Hybrid Access Control Mechanism for Mobile Cloud Computing

1. Mrs. Rama Devi, Associate Professor, from Santhiram Engineering College, 2. J. N. Murali Krishna Rao, 3. S. Pavan Kalyan, 4. M. Raghu Niranjan Reddy, and 5. P. Ravi Kumar Reddy 2,3,4,5→IV-B.Tech CSE Students from SREC

***Abstract*—Cloud Computing is the use of hardware and software to deliver a service over a network. With Integrating into cloud computing, users can access files and use applications from any device that can access the internet, and this integration performs in the cloud based on multi-user data shared environment. With integrating by this security issues like data confidentiality and user authority may arise in the mobile cloud computing system, and this considered to the developments of mobile cloud computing. For this we provide safe and secure operation, we are using the hybrid access control mechanism (HAC) and it is a modified layered structure is proposed in this paper. In this model, the data from all the kinds of mobile devices, phones, PDAs can be monitored and controlled by the system, and the data known for the authorized persons but not to unauthorized users. The novel scheme can be more adaptive for mobile cloud computing environment to process, store and access the enormous data and files while the novel system can let different privilege entities access their permitted data and files, which is designed to only authorized users and restrict to unauthorized users to get access to the data, it makes suitable for the mobile cloud computing paradigms.**

Index Terms-Mobile cloud computing, Hybrid access control.

1. INTRODUCTION TO MOBILE CLOUD COMPUTING

With explosive growth of mobile devices such as smart phones, PDAs, and tablet computers and the applications installed in them, the mobile-Internet will maintain the development with trend as 4G communication network is extensively promoted to our lives. What users of the mobile devices and applications need is that mobile internet can provide them with the service which is user-friendly, high-speed, and steady. In addition, the security issues of mobile terminals and the Internet access are attached importance to. And as a combination of cloud computing, mobile devices and wireless networks, mobile cloud computing is an emerging but very promising paradigm which brings rich computational resources to mobile users, network operators, as well as cloud computing providers [4], [5], [6]. The flaws of data storing and data computing in mobile-Internet applications can be overcome by mobile cloud computing while the new paradigm can also accomplish cloud based multi-user data sharing, end geographical service limitation, and process real-time tasks efficiently at the same time.

There is no accurate definition of mobile cloud computing, several concepts were proposed, and two most popular schemes can be described as follows:

1. Mobile cloud computing is a kind of scheme which could run an application such as a health monitor application on remote cloud servers as displayed in Fig. 1, while the mobile devices just act like normal PCs except that the mobile devices connect to cloud servers via 3G or 4G while PCs through Internet. And this concept is considered as the most popular definition of mobile cloud computing[1].
2. Taking advantages of leisure resources such as CPU, memory, and storing disks, another model of mobile cloud computing exploits the mobile devices them- selves as resources providers of cloud [2]. And the scheme supports user mobility, and recognizes the potential of mobile clouds to do collective sensing as well.
3. In this paper, we mainly focus on the first paradigm mentioned above, and the second one only assumes that what are the mobile devices do not provide computing resources?
4. In addition, the mobile devices which are capable like for example, every smart phone are done with accelerometer,gyroscope,compass,barometer,camera,GPS,microscope[3],etc.by this we can monitor and control the system.

Fig. 1.A Mobile Cloud Computing Model.

2. SECURITY ISSUES IN MOBILE CLOUD COMPUTING

So many users are starting to use mobile cloud computing services such as iCloud and One Drive services because of the poor storage and computation capability of current mobile devices. However this kind of mobile cloud services are considered in security and users may lose their files and documents. In September, 2014, Apple admitted computation capability of current mobile devices. However this kind of mobile cloud services are

considered in security and users may lose their files and documents.

In September, 2014, Apple admitted that iCloud was compromised by hackers and many pictures of celebrities leaked out [7].

Such event required us that the security issues of mobile cloud should be taken seriously. For solving such security challenges, data authority and data confidentiality should be useful for more.

Authority of data users: Different authority level system to get access to current data for application users should be established since the paradigm is applied in the hierarchical multi-user shared environment, which also means that the with higher authority level users should get all the data that while the users of lower privilege can't get the data beyond his/her authority.

Confidentiality of data: Although the cloud services utilized in the scenario are provided by private cloud which is supposed to be secure and secret to the consumers, it is still necessary to ensure the sensing data protected from third parties that do not belong to the mobile cloud system. Therefore it is important for the system to bring in a secure and efficient encryption scheme.

