INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
(Volume2, Issue4)
Available online at: www.Ijariit.com

A robust cryptographic approach using multilevel key sharing paradigm

Tajinder Kaur[1]
[1]Sainiik Institute of Management & Technology,
Ropar , Punjab 140001, India
tajindersaini1992@gmail.com

Abstract: Cloud computing is a popular technology that provides services to the users on demand and on pay-per-usage fee that is they only pay for the data utilized when required. With the vast growth in the use of mobile phone applications, the users are relying on their phones for their personal as well as professional work and suffering from many problems (storage, processing, security etc). To overcome these limitations and growth in the use of cloud applications, a new development area has emerged recently called as Mobile cloud computing. Mobile cloud computing is an integration of three technologies cloud computing, mobile computing and internet, enabling the users to access the services at any time and from any place. Mobile phones are sensitive devices and the personal data is not secured when user stores data on cloud and can be easily attacked by unauthorized person. This paper presents a two level encryption through a mobile application that encrypts the data before moving it to the cloud that ensures the security and the users authentication.

Keywords: Cloud Computing,IAAS, PAAS, SAAS, mobile cloud computing, Data security,Ghost, AES encryption.

I. INTRODUCTION

Cloud computing is a advanced technology that is growing continuously since the 90's. The concept of cloud computing emerged from the telecommunication industry in 1990's when the providers began to use virtual private networks for the data communication [14]. Cloud computing is basically a virtual distributed computing that consists of Data server i.e. cluster of servers remotely allocating the services to fulfill the demands of the users.

During last decade, the use of internet has increased drastically and had strong impact on the world in terms of business, education, communication and other fields. Internet has become an integral part of an individual's life but this has also raised the costs of hardware and software. This is also a major point in the rise of cloud computing that begun the source of providing services to the customers cutting down the costs related with hardware and software with high flexibility and reliability.

Cloud computing has number of definitions but the U.S NIST (National Institute of Standards and Technology) has defined the cloud computing as "cloud computing is a model for enabling on demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned by and released with minimal effort or service provider interaction."

Although this resulted in attraction of the enterprises, educational organizations, government agencies etc towards the cloud computing like Amazon, IBM, Google etc creating their own cloud platforms to provide more services and grow their business [9][10][11].

II. CLOUD COMPUTING SERVICE MODELS

Cloud computing is composed of three service models which are - IAAS, PAAS, SAAS.

Infrastructure-as-a-service (IAAS): IAAS is the base layer and a virtualized platform. The main objective is to provide computer infrastructure to the consumers at any time and any place. Infrastructure includes the processing, storage, network and servers etc are provisioned to the customers on demand. Here the client pays for only what they use i.e. pay-per-use basis and have no responsibility of maintaining the infrastructure [3]. Examples include Amazon EC2 etc.

Platform-as-a-service (PAAS): PAAS provides an environment where the end-users, developers can create their own software and applications without any software installation i.e. by using the development tools/kit (GUI tools, IDE etc) provided by the platform provider. PAAS offers the facility to end-users and developers to deploy their applications over the cloud without the complexity of buying any hardware and software. The consumers can manage the deployed applications and can enhance also when needed. Example of PAAS includes Google Apps and Force.com [3][9][10].

Software-as-a-service (SAAS): SAAS is a cloud model where the software applications are not created instead the provider provides the software applications running on cloud infrastructure that can be accessed easily by any user through web portal/browser. The user is free from buying, installing or maintaining the software and only pay for the amount of services used [2][3]. Example of SaaS includes Gmail, Yahoo mail etc.

III. MOBILE CLOUD COMPUTING

Mobile cloud computing is a paradigm that has recently gained attention because of the tremendous growth in the use of mobile devices like Smart phones, Tablets, Laptops etc and to meet the used demands for using richer and complex application on mobile devices [7][13]. There are several definitions of MCC available, and one of them is for example, Mobile cloud computing is "a rich mobile computing technology that leverages unified elastic resources of varied clouds and network technologies toward unrestricted functionality, storage and mobility. It serves a multitude of mobile devices anywhere anytime through the channel Ethernet or Internet regardless of heterogeneous environments and platforms based on the pay-as-you-use principle [6]."

