ISSN:0975-9646

Encrypting Contacts in Mobile Cloud using Polyalphabetic Substitution

Ramandeep Singh Rajpal[1], Raghvendra Kumar[2]

[1]Computer Science Engineering , RGPV
LNCT Jabalpur INDIA

[2]Asst Prof Computer Science Department
LNCT Jabalpur INDIA

***Abstract*— Cloud computing environment provides a great flexibility and availability of computing resources at a lower cost. This emerging technology opens a new era of e-services in different disciplines. In fact, the researchers take into account the mobile cloud computing because the combination of mobile computing, mobile web and cloud computing .The mobile cloud computing is basically an integration of cloud computing with mobile. The main issue mobile cloud computing facing today is security and authenticity. We have tried to address this issue by securing contacts of mobile in cloud using polyalphabetic substitution method.**

***Keywords*— cloud, cloud computing, mobile, security, polyalphabetic.**

I. INTRODUCTION

Mobile devices (e.g., Smartphone, tablet pcs, etc) are increasingly becoming an essential part of human life as the most effective and convenient communication tools not bounded by time and place. Mobile users accumulate rich experience of various services from mobile applications (e.g., iPhone apps, Google apps, etc), which run on the devices and/or on remote servers via wireless networks. The rapid progress of mobile computing (MC) becomes a powerful trend in the development of IT technology as well as commerce and industry fields. However, the mobile devices are facing many challenges in their resources (e.g., battery life, storage, and bandwidth) and communications (e.g., mobility and security). The limited resources significantly impede the improvement of service qualities. Cloud computing (CC) has been widely recognized as the next generation's computing infrastructure. CC offers some advantages by allowing users to use infrastructure (e.g., servers, networks, and storages), platforms (e.g., middleware services and operating systems), and softwares (e.g., application programs) provided by cloud providers (e.g., Google, Amazon, and Sales force) at low cost. In addition, CC enables users to elastically utilize resources in an on-demand fashion. As a result, mobile applications can be rapidly provisioned and released with the minimal management efforts or service provider's interactions. With the explosion of mobile applications and the support of CC for a variety of services for mobile users, mobile cloud computing (MCC) is introduced as an integration of cloud computing into the mobile environment. Mobile cloud computing brings new types of services and facilities for mobile users to take full advantages of cloud computing.

The term "mobile cloud computing" was introduced not long after the concept of "cloud computing" launched in mid-2007. It has been attracting the attentions of entrepreneurs as a profitable business option that reduces the development and running cost of mobile applications, of mobile users as a new technology to achieve rich experience of a variety of mobile services at low cost, and of researchers as a promising solution for green IT . This section provides an overview of MCC including definition, architecture, and advantages of MCC. A. What is Mobile Cloud Computing? The Mobile Cloud Computing Forum defines MCC as follows: "Mobile Cloud Computing at its simplest, refers to an infrastructure where both the data storage and the data processing happen outside of the mobile device. Mobile cloud applications move the computing power and data storage away from mobile phones and into the cloud, bringing applications and mobile computing to not just smart phone users but a much broader range of mobile subscribers".

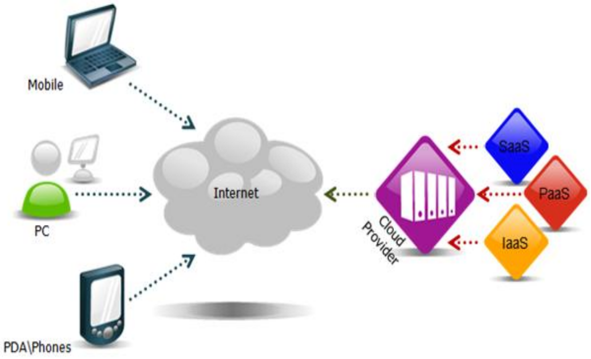

FIGURE 1. MOBILE CLOUD COMPUTING

1.1 Features of Mobile Cloud Computing

1. **Effectiveness of Task Processing: -** Rapidly deploys and increase employment by speedy providing physical machines or virtual machines. This advantage clearly indicates that users will see the results of tasks directly by mobile devices though the interface of input and output isn't ok.
2. **Convenience of Sharing Data**: - A great deal of knowledge is hold on within the cloud finish of servers, sanction active sharing knowledge handily. If the information measure is wide enough, it'll work as fluently as domestically, that is straightforward to comprehend for mobile devices.
3. **Elimination of Rationality: -** Mobile cloud computing eliminates the limitation of rationality, sanction active individuals to get what they need at anytime and anyplace from the mobile web. At identical time, MCC

will monitor real-timely resources usage and rebalance the allocation of resources once required.

