International Journal of Engineering and Techniques - Volume 4 Issue 2, Mar-Apr 2018

RESEARCH ARTICLE OPEN ACCESS

SECURE PRIVACY DATA COLLECTION, STORAGE AND ACCESS IN CLOUD-ASSISTED INTERNET OF THINGS

[1*]AILINENI SAI PRASANNA, MODDU SAMPOORNA[2]

[12]ASSISTANT PROFESSOR ,DEPT OF CSE, SRI INDU COLLEGE OF ENGINEERING AND TECHNOLOGY,TELANGANA

Abstract

Cloud-assisted Internet of Things (IoT) gives a promising answer for data blasting issues for the capacity imperatives of individual items. Notwithstanding, with the use of cloud, IoT faces new security challenges for data commonality between two gatherings, which is presented without precedent for this paper and not as of now tended to by customary methodologies. We explore a safe cloud-assisted IoT data overseeing technique to keep data confidentiality when gathering, putting away and getting to IoT data with the help of a cloud with the thought of clients' addition. The proposed framework novelly applies an intermediary re-encryption plot, which was proposed in [5]. Subsequently, a safe IoT under our proposed technique could oppose most assaults from the two insiders and outcasts of IoT to break data confidentiality, and in the mean time with steady correspondence cost for re-encrytion against incremental size of IoT. We additionally demonstrate the strategy is viable by numerical outcomes.

Index Terms—Cloud-Assisted IoT, Data Security, Confidentiality.

I. INTRODUCTION

As of late, flexible IoT frameworks have been generally conveyed in day by day life, for instance, in human services and activity observing, which produce giga-level top notch pictures and recordings consistently. Gigantic IoT data require unreasonably vast capacity and superior calculation that a typical client or keen question inside IoT scarcely bolsters. Cloud-assisted IoT is prominently connected to use the calculation and capacity ability of a cloud for monstrous IoT data [1]. A cloud is an intense stage that can give extra comforts as a data dispersion appoint. At the point when an IoT client has lawful demands for specific data being gathered, put away and got to, he can specifically assign the solicitations to the cloud whenever with more prominent comfort.

In any case, the accommodation that cloud conveys to IoT comes at the cost of conceivably new security dangers, which have never been considered in a customary IoT framework. In both hypothesis and practice, a cloud is broadly perceived as a genuine yet inquisitive gathering [2]. This implies a cloud will deal with client appointed undertakings yet scarcely ensure confidentiality of client data.

This drawback is a basic snag when constructing any cloud-assisted IoT framework. Also, overcoming these secu-rity challenges is a major issue because of the flexible elements of cloud-assisted IoT frameworks and the adaptable security re-quirements of clients. Dissimilar to the security of conventional IoT [3], this kind of issue can't be consummately settled in a brief span period. Ordinarily, trust-depended framework is connected as an answer for those dangers . Be that as it may, trust-depended framework can not give provable security, which brings down the security level of IoT. Likewise, in IoT situations, it isn't viable to apply data anonymization and muddling [4] to ensure security for dynamical task (addition or erasure) particularly when converging with cloud, since they are connected for protection pre-serving without provable security. Since that we propose a structure in light of cryptographic techniques to help data security in cloud-assisted IoT. In this paper, conventional IoT alludes to IoT without the help of a cloud. Aside from confidentiality, different sorts of security issues, for example, honesty and verification are not considered.

