ISSN: 2455-1848
International Journal of Innovative Research & Growth
A Peer Reviewed & Referred International Journal
Volume-6 Issue-4 February-2018
Impact Factor-3.0
www.ijirg.com, editor@ijirg.com

M-HABE: A New Access Control Method For Secure Cloud Computing On Mobile Devices

Barkha Nandwana
Scholar, Computer Science and Engineering, Pacific Institute of Technology, Pacific University, Udaipur, Rajasthan, India
Email- barkhanandwana30@gmail.com

Abstract
In current scenarios, cloud computing gaining a great drive and plays a significant role in improving the infrastructure of internet computing. It's a developing technology but however it's a very challenging to integrate cloud computing in mobile devices. With integration, Mobile Cloud Computing (MCC) facing security issues like user authority, data confidentiality, etc. MCC is an essential technology in current environment as it became one of the main processing devices for the users now-a-days. Recent studies on this aspect are not yet efficient in eliminating the security issues. So, this research paper presents an effective safe and secure hierarchical access control method known as M-HABE (Modified Hierarchical Attribute-Based Encryption) and a modified three-layer structure. This proposed solution enables the users to control and monitor their enormous sensitive data from mobile devices from unauthorized third party. This new method mainly concentrates on the data storing, processing and accessing where it make sure that only the user with legal authorities get access to information and restricts the unauthorized users. Finally, this research clearly explains the introduced method through Java technology. Hence, the proposed method will be very suitable for the mobile cloud computing in securing user data.

***Keywords:** - Cloud computing, Mobile cloud computing, M-HABE, access control.*

1- INTRODUCTION

Cloud computing is referred as accessing and storing the information and programs over the internet rather than using computer's hardware and software by sitting in front of their desktop or inside the firm's network. Some of the main examples of cloud computing which are probably using by the users are Google drive, Apple iCloud, Amazon Cloud Drive, Box, SugarSync, Dropbox, etc. One of the most important differences among cloud computing with hardware drive is that it manages the files or documents on behalf of the user. Final one is that the cloud computing offers services to users in two basic flavours which include public and private. Here, public clouds provides free services to and on other hand private clouds allows the access for the users only through secure network connections [1].

Three layer of cloud computing are: Platform as-a Service (PaaS) - It offers a cloud-based environment with all the things that are needed to support the entire lifecycle of building and delivering the web based applications without the cost and difficulty of purchasing and managing the underlying software, hardware, hosting and provisioning [1]. Infrastructure as-a Service (IaaS)- It offers computing resources to the organizations including networking, storage, servers, and data centre space on a pay-per-use basis [1]. Software as-a Service (SaaS) - In this type, the cloud based applications run on distant computers in the cloud which are operated and owned by others. Further it will be connected to the user computers through the internet and a web browser [1].

Mobile Cloud Computing (MCC) is referred as infrastructure where the data processing and data storage is being carried out outside the mobile device. The applications of mobile cloud move the data storage and computing power far from the mobile devices into centralized computing platforms which are placed in clouds. Further these are accessed over wireless connection [2]. Generally the mobile devices face numerous issues with the resources like storage, bandwidth and battery life. MCC provides various benefits to the users by permitting them to make use of software, platforms and infrastructure at very low cost by cloud providers [2].

Benefits of MCC are - Some of the major advantages that the user can acquire from MCC are discussed below [2]

It allows the mobile users to access and store huge information stored on the cloud.

Storing applications and data in cloud will decrease the potential for data loss.

Even if the user moves from one place to another, both the data and services in cloud can be accessed.

The mobile apps can be scaled in order to meet the increasing demand of users.

Security Issues in MCC - The users of mobile devices will run their applications on remote cloud servers. This is same as general cloud computing but here the model connects the mobile devices with cloud servers via 3G or 4G. So the MCC have security threats which are particular to the mobile devices. Some of the common security issues in cloud computing are discussed below [3]

Availability – thee cloud provider must ensure their customers that they view their data at any place and time.

Confidentiality – the sensitive information of customers must be secured in cloud system.