With the explosion of mobile rich applications, mobile users are able to do almost everything (email, making spreadsheets, slides etc) using phones but so the problem of battery life, storage, processing, security etc had also became a constraint for mobile computing [16][17]. The integration of cloud computing with mobile computing and the internet had significantly overcome all the limitations of the resource constrained mobile phones and given the new development area of technology called Mobile cloud computing.

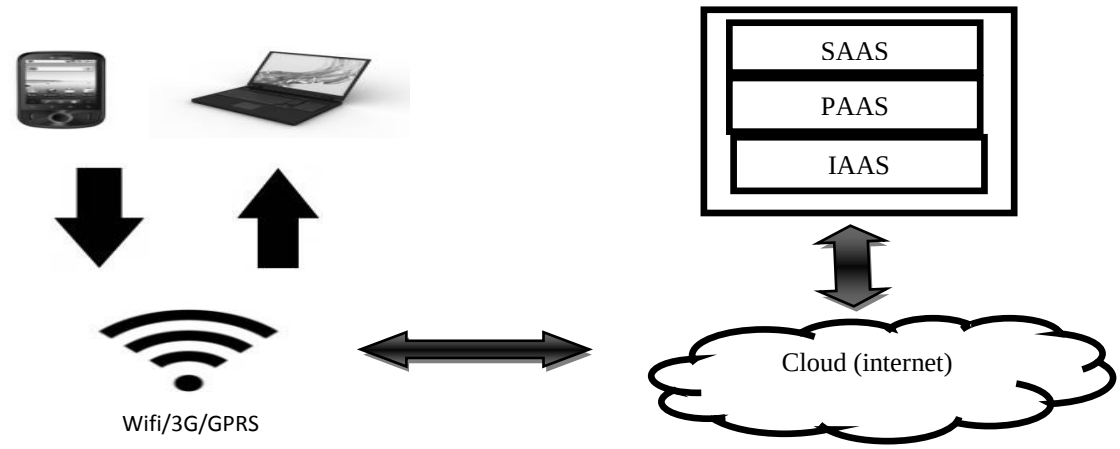


Figure 2. Architecture of Mobile cloud computing.

The figure 1. shows the model of mobile cloud computing. The mobile devices connect with a hotspot or base station by mobile internet like 3G, WiFi or GPRS [9]. The cloud constitutes infrastructure centers and servers providing IT resources [18] e.g. SAAS, PAAS, IAAS that act in response to the requests by the users. . MCC enables user to access online extensive range of services without getting attached to hardware [9].

Data security is always a major concern in every technology and so in the mobile cloud computing. Smartphone's contain sensitive data and when the user sends data using smart phones or stores the data on the cloud, it could be easily stolen by the attacker, because there is no security of the data in the phone and the data at rest on the cloud, so the data should be encrypted before it is moved to the cloud storage.

IV. PROPOSED WORK

A. Proposed methodology

As discussed in section III that security is always a constraint and to resolve this, proposed work includes a model that provides security through a android mobile application.