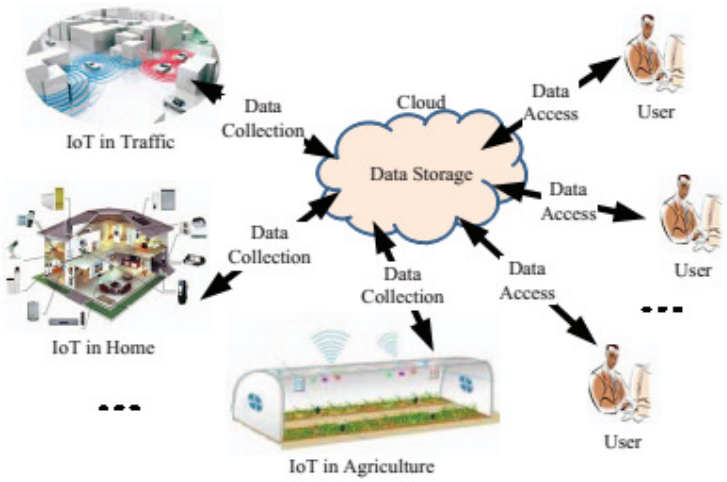

Fig. 1. Some Fundamental Functions of A Cloud-Assisted IoT.

In this paper, we dynamic some crucial models of data move in a cloud-assisted IoT framework (as appeared in Figure 1), and talk about promising cryptographic techniques to keep data confidentiality in these models. In a cloud-assisted IoT framework, clients can assign their data gathering undertakings to cloud, store their IoT data in cloud and access the normal data on cloud. Correspondingly, the primary test is that the security models of IoT ought to be altered to characterize potential assailants that could show up while spanning IoT with a cloud. The second test is the effects under the adaptability of an IoT while keeping security. Encoded figure will costs incremental weight to the framework with expanded number of clients.

We explore our intermediary re-encryption conspire named contingent personality based communicate intermediary re-encryption (CIBPRE) in [5] and think that its accessible to our models for security. Consequently we individually propose conventions to the data exchange models in view of CIBPRE. The new technique seems promising with provable security when re-encoding data in data accumulation step and meaning keys to clients by key age focus (KGC). It could oppose assaults from both in-siders and outcasts of IoT to soften data confidentiality up our security show and keep up consistent cost on correspondence with expanding number of IoT clients.

In the accompanying areas, we for the most part center around our promising arrangements against dangers in the principal data exchange models. We separately talk about our decision on the best possible encryption strategies in cloud-assisted IoT, survey our CIBPRE plots and present the safe data exchange conventions in light of the CIBPRE plan and encryption techniques to accomplish confiden-tiality when gathering, putting away and getting to IoT data with the help of a cloud. Finally, we dissect the exhibitions of our proposed conventions and examinations with the customary IBE and PKE plans.

II. SECURITY RISKS AND CHALLENGES

Over the previous decade, the exploration on the confidentiality of customary IoT has pulled in a great deal of consideration. Accordingly, numerous cryptographic strategies, for example, the works recorded in [6], [7], were proposed to ensure data confidentiality of IoT while sparing however much of the calculation and correspondence costs as could reasonably be expected because of the restricted capacity of IoT. These past works give a principal foundation to considering the dangers and difficulties in cloud-assisted IoT when a cloud is utilized.

As needs be, we separate every single savvy question of IoT into two classifications: IoT-inside items and IoT-edge objects. IoT-inside items just speak with different questions in an IoT, while IoT-edge objects are brilliant articles that likewise speak with cloud servers. In this paper, we just focus on the new issues of IoT-edge confidentiality, which are caused by commonality between any IoT-edge question and any cloud server. As it were, IoT-inside confidentiality, which is the confidentiality of data conveyed among brilliant articles exhibited in [12], [10], [11], is excluded in this paper.

In this area, we talk about security models of IoT-edge confidentiality. These models build up rules, including who could be aggressors to break the confidentiality of cloud-assisted IoTs, and a few difficulties while embracing encryption techniques to oppose these assailants. Alluding to Fig. 1, the conceivable assailants are as per the following:

- IoT-edge items could be aggressors. By and by, those promotion versarial items might be caused by some illicit people. They wrongfully control existing articles or produce some new protests join an IoT framework. These ill-disposed articles are inside assailants who take delicate data from other legitimate items.

- The fair however inquisitive cloud could be an assailant (as said in the primary segment). Besides, some outstanding and customary assurance procedures are ineffectual for accomplishing our coveted goals.