4. **Mobile Devices Independence of MCC System: -** The entire computation area unit carried on within the cloud-far finish servers, therefore, mobile cloud computing doesn't have demand for mobile devices, even imbecilic cell phones may also notice mobile cloud computing.

5:- **Robust Accommodative Ability**: - Mobile cloud computing manages a spread of various workloads, together with the batch of back-end operations and user-oriented interactive applications . It support for redundancy, self-healing and extremely ascendable programming model, in order that employment are often pass though a spread of inevitable hardware/software failure.

1.2 Security Threats Present in Mobile Cloud Computing (MCC)

There are a unit three vital things to be considered the safety of mobile cloud computing. Firstly, the safety of mobile cloud computing is nearly specifically just like the security of mobile web. The safety tools that area unit used these days to guard the inner network cloud, conjointly accustomed defend knowledge within the mobile cloud. Secondly, for remaining financially competitive, a number of these security technologies ought to be touched to the mobile cloud. Thirdly, if a top quality mobile cloud service supplier is chosen, the safeties within the mobile cloud are pretty much as good as or higher than this security in most cases.

In this section, we tend to offer the attainable security threats in step with the system structure of the mobile cloud computing.

A. Physical layer

1. Isolation Failure: - The parts of MCC that accustomed build disk partitions, CPU cache, graphics process units etc aren't designed to supply robust isolation properties or compartmentalization.

2. Malicious Insiders: - This threat is known because the security class of physical layer. Malicious insiders' impact on organization is hefty. Given their level of access, they will infiltrate organizations and assets and do complete harm, monetary losses and productivity losses. Therefore, it's important for purchasers of mobile cloud services on what controls are provided by mobile cloud suppliers to notice and defend against the malicious within threats.

B. Virtual layer

VM-Level attacks: - The mobile cloud computing relies on VM technology. For implementation of the mobile cloud computing, a hypervisor used can seem the vulnerabilities because of some bug of itself cryptography level.

C. Managing layer

1. Loss of Governance: - The service level agreements (SLA) might not have commitment on the part of cloud supplier, to supply such services, so having a spot in security defences moving security. This loss of management might cause an absence of confidentiality, integrity and convenience of knowledge.

2. Lock-In: - Lock-In suggests that inability of the client to migrate from one cloud service supplier to a different. At current, there area unit few tools, procedures or normal knowledge formats which give knowledge, application or service move ability.

3. Knowledge Loss or Discharge: - This knowledge loss or leakage is also because of lean authentication, authorization and audit controls, inconsistent use of coding and then software keys and so on.

4. Compliance Risks: - This threat arises because of lack of governance over audits and use normal assessments. Because of this, customers of mobile cloud services don't have a read into the processes, procedures and practices of the supplier within the areas of access, identity management and segregation of duties. The mobile cloud computing service suppliers might not be ready to offer proof of their own compliance with the required necessities or might not allow AN audit by cloud client.

D. Access layer

1. Abuse Use of Mobile Cloud Computing: - The threat arises because of comparatively weak registration systems gift within the mobile cloud computing setting. In mobile cloud computing registration method, anyone having a legitimate account will register and use the service.

Once the valid account is employed by the malicious actors, the mobile cloud computing are vulnerable.

2. Insecure Interfaces and APIs: - The provisioning, management, orchestration and observance of the mobile cloud computing service area unit typically done mistreatment these interfaces. If the weak set of interfaces and arthropod genus area unit used, this might expose organizations to numerous security threats, like anonymous access, improper authorizations, restricted observance so on.

