International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

Improving Privacy and Security in Decentralized Cipher text Policy Attribute-Based Encryption (CP-ABE)

1 Para Ramu. 2 K.Srinivas M.Tech 3 Samrat Krishna M.Tech.(Phd)
[1] (M-tech) Department of CSE Mandava Institute of Engineering Technology Vidya Nagar, Jaggayyapet. Krishna Dist, Andhra Pradesh
[2]Assistent Professor, Department of CSE Mandava Institute of Engineering Technology Vidya Nagar, Jaggayyapet. Krishna Dist, Andhra Pradesh
[3]Associate Professor, Department of CSE Mandava Institute of Engineering Technology Vidya Nagar, Jaggayyapet. Krishna Dist, Andhra Pradesh

Abstract: *In past protection safeguarding multi-expert quality based encryption (PPMA-ABE) plans, a client can secure mystery keys from numerous specialists with them knowing his/her properties and besides, a focal specialist is required. Outstandingly, a client's personality data can be separated from his/her some delicate characteristics. Consequently, existing PPMAABE plans can't completely secure clients' protection as numerous specialists can team up to recognize a client by gathering and breaking down his characteristics. Besides, ciphertext-approach ABE (CPABE) is a more effective open key encryption where the encryptor can choose adaptable access structures to encode messages. In this manner, a testing and critical work is to build a PPMA-ABE conspire where there is no need of having the focal expert and besides, both the identifiers and the ascribes can be secured to be known by the specialists. In this paper, a security saving decentralized CP-ABE (PPDCPABE) is proposed to decrease the trust on the focal specialist and ensure clients' protection. In our PPDCPABE plot, every specialist can work autonomously with no cooperation to starting the framework and issue mystery keys to clients. Moreover, a client can get mystery keys from numerous experts without them knowing anything about his worldwide identifier (GID) and properties*

Keywords: CP-ABE, Decentralization, Privacy

1. INTRODUCTION

With the improvement of the Internet and the dispersed registering innovation, there is a developing interest for information sharing and preparing in an open conveyed figuring condition. The information supplier needs to give expressive access control and information classification when speaking with clients. In addition, it is earnest for huge scale appropriated applications to help one-to-numerous correspondence mode to diminish the colossal expenses of information encryption. The traditional encryption mechanism based on public key infrastructure (PKI) [1] can achieve data confidentiality; however, it has disadvantages. On one hand, in order to encrypt data, the data provider needs firstly to obtain the public keys of authorized users and then sends the encrypted data separately tothe corresponding user, which increases the processing overhead and the bandwidth demand [2]. On the other hand, although broadcast encryption [3] can solve the efficiency problem mentioned above, the data provider must obtain the user's list before encryption. In addition, if the data

provider wants the recipient to be the one with certain identity not the one who is specified, the public key encryption will not work anymore. Therefore, more applicable encryption mechanisms are required. Identity-based encryption (IBE) [4] mechanism allows a sender to encrypt a message to an identity without accessing his public key certificate, which simplifies the certificate management procedure and reduces certificate transmission overhead. The ability to carry out public key encryption without certificates makes IBE suitable for many practical applications. For example, Alice can send a message encrypted by Bob's email address (e.g., Bob@hotmail.com) to Bob without the support of PKI. One common feature of all previous IBE schemes is that they regard identities as a string of characters. However, in 2005, Sahai and Waters [5] proposed a new type of IBE scheme called fuzzy IBE (FIBE) which regards identities as a set of descriptive attributes. FIBE can be viewed as the primary idea of ABE in which the information proprietor can scramble a message to all clients that have a specific arrangement of properties. Around the same time, Nali et al. [6] proposed an edge ABE conspire. Despite the fact that this plan can keep the agreement assaults, it presents new drawback that the edge semantics are restricted in outlining more broad frameworks which require expressive access control. In ABE plot, trait assumes an essential part. Ascribes have been abused to create an open key for encryption information and have been utilized as an entrance approach to control clients' entrance. In view of the entrance approach, resulting explores can be generally ordered [7] as either key-strategy or ciphertext-arrangement. The primary KP-ABE plot that permits any monotone access structures was proposed by Goyal et al. [7], and the primary CP-ABE plot was exhibited by Bethencourt et al. [8]. From that point onward, a few KP-ABE [9– 11] and CP-ABE plans [12– 20] were proposed. Goyal et al. [12] exhibited a limited CP-ABE conspire in the standard model, yet the principal completely expressive CP-ABE plot in the standard model was proposed by Waters [13]. In this manner, Attrapadung and Imai [21] proposed a DualPolicy ABE conspire which enables key-approach and ciphertextpolicy to follow up on encoded information simultaneously.Moreover, Müller et al. [22, 23] proposed a dispersed ABE conspire with a steady number of bilinear blending activities amid unscrambling. Yu et al. [24] proposed a fine-grained information get to control encryption plot. Tang and Ji [25] proposed an evident ABE plan, and Wang et al. [26, 27] proposed a progressive ABE (HABE) conspire in 2010 and 2011, individually. In these plans, Wang et al. utilized the disjunctive ordinary frame arrangement to create the keys progressively, accepting that all qualities in a single conjunctive provision are directed by a similar area expert. More investigations on HABE are in literary works [28– 30]. In each ABE conspire specified over, the client must go to a trusted gathering to demonstrate his personality before getting a mystery key which enables him to decode messages. Pursue [31] gave a proficient multiauthority ABE plot in which the client's mystery key is never again approved by a solitary focus expert however approved independently by various helpful