- A client who gets to IoT data from the cloud could be an assailant. The cloud is an open stage that gives data gathering, stockpiling and access administrations for various clients. Practically speaking, distinctive clients clearly have diverse rights to get to various IoT data. A few clients might be interested about other clients' IoT data.

- The last kind of aggressor is a spy. A roof dropper can acquire all the exchanged data, for example, the data exchanged between an IoT-edge question and the cloud, and the data between the cloud and clients. We don't consider a spy who might want to listen stealthily within correspondence of an IoT framework on the grounds that such a meddler has been broadly considered in past works [6], [7].

As investigated by [9], a dream of conceivable dangers in cloud-assisted IoT is investigated, which list the data confidentiality of IoT as the fundamental one in IoT however without powerful arrangements. There additionally exists comparable works [8] to keep these dangers chiefly by conventional PKI plans, which claims the deficiencies of customary PKI plans that we list in the accompanying area. As alluded, most past works depend on conventional cryptographic strategies.

Our work comprises of three stages: security ensures on data gathering, data stockpiling and data get to. Diverse stages think about various aggressors. In the data accumulation stage, the principle assaults are normally caused by antagonistic IoT-edge items and spies. Cloud submits the primary assaults in the data stockpiling stage. In the data get to stage, the antagonistic clients and spies are the fundamental assailants.

As per the diverse attributes of aggressors, the accompanying difficulties must be tended to:

- To oppose busybodies, all correspondences ought to be made in a safe channel or encoded. In addition, no busybody should recognize what the decoding keys are.

- To oppose the ill-disposed IoT-edge questions, all IoT-edge objects must have diverse keys to encode their data in the data accumulation stage. At the end of the day, no question can unscramble other articles' ciphertexts.

- To oppose the hazard caused by the cloud, all IoT data are put away as ciphertexts in the cloud. Additionally, the cloud can't decode any ciphertext.

- To oppose the ill-disposed clients, the customary access control is ineffectual. Conventional access control enables a server to react to a client's data ask for if the client has the relating right. All data are normally put away as plaintexts in the server. Henceforth, the customary access control can oppose the antagonistic clients if the server is completely trusted. Something else, the server will sidestep the customary access control and straightforwardly send touchy data to the ill-disposed clients. Since the cloud is straightforward however inquisitive, plainly conventional access control can't be utilized to accomplish our destinations. In the accompanying area, we propose that encryption-based access control is a promising arrangement.

In synopsis, the above discourses show the security challenges in our work and propose that encryption is a promis-ing strategy to address them. Nonetheless, the utilization of encryption alone does not address the greater part of our goals. In cryptography, there are a wide range of encryption strategies that have particular properties. Our next undertaking is picking a particular encryption strategy.

III. ENCRYPTION SCHEMES IN A CLOUD-ASSISTED IOT

The initial step to building up a safe cloud-assisted IoT is to pick idealize encryption techniques between two classified plans, open key encryption (PKE) and symmetric-key encryption (SKE).

The essential contrast of PKE and SKE is whether to apply unbalanced key or symmetric key. Since that, while receiving PKE in cloud-assisted IoT, clients and IoT-edge objects don't should be online at the same time. Interestingly, with SKE, clients and IoT-edge objects must be online all the while.

PKE more often than not requires substantially more time than SKE to produce a ciphertext. In any case, the execution time isn't a critical shortcoming of PKE since the time cost of PKE isn't specifically connected to the record however to its private key. While scrambling a record with a marginally bigger size, the time cost of PKE won't be the principle factor influencing the execution of the cloud-assisted IoT framework.

In rundown, PKE (uniquely IBE) is a superior decision than SKE. Review that cloud is useful for IoT on the grounds that more IoT frameworks produce enormous data that clients regularly don't have the ability to deal with. For gigantic IoT data, the time cost of PKE won't be a huge factor influencing the execution of the cloud-assisted IoT framework.