3. Account/ Service hijacking: - Attackers will steal credentials and gain access to important areas of deployed cloud computing services, leading to compromise of the confidentiality, integrity and convenience of those services.

4. Management Interface Compromise: - The client management interface of the mobile cloud supplier is accessible through the mobile web. In mobile cloud computing, larger set of resources area unit accessed through these interfaces than ancient hosting, since mobile cloud computing provides remote access to customers through these management interfaces. This might create a significant threat if Um or radio interface vulnerabilities area unit gift**.**

A. Access Control

Access management mechanisms area unit thought-about as tools to confirm approved user access and to forestall unauthorized access to data systems. Such mechanisms ought to cowl all stages within the lifecycle of user access, from the initial registration of recent users to the ultimate de-registration of users. Special attention ought to be, wherever applicable, to the requirement to manage the allocation of privileged access rights. The subsequent area unit the six management statement ought to be bear in mind to guarantee correct access management:

1. Control access to information.
2. Manage user access rights.
3. Encourage good access practices.

4. Control access to network services.
5. Control access to operating systems.
6. Control access to applications and systems.

B. Supervisory Control

One of the vital viewpoints in mobile cloud security is finding issues and vulnerabilities that exist in mobile cloud, however a lot of vital that finding them is applying applicable response against the matter found. To realize flexibility, measurability, and potency usage of accessible resources, the mobile cloud suppliers should face major challenges within the space of ability, employment analysis, and prototypes .

1. Partitioning: - It is vital to divide knowledge of mobile cloud finish into partitions that maximize group action and question performance.

2. Migration: - Flexibility within the space of the mobile cloud suggests that dedicating resources wherever they're most required. Notably, an oversized amount of knowledge might have to be touched so as to reconcile during a information setting.

3. Resources Allocation: - It is important to research and classify their resource necessities to choose however those be assign to virtual machines.

1.3 Advantages of mobile cloud computing

- Mobile applications leverage remote processing, extending battery lifetime
- MCC enables mobile users to store and access large data on the cloud. Mobile applications are no longer constrained by the storage capacity of the device.
- Keeping data and applications in the cloud reduces the potential for loss of data in the event of a hardware failure, improving reliability and availability
- MCC can be designed with a comprehensive data security model for both service providers and users by allowing protected copyrighted digital contents in the cloud. MCC providers have security services in place such as virus scanning, malicious code detection and authentication for mobile users
- The data and services in the cloud are always available even when the users are moving from place to place
- Sharing data in the Cloud provides the user with access to the latest documentation even while ‘on the go’
- Mobile applications can be scaled to meet the growing user demands
- Service providers can easily add and expand their service offerings
- Multiple services from different providers can be integrated easily through the cloud to meet today’s complex user demands

1.4 Cloud Computing Applications

1. **Cloud Computing For E-Learning: -** E-learning is a new trend in education that tries to make the best use of information technology (IT). Cloud computing is an attractive environment for students, faculty members and researchers. As an emerging IT, cloud computing can provide universities and research centres with powerful and cost-effective computational infrastructure. Students can connect to campus educational services through their personal mobile devices from anywhere. Faculty members can have efficient and flexible access to their course material in their class rooms. Researchers can find articles, models and run their experiments on the cloud faster than ever.
2. **Cloud Computing for ERP**: - Traditional Enterprise Resource Planning (ERP) (Figure4) systems have some limitations. As the business grows inside an organization, different software applications may be needed to manage information in many areas such as human resources, payroll, finance administration. Obviously, purchasing, installing and maintaining such multiple types of software applications represent a challenge for business growing. Furthermore, traditional ERP systems are limited in terms of multiple user accessibility, performance and availability of resources. ERP cloud refers to installing the ERP applications on the cloud infrastructure (e.g. servers in data centres) so that they can be accessed by the organizations ubiquitously through a network connection. Therefore, with this technology, project managers do not need to worry about installing, upgrading and maintaining applications inside their organizations. In addition, ERP cloud provides organizations with cost-effective scalable resources, high availability of data and applications and multitenant accessibility. Organizations can reduce their capital expenses and achieve higher Return on Investment (ROI) and shorter payback period by leasing resources and services on the cloud rather than purchasing new equipments and software applications. This is important especially for small and medium scale business where budgets are limited
3. **Cloud Computing For E-Government: -** Traditional e-governance faces different challenges such as resources cannot scale up and down with the demands that change over time. This may result in insufficient or redundant resources.