Data integrity –the information stored in cloud system should require a mechanism to make sure that the data was not lost or changed by unauthorized users.

Control – in different occasions a secure control system distributes apt resources.

2- LITERATURE SURVEY

Chatterjee and Roy (2017) Cloud are categorized into various types and services. Mainly there are two group models which include service model and deployment model. The first model includes IaaS, SaaS and PaaS. The second model namely known as deployment model includes public cloud, hybrid cloud, private cloud and community cloud. Numerous types of service models under the cloud computing facilitate the numerous levels of privacy. For instance, IaaS will have a minimum security and SaaS have more security. Here, in the research paper they focused on knowing the cloud security challenges. Further proposed crypto algorithms and effective measurements in order to make sure the security for the cloud stored in the cloud. Apart from this they also discussed about the security aspects regarding cryptography by explaining the privacy issues of present cloud computing [4].

Sajitha and Catherine (2017) Cloud computing is one such technology that allows the user to store a huge amount of information and can further retrieve their data on demand. The sensitive user data must be kept confidential against the entrusted CSPs one way is to make use of cryptographic approaches through decryption keys which are given to only the authorized users. In the current research paper, a scheme is being proposed in order to help the firms to efficiently share the sensitive information on cloud servers. This is being achieved by merging HIBE and CP-ABE [5].

Han et al. (2015) In this article mobile sensing and cloud computing separately and in detail, then combine the two concepts to form the singular idea of mobile cloud sensing. It will also give an intuitive architectural description of mobile cloud sensing, along with discussions about each of its individual building blocks. There are limitations to mobile cloud sensing today, but with the emergence of 5G coupled with the analysis of big data, it can address the current issues at hand [6].

Abolfazli et al. (2014) Recently, Cloud-based Mobile Augmentation (CMA) approaches have gained remarkable ground from academia and industry. Augmented mobile devices envision to perform extensive computations and to store big data beyond their intrinsic capabilities with least footprint and vulnerability. This paper comprehensively surveys the mobile augmentation domain and presents taxonomy of CMA approaches. The objectives of this study is to highlight the effects of remote resources on the quality and reliability of augmentation processes and discuss the challenges and opportunities of employing varied cloud-based resources in augmenting mobile devices. This author presents augmentation definition, motivation, and taxonomy of augmentation types, including traditional and cloud-based. Critically analysed the state-of-the-art CMA approaches and classify them into four groups of distant fixed, proximate fixed, proximate mobile, and hybrid to present taxonomy. Impacts of CMA approaches on mobile computing is discussed and open challenges are presented as the future research directions [7].

Fernando et al. (2013) Mobile cloud computing: In this paper, an extensive survey of mobile cloud computing research, while highlighting the specific concerns in mobile cloud computing. It present taxonomy based on the key issues in this area, and discuss the different approaches taken to tackle these issues. It can be concluded that the paper with a critical analysis of challenges that have not yet been fully met, and highlight directions for future work [2].

Kumar and Rajalakshmi (2013) Mobile cloud computing: Standard approach to protecting and securing of mobile cloud ecosystems: The concepts of Cloud computing is naturally meshed with mobile devices to enable on-the-go functionalities and benefits. Understanding the true potential of mobile cloud computing and identifying issues with mobile cloud security, privacy, feasibility and accessibility remain a major concern for both the customers and the enterprises. This paper covers the mobile cloud security issues and challenges by looking at the current state of cloud security breaches, vulnerabilities of mobile cloud devices, and how to address those vulnerabilities in future work in aspect of mobile device management and mobile data protection. Also, it highlights on usage of SCWS (Smart Card Web Services) rivalry to intensify security of mobile cloud computing [8].

Stojmenovic (2011) Access control in distributed systems: it ensures that only authorized users have access to data and services. This problem becomes challenging in distributed systems, where coordination of activities by a central authority might not be possible or could be resource demanding [9]. Attribute Based Encryption (ABE) is a recent cryptographic primitive which is being used for access control [10]. We address some contemporary access control problems in distributed systems such as mobile ad hoc networks, vehicular networks, smart grids and cloud computing. Each of these applications has different constraints and requirements. We show how ABE and different variants of it can be tailored to suit the specific needs of the above applications.