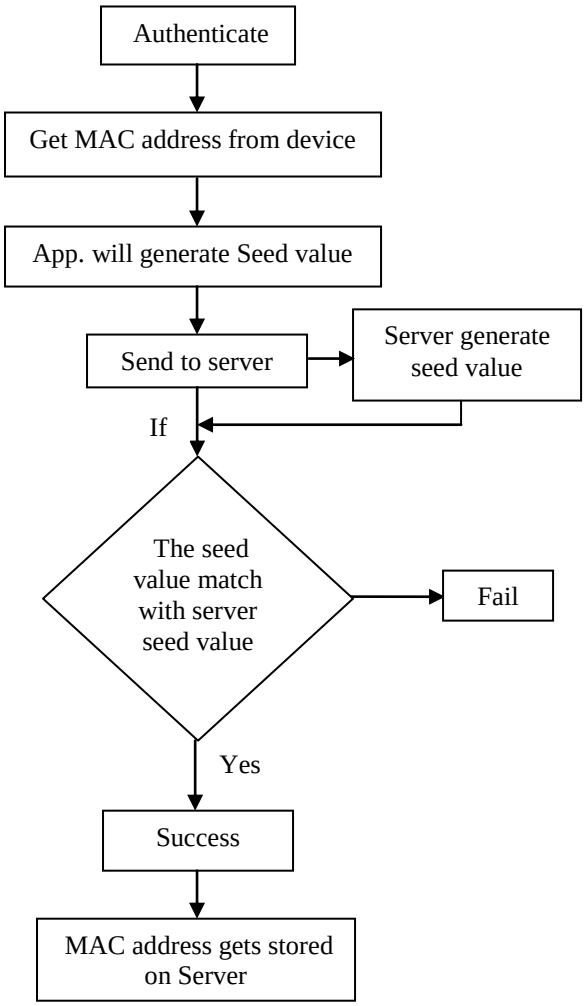


Figure 3. flow chart of authentication

The app. stores the MAC address of the device and generates seed value which authenticates the user by matching values at both client and server end. The user gets authenticated again at the registration and login phase that ensures that only the authenticated user has the access to data. For the security of data, first it is encrypted with the Ghost encryption algorithm [3] and is further encrypted with the AES algorithm [22] [23] that provides high level of security. The working is explained in detail as below:-

Fig. 3 shows that during the first authentication phase if the Mac address of the device and seed value gets matched at both the ends i.e. client and server, the user get authenticated successfully else if not matched then fails.

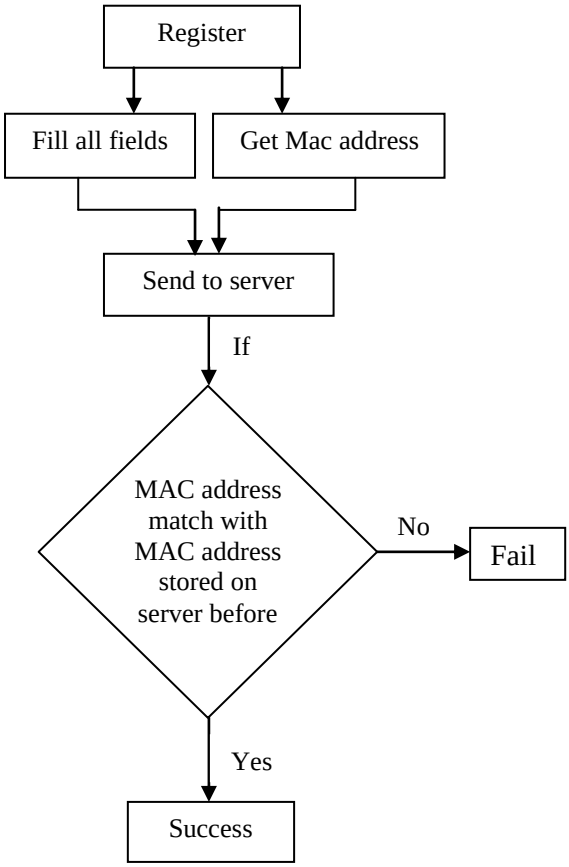


Figure 4. Flow chart of Registration

After authentication the user can register. Fig. 4 shows when user fills the details and submits, then user will only get registered if the Mac address gets matched with that stored on the server during first authentication phase.

Once got registered, the user can now login. Figure 5 shows that Mac address is again sent to the server when the user submits the login credentials. If the credentials and Mac gets matched with the values stored on server, user get login otherwise fails. The next window appears where the user can upload and download files.