3.1 SW and HW have to be frequently upgraded and maintained which costs time and money

3.2 New SW licences have to be purchase

3.3 System should be available 24x7

3.4 Limited data storage and recover

3.5 Need to provide secure environment with authentication and access control

3.6 Lack of accountability Cloud computing technology can significantly improve the way a government functions, the services it provides to its citizens and institutions and its cooperation with other governments. It can help address these challenges by providing elastic scalable, customized andhighly available environment. It also relieves governments from the burden of upgrading, maintenance and licensing SW and allows them to focus on the core work. Scalable and cost effective data storage can also be provided and file replication and multiple installations in geographically separated locations can be used for data recover in case of disasters.

1.5 Issues in Mobile Cloud Computing

Although some research paper of mobile cloud computing has already been deployed around the world, there is still a long way for business implementation, and some research aspects should be considered in further work.

A. Data Delivery
B. Task Division
C. Better Service
D. Security
E.Complexity
F. Access Speed

1.6 Polyalphabetic Substitution

1. Encryption is an effective way to achieve the security of data. The word of encryption came in mind of King Julius Ceaser because he did not believe on his messenger so he thought to encrypt the data or message by replacing every alphabet of data by 3rd next alphabet . The process of Encryption hides the data in a way that an attacker cannot hack the data. The main purpose of encryption is to hide the data from unauthorized parties from viewing, altering the data. Encryption techniques occur or used by using the shifting techniques, mathematical operations and shifting techniques. The Simple data is known as Plain text and Data after encryption is known as Cipher text. Substitution and transposition techniques are mainly used for it.
2. In encryption methods, two methods are used for encryption purpose-
   a. Substitution techniques-Change the one letter by another using secret key.
   b. Transposition techniques-Replace the place of letters of plaintext.
3. In substitution techs mono alphabetic and polyalphabetic techniques are used. In mono alphabetic, a single cipher alphabet is used per message. This technique was easy to break because they show the frequency data of plaintext alphabet. So polyalphabetic techniques came into knowledge in which different mono alphabetic substitution as one proceeds through original message.

Types of Poly alphabetic Cipher

There are three types of polyalphabetic cipher, these are
A. Vignere cipher B. Vernam cipher

A. ***Vignere Cipher-*** This is the best one and one of the simplest techniques. In this the set of related mono alphabetic substitution rules consist of the 26 ceaser cipher from (0 to 25). Each cipher is denoted by a key letter, which is substitute for plaintext letters.

To understand this scheme, we use a table known as VIGNERE TABLEAU. All 26 ciphers (A-Z) letters is laid out horizontally with the key letter to its left.

a. Process used for Encryption- There is a given key letter(x) and plaintext letter (y), then cipher text letter for it will be the intersections of the row labeled „X‟ and column labeled „Y‟. To encrypt the message, there is a key required that is as long as the message. Here key is used as repeating keyword.

Example-

Key- d e f e n s e d e f e n s e d e f e n s e d e f e n s
Plaintext- w e a r e a c c e p t i n g y o u r c o n d i t i o n
Cipher text- z i f v r s g f i u x v f k b s z v p h r g m y m b f

b. Decryption Process- It is also as simple as encryption. The position of cipher text letter in that row determines the column and plaintext will be letter at the top of that column. So in this example cipher text came "zifvrsgfiuxvfkbszvphrgmymbf" and the key is "defensedefensedefensedefens" so at time of decryption first key letter is „d‟ and first cipher text letter is z then when we find „ z‟ in row of key letter d, we get it in the column of „w‟ of plaintext field. So, first letter that we decrypt is „w‟ and so on.

c. Advantage- We get different ciphers text of same plaintext with changing the key letter.

d. Disadvantage- Repetition of key letter again makes it less secure. As in above taken example after 7 key alphabets again repeat first letter of keyword. So an analyst can easily detect the repeated sequence of same cipher text and make the assumption that the keyword is of same length.