and autonomous specialists. Furthermore, there are additionally some multiauthority ABE plans [31– 37]. As per the current plans, a synopsis [38] of the criterial functionalities in a perfect ABE conspire is recorded as takes after. (1) Data secrecy: unapproved members can't know the data about the scrambled information. (2) Fine-grained get to control: with a specific end goal to accomplish adaptable access control, notwithstanding for clients in a similar gathering, their entrance rights are not the same. (3) Scalability: the quantity of approved clients can't influence the execution of the plan. In other words, the plan can manage the case that the quantity of the approved clients increments **progressively**. (4) User/characteristic disavowal: if a client stops the framework, the plan can renounce his entrance right. So also, quality disavowal is unavoidable. (5) Accountability: in every past plan, the untrustworthy clients can just specifically give away piece of their unique or changed keys with the end goal that no one can tell who has appropriated these keys. The above issue which is called key mishandle ought to be avoided by responsibility. (6) Collusion protection: the untrustworthy clients can't consolidate their ascribes to unscramble the encoded information. Keeping in mind the end goal to understand a perfect ABE conspire, some investigates which are gone for tending to the issue of client/quality denial [8, 9, 39– 48] and responsibility [49– 53] in ABE plans have been distributed on diaries or scholastic meetings. In addition, with its own particular points of interest, the characteristic based cryptosystem has the capacity and plausibility to be connected to different territories. Especially, heaps of studies which center around the uses of ABE in intermediary reencryption [54– 59] have been proposed.

2. Review:

Enhancing protection and security in decentralized ciphertext-arrangement property based encryption :Attributebased Encryption Sahai and Waters presented the main quality based encryption (ABE) where both the ciphertext and the mystery key are marked with an arrangement of properties. A client can unscramble a ciphertext if and just if there is a match between the properties recorded in the ciphertext and the qualities held by him. ABE plans can be arranged into two sorts: key-approach ABE (KPABE) and ciphertext-strategy ABE (CP-ABE). KP-ABE. In a KP-ABE plot, the ciphertext is related with an arrangement of qualities, while an entrance structure is installed in the mystery keys CP-ABE. In a CP-ABE conspire, an entrance structure is inserted in the ciphertext, while the mystery keys are related with an arrangement of characteristics

Multi-Authority Attribute-based Encryption : In the original work, Sahai and Waters left an open issue, specifically how to build an ABE plot where the mystery keys can be separated from various experts with the goal that clients can diminish the trust on the focal specialist. Pursue addressed this inquiry positively by proposing a MAABE conspire. As specified in, the specialized obstacle in building a MA-ABE plot is to oppose the agreement assaults. To beat this obstacle, all mystery keys of a client are fixing to his GID. In [10], different experts must collaborate to instate the framework,

and a focal specialist is required. Lin et al. proposed a MAABE plot where the focal specialist isn't required. This plan was inferred fromthe conveyed key age (DKG) convention and the joint zero mystery sharing (JZSS) convention. To instate the framework, the numerous experts should cooperatively execute the DKG convention and the JZSS convention twice and k times, individually, where k is the level of the polynomial chose by every specialist. Every expert must keep k+2 mystery keys. Besides, this plan is k-versatile, to be specific the plan is secure if and just if the quantity of the traded off clients is close to k, and k must be settled in the setup arrange. Muller et al. [20] proposed a disseminated CP-ABE conspire.