- When the user wants to upload a file
- Select the file
- File gets encrypted with the Ghost and AES algorithm
- File gets stored on the server

Similarly when the user wants to download a file, a list of uploaded files appears. The user selects the file which gets decrypted using the both algorithms and gets stored on the device.

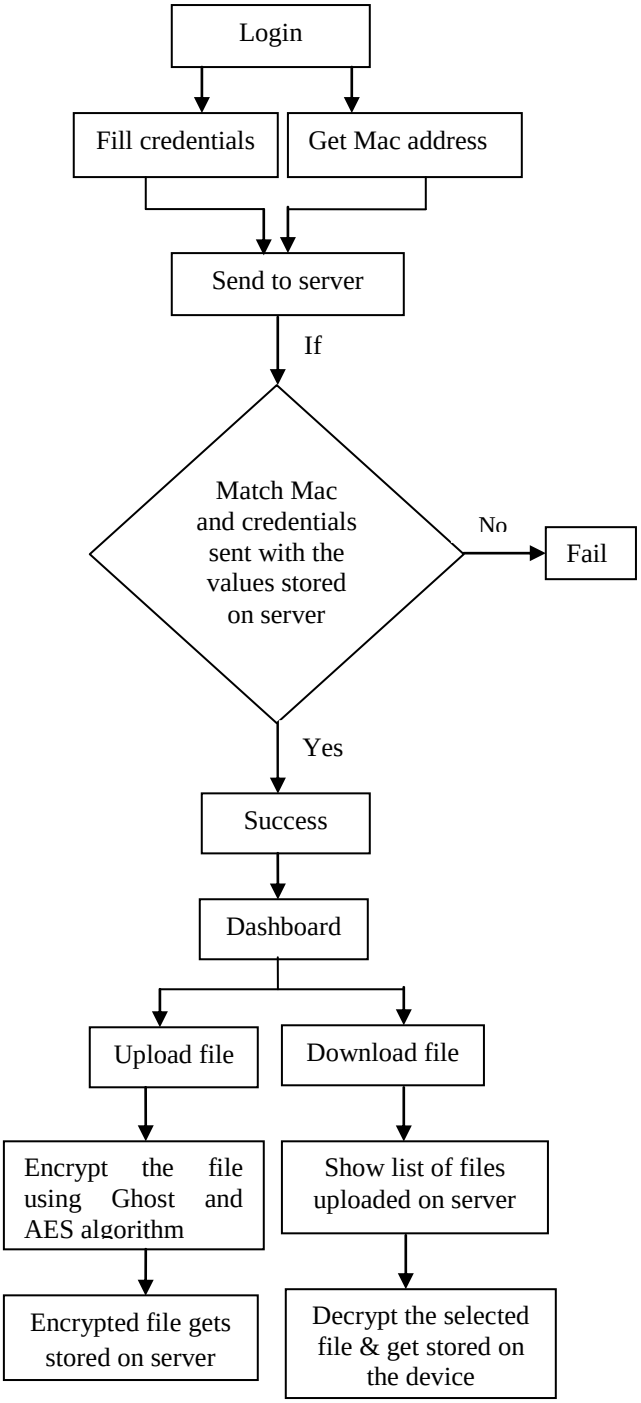


Figure 5. Flowchart of login phase

V. RESULTS

The results show that the proposed scheme provides more security and has strong authentication as shown below:-

1. Authentication failover testing

   Table 1. represent the testing results for authentication. The process has been tested by no. of users. In this process, the Mac address of the client and the generated seed value at client end is sent to the server. At server the values gets matched with the server generated values. Proposed scheme has above 90% security results.