Solution- This periodic nature of keyword can be eliminated by using non repeated sequence of keyword that is as long as the message itself.

VIGNERE proposed what is referred as "**AUTOKEY SYSTEM**", in which a keyword is concatenated with the plaintext itself to provide further key.

Key- d e f e n s e **w e a r e a c c e p t i n g y o u r c o**
P.Text- w e a r e a c c e p t i n g y o u r c o n d i t i o n
C.Text- z i f v r s g y i p k m n i a s j k k b t b w n z q b

So as shown here in this example now there is no repletion of alphabets. And we get this cipher text with help of vignere tableau, when we pick 1st alphabet of plaintext and 1st alphabet of keyword and go to check the related alphabet as a cipher text in vignere tableau then get the „Z‟ as1st alphabet of cipher text and so on till last. In above example it is clearly shown that how plaintext is used as a keyword after once using the keyword letter. When we use the plaintext to complete the keyword for encryption, we do not get the same frequency of letters in cipher text which makes the poor security.

1.7 Proposed Work

Algorithm

Step 1: A User interface shall be created over cloud for adding the mobile id online, which is added after password authentication by the mobile user.

Step 2: Mobile application shall be created using android application development tool, which shall connect to the cloud database using SaaS application developed over the cloud.

Step 3: As the mobile app tries to communicate with the cloud application, it will require authenticating internally with the mobile id which was added by the user through web application.

Step 4: After authentication, mobile will communicate with the cloud application using encrypted data.

Step 5: For encryption of the mobile data poly alphabetic substitution cipher will be used which is faster and secure as require n26 permutations by the brute force attack.
Step 6: The work shall have following implementation modules:
Mobile App Module
Authentication
Encryption using Poly Alphabetic Substitution Cipher
Decryption using Poly Alphabetic Substitution Cipher
SaaS Layer Application Module
Web Interface for Mobile Users
Encryption using Poly Alphabetic Substitution Cipher
Decryption using Poly Alphabetic Substitution Cipher
Communication module with Mobile Application
Step 7: Poly Alphabetic Substitution Cipher requires O(n) complexity to encrypt or decrypt the data.
The data or contacts (Figure1) earlier were stored in the mobile, then the mobile's internal memory is been used. In this we are saving mobile data in cloud and can be retrieving quickly when required. The data is been stored in clouds database.

Flow Chart

1. Initially you have to register our information with cloud, by the means of user name and password.
2. After registration you have to sign in our account.
3. After login to your account you have to select that contact which is to be stored in to the cloud.
4. After selecting that contact ,the data is been encrypted and sent to the cloud.
5. Now that contact is been saved to the cloud and is fetched only when user name and password is entered correctly.
6. Now you have data saved in the cloud and the memory is not been occupied by the data in mobile.
7. In order to fetch data we have to just type the name and data will be in your phone**.**

1.8 Results and Comparison

After implementing our method and implementing it, we compare the results with existing wok.

TABLE I

Sno.	Feature	Existing work	Proposed Work
1.	Performance	Increases with increase of data and high due to double encryption and decryption applied	High as the encryption is applied only once and key level identification is done
2.	Database	Works for Text data and high performance SQL queries are not applicable	Use MySql database to store and retrieve the the cipher text. High performance SQL queries are applicable
3	Security	Moderate as the dependency is on the chosen methods of encryption and decryption. But dual encryption makes it worth	High as after encryption key is applied for further processing. The different techniques also makes the security worth and user dependency is reduced
4	Complexity	High as the multiple level encryption and decryption requires O(f1()) * O (f2()) complexity and O(f()) depends upon the algorithms of encryption and decryption chosen	Moderate as the data being processed at a time is only for one particular user and only one level of encryption is performed. Complexity of key processing is very less in respect of the other processing
5	Cost	High resources are required as the ciphertext and plaintext both reside in memory	Low as the SQL query retrieves only filtered data from the database

