks and the customary PKI upheld open key cryptography.

Identity-Based Public Key Cryptography

One of the troubles characteristic in running a PKI is in the overseeing of the testament and related key. Personality – and along these lines identifier – based cryptography was made as a method for defeating this issue. The plan gave a mark calculation, however couldn't be utilized for encryption. It is just as of late that an effective character based encryption framework was proposed [16].

The center contrast between an ID-PKC and a conventional unbalanced calculation in the method for producing the keys. The distinction is identifiable in two ways:

- As said above, in both the mark and encryption variations, people in general keys are created from openly identifiable data. This permits a customer A to produce general society key of another customer B without doing an inquiry in a catalog or approach B for a duplicate of their key.
- Because of the science that support the calculations, the production of the private key requires the learning of an expert mystery that is held by the Trusted Authority (TA), who is the simple of the CA in a PKI.

As of late, it has been perceived that a personality need not be the main determinant of a customer's open key. For instance, data, for example, the customer's position inside an association, the legitimacy time frame for the keys, and so forth can be incorporated into the information used to infer the key pair. This outcomes in the more extensive idea of identifier-based open key cryptography.

Since the TA is straightforwardly in charge of the era of the private key in an ID-PKC instrument, there is an inborn escrow office in the framework. This could possibly be alluring.

This strengths an adjustment in the part of the trusted outsider inside the framework. In a PKI, the CA is worried with accepting the realness of the data present in the declaration, while, in an ID-PKC the TA is specifically in charge of creating and disseminating all keying material inside the framework [16]. There is likewise the prerequisite that TA and customer can set up a free secure channel for the dispersion of private key material. This channel needs to secure both the realness and secrecy of the private key.

Despite the fact that utilizing a customer's way of life as the base for their key pair is exceptionally engaging, it doesn't come without results. The two principle issues that will impact the discourse in the rest of this paper are as per the following:

- Coping with the items of common sense of execution are not inconsequential. In the event that we take renouncement as an illustration, since we can't repudiate a man's character, there is a prerequisite for extra contribution to the key era process. On the off chance that we incorporate legitimacy dates, key use, and so on then a push toward more extensive utilization of distinguishing data results, driving actually to identifier-based cryptography. We will come back to repudiation issues.
- The credibility of the data that is utilized as the character or identifier is presently urgent to the security of the framework. In a PKI, the declaration should show the realness of distinguishing data. In ID-PKC, in light of the fact that a private key might be produced after general society key, the TA might not have approved the realness of the data identifying with the key pair preceding the general population key's utilization. For instance, A might utilize data it supposes is legitimate to create an open key for B, yet the data An utilizations could either identify with the wrong B, or might be totally invalid according to the TA.

IDENTITY-BASED MRSA:

The primary component of character based encryption is the sender's capacity to scramble messages utilizing people in general key got from the beneficiary's personality and other open data. The character can be the recipient's email address, client id or any quality exceptional to the beneficiary; basically, a subjective string. To process the encryption key, a productive (and open) mapping capacity KG must be set already. This capacity must be a balanced mapping from character strings to open keys. The fundamental thought behind character based mRSA is the utilization of a solitary regular RSA modulus n for all clients inside a framework (or area). This modulus is open and contained in a framework wide endorsement issued, of course, by some Certificate Authority (CA).

To scramble a message for a specific beneficiary (Bob), the sender (Alice) first registers eBob=KG(IDBob) where IDBob is the beneficiary's personality quality, for example, Bob's email address [17]. From that point, the pair (eBob,n) is dealt with as a plain RSA open key and typical RSA encryption is performed. On Bob's side, the decoding procedure is indistinguishable to that of mRSA.We push that utilizing the same modulus by numerous clients in a typical RSA setting is totally shaky. It is subject t oa unimportant assault whereby any one using one's information of a solitary key-pair – can essentially consider the modulus and register the other client's private key. Be that as it may, in the present setting, we make a critical presumption that:

All through the lifetime of the framework, the enemy can't trade off a SEM. Clearly, without this suspicion, IB-mRSA would offer no security what soever: a solitary SEM soften up combined with the trade off of only one client's key offer would bring about the bargain of all clients' (for that SEM) private keys. The IB-mRSA supposition is somewhat more grounded than its mRSA partner. Review that, in mRSA, every client has an alternate RSA setting, i.e., a one of a kind modulus. Along these lines, to trade off a given client an enemy needs to break into both the client and its SEM. We now swing to the point by point depiction of the IB-mRSA plan.

We actualized IB-mRSA for the motivations behind experimentation and acceptance. The product is made out of three sections:
1. CA and Admin Utilities: area endorsement, client key era, (discretionary) declaration issuance and renouncement interface.
2. SEM daemon: SEM process
3. Customer libraries: IB-mRSA client capacities open by means of an API.

The code is based on top of the well known OpenSSL library. OpenSSL fuses a huge number of cryptographic capacities and substantial number-crunching primitives. Notwithstanding being productive and accessible on numerous regular equipment and programming stages, OpenSSL sticks to the basic PKCS principles and is in the general population space.

The SEM daemon and the CA/Admin utilities are actualized on Linux, while the customer libraries are accessible on both Linux and Windows stages. In the instatement stage, a CA introduces the space wide cryptographic setting, in particular (n, p, q, p',q') and chooses a mapping capacity (presently defaulting to MD5) for all area customers.