While utilizing PKE in the cloud-assisted IoT arrangement of our work, all IoT-edge articles and clients have singular open and private keys, and private keys are utilized to decode the relating PKE ciphertexts. Typically an open key administration framework, for example, open key foundation (PKI [13] isrequired; otherwise,the expected collector's open key may not be acquired. Be that as it may, the administration framework could be excessively intricate for a cloud-assisted IoT framework to be pragmatic. Thus, we present character based encryption (IBE) [14] to keep away from the necessity of an administration framework. In IBE, any one can accept an open way of life as an open key. Subsequently, it is anything but difficult to acquire others' personalities. Decisively, IBE is a promising decision to our protected cloud-assisted IoT. We apply a particular IBE conspire proposed in our past work [5] in this paper since its special properties.

IV. A SPECIFIC IBE SCHEME

In reference [5], we proposed an extraordinary IBE plot called restrictive character based communicate intermediary re-encryption (CIBPRE). As a rule, in a CIBPRE framework, a trusted KGC instates the framework parameters of CIBPRE and produces private keys for clients. To secretly share a few data to different recipients, a sender can encode the data with the planned beneficiaries' personalities under a data-sharing condition.

While accepting the encoded data, these collectors can in-conditionally decode the data utilizing their private keys. On the off chance that the sender might later additionally want to share the data related with a similar condition with different beneficiaries, the sender can assign a re-encryption key marked with the condition to the intermediary. At that point, the intermediary can re-encode the underlying ciphertexts coordinating the condition to the subsequent collector set. While accepting the re-scrambled ciphertexts, these new recipients can

autonomously decode the data utilizing their private keys. The underlying ciphertexts might be put away remotely while being kept mystery. The sender does not have to download and re-encode tediously but rather can rather appoint a solitary key coordinating the condition to the intermediary. These highlights make CIBPRE a flexible device for securing remotely put away data, particularly when there are distinctive beneficiaries to share the data.

Let N ∈ N be the maximal size of the recipient set for one CIBPRE encryption or re-encryption. Let (X , SEx, SDx) be a SKE plan, for example, AES (the well known decision practically speaking), where X is the symmetric-key space and SEx and SDx separately indicate the encryption and decoding calculations, both with a symmetric key x ∈ X . CIBPRE comprises of following calculations:

- Setup(λ, N): Given a security parameter λ ∈ N and esteem N , this calculation yields the ace open param-eters PK and the ace mystery parameters MK, where (X , SEx, SDx) ⊂ PK .

- Extract(MK, ID): Given MK and a personality ID, this calculation yields the private key SKID .

- Enc(PK, S, F, α): Given PK, a set S of a few personalities (where |S| ≤ N), data F and a condition α, this algo-rithm haphazardly picks a mystery key k ∈ X , creates an underlying CIBPRE ciphertext C1 of k and a SKE ciphertext C2 = SEk(F) of F and yields an underlying ciphertext C = (C1, C2).

- RKExtract(PK, ID, SKID , S , α): Given PK, a character ID and its private key SKID , a set S of a few personalities (where |S | ≤ N) and a condition α, this calculation yields a re-encryption key dID→S |α.

- ReEnc(PK, dID→S |α, C, S): Given PK, a re-encryption key dID→S |α, an initial ciphertext

C = (C1, C2) and a set S of a few characters (where |S| ≤ N), this algorithm generates a re-encoded and yields a re-scrambled CIBPRE ciphertext C1 of C1 ~ ~ , C2).ciphertext C = (C1

- Dec-1(PK, ID, SKID , C, S): Given PK, an identityID and its private key SKID , an underlying ciphertext C = (C1, C2), and a set S of a few personalities (where |S| ≤ N), if ID ∈ S, this calculation unscrambles the underlying CIBPRE ciphertext C1 to get a mystery key k and yields data F = SDk(C2).

- -(, ID , SKID , C,): Given , a personality ID and its private key SKID , a re-encoded ciphertext S C = (C1, C2) and a set of a few characters (where |S | ≤ N), if ID ∈ S , this calculation unscrambles the re-scrambled CIBPRE ciphertext C1 to get a mystery key k and yields data F = SDk(C2).