Conclusion And Future Work

This paper introduced mobile cloud computing as the latest emerging technology. Besides there are several critical drawbacks in devices, which include battery life time, security issues etc. This research presents an approach for improving the security and authenticity of mobile cloud computing in an mobile environment. In future, next step will be to improve the battery lifetime of devices, which is using mobile cloud computing. In future as ground for mobile and web security is been growing day by day, there can be other encryption and decryption techniques which can be implemented, and and there is a scope that they can give better security options.

References

[1] Radu Prodan and Simon Ostermann, [1]. YekiniN. Asafe Aigbokhan E. Edwin Okiki F. Mercy "Cryptography System for Online Communication Using Polyalphabetic Substitution Method" Int. J. Advanced Networking and Applications. (2014) ISSN : 0975-0290.

[2] Sarika U Kadlag , Rahul L Paikrao ." Hybrid Cryptosystem for Secure Text File for Cloud" Volume 2, Issue 2, February 2014 International Journal of Advance Research in Computer Science and Management Studies.

[3].Bhavya Sareen ,Sugandha Sharma, Mayank Arora " Mobile Cloud Computing Security as a Service Using Android" International Journal of Computer Applications (0975 – 8887) Volume 99 – No.17, August 2014

[4] Michael Miller, "Cloud Computing Pros and Cons for End Users", microsoftpartnercommunity.co.uk, 2009.

[5] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz,A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing", UC Berkeley Reliable Adaptive Distributed Systems Laboratory,2009.

[6] Kresimir Popvoic and Zeljko Hocenski, "Cloud Computing Security Issues and Challenges", MIPRO, Opatijia, Croatia, May 24-28, 2010.

[7]Radu Prodan and Simon Ostermann "A Survey and Taxonomy of Infrastructure as a Service and Web Hosting Cloud Providers", 10th IEEE/ACM International Conference on Grid Computing, 2009

[8] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing", Communication of the ACM, Vol. 53, No. 4, April 2010.

[9] K. Chard, S. Caton, O. Rana and K. Bubendorfer, "Social Cloud: Cloud Computing in Social Networks", 3rd IEEE International Conference on Cloud Computing, Miami, FL, USA, July 5-10,2010.

[10] L. Tang, J. Dong, Y. Zhao and L. Zhang "Enterprise Cloud Service Architecture", 3rd IEEE International Conference on Cloud Computing ,Miami, FL, USA, July 5-10,2010.

[11] W. Jansen and T.Grance "Guidelines on Security and Privacy in Public Cloud Computing", NIST Draft Special Publication 800-144, 2011.

[12] N. Robinson, L. Valeri, J. Cave, T. Starkey, H. Graux,\ S. Creese and P. Hopkins, "The Cloud: Understanding the Security, Privacy and Trust Challenges", RAND Corporation, 2010.

[13] W. Tsai, X. Sun, J. Balasooriya, "Service-Oriented Cloud Computing Architecture", 7th IEEE International Conference on Information Technology, 2010. Vol. 3, NO. 6, July 2012 ISSN 2079-8407

[14] T. Dillon, C. Wu and E. Chang, "Cloud Computing: Issues and Challenges", 24th IEEE International Conference on Advanced Information Networking and Appications, 2010.

[15] Introduction to Cloud Computing, White Paper,Dialogic Corporation, 2010.

[16] Ramgovind S, Eloff MM and Smith E. "The Management of Security in Cloud Computing", Information Security for South Africa (ISSA), Sandton, Johannesburg, 2-4 Aug, 2010.

[17] V. Sarathy, P. Narayan, and R. Mikkilineni, "Next generation Cloud Computing Architecture", 2nd International IEEE Workshop On collaboration & Cloud Computing, 2010.

[18] P. Mell and T. Grance, "The NIST Definition of Cloud Computing" Recommendation of NIST, Special Publication 800-145, 2011.