In this section, we mainly discuss the general cloud computing security issues.

2.1 Security Issues for Cloud Computing

As well as the data is transmitted to cloud, it is utilizing cloud services like IaaS, security challenges of which must be overcome since then. There are many of research results about cloud security; in conclusion, a secure cloud should at least satisfy 4 basic urges of consumers [8], say availability, confidentiality, data integrity, control.

2.1.1 Availability

Cloud providers should offer services that consumers could get and use at any places and any time. There are mainly two methods to enhance availability in cloud, which are virtualization and redundancy. Currently, cloud technology is mainly based virtual machine [9], since cloud providers can provide separated virtualized memory, virtualized storage, and virtualized CPU cycles. For example, Google set three replications for each object stored in it [10], all these redundancy strategies are enhancing the availability for consumers to get data they want at any time and any place.

HTTP protocol too much as it is a stateless protocol for attackers, which may cause unauthorized access to the management interface of cloud infrastructures [9].

2.1.2 Confidentiality

Confidentiality has been a huge barrier for cloud providers to popularize cloud to consumers since it comes out.

There basically exist two common approaches in current cloud infrastructures, say physical isolation and encryption. In Physical isolation context, virtual physical isolation [11], [19] are using VPN and firewalls to secure database [8]. Encrypting vital and confidential data before placing it in cloud infrastructures is another method to enhance confidentiality of cloud. But do not count on that approach too much because novel methods of breaking cryptographic algorithms are discovered [9].

TABLE 1
Security Issues For Cloud Computing

Security Challenges	Descriptions
Availability	Cloud providers are supposed to guarantee to consumers that they can get and use their data at any place and any time.
Confidentiality	Consumers data be kept secret in cloud system.
Data Integrity	The data stored in cloud need a mechanism to ensure their data in not lost or modified by unauthorized users
Control	A secure control system distributes' appropriate resources to be utilized.

2.1.3 Data Integrity

Data integrity ensures consumers that their storing data is not modified by others or collapsing owing to system failure. Besides the method, a "cloud security capture application" [18] could be in use to show consumers when and where their data was modified or transmitted.

2.1.4 Control

It is a sophisticated work to control a cloud system; a controlling work mainly includes deciding what resource could be utilized in what occasions.

In order to own a secure control system. And poor key management procedures of virtualized based cloud services make it worse [9]. Because virtual machines don't have a fixed hardware infrastructure and cloud-based content is often geographically distributed, it is a very tough task to ensure a secure control in cloud.

We gave the discussion in Table 1.

2.2 Security Issues for Mobile Cloud Computing

The paradigm performs almost the same as cloud computing with computers except that mobile cloud model connects mobile devices and cloud servers through 3G or 4G while cloud computing paradigm via Internet, therefore, mobile cloud computing inherits the security threats of traditional cloud computing. The security issues that are specific to mobile devices such as battery exhaustion attacks [21] mobile bonnets and targeted attacks [20] should be concerned as well [4].

3. EXISTING WORK

In order to give solution from security issues of the whole system should not be ignored, among those

security issues the most important two security issues in model can be divided into two parts: authority of users and the confidentiality of data. Those issues can

be solved by providing methods of access control [17]. Attribute Based Encryption (ABE)[22] is a current cryptographic primitive which has been used for access control [12], [13], [14], [15]. Access control deals with data access to authorized users and preventing from unauthorized users. Attachment of a list of authorized users to each data is the easy solution to achieve access control. But, this solution is somewhat difficult in the present scenario with a large and number of users, so that the application mentioned above within the environment of cloud. Public cryptographic scheme is second solution, in which public / secret key pair is given to each user and encrypt each message with public key of the authorized user, so that only the specific authorized users are able to decrypt it. In the proposed scenario, users with different privilege levels have different rights to access the sensing data coming from the mobile devices. Therefore, one same data has to be encrypted into ciphertext once, which ought to be able to be decrypted multiple times by different authorized users.

Based on this application demands, the concept of attribute based encryption is introduced [15]. Senders encrypt message with certain attributes of the authorized receivers. The ABE based access control method uses tags to mark the attributes that a specific authorized user needs to possess. Lots of paper [8], [9], [10], [11] introduced the scheme about the attribute based encryption access control method in the cloud computing. In the mobile loud computing environment, there are tremendous data which needs to be processed and marked with attributions for the convenient attributing access before storing. At the same time, the hierarchical structures of the application users need an authentication center entity to control their attributes.