Goyal et al. (2006) Cipher text-policy Attribute-Based Encryption (CP-ABE) [11] currently the existed system is ABE (Attribute Based Encryption) access control method. This technique makes use of numerous tags for marking the attributes whenever an authorized user desires to poses. One of the main drawbacks of this method is that if the user sets a certain tag then they can easily access the information and decrypt the data. Numerous studies have been carried out on this technique regarding ABE in cloud computing. In case of mobile cloud computing, there is a lot of huge data that needs to be processed and must marked with attributions before storing it. This is a quite risky task. Moreover, the application users should have an authentication centre to have a control over their attributes. Limitations of Existing System ABE: Data confidentiality, No multiple controls, Data integrity, No one guarantees the data availability.

Horwitz and Lynn (2002) Horwitz introduced the idea of HIBE (Hierarchical Identity based encryption) [12] where user in higher hierarchical position of system generate prs private keys for their lower level users with private keys. From the above discussion on existed technologies, it can be understood that various researchers carried out study on securing the data stored in mobile cloud computing as the usage of mobile is increasing day by day.

Shamir (2000) Identity-based Encryption [13] initially in 1984, the concept of IBE (Identity Based Encryption) was introduced by Shamir which is different from the traditional symmetrical encryption system. This method takes the arbitrary character strings which can represent the user's identities like e-mail address, ID numbers, etc. The benefit of IBE is that there is no need to search public keys data on CA (Certificate Authority). Hence, it can be stated that many authors made an attempt to research on mobile cloud computing concept and proposed various approaches to reach the objective of the study. All these research's didn't concentrated on providing access to only the authorized users with good security for their mobile cloud computing and moreover they end with some issues. So, I preferred to design a modified HABE and three-layer structure to provide effective and secure control methods to the users with the Java technology.

We are using three methodology from previous work as : Cipher text policy Attribute based encryption (CP-ABE) , Hierarchical Identity based encryption (HIBE) , Acceess control method.

3- OBJECTIVE OF STUDY

Some of the main objectives of the current research project are listed below:

To study the concepts related to cloud computing and mobile cloud computing.

To introduce a new safe and secure hierarchical access control method to control and monitor the private information in mobile devices from unauthorized people.

To evaluate the outcome of the proposed method to analyse its effectiveness.

This new method mainly concentrates on the data storing, processing and accessing where it make sure that only the user with legal authorities get access to information and restricts the unauthorized users.

Finally, this research clearly explains the introduced method through Java technology. Hence, the proposed method will be very adapted for the mobile cloud computing in securing user data.

4- PROPOSED WORK

The current method M-HABE is being designed such that it overcome all the issues that are being faced by the people with the existed methods such as Cipher text-policy ABE, Hierarchical identity based encryption, CMA approach, etc.

In this paper, a hierarchical access control method using a modified hierarchical attribute –based encryption (M-HABE) [14] and a modified three layer structure [15] is proposed. 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 [10], M-HABE combines the hierarchical identity based encryption(HIBE) [12] and the cipher text policy- attribute based encryption (CP-ABE) [11] . The cipher text policy-ABE (CP-ABE) [11] makes use of tags for the attributes when the authorized users wish to retrieve the data from cloud. However this approach cannot be suitable for mobile cloud computing since in this case there will be a huge data that must be retrieved and in order to retrieve the information it must be marked with attributions which is a difficult task to make tag for all the attributions. Some other limitations of ABE system include data confidentiality, data integrity, no multiple controls; none of them guarantees the availability of data, etc. Another hand the proposed method in this paper needs only two keys for the user to retrieve the information one is private key and other is decrypt key which is a simple and secured process and more suitable for mobile cloud computing.

The second existed method is hierarchical identity based encryption(HIBE) [12] which takes the arbitrary character strings where it represent the identities of the users such as ID numbers, e-mail, etc. This approach is somewhat similar to the method discussed in this paper. Since, even this approach generates the private key in a hierarchical position system for the lower level users. However, this approach can be easily traced out by unauthorized user since only with the help of one key user can retrieve the data from the cloud. In case of the current research method, both keys are needed for retrieving the data as discussed in the above case.