Extra scientific insights about CIBPRE are let well enough alone for this paper because of the constrained space.

V. CONFIDENTIAL DATA COLLECTION

In this section, we describe how to to apply CIBPRE to achieve confidential data collection in a cloud-assisted IoT system. In the data collection phase, a user (note that an IoT-edge object can also be a user) can delegate a data collection task to the cloud, and all related IoT-edge objects then upload their data to the cloud. As we have mentioned previously, all IoT-edge objects must have different keys to encrypt their data before sending their data to the cloud. This requirement is easy with CIBPRE because the real key for encrypting data in algorithm Enc is randomly chosen. Suppose that KGC has published the generated master public parameters PK and has generated private keys for all IoT-edge objects and users and that KGC never generates any private key for the cloud (this assumption is valid because no one would like to generate such critical information for a potential attacker). These assumptions are also valid in the other phases of our work. Fig. 2 shows the main steps of the data collection phase.

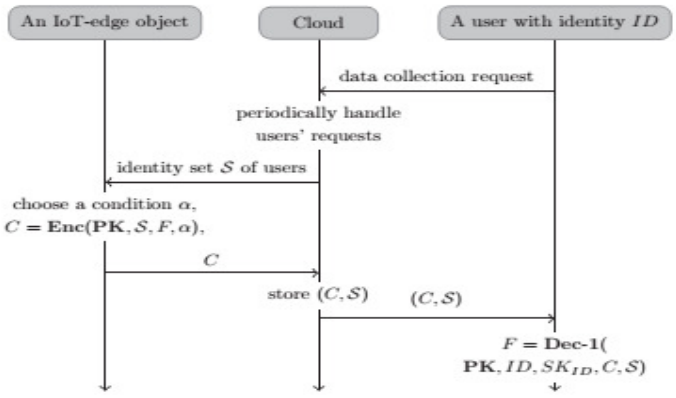

Fig. 2. The main steps of the data collection phase.

Fig. 2. The main steps of the data collection phase.

The details are described as follows:

1) Users sends their data collection request and identities to the cloud.

2) The cloud periodically handles users' requests. Suppose that the users in identity set S want to collect the data F from an IoT-edge object. The cloud sends the set S and data collection request to the IoT-edge object.

3) The IoT-edge object verifies the users' identities in the set S and eliminates the invalid identities. Suppose that all users in the set S are valid. The IoT-edge object chooses a data-sharing condition α (which will be useful in the data access phase), encrypts the data F by algorithm C = Enc(PK, S, F, α), and sends the ciphertext C to the cloud.

4) The cloud stores the ciphertext C and the set S and forwards (C, S) to the users in S.

5) All users in S independently decrypt the data F using algorithm Dec-1(PK, ID, SKID , C, S).

In step 2 above, we allow the cloud to periodically handle users' requests. This method can save us the communication cost associated with ciphertexts because CIBPRE allows the IoT-edge object to generate a constant-size ciphertext for mul-tiple users. However, if the cloud handles users requests one by one, it is obvious that the size of the generated ciphertexts is linearly related to the number of users. In addition, a user can start a data collection request, as is done in the above data collection phase, and an IoT-edge object can also actively start a data collection task by itself. To achieve this, an IoT-edge object encrypts its data by its own identity using algorithm Enc and uploads the generated initial ciphertext to the cloud. Because this step is very easy, we omit it in the above data collection phase.

With the respect of confidentiality, all data are transferred as ciphertexts. According to the confidentiality of CIBPRE, only the users in the set S can decrypt the ciphertext C. In other words, none of the eavesdroppers, cloud and non-intended users can learn anything about the data F from the ciphertext C.