Hierarchical Attribute-Based Encryption (HABE) [16] model by combining a HIBE system and a CP-ABE system, to provide fine-grained access control and full delegation, Goyal et al 2006. Based on the HABE model, we construct a HABE scheme by making a performance-expressivity tradeoff, to achieve high performance.

HABE is derived by Wang et al The HABE model consists of a Root Master (RM) that corresponds to the Third Trusted Party (TTP),Multiple Domain Masters (DMs) in which the top-level DMs correspond to multiple enterprise users, and numerous users that correspond to all personnel in an enterprise. This scheme used the property of hierarchical generation of keys in HIBE scheme to generate keys. This scheme can satisfy the property of fine grained access control, scalability and full delegation. It can share data for users in the cloud in an enterprise environment.

Furthermore, it can apply to achieve proxy re-encryption. But in practice, it is unsuitable to implement. Since all attributes in one conjunctive clause in this scheme may be administered by the same domain authority, the same attribute may be administered by multiple domain authorities.

In this model, the RM's role closely follows the root private key generator (PKG) in a HIBE system, is responsible for the generation and distribution of system parameters and domain keys. The DM, whose role integrates both the properties of the domain PKG in a HIBE system and AA in a CP-ABE system,.

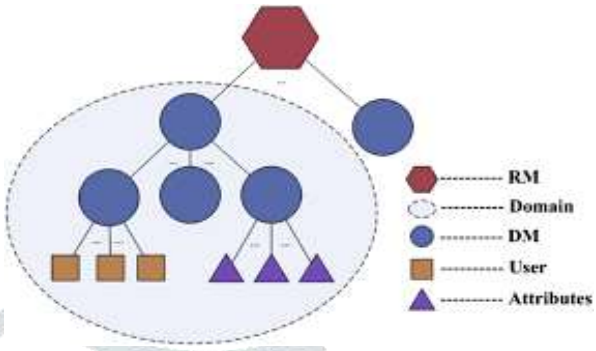


Fig. 2 HABE Model

4. PROPOSED/RELATED WORK

In this paper, a hierarchical access control method using a modified hierarchical attribute-based encryption (M-HABE) and a modified three-layer structure [23] is proposed. This method Differs from the existing paradigms like the HABE algorithm and the original three-layer structure, the novel scheme mainly focuses on the data processing, storing and accessing, which is designed to ensure the application users with legal access authorities to get corresponding sensing data and to restrict illegal users and unauthorized legal users get access to the data, the proposed promising paradigm makes it extremely suitable for the mobile cloud computing based paradigm. What should be emphasized is that the most important highlight of all in the proposed paper can be described as that the modified three-layer structure is designed for solving the security issues illustrated above.

In this the remaining of the paper can be arranged as follows. Section 2 explains out the security issues in mobile cloud computing, which can be divided into two methods including security issues of cloud computing and security issues of mobile cloud computing. The proposed modified hierarchical attribute based encryption access control method is described in Section 4 demonstrates how the proposed access control method based on M-HABE applies in a health monitoring application scenario specifically. Conclusions are given in Section 6.

As the mobile cloud computing defines [4], [24], there would be so much sensing data from the mobile devices in bursting into the cloud infrastructures to process and store the data.

The access structure should meet the following requirements:

a) One encrypted data can be received by several users.

b) Not only precise level descriptions, but users' attributes are there in the access structure. Which are described as the attributes while the other one is described as an accurate privilege level?

c) The structure of encryption keys should

just as the hierarchical structure of the mobile cloud computing users.

In order to secure these requirements, are proposed to access control method should contain the following features:

a) One ciphertext can be decrypted by several keys.

b) Both precise level description and user attribute should be supported in the access structure of the method.

c) The keys in the authentication center ought to have the same hierarchical structure just as the privilege levels..

A modified hierarchical attribute-based encryption (M- HABE) access control method applied in mobile cloud computing is proposed in this paper, which changes a proposed scheme called hierarchical attribute-based encryption HABE [12], M-HABE combines the hierarchical identity-based encryption [13] and the ciphertext-policy attribute-based encryption (CP-ABE) [14] to meet the conditions described above.