In the proposed scheme, the user will store and then again request to access the data from mobile device. The user information is stored in cloud and is secured with proposed scheme. Here, the cloud includes three layers (layer1, layer 2 and layer 3). Once the user upload the file to store in the cloud then the information is converted into cipher text with M-HABE encryption algorithm and this cipher text is sent to layer 3 in the cloud. Now if the user wants to access the file stored in the form of cipher text then they require decrypt key.

To exhibit the output for the proposed scheme, Java technology have been chosen when compare to other platforms.

5- MODIFIED HIERARCHICAL ATTRIBUTE–BASED ENCRYPTION (M-HABE)

As per the definition of mobile cloud computing, there are much more sensing information from the mobile devices which are stuffed into cloud infrastructure for processing and storing the information. One of the main points that is to be considered here is that the data stored in the mobile cloud computing includes the data belonging to various hierarchies.

In order to get a clear idea on this concept consider an organization 'XYZ', which is one of the various types of books to numerous people belonging to different sectors. Now, the management should provide different access to each of the employees. Here each of the employees will sell the books to various user levels. Consider three user levels which consists of user level 1 include teachers, office staffs, etc., user level 2 includes professor, higher study students, doctors, lawyers, etc. and Finally user level 3 includes scientists, MNC company CEO, government higher officers, defence, etc. Now the key concept in this approach is that the employees with lower privilege where these people will not have permission to view some data that the higher privilege can access it. On another hand, the higher level management users will have the permission to the entire information that is viewed by lower level employees. Since, mobile cloud computing various users will have a hierarchical authority system. In the mean-time, all the data must be encrypted correctly because the information should not have access to any of the third party who not at all included in the system. To achieve this task, a hierarchical and secure access control method has been introduced in this research in order to apply the method in cloud computing system. The access control system is shown in Table 1.

Information Type	Access Structure
Books available in the firm	All employees
Access the books only related to teachers, office, staffs, etc.	User level 1 include teachers, office staffs, etc.
Access the books related to teachers, office, staffs, professor, higher study students, doctors, lawyers.	User level 2 includes professor, higher study students, doctors, lawyers, etc.
Have access to all the books including teachers, office, staffs, professor, higher study students, doctors, lawyers, scientists, MNC company CEO, government higher officers, defence	User level 3 includes scientists, MNC company CEO, government higher officers, defence, etc.

Table 1: Shows the mobile cloud computing list of access structure.

According to access structure list in the Table 1, now the designed approach must fulfil the requirements that are being mentioned below:

Numerous users can receive one encrypted data.

The users of level 2 can access their own data and also the user level 1 and all employees' information. In the same way, user level 3 can view the data related to their own information, user level 2, user level 1 and all employees.

The encryption keys structure must execute just as the mobile cloud computing user's hierarchical structure.

In order to attain all the above discussed requirements, the proposed control method must include some features which are listed below:

With the help of numerous keys a single cipher text should be decrypted.

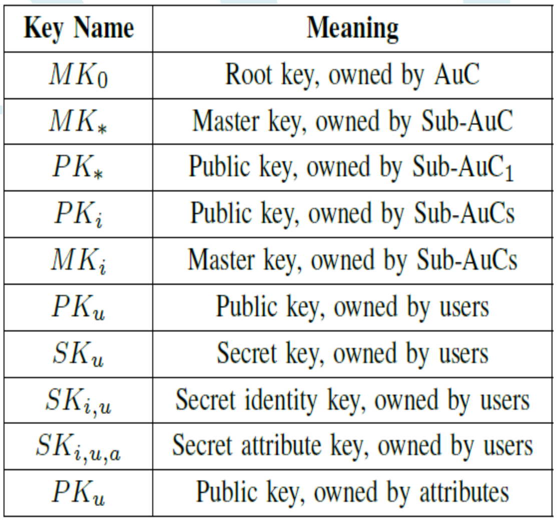
In the method of access structure, the user attribute and precise level must be supported.