Table 1. Authentication failover

Users	MAC address	Seed value client	Seed value server	Match/ unmatch
User 1	b4:ce:f6:0d:4f:2n	48	48	Match
User 2	e6:f8:9y:7c:6d:0j	141	144	Unmatch
User 3	f5:c8:9y:0a:y1:5m	112	112	Match
User 4	b2:5j:fh:7n:d2:p6	66	66	Match
User 5	h8:d2:1k:3s:4j:2f	60	60	Match
User 6	J3:li:4k:a6:8b:5r	90	104	Unmatch
User 7	00:a1:c9:14:c8:2h	136	136	Match
User 8	1C:b3:d9:8i:6z:5s	128	128	Match
User 9	af:r7:y2:e9:3c:3h	72	72	Match
User 10	5b:e6:3j:2h:9i:5v	120	120	Match

Table 2. Login table

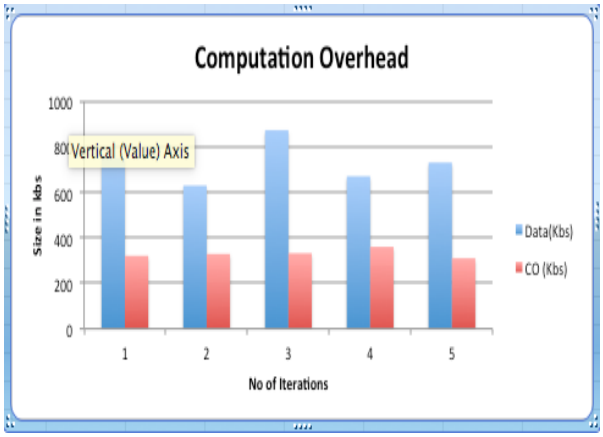
Users	User-name	Pass-word	MAC address	Authen-ticated
User 1	✓	✓	✓	✓
User 2	×	✓	✓	×
User 3	✓	✓	×	×
User 4	✓	✓	✓	✓
User 5	✓	×	✓	×
User 6	✓	✓	✓	✓
User 7	✓	×	×	×
User 8	✓	✓	✓	✓
User 9	✓	✓	✓	✓
User 10	✓	✓	✓	✓

2. Login testing

Table 2. represents the testing result of authentication. Second level of authentication is done by the 10 number of users. In this e-mail id , password and Mac address will be sent by the client for authentication. If one of these three parameters does not get match, then user will not be able to proceed further which ensures strong authentication. The proposed scheme has 100% accuracy results in case of authenticated users.

3. Computation overhead

Sr. No.	Data(Kbs)	File Size(Kbs)	CO (Kbs)
1	750	429	321
2	629	300	329
3	872	540	332
4	670	310	360
5	730	420	310



VI. CONCLUSION AND FUTURE SCOPE

In this paper, we have presented a security scheme for the user's data when it is sent to the cloud and data stored on the cloud through a Smartphone application. In this paper, we have used two algorithms i.e. Ghost and AES that means data goes through two levels of encryption ensuring more security. The user can access the data by using the application when ever required. The future work lies in further increasing the security by adding other security features as it is still a developing technology.

REFERENCES

[1] Alam, M. M., Hati, S., De, D., & Chattopadhyay, S. (2014, September). SeCure Sharing Of Mobile Device Data Using Public Cloud. In Confluence The Next Generation Information Technology Summit (Confluence), 2014 5th International Conference- (pp. 149-154). IEEE.

[2] Anbazhagan, S., & Somasundaram, K (2014, June). CLOUD COMPUTING SECURITY THROUGH SYMMETRIC CIPHER MODEL. International Journal of Computer Science & Information Technology (IJCSIT)

[3] Armel, A. S. R., & Thavavel, V. (2013, December). Ghost encryption: Mobile data security model encrypting data before moving it to the cloud service provider. In Advanced Computing (ICoAC), 2013 Fifth International Conference on (pp. 512-516). IEEE.

[4] Banupriya, K., & Andrews, S. (2014, November). A privacy preserving mechanism for protecting data in mobile ad-hoc network for mobile applications. In Circuits, Communication, Control and Computing (I4C), 2014 International Conference on (pp. 348-352). IEEE.

[5] Behl, A., & Behl, K. (2012, October). An analysis of cloud computing security issues. In Information and Communication Technologies (WICT), 2012 World Congress on (pp. 109-114). IEEE.