VI. CONFIDENTIAL DATA STORAGE

According to the above data collection phase, it is easily determined that the data storage phase is confidential. Without loss of generality, suppose that the cloud want to learn some-thing encrypted in the ciphertext C, which was generated in the above data collection phase. The confidentiality of CIBPRE guarantees that except the users in the set S, no one can learn anything about the data F from the ciphertext C. Hence, the only possible method for the cloud to break the ciphertext C in the data storage phase is colluding with one of the users in the

set S. However, it is practical to assume none of the users in the set S collude with the cloud, as no one would like to actively leak his sensitive data to an attacker.In the data access phase, the cloud can break the ciphertext C using another possible method, which is discussed in the next section.

VII. CONFIDENTIAL DATA ACCESS

In this section, we show how to apply CIBPRE to confi-dential data access in a cloud-assisted IoT system. In the data access phase, a user can share his collected IoT data with other users with the assistance of the cloud. At the same time, the cloud cannot disobey the user's request to share the non-expected data with other users or share the expected data with non-intended users. Otherwise, the cloud can possibly know the users' data. Suppose that a user with identity ID wants to share another user's data F , where the latter user has identity ID and the data F were stored as an initial ciphertext C in cloud (this step was achieved in the above data collection phase). Fig. 3 shows the main steps of the data access phase.

The details are described as follows:

1) The user ID sends his identity and data-sharing request to the cloud.

2) The cloud periodically handles users' data-sharing re-quests. Suppose that all users in identity set S want to share the same data of user ID. The cloud sends the data-sharing request and the set S to the user ID.

An user with identity ID Cloud A user with identity ID

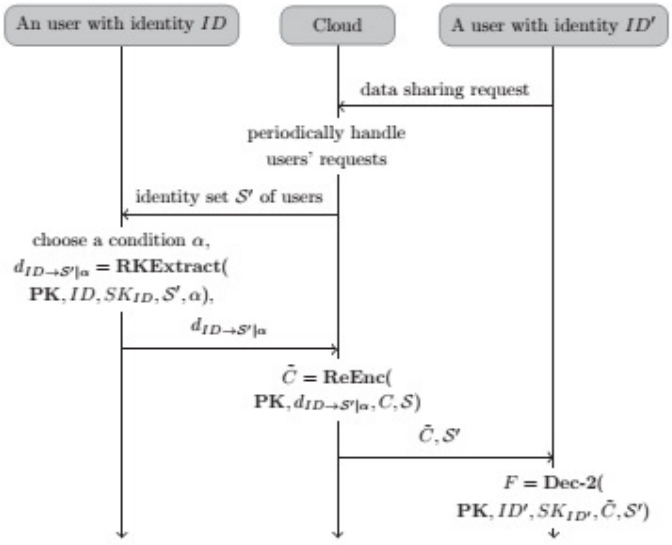

Fig. 3. The main steps of the data access phase.

3) The user ID verifies the validity of the identities in the set S and eliminates the invalid identities. Invalid identities mean that the corresponding users have no right to share the requested data. Suppose that all identities in the set S are valid. Then, user ID chooses the same condition α that was used to generate the initial ciphertext C and generates and sends a re-encryption key dID→S |α = RKExtract(PK, ID, SKID , S , α) to the cloud.

4) The cloud re-encrypts the initial ciphertext C to generate ˜ ReEnc PKa re-encrypted ciphertext c=ReEnc(PK,d1d)S˜S S C,) and sends (C,) to the users sin the set .

5) All users in the set S independently decrypt the re-encrypted CIBPRE ciphertext C to get the data F =

Dec 2 PK ˜ S- (, ID , SKID , C,).

Note that we additionally enable the cloud to occasionally deal with clients' data-sharing solicitations in stage 2 above. This technique gives an indistinguishable favorable position from does the comparable treatment in the data accumulation stage.

As far as confidentiality, CIBPRE ensures that (1) just the clients in the set S can unscramble the re-encoded ciphertext C and (2) the cloud can't impart data to various offering conditions to any client. At the end of the day, any underlying ciphertext with various sharing conditions can't be accurately re-scrambled by the cloud.