This plan was turned out to be secure in the bland gathering [4], rather than lessening to a many-sided quality supposition. In this plan, a focal specialist is required to produce the worldwide key and issue mystery keys to clients. A completely secure multi-expert CP-ABE (MACP-ABE) conspire in the standard model was proposed by Liu et al.[21]. This plan depended on the past CP-ABE plot [8]. In this plan, there are numerous focal experts and quality specialists. The focal experts circulate character related keys to clients, while the trait specialists disseminate ascribe related keys to clients. Preceding having property keys from the characteristic specialists, the client must get mystery keys from the numerous focal experts. This plan was developed in the bilinear gathering with Composite request (N = p1p2p3). Lekwo and Waters [11] proposed another MA-ABE schemecalled decentralizing CP-ABE (DCP-ABE) conspire. This plan enhanced the past MA-ABE plans that require joint efforts among different specialists to beginning the system.In this plan, no collaboration between the numerous experts is required in the setup organize and the key age arrange, and a focal specialist isn't required. Quite, an expert in this plan can join or leave the framework progressively without the need to reinitialize the framework. The plan was developed in the bilinear gathering with composite request (N = p1p2p3), and accomplished full (versatile) security in the arbitrary prophet display. Moreover, they additionally proposed two strategies to make a prime request gather variation of their plan. All things considered, the specialists can gather a client's traits by following his GID. Pursue and Chow initially proposed [12] a security saving MAABE (PPMA-ABE) conspire which enhanced the past plan [10] and expelled the need of a focal authority.In past MA-ABE plans, to acquire the relating mystery keys, a client must present his GID to every specialist.

Henceforth, numerous experts can team up to gather the client's characteristics by his GID. In Chase and Chow gave a mysterious key issuing convention for the GID by utilizing the 2-party secure figuring procedure. Accordingly, a gathering of specialists can't team up to gather the clients properties by following his GID. In any case, the various specialists must coordinate to beginning the framework. In the interim, each match of experts must execute the 2-party key trade convention to share the seeds of the chose pseudorandom capacities (PRFs) [22]. This plan is N −2 tolerant, specifically the plan is secure if and just if the quantity of the bargained experts is close to N − 2, where N is the quantity of the

experts in the framework. The experts can't know any data about the client's GID, yet they can know the client's qualities. Pursue and Chow [12] additionally left an open testing research issue on the most proficient method to build a PPMA-ABE conspire without the need of participation's among specialists. Li [15] proposed a MACP-ABE plot with responsibility. In this plan, the mysterious key issuing convention [12] was utilized. In particular, a client can be recognized when he shared His mystery keys with others. In like manner, the various experts must coordinate to introduce the framework. As of late, a protection saving decentralized KP-ABE (PPDKP-ABE) conspire was proposed by Han et al. . In this plan, various specialists can work freely with no coordinated effort. Particularly, a client can get mystery keys from various specialists without discharging anything about his GID to them, and the focal expert isn't required. Qian et al. Proposed a security safeguarding decentralized CPABE (PPDCP-ABE) conspire where basic access structures can be executed. All things considered, like that in the experts in these plans can likewise gather the client's properties. C. Mysterious Credential In an unknown accreditation framework [23], a client can get a certification from a guarantor, which incorporates the client's pen name properties. By utilizing it, the client can persuade an outsider that he gets a qualification containing the given pen name characteristics without discharging some other data. In a numerous show accreditation framework [24], a certification can be shown a subjective number of times, and can't be connected to each other. In this manner, while developing our PPDCP-ABE, we expect that every client has gotten an unknown certification including his GID and qualities. At that point, he can persuade the different experts that he has a GID and holds the relating traits by utilizing the unknown accreditation procedure.