For every client, two structures are sent out:

1. SEM bundle, which incorporates the SEM's half-key dSEM i, and 2) client group, which incorporates dui and the whole server pack. The server pack is in PKCS#7 [17] position, which is fundamentally a RSA envelope marked by the CA and encoded with the SEM's open key. The customer pack is in PKCS#12 design, which is a common key envelope additionally marked by the CA and scrambled with the client supplied key which can be a pre-set key, a secret key or a pass-expression. (A client is not expected to have a prior open key.)
2. After issuance, every client group is circulated in an out-of-band design to the fitting client. Before endeavoring any IB-mRSA exchanges, the client should first decode and check the group. A different utility project is accommodated this reason. With it, the pack is decoded with the client supplied key, the CA's mark is checked, and, at long last, the client's half-key are removed and put away locally. To unscramble a message, the client begins with sending an IB-mRSA ask for, with the SEM group piggybacked. The SEM first check the status of the customer.

Just when the customer is esteemed to be a true blue client, does the SEM procedure the solicitation utilizing the pack contained in that. As said before, to scramble a message for an IB-mRSA, that client's space endorsement should be acquired [18]. Conveyance and administration of space testaments is thought to be done in a way like that of typical endorsement, e.g., by means of LDAP or DNS.

CONCLUSION

Despite the fact that exploration enthusiasm for ID-PKC is exceptionally solid right now, it is a moderately new innovation in contrast with PKI. In our article, we have tried to investigate what isolates ID-PKC from PKI. Our underlying judgment, in fact made with regards to almost no business organization of ID-PKC frameworks, is that there is next to no to isolate the two.

Maybe the imperative info when choosing whether to embrace PKI or ID-PKC is the diverse path in which the two advances normally produce and confirm rights and keys. Similarly as with symmetric and hilter kilter cryptography, the central elements when picking amongst PKI and ID-PKC are prone to be ecological. This effect of the restrictions incorporating the utilization are inclined to be more noteworthy given that there doesn't give off an impression of being such a strong disconnecting component as the ability to give non-renouncement is among symmetric and upside down cryptography.

The paper portrays the IB-mRSA, a commonsense and secure character based encryption plan. It is perfect with standard RSA encryption and offers fine-grained control (renouncement) of clients security benefits. A few issues stay for future work. It is indistinct whether IB-mRSA can be indicated secure under the standard model (our contention uses the arbitrary prophet setting).

Also, we require a more formal investigation of semantic security. Another issue identifies with IB-mRSA execution. Utilizing a hash capacity for open key mapping makes encryption more costly than RSA since people in general type is arbitrary (and on the normal portion of the bits are set). We have to examine elective mapping capacities that can create more "effective" RSA types.

REFERENCES:

1. Lewko, A., & Waters, B. (2011). Decentralizing attribute-based encryption. In Advances in Cryptology–EUROCRYPT 2011 (pp. 568-588). Springer Berlin Heidelberg.

2. Boneh, D., & Hamburg, M. (2008). Generalized identity based and broadcast encryption schemes. In Advances in Cryptology-ASIACRYPT 2008 (pp. 455-470). Springer Berlin Heidelberg.

3. Waters, B. (2011). Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In Public Key Cryptography–PKC 2011 (pp. 53-70). Springer Berlin Heidelberg.

4. Hajny, J., & Malina, L. (2012). Unlinkable attribute-based credentials with practical revocation on smart-cards (pp. 62-76). Springer Berlin Heidelberg.

5. Li, J., Huang, Q., Chen, X., Chow, S. S., Wong, D. S., & Xie, D. (2011, March). Multi-authority ciphertext-policy attribute-based encryption with accountability. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (pp. 386-390). ACM.

6. Li, J., Ren, K., Zhu, B., & Wan, Z. (2009). Privacy-aware attribute-based encryption with user accountability. In Information Security (pp. 347-362). Springer Berlin Heidelberg.

7. Camenisch, J., Neven, G., & Rückert, M. (2012). Fully anonymous attribute tokens from lattices. In Security and Cryptography for Networks (pp. 57-75). Springer Berlin Heidelberg.

8. Shahandashti, S. F., & Safavi-Naini, R. (2009). Threshold attribute-based signatures and their application to anonymous credential systems. In Progress in Cryptology–AFRICACRYPT 2009 (pp. 198-216). Springer Berlin Heidelberg.

9. O. Baudron, D. Pointcheval, and J. Stern. Extended notions of security for multicast public key cryptosystems. In 27th International Colloquium on Automata, Languages and Programming (ICALP ’2000), number 1853 in Lecture Notes in Computer Science. Springer-Verlag, Berlin Germany, July 2000.

10. M. Bellare, A. Boldyreva, and S. Micali. Public-key encryption in a multi-user setting: Security proofs and improvements. In Preneel, pages 259–274.

11. M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations among notions of security for public-key encryption schemes. In H. Krawczyk, editor, Advances in Cryptology – CRYPTO ’98, number 1462

in Lecture Notes in Computer Science, pages 26–45. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1998.

12. M. Bellare and P. Rogaway. Optimal asymmetric encryption — how to encrypt with RSA. In A.D. Santis, editor, Advances in Cryptology – EUROCRYPT ’94, number 950 in Lecture Notes in Computer Science, pages 92–111. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1995.

13. D. Boneh, X. Ding, and G. Tsudik. Identity based encryption using mediated rsa. In 3rd Workshop on Information Security Application, Jeju Island, Korea, Aug. 2002. KIISC.

14. D. Boneh, X. Ding, G. Tsudik, and C.M. Wong. A method for fast revocation of public key certificates and security capabilities. In 10th USENIX Security Symposium, Washington, D.C., Aug. 2001. USENIX.

15. D. Boneh and M. Franklin. Identity-based encryption from the Weil Pairing. In Kilian, pages 213–229.