Contrasted and SKE, CIBPRE influences the data to get to stage significantly more advantageous. Assume that we just receive SKE for the data get to stage and that the greater part of a client's data are encoded utilizing the client's mystery key. For instance, Alice scrambled her data with her mystery key s and put away the produced ciphertext in the cloud; when Bob needs to share Alice's data, Alice should privately send the mystery key s to Bob.

Conclusion

Cloud-assisted IoT is a mainstream and valuable system for taking care of enormous IoT data. This paper centers around the data confidentiality when gathering, putting away and getting to IoT data with the help of a cloud and presents a promising strategy called CIBPRE for this reason. CIBPRE enables clients to privately gather and store an IoT-edge protest's data with the help of the cloud and offer these data with others. Notwithstanding confidentiality, CIBPRE is invaluable regarding execution. Its "communicate" property permits the data accumulation and data get to capacities to be accomplished in a clump way. Its "contingent" property enables the data to be gotten to in a fine-grained way. Its "character based" property maintains a strategic distance from the intricate open key administration of the conventional PKE. This paper likewise gives numerical outcomes exhibiting the achievability of our work.

REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami. Internet of Things (IoT): A vision, Architectural Elements, and Future Directions [J]. Future Generation Computer Systems, 29(7), pp. 1645-1660, 2013.

[2] M. Kaufman. Data Security in the World of Cloud Computing. IEEE Security & Privacy, 7(4), pp. 61-64, 2009.

[3] Y. Liu, Y. Peng, B. Wang, X. Bai, X. Yuan, and G. Li. IOT secure transmission based on integration of IBE and PKI/CA [J]. International Journal of Control & Automation, 6(2), pp. 245-254, 2013.

[4] D.E. Bakken, R. Parameswaran, D.M. Blough, A.A. Franz, and T.J. Palmer. Data obfuscation: Anonymity and desensitization of usable data sets [J]. IEEE Security & Privacy, 2(6), pp. 34-41, 2004.

[5] P. Xu, T. Jiao, Q. Wu, W. Wang, and H. Jin. Conditional Identity-based Broadcast Proxy Re-Encryption and Its Application to Cloud Email [J]. IEEE Transactions on Computers, 65(1), pp. 66-79, 2016.

[6] R. Roman, P. Najera, and J. Lopez. Securing the Internet of Things [J]. Computer, 44(9), pp. 51-58, 2011.

[7] K. T. Nguyen, M. Laurent, and N. Oualha. Survey on Secure Commu-nication Protocols for the Internet of Things [J]. Ad Hoc Networks, 32, pp. 17-31, 2015.

[8] V. Bhuse. Security and Privacy Challenges for Healthcare Records and Wearable Sensors in Cloud. Transaction on IoT and Cloud Computing, 2(3), pp. 11-17, 2014.

[9] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers. Twenty Security Considerations for Cloud-supported Internet of Things. IEEE Internet of Things Journal, 3(3), pp. 269-284, 2016.

[10] A. Mukherjee. Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints [J]. Proceedings of the IEEE, 103(10), pp. 1747-1761, 2015.

[11] I.E. Bagci, S. Raza, U. Roedig, T. Voigt. Fusion: Coalesced Confidential Storage and Communication Framework for the IoT [J]. Security and Communication Networks, 9(15), pp. 2656-2673, 2016.

[12] R. H. Weber. Internet of Things-New Security and Privacy Challenges [J]. Computer Law & Security Review, 26(1), pp. 23-30, 2010.

[13] A. Boldyreva, M. Fischlin, A. Palacio, and B. Warinschi. A Closer Look at PKI: Security and Efficiency. In: PKC 2007, LNCS, vol. 4450, pp. 458-475, Springer, Heidelberg, 2007.

[14] D. Boneh, M. Franklin. Identity-Based Encryption from the Weil Pair-ing [C]. In: CRYPTO 2001, LNCS, vol. 2139, pp. 213-239, Springer, Heidelberg, 2001.

[15] B. Lynn. PBC Ver. 0.5.14. https://crypto.stanford.edu/pbc/download.html.