Multi-Processor Architectural Support for Protecting Virtual Machine Privacy in Untrusted Cloud Environment :Cloud figuring is altering the data innovation, extending from individual to big business to government registering. While distributed computing can give computational and capacity assets on request and requiring little to no effort, it makes new security/protection issues. This is on a very basic level caused by the division of asset clients (i.e., cloud inhabitants) from asset proprietors (i.e., cloud providers).New dangers and concerns include: (I) disappointments in guaranteeing detachment between occupants as far as capacity and memory;(ii) subversion of hypervisor or Virtual Machine Monitor (VMM) [1]; (iii) assaults propelled from one Virtual Machine (VM) against the host stage or the other found VMs on a similar stage [2, 3]; (iv) listening stealthily an occupant's VM substance by a bargained VMM, untrusted asset proprietors, or vindictive insiders. These dangers have caused a huge level of hesitance in embracing the cloud worldview [4,5]. As indicated by a review of in excess of 500 worldwide administrators and IT chiefs in 17 nations [6], 20% officials put stock in their inner frameworks over the cloud because of worries about security dangers and loss of control over information and frameworks. To be sure, numerous

server farm clients request their administrations to be facilitated by devoted servers that are physically separated from other clients' servers. This would demolish, to a vast degree, the benefits of distributed computing that are basically in light of virtualization and sharing of physical assets.

Access control and secure information recovery in light of ciphertext strategy property based encryption in decentralized DTNS : Now days numerous figuring gadgets e.g. PDAs, advanced mobile phones, sensors have remote interfaces and subsequently can frame specially appointed systems. Remote adhoc systems enable hubs to speak with each other without depending on any settled framework. These quickly deployable systems are extremely valuable in a few situations e.g. [1] military system conditions, associations of remote gadgets conveyed by troopers might be briefly disengaged by ecological variables, sticking and versatility, particularly when they work in earthly situations. Disturbance tolerant system (DTN) innovations are getting to be effective arrangements that enable hubs to speak with each other in these extraordinary earthbound conditions [2]-[4]. Commonly, when there is no conclusion to-end association between a source and a goal combine, the messages from the source hub may need.To sit tight in the transitional hubs for a significant measure of time until the point when the association would be in the long run set up. For capacity and imitate the information stockpiling hub is presented [5][6]where approved portable hubs can get to the essential data rapidly. Numerous military applications require expanded security of secret information including access control techniques that are cryptographically upheld [7], [8]. By and large, it is alluring to give separated access administrations with the end goal that information get to approaches are characterized over client properties or parts, which are overseen by the key specialists. Numerous key specialists deal with their quality autonomously in DTN [9], [10]. The idea of property based encryption (ABE) [11]– [14] is a promising methodology that satisfies the prerequisites for secure information recovery in DTNs. ABE highlights a system that empowers an entrance control over scrambled information utilizing access strategies and credited characteristics among private keys and ciphertexts. Particularly, ciphertexts-arrangement ABE (CP-ABE) gives a versatile method for encoding information with the end goal that the encryptor characterizes the characteristic set that the decryptor needs to have so as to decode the ciphertext [13].Thus, diverse clients are permitted to unscramble distinctive bits of information per the security approach. Be that as it may, the issue of applying the ABE to DTNs presents a few security and protection challenges. Since a few clients may change their related characteristics sooner or later (for instance, moving their locale), or some private keys may be traded off, key renouncement (or refresh) for each property is essential keeping in mind the end goal to make frameworks secure. In any case, this issue is much more troublesome, particularly in ABE frameworks, since every characteristic possibly shared by different clients (from now on, we allude to such a gathering of clients as a trait gathering).

This derives renouncement of any property or any single customer in a trademark social occasion would impact exchange customers in the group.For case, if a customer joins or leaves a quality assembling, the associatedattribute key should be changed and redistributed to the different people in a comparable get-together for in invert or forward puzzle. It may realize bottleneck in the midst of rekeying procedure or security debasement as a result of the windows of powerlessness if the past trademark key isn't revived in a flash. One all the more troublesome issue is Key escrow issues ,CP-ABE, master's ruler puzzle key is used to makes private keys of customers related course of action of attributes. Along these lines, the key specialist can decode each figure content routed to particular clients by creating their trait keys. In the event that the key specialist is bargained by foes when conveyed in the threatening conditions, this could be a potential danger to the information secrecy or security particularly when the information is exceptionally delicate. The key escrow is an inalienable issue even in the multipleauthority frameworks as long as each key expert has the entire benefit to create their own quality keys with their own particular ace insider facts. Since such a key age instrument in view of the single ace mystery is the fundamental strategy for a large portion of the unbalanced encryption frameworks, for example, the property based or character based encryption conventions expelling escrow in single or various expert CP-ABE is a critical issue. The last test is the coordination of characteristics issued from various experts. At the point when various specialists oversee and issue ascribe keys to clients autonomously with their own particular ace insider facts, it is difficult to characterize fine-grained get to approaches over traits issued from various experts. For instance, assume that traits "part 1" and "district 1" are overseen by the specialist An, and "part 2" and "locale 2" are overseen by the expert B. At that point, it is difficult to create an entrance strategy (("part 1" OR "part 2") AND ("locale 1" or "area 2")) in the past plans on the grounds that the OR rationale between traits issued from various specialists can't be actualized. This is because of the way that the distinctive specialists produce their own trait keys utilizing their own particular free and individual ace mystery keys. Along these lines, general access strategies, for example, " - out-of-"rationale, can't be communicated in the past plans, which is an extremely reasonable and normally required access arrangement.