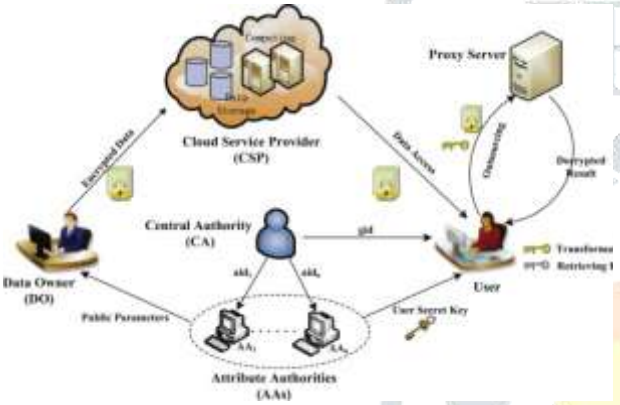


Fig. 3.M-HABE model

As the Fig. 3 shows, the proposal consists of an center authority (AuC), Sub-AuCs, and users. The AuC is responsible for generating and publishing system parameter and the system master key; Sub-AuCs can be divided into first-level Sub-AuC(Sub-AuC$_i$) and other Sub- AuCs, among which the AuC just need to be in charge of users and create their private keys, while other Sub-AuCs take charge of users attributes and create their secret iden- tity keys and secret attribute keys for users.

Each data user shown in the figure possesses a unique ID which is a character string designed to describe the features of internal parties within the system, and so do AuC, Sub- AuCs, and users attributes, especially, the ID of each user contains an integer for describing the privilege level of the user.

4.1 Key Description

Public key encryption is utilized in the proposed system; the related keys are summarized below.

1. Root key MK_0 possessed by AuC is used to create Master key for Sub-AuC$_1$.
2. Each Sub-AuC owns a public key PK_i and a master key MK_i, among which PK_i is composed as $\eth PK_{i-1}; ID_i\flat$ where PK_{i-1} is the public key of the Sub-AuC's parent node, and MK_i is also created by the paper node. PK_m is the public key of Sub-AuC$_1$, which can be demonstrated as ID_m meaning that it is composed by its own *ID*s. Create their secret keys SK_u for them. And other Sub-AuCs have a set of attributes to manage, while they also create users' secret identity keys $SK_{i;u}$ and data users' secret attribute keys $SK_{i;u;a}$ at the same time.
3. Each data consumer is described by one precise *ID* denoted as ID_u,.
4. Each attribute a is described by a precise *ID* denoted as ID_a. And even an attribute owns a public key in the form of $\eth PK_{i-1}; ID_i\flat$ where PK_i is the public key of Sub-AuC that takes charge of the attribute.

Fig: 4.General structure of a M-HABE access control method for mobile cloud computing.

4.2 M-HAC Definition

The M-HAC is composed by the following algorithms:

Setup: Given a security parameter K that is huge enough, AUC will generate a system parameter and a root master key MK_0.

CreateMK: Using system parameter and their own master keys, AUC can create master keys for lower-level Sub-AuCs.

CreateSK: With their own master key MK_m and system parameter, Sub-AuC$_1$ creates secret key SK_u for each consumer if it is confident that the public key of the user is PK_u, or there would be no secret key for the user.

CreateUser: Sub-AuCs will create users' secret identity keys $SK_{i;u}$ and secret attribute keys $SK_{i;u;a}$ for them if the AuC makes sure that the attribute a is in charge of it and the user u satisfies a. And if not there would be no secret identity keys or secret attribute keys.

Encrypt: With R denoting a set of users' *ID*s, A representing the attribute-based access structure, the pubic keys of all the users that are in R, and the public keys of all the attributes that are in A, the data provider, which is also a data user of the cloud computing in this case, can encrypt the sensing data D plaintext into ciphertext C.

RDcrypt: Given the ciphertext C, a data user processing the precise *ID* that is in R can decrypt the ciphertext C into plaintext D with parameters and the user's secret key SK_u.

ADcrypt: Given the ciphertext C, a data user possessing an attribute set $\mathbf{f}ag$ that satisfies A,

which means that the consumer owns at least an attribute key $SK_{i;u;a}$, can also decrypt the ciphertext C into plaintext D with system parameter the user's secret identity key $SK_{i;u}$, and the secret attribute key $SK_{i;u;a}$.

For example, if the users of the system are employees of a group of companies, then each company is able to generate the private keys for their employees, so that employees request their keys from their company, rather than the top level root PKG. Only companies can request only at once their domain secret from the top-level PKG.