In the authentication centre the keys should have the same identical hierarchical structure as user's privilege levels structure has.

Based on all these aspects, a modified hierarchical attribute-based encryption (M-HABE) [14] have been proposed in this research and further this access control method is applied in mobile cloud computing. This proposed method is the advanced scheme of HABE (Hierarchical Attribute-Based Encryption) [10]. This approach is a combination of cipher text-policy attribute-based encryption (CP-ABE) [11] and hierarchical identity-based encryption (HIBE) [12] in order to fulfil the requirements and the conditions that are being discussed above.

A. M-HABE Model Key Description

In the proposed system, the public encryption is being used and the related keys are discussed in Table 2 [14].



Key Name	Meaning
MK_0	Root key, owned by AuC
MK_*	Master key, owned by Sub-AuC
PK_*	Public key, owned by Sub-AuC$_1$
PK_i	Public key, owned by Sub-AuCs
MK_i	Master key, owned by Sub-AuCs
PK_u	Public key, owned by users
SK_u	Secret key, owned by users
$SK_{i,u}$	Secret identity key, owned by users
$SK_{i,u,a}$	Secret attribute key, owned by users
PK_u	Public key, owned by attributes

Table 2: Shows the major keys in HABE

Authentication (AuC) controls the root key MK_0 and this key is used to create MK^* for first sub-authentication (Sub-AuC 1).

Each of the Sub-AuC has their own public key (PK_i) and the master key (MK_i). Now PK_i is represented as (PK_i -1, idi), here pki-1is Sub-Auc's father node public key and this father node is further created by MK_i.

Sub-AuC1 public key is PK^* and can be revealed as ID^*. It means that it is composed by its own IDs. The Sub-AuC1 takes the responsibility of users and further builds their own secret keys SK_u for them. Remaining Sub-AuCs manages with set of attributes. At the same time, it create the users secret identity keys $SK_{i,u}$ and data users secret attribute keys $SK_{i,u,a}$.

Each customer's information is designated by a specific ID known as IDu and data users attributes set is signified as {a}. Apart from all these aspects, each of the user has their own a public key PK_u which is denoted as { PK^*, ID_u } and a secret key of customer SK_u, user secret identity key set { $SK_{i,u}$ } and customer secret attribute key set { $SK_{i,u,a}$ }.

Each attribute a is explained by precise ID represented as IDa and it also have a public key in form of (PK_i -1, IDi). Here PK_i is Sub-AuC public key that takes the responsibilities of attribute.

B. Definition of M-HABE

The algorithms that are being used to compose M-HABE is discussed below [14]:

Setup: A security parameter K has been given here. Further AUC produces root master key MK_0 and a system parameter params.

CreateMK: Now, Sub-AuCs or AuC create the lower level Sub-AuCs master keys by making use of system parameter params.

Create SK : For every customer, the secret key SK_u has been created by Sub-AuC1 with the help of their own system parameter params and master key MK^*. This happens only if it ensures that the user public key is PK_u or either there should not be any secret key for user.

Create User: If the AuC ensure that the attribute a is responsible of it and user u satisfies a then the Sub-AuCs creates the secret identity keys for users $SK_{i,u}$ and also the secret attribute keys $SK_{i,u,a}$.

Encrypt: A set of users IDs are denoted by R, attribute based access structure is represented by A. Now users all public keys which are in R and attributes are in A and the data provider (which is cloud computing data user) will encrypt the sensing data D into cipher text C.

RDcrypt: The data user who have precise ID in R can decrypt the given cipher text C into plaintext D by using user's secret key SK_u and params.

ADcrypt: The data user who are having attribute set {a} which satisfies A for the given cipher text C. It means that the customer will have at least an attribute key $SK_{i,u,a}$ and further they can decrypt the cipher text C into plaintext D with the help of system parameter params, users secret attribute key $SK_{i,u,a}$ and secret identity key $SK_{i,u}$.