[19] Z. Wang, "Security and Privacy Issues Within Cloud Computing", IEEE Int. conference on computational and information sciences, Chengdu, China, Oct. 2011.

[20] Andrew Joint and Edwin Baker, "Knowing the past to understand the present- issues in the contracting for cloud based services", Computer Law and Security Review 27, pp 407-415, 2011

[21] Vania Goncalves and Pieter Ballon, "Adding value to the network: Mobile operators' experiments with Software-as-a-Service and Patform-as-a-Service models", Telematics and Informatics 28, pp 12-21, 2011

[22] Dimitrios Zissis and Dimitrios Lekkas, "Addressing cloud computing security issues", Future Geberation Computer Systems 28, pp. 583-592, 2012.

[23] Rajnish Choubey, Rajshree Dubey and Joy Bhattacharjee, " A Survey on Cloud Computing Security, Callenges and Threats", International Journal on Computer Science and Engineering (IJCSE), vol. 3, No. 3, 2011.

[24] S. Subashini and V. Kavitha, " A survey on security issues in service delivery models of cloud computing", Journal of Networks and Computer Applications 34, pp. 1-11, 2011.

[25] Abdulaah Alshwaier, Ahmed Youssef and Ahmed Emam "A New Trend for E-Learning in KSA Using Educational Cloud", Advanced Computing: An International Journal (ACIJ), Academy & Industry Research Collaboration Center (AIRCC), 2012.

[26] Y. Chen, X. Li and F. Chen, "Overview and Analysis of Cloud Computing Research and Application", International Conference on E -Business and E - Government (ICEE), May 2011

[27] Ahmed Youssef and Manal Alageel "Security Issues in Cloud Computing", in the GSTF International Journal on Computing , Vol.1 No. 3, 2011.

[28]. Shiraz, M.; Gani, A.; Khokhar, R.H.; Buyya, R., "A Review on Distributed Application Processing Frameworks in Smart Mobile Devices for Mobile Cloud Computing," Communications Surveys & Tutorials, IEEE , vol.15, no.3.

[29]. Popa, D.; Cremene, M.; Borda, M.; Boudaoud, K., "A security framework for mobile cloud applications," Roedunet International Conference (RoEduNet), 2013

[30]. Qinyun Dai; Haijun Yang; Qinfeng Yao; Yaliang Chen, "An improved security service scheme in mobile cloud environment," Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference on , vol.01

[31]. Khan, A.R.; Othman, M.; Madani, S.A.; Khan, S.U., "A Survey of Mobile Cloud Computing Application Models," Communications Surveys & Tutorials, IEEE , vol.16, no.1

[32]. Huang Lin; Jun Shao; Chi Zhang; Yuguang Fang, "CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring," Information Forensics and Security, IEEE Transactions on, vol.8, no.6.

[33]. Fangming Liu; Peng Shu; Hai Jin; Linjie Ding; Jie Yu; Di Niu; Bo Li, "Gearing resource-poor mobile devices with powerful clouds: architectures, challenges, and applications," Wireless Communications, IEEE, vol.20, no.3, pp.14,22, June 2013

[34]. Dijiang Huang; Tianyi Xing; Huijun Wu, "Mobile cloud computing service models: a user-centric approach," Network, IEEE , vol.27, no.5, pp.6,11, September-October 2013

[35]. Lomotey, R.K.; Deters, R., "SaaS Authentication Middleware for Mobile Consumers of IaaS Cloud," Services (SERVICES), 2013 IEEE Ninth World Congress on , vol., no., pp.448,455, June 28 2013-July 3 2013 doi: 10.1109/SERVICES.2013.34

[36] GTSI Group, "Cloud Computing - Building a Framework for Successful Transition," White Paper, GTSI Corporation, 2009

[37] L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, ".A Break in the Clouds: Towards a Cloud Definition", ACM SIGCOMM Computer Communication Review, Volume 39 Issue 1, pages 50-55, January 2009.

[38] M. Boroujerdi and S. Nazem, "Cloud Computing: Changing Cogitation about Computing", World Academy of Science, Engineering and Technology, 2009