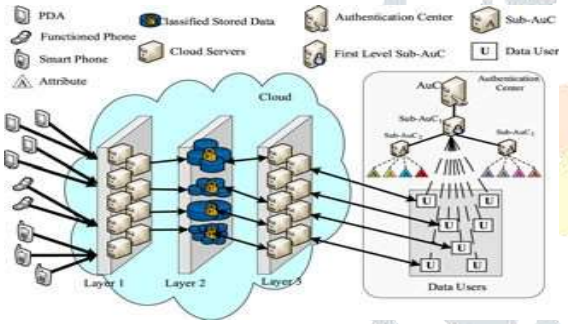
5. APPLICATION

Applying M-HABE, the proposed scheme is illustrated in Fig. 3. The whole system works as following steps:

All kinds of mobile devices which are installed with the mobile cloud computing based weather application are distributed into different locations all over the country with users.

Fig: 4. General structure of M-HABE access control method for mobile cloud computing.

The sensing data is transported to the layer1 which is a kind of IaaS cloud service provided by the cloud provider [26].Therefore, a raw data can be expressed *Data<format;mobiledeviceID;time;period>*.



There are different kinds of formats depended on different kinds of mobile devices, for example, JPEG,WMA,TXT,PNG,WMV,etc.

- Before sent to layer 2, the sensing data is classified by its data model [23] in layer 1 with its excellent ability of computing and storing, the step can be illustrated by Fig. 4. The data model we present is inspired by the data model proposed in [25], based on which our data model is composed by format, device ID, size, time, value and period.

- The sensing data is encrypted into cipher- text in layer 2 by M-HABE encryption algorithm using the key in form of ðR; A; PK_aja2A; ID_u2Rþ; º and the cyphertext is sent to layer 3 which is also a kind of IaaS cloud service in cloud. The encryption step can be demonstrated as Fig. 5.

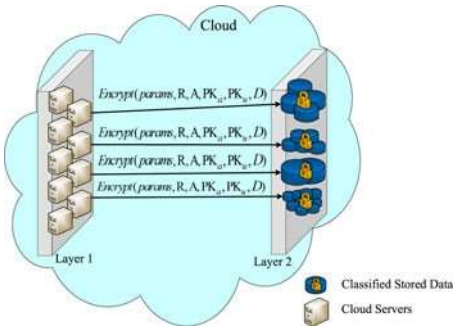


Fig. 5.Encryption procedure

- The data users of the scheme are in charge of just like Fig. 2 indicates. The users can get access to the ciphertexts only if he/she satisfies the requirements of RDcrypt algorithm or *ADcrypt* algorithm that are described in Section 3. The decryption procedure is shown in Fig. 6.

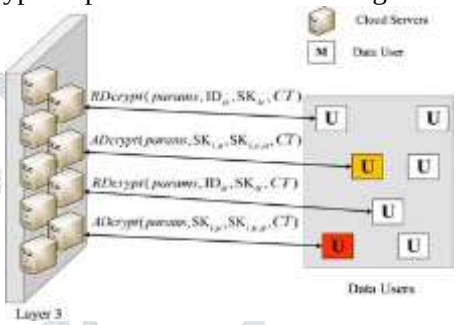


Fig. 6.Decryption procedure

6. CONCLUSION

The proposed paper a hybrid access control scheme by taking advantages of attributes based encryption (ABE) and hierarchical attribute based encryption (HABE) access control processing. The proposed access control method using HAC is designed to be utilized within a hierarchical multi-user data-shared environment, which is extremely suitable for a mobile cloud computing model to protect the data privacy and defend unauthorized access. Compared with the original HABE scheme, the novel scheme mainly focuses on the data processing, storing and accessing, which is designed to ensure the users with legal authorities to get corresponding classified data and to restrict illegal users and unauthorized legal users get access to the data, which makes it extremely suitable for the mobile cloud computing paradigms. The scheme not only accomplishes the hierarchical access control of mobile sensing data in the mobile cloud computing model, but protects the data from being obtained by an untrusted third party.

REFERENCES

[1]J.Carolan,S.Gaede,J. Baty, G. Brunette, A. Licht, J. Remmell,L. Tucker, and J. Weise, "Introduction to cloud computing architecture," White Paper, 1st edn. Sun Micro Systems Inc, Santa Clara, CA, USA, 2009.

[2] E. E. Marinelli, "Hyrax: Cloud Computing on Mobile Devices Using Mapreduce," DTIC Document, Fort Belvoir, VA, Tech. Rep. CMU-CS-09-164, 2009.