ABE comes in two flavors called key-strategy ABE (KP-ABE)andciphertext-arrangement ABE (CP-ABE). In KP-ABE, the encryptor just gets the opportunity to mark a ciphertext with an arrangement of properties. The key expert picks an approach for every client that figures out which ciphertexts he can unscramble and issues the way to every client by inserting the strategy into the client's critical. However the parts of the figure messages and keys are turned around in CP-ABE. In CP-ABE, the ciphertext is scrambled with an entrance arrangement picked by an encryptor, however a key is basically made as for a characteristics set. CP-ABE is more proper to DTNs than KP-ABE in light of the fact that it empowers encryptorssuch as a leader to pick an entrance approach on credits and

to scramble private information under the entrance structure by means of encoding with the relating open keys or characteristics [4], [7], [15] area of hub followed to lessen overhead [18].

Powerful Data Retrieval in Disruption Tolerant Networks Using Cipher Text Policy-Attribute Based Encryption :The Disruption tolerant systems [1] has numerous application, for example, space condition and earthly condition in which earthbound condition for the most part worried about IntermittentlyConnected Networks(ICNs) and recurrence partitions(FPs), where ICNs doesn't avert correspondence between the disengaged territories and FPs doesn't take into account asset distribution. The earthly condition of DTN is imagined for Under Water Networks (UMNs), Pocket Switched Networks (PSNs), Vehicular Ad-hoc Networks (VANETs) and Airborne Networks (ANs). UMNs are sent to perform community oriented checking assignments over an oceanographic territory. The qualities of UMNs are transmission misfortune, clamor, multipath, high deferral and postpone difference and doppler spread PSN is another correspondence worldview for cell phones. It exploits each correspondence opportunity, and the physical versatility of the gadgets, so as to transport information to goals. VANET utilizes autos as versatile hubs in a MANET to make a portable system. A VANET changes each sharing auto into a remote switch or center, allowing automobiles around 100 to 300 meters of each other to interface and, in this manner, make a framework with a wide range. ANs are proposed arrange in which all hubs would be situated in flying machine. The system is proposed for use in flying interchanges, route, and reconnaissance (CNS) and would likewise be valuable to organizations, private Internet clients, and government offices, particularly the military. The property based encryption is a promising methodology for encryption and decoding utilizing open key encryption (PKE), Identity based encryption (IDE), Fuzzy character based encryption (FuzzyIDE), Cipher-content strategy or key approach characteristic based encryption (CP-ABE or KP-ABE) [2], [8]. The idea of trait based encryption (ABE) [4],[7] gives get to arrangements and portrayed qualities among private keys and Cipher content. The significant contrast between CP-ABE and KP-ABE in Cipher text– strategy ABE [2], [5], get to arrangement is related in the Cipher content and in key-approach ABE get to strategy is related with the private key.

Figure Text - Policy Attribute based Encryption for Secure Data Retrieval in Disruption Tolerant Military Networks (DTN) :The Cipher content - approach Attribute Based Encryption for secure information recovery in decentralized Disruption Tolerant Networks (DTNs) where different key specialists deal with their traits freely. Prompt trait renouncement improves in reverse/forward mystery of secret information by decreasing the windows of weakness. Key escrow issue is settled by a sans escrow key issuing g tradition that undertakings the typical for the decentralized Disruption Tolerant Networks configuration proposed a decentralized approach; their strategy does not validate clients. Show how to apply the proposed system to safely and effectively deal with

the private information disseminated in the interruption - tolerant military system.

3. Implementation:-

Existing System :Our scheme is constructed in the standard model, while the existing DCP-ABE scheme was designed in the random oracle model. The existing scheme. Since delicate traits can likewise uncover the clients' characters, existing plans can't give a full answer for ensure clients' security in MA-ABE plans. We misuse the set-enrollment confirmation system. For each trait, the expert indicates an un forgeable confirmation label with the end goal that a client can demonstrate in zero information that the characteristic for which he is having a mystery key is observed by the specialist.