6- APPLICATION OF M-HABE IN CLOUD BASED SMART GRID

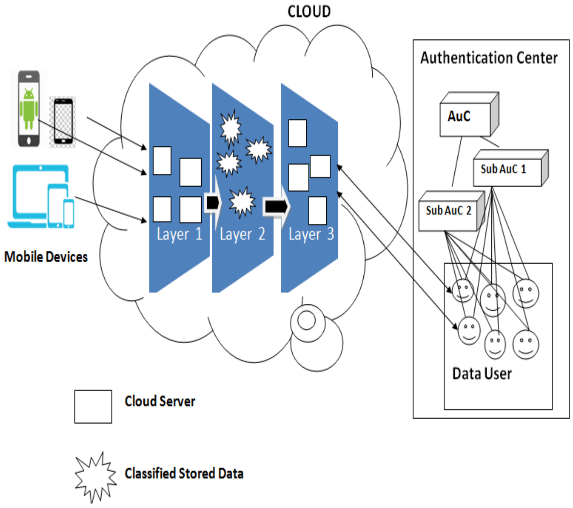


Figure: The proposed scheme M-HABE application in cloud based smart grid.

Step 1 - Initially all types of mobile devices are being distributed to various employees into different locations. These mobile devices are installed with the mobile cloud computing. The applications will exploit the sensors that are installed in mobile devices in order to capture the information that the applications required.

Step 2 - The sensing information required for the user is transported to the first layer (that is layer 1).Here this layer is kind of IaaS cloud service which is being offered by cloud provider.

Step 3 - Now the data model in layer 1 categories all the sensing information before sending the data to layer 2 as shown in figure .This model has an excellent ability of storing and computing .

Here, this data model is designed based on the data model that is being proposed by .This data model is composed by device ID, format, time, size, period and value. Thus, the raw information can be represented as vector Data (format; size/time/value; mobile device ID; period).

Step 4 - In layer 2, the sensing information is initially encrypted intocipher text through M-HABE encryption algorithm by making use of the key in the form of (R, A, PKa|a A, IDu R), L. Now this ciphertext is further sent to layer 3, where this layer is similar to IaaS cloud service in cloud.

Step 5 - The users can access the ciphertext only if they satisfies the needs of RDcrypt or ADcrypt algorithm which are discussed in above section.

Hence, it can be concluded that the data is being categorized, encrypted into cipher-text and allows only authorized users to decrypt the data from the coud.

7- EVALUATION OF RESULT

The application of proposed scheme M-HABE in mobile cloud computing is a very effective method. Since it allows the users to store their data in cloud and further it provides better security to the files stored in cloud when compare to the existing methods. The proposed scheme shows only the cipher-text for all the users who views the information. Here the cipher text is nothing but the data in encrypted form. Even the previous existed technologies will encrypt the information but with the help of the decrypt key the third-party can easily accessed the data. However, in this case if the unauthorized users need to decrypt the file then definitely they need to have two keys private key and decrypt key. In this proposed scheme there are two sub-authentication where these two people will provide the keys to users unless they verified that the user is an authorized user. This was verified based on the type of level that the user belong to and accordingly reveals the files to the users. Hence, it can be stated that the proposed M-HABE is more effective than other existed methods.

In proposed work, the entire process mainly deals with the four actors which include user, authentication, sub-authentication 1 and sub-authentication 2. Here, the user will initially login to the account and request for accessing the file. Here in this study, to decrypt the file the data user needs two keys one is private key and other is decrypt key. Here these two keys will be generated by two different servers. Sub-authentication 1 generates private key to the data user once the all the fields entered by the user is correct and accurate. In the same way, sub-authentication 2 verifies the user data and generates the decrypt key to the user. Here, if any of the sub-authentication doesn’t generate the key to the user then that particular user cannot decrypt the cipher text and can view the file.