[3] Q. Han, S. Liang, and H. Zhang, "Mobile cloud sensing, big data, and 5G networks make an

intelligent and smart world," *IEEE Netw.*, vol. 29, no. 2, pp. 40–45, Mar./Apr. 2015.

[4] N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud comput- ing: A survey," *Future Generation Comput. Syst.*, vol. 29, no. 1, pp. 84–106, 2013.

[5] S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya, "Cloudbased augmentation for mobile devices: motivation, taxon- omies, and open challenges," *IEEE Commun. Surveys Tutorials*, vol. 16, no. 1, pp. 337–368, Jan.-Mar. 2014.

[6] R. Kumar and S. Rajalakshmi, "Mobile cloud computing: Standard approach to protecting and securing of mobile cloud ecosystems," in *Proc. Int. Conf. Comput. Sci. Appl.*, 2013, pp. 663–669.

[7] R. Walters, "Cyber attacks on US companies in 2014," Heritage Foundation, Washington, DC, USA, Issue Brief no. 4289, 2014.

[8] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and privacy in cloud computing: A survey," in *Proc.6th Int. Conf. Semantics Knowl. Grid*, 2010, pp. 105–112.

[9] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding cloud computing vulnerabilities," *IEEE Security Privacy*, vol. 9, no. 2, pp. 5057, Mar./Apr. 2011.

[10] S. Ghemawat, H. Gobioff, and S.-T. Leung, "The Google file sys- tem," in *Proc. ACM SIGOPS Operating Syst. Rev.*, 2003, vol. 37, no. 5, pp. 29–43.

[11] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and privacy in cloud computing: A survey," in *Proc.6th Int. Conf. Semantics Knowl. Grid*, 2010, pp. 105–112.

[12] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-
Plasma Sci. [Online]. *21(3).* pp. 876—880. Available: http://www.halcyon.com/pub/journals/21ps03-vidmar

[13] C. Gentry and A. Silverberg, "Hierarchical ID-based cryptography," in *Proc. Advances Cryptology,ASIACRYPT*, 2002, pp. 548–566.

[14] J. Bethencourt, A.Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in *Proc. IEEE Symp. Security Privacy*, 2007, pp. 321–334.

[15] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Advances Cryptology*, 1985, pp. 47–53.

[16] J. Horwitz and B. Lynn, "Toward hierarchical identity-based encryption," in *Proc. Advances Cryptology EUROCRYPT*, 2002, pp. 466–481.

[17] I. Stojmenovic, "Access control in distributed systems: Merging theory with practice," in *Proc. IEEE 10th Int. Conf. Trust, Security Privacy Comput. Commun.*, 2011, pp. 1–2.

[18] L. Sumter, "Cloud computing: Security risk," in *Proc. 48th Annu. Southeast Regional Conf.*, 2010, p. 112.

[19] A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "Above the clouds: A Berke- ley view of cloud computing," Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, CA, USA, Rep. UCB/ EECS, vol. 28, p. 13, 2009.

[20] J. Oberheide and F. Jahanian, "When mobile is harder than fixed (and vice versa): Demystifying security challenges in mobile envi- ronments," in *Proc. 11th Workshop Mobile Comput. Syst. Appl.*, 2010, pp. 43–48.

[21] B. R. Moyers, J. P. Dunning, R. C. Marchany, and J. G. Tront, "Effects of Wi-Fi and bluetooth battery exhaustion attacks on mobile devices," in *Proc. 43rd Hawaii Int. Conf. Syst. Sci.*, 2010, pp. 1–9.

[22] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun. Security*, 2006, pp. 89–98.

[23] Y. Xie, J. Zhang, G. Fu, H. Wen, Q. Han, X. Zhu, Y. Jiang, and X. Guo, "The security issue of WSNs based on cloud computing," in *Proc. IEEE Conf. Commun. Netw. Security*, 2013, pp. 383–384.

[24] W. Zhang, Y. Wen, and H.-H. Chen, "Toward transcoding as a service: Energy-efficient offloading policy for green mobile cloud," *IEEE Netw.*, vol. 28, no. 6, pp. 67–73, Nov./Dec. 2014.

[25] T.-D. Nguyen and E.-N. Huh, "An efficient key management for secure multicast in sensor-cloud," in *Proc.1st ACIS/JNU Int. Conf. Comput., Netw., Syst. Ind. Eng.*, 2011, pp. 3–9.

[26] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz,A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, et al., "A view of cloud computing," *Commun. the ACM*, vol. 53, no. 4, pp. 50–58, 2010.