Proposed System:

The proposed PPDCP-ABE plan can give more grounded security insurance contrasted with the past PPMA-ABE plans where just the GID is ensured. Proposed a disseminated CP-ABE plot. This plan was ended up being secure in the non specific gathering, rather than decreasing to a multifaceted nature supposition. In this plan, a focal specialist is required to create the worldwide key and issue mystery keys to clients. A totally secure multi-master CP-ABE (MACP-ABE) scheme in the standard model was proposed. This arrangement relied upon the past CP-ABE plan. In this arrangement, there are various central specialists and quality masters.

Advantage

- The central authorities distribute identity related keys to users, while the attribute authorities distribute attribute-related keys to users.
- Preceding having quality keys from the trait experts, the client must get mystery keys from the various focal specialists.
- In this scheme, multiple authorities can work independently without any collaboration. Drawback of these papers (future work)
- This scheme not effective result for key encryption processes.
- Need for more privacy.
- Need for new method for security enhancement
- This key process is centralized authority using here. But key static process using there.
- We need change the random key process
- We must using AES 256bit key process. This is high level bit encryptions.
- Need for time limit for key process.
- Find the internal packet missing problem.
- Trace out the missing packet

4. Conclusion:-

The paper discusses here provide secure and scalable sharing of data in a multiple owner, multiple user, multiple authority scenario. The Security in transmitting file is ensuredthrough AES. As the next level, ABE is used to encrypt the owner’s data and

the encrypted file is stored in cloud server. Steganography ensures the secured key transformation from sender to receiver. Proxy cloud is established to reject the unauthorized access .once unauthorized access is suspected then sender can destroy the connection with the receiver .Thus the paper provide two level security using ABE and AES with proxy. Hence the paper is more secured than the previous privacy preserving decentralized cipher-text policy attribute based encryption (PPDCP-ABE) .

REFERENCES

[1] N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: survey," Future Gen. Comput. Sys., vol. 29, no. 1, pp. 84–106, Jan. 2013.

[2] G. Le, K. Xu, M. Song, and J. Song, "A survey on research on mobile cloud computing," in Proc. 10th IEEE/ACIS/Int. Conf. Comput. Inf. Sci.,2011, pp. 387–392.
[3] X. F. Qiu, J. W. Liu, and P. C. Zhao, "Secure cloud computing architecture on mobile Internet," in Proc. 2nd Int. Conf. AIMSEC, 2011, pp.619–622.

[4] W. G. Song and X. L. Su, "Review of mobile cloud computing," in Proc. IEEE 3rd ICCSN, 2011, pp. 1–4.

[5] ABI Research Report, Mobile Cloud Applications.
[Online].Available:http://www.abiresearch.com/res earch/ 1003385-Mobile+Cloud+ Computing

[6] P. Urien, E. Marie, and C. Kiennert, "An innovative solution for cloud computing authentication: Grids of EAP-TLS smart cards," in Proc. 5th Int. Conf. Digit. Telecommun., 2010, pp. 22–27.

[7] H. Ahn, H. Chang, C. Jang, and E. Choi, "User authentication platform using provisioning in cloud computing environment," in Proc. ACN CCIS,2011, vol. 199, pp. 132– 138.

[8] H. Chang and E. Choi, "User authentication in cloud computing," in Proc. UCMA CCIS, 2011, vol. 151, pp. 338–342.

[9] J. L. Tsai, N. W. Lo, and T. C. Wu, "Secure delegation-based authentication protocol for wireless roaming service," IEEE Commun. Lett., vol. 16, no. 7, pp. 1100–1102, Jul. 2012.

[10] W. Itani, A. Kayssi, and A. Chehab, "Privacy as a service: Privacy-aware data storage and processing in cloud computing architectures," in Proc. IEEE Int. Conf. Dependable Auton. Secure Comput., 2009, pp. 711–716.

[11] S. Pearson, "Taking account of privacy when designing cloud computing services," in Proc. CLOUD ICSE Workshop Softw. Eng. Challenges CloudComput., 2009, pp. 44–52.

[12] H. Takabi, J. B. D. Joshi, and G. Ahn, "Security and privacy challenges in cloud computing environments," IEEE Security Privacy, vol. 8, no. 6, pp.24–31, Nov./Dec. 2010.