8- CONCLUSION

This research proposed M-HABE scheme by considering the benefits that can be acquired through the ABE and HIBE access control processing. Here, this proposed method is mainly designed to be used in hierarchical multi-user-data shared environment. So, this environment is very apt for mobile cloud computing model in order to secure the privacy for the information and also rejects access to unauthorized users. When compare to the existed HABE scheme the proposed M-

HABE is very more adaptive for the mobile cloud computing in order to store, process, and access the huge information and files. Moreover, this system will provide different privilege entities for various people and provides access only to their permitted files and data.

The result of the proposed scheme have been shown by making use of Java technology and explained how effectively the data is being secured and allows the users to successfully retrieve the files from the cloud. When compare to other technologies like dot net, etc. the Java technology have been chosen as it provides better features to the researchers in providing the effective results accordingly to the proposed scheme.

The effectiveness of the proposed scheme showed better and secure results when compare to the existed technologies as it failed to provide hierarchical priority in accessing the data and also in securing the information. Hence, it can be concluded that the proposed scheme will not only achieve the hierarchical access control of mobile sensing information in mobile cloud computing model however it secures the information that is being acquired by unauthorized third party user.

9- FUTURE WORK

In the proposed scheme, private key and decrypt key have been sent to the authorized user to in order to allow access for the user to retrieve the data and to download the file. With the help of sub-authentication 1 and sub-authentication 2, these two keys are generated. However, in order to provide more security to the files stored in the cloud further this research can be extended and can be work out by introducing concept of attributes which may further used to verify whether the user is authorized or a third-party member.

10- 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, 2009.

[2] N. Fernando, S. W. Loke and W. Rahayu, “Mobile cloud computing: A survey,”ELSEVIER Future Generation Computer Systems, Vol. 29, no. 1, pp. 84-106, 2013.

[3] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, “Security and Privacy in Cloud Computing: A Survey,” in Sixth International Conference on Semantics, Knowledge and Grids, pp. 105–112 , 2010.

[4] R. Chatterjee and S. Roy, “Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud”, International Journal of Engineering Science and Computing, Vol. 7, Issue No.5, 2017.

[5] V.S. Sajitha and V. Reena Catherine, “Hierarchical Attribute-Based Encryption: A Survey”, International Journal of Engineering Development and Research, Vol. 5, Issue 2, ISSN: 2321-9939, 2017.

[6] Q. Han, S. Liang and H. Zhang, “Mobile cloud sensing, big data, and 5g networks make an intelligent and smart world,” IEEE Network , Vol. 29, no. 2, pp. 40–45, 2015.

[7] S. Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya, “Cloud-Based Augmentation for Mobile Devices: Motivation, Taxonomies, and Open Challenges,” IEEE , Communications Surveys & Tutorials ,Vol. 16, no. 1, pp. 337–368, 2014.

[8] R. Kumar and S. Rajalakshmi, “Mobile cloud computing: Standard approach to protecting and securing of mobile cloud ecosystems,” in Computer Sciences and applications (CSA), International Conference on IEEE, pp. 663–669, 2013.

[9] I. Stojmenovic, “Access Control in Distributed Systems: Merging Theory with Practice,” in 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 1–2 , 2011.

[10] G. Wang, Q. Liu and J. Wu, “Hierarchical attribute–based encryption for fine grained access control in cloud storage services”, in Proceedings of the

17th ACM conference on Computer and Communication Security , ACM , pp. 735-737, 2010.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proceedings of the 13th ACM conference on Computer and communications security - CCS ’06, p. 89 , 2006.

[12] J. Horwitz and B. Lynn, “Toward Hierarchical Identity-Based Encryption,” in Advanced in Cryptology EUROCRYPT 2002 Springer, Berlin, Heidelberg, pp. 466–481, 2002.

[13]A.Shamir,“Identity-Based Cryptosystems and Signature Schemes,” in Advances in Cryptology, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 47–53 , 2000.

[14] Y. Xie, H. Wen, B. Wu, Y. Jiang, and J. Meng, “A Modified Hierarchical Attribute-based Encryption Access Control Method for Mobile Cloud Computing,” IEEE Transactions on Cloud Computing, pp. 1–1, 2016.

[15] 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 Communication and Network Security (CNS), 2013 IEEE Conference on IEEE, pp. 383-384, 2013.