[6] Chang, R. S., Gao, J., Gruhn, V., He, J., Roussos, G., & Tsai, W. T. (2013, March). Mobile Cloud Computing Research-Issues, Challenges and Needs. In Service Oriented System Engineering (SOSE), 2013 IEEE 7th International Symposium on (pp. 442-453). IEEE

[7] Dinh, H. T., Lee, C., Niyato, D., & Wang, P. (2013). A survey of mobile cloud computing: architecture, applications, and approaches. Wireless communications and mobile computing, 13(18), 1587-1611.

[8] Dharmale, P. N., & Ramteke, P. L. Mobile Cloud Computing. International journal of science and research(IJSR),2013

[9] Dai, Q., Yang, H., Yao, Q., & Chen, Y. (2012, October). An improved security service scheme in mobile cloud environment. In ClouComputing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference on (Vol. 1, pp. 407-412). IEEE.

[10] Ennajjar, I., Tabii, Y., & Benkaddour, A. (2014, October). Security in cloud computing approaches and solutions. In Information Science and Technology (CIST), 2014 Third IEEE International Colloquium in (pp. 57-61). IEEE.

[11] Grover, J., & Sharma, M. (2014, July). Cloud computing and its security issues—A review. In Computing, Communication and Networking Technologies (ICCCNT), 2014 International Conference on (pp. 1-5). IEEE.

[12] https://en.wikipedia.org/wiki/Mobile_cloud_computing

[13] Liu, F., Shu, P., Jin, H., Ding, L., Yu, J., Niu, D., & Li, B. (2013). Gearing resource-poor mobile devices with powerful clouds: architectures, challenges, and applications. Wireless Communications, IEEE, 20(3), 14-22.

[14] Lori, M. (2009). Data security in the world of cloud computing. Co-published by the IEEE Computer And reliability Societies, 61-64.

[15] Mathisen, E. (2011, May). Security challenges and solutions in cloud computing. In Digital Ecosystems and Technologies Conference (DEST), 2011 Proceedings of the 5th IEEE International Conference on (pp. 208-212). IEEE.

[16] Qi, H., & Gani, A. (2012, May). Research on mobile cloud computing: Review, trend and perspectives. In Digital Information and Communication Technology and it's Applications (DICTAP), 2012 Second International Conference on (pp. 195-202). IEEE.

[17] Sanaei, Z., Abolfazli, S., Gani, A., & Buyya, R. (2014). Heterogeneity in mobile cloud computing: taxonomy and open challenges. Communications Surveys & Tutorials, IEEE, 16(1), 369-392.

[18] Suo, H., Liu, Z., Wan, J., & Zhou, K. (2013, July). Security and privacy in mobile cloud computing. In Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International (pp. 655-659). IEEE.

[19] Singh, A., & Shrivastava, M. (2012). Overview of security issues in cloud computing. International Journal of Advanced Computer Research (IJACR) Volume, 2.

[20] Singh, N., & Raj, G. (2012). Security on bccp trough AES encryption technique. Special Issue of INTERNATIONAL journal of engineering science & avanced technology (2250–3676) Jul-Aug.

[21] Thiyagarajan, B., & Kamalakannan, R. (2014, February). Data integrity and security in cloud environment using AES algorithm. In Information Communication and Embedded Systems (ICICES), 2014 International Conference on (pp. 1-5). IEEE.

[22] Usman, M., & Akram, U. (2014, October). Ensuring Data Security by AES for Global Software Development in Cloud Computing. In IT Convergence and Security (ICITCS), 2014 International Conference on (pp. 1-7). IEEE

[23] You, P., Peng, Y., Liu, W., & Xue, S. (2012, June). Security issues and solutions in cloud computing. In Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on (pp. 573-577). IEEE.

[24] www.ibm.com/developerworks/cloud/library/cl-mobilecloudcomputing

[25] www.thoughtsoncloud.com/2013/06/mobile-cloud-computing