# Enabling DUI Systems in Handheld Devices Using Cloud

S. Gowri[1]
PGScholar/Department of CSE,
Angel College of Engineering and Technology, Tirupur.
gowri1666@gmail.com

T.Gnanaprakasam[2]
Assistant Professor/Dept. of CSE,
Angel College of Engineering and Technology, Tirupur.
gpatangel@gmail.com

T.Rajendran[3]
Professor/Dept.of CSE,
Angel College of Engineering and Technology,Tirupur.
rajendran_tm@yahoo.com

*Abstract*—: Application distribution among Mobile devices through cloud. Cloud computing support for energy saving, privacy, security, data protection, and fast exchange of data over the internet currently, application can't scale over multiple Cloud Computing Service Providers. Since there is no interoperability between Cloud Computing Service Providers due to device interoperability it's still in its infancy, that is one device produce a message or application can't be access by the other device. Currently, there's not a standard available for it. Android offers an open and equal alternative. Existing mobile development built on proprietary operating systems that restrict the third-party applications. Android application runs on different devices and different platforms. Files owned by one application are, by default, inaccessible by other applications. But we deploy the applications in the cloud, its raise the security issues of Data recovery vulnerability. The cloud characteristics of pooling and elasticity entail that resources allocated to one user will be reallocated to a different user at a later time. For memory or storage resources, it might therefore be possible to recover data written by a previous user. Ensuring the integrity of the data (transfer, storage, and retrieval) really means that it changes only in response to authorized transactions enable the cloud storage providers have excessive privileges to allow unauthorized access.

***Index Terms*— Cloud computing, Mobile Banking Application, Vulnerability, Security, Android.**

## I. Introduction

Cloud computing provides Resources as a service over the internet to provide infinite computing resources available on demand and resources are stored in a datacenter and distributed center that provide those services based on pay per usage. Data center is referred as hardware and software, which is pooled together, is what we will call a cloud[1]. Cloud computing support for energy saving, privacy, security, Content protection, and fast exchange of Content over the internet. Services themselves referred as Software as a Service (Sass).Some vendors use the terms (IaaS) Infrastructure as a Service and PaaS (Platform as a Service) to describe their products. Where the resources are accessible from anyone is called as a Public cloud. We use the expression private cloud to refer internal data centers of a business or other Bank, not available to the general public. The ability to pay for use of computing resources on a short-term basis as needed and release them as needed, thereby rewarding conservation by letting machines and storage go when they are no longer useful[2,3].

The ability to pay for use of computing resources on a short-term basis as needed (for example, processors by the hour and storage by the day) and release them as needed, thereby rewarding conservation by letting machines and storage go when they are no longer useful. In recent years, we have witnessed the strong growth of cloud computing, which refers to both applications delivered as services over the Internet in the datacenter that supports those services.

### *A. Mobile Cloud Computing*

Mobile cloud computing is the combination of mobile computing, mobile internet and cloud computing. Mobile computing technology [5] is to share resources and transport data of computers or other intelligent terminal equipments such as cell phones. The essence of mobile cloud computing is to provide valuable, precise and real time information to any clients at any time, at any place.

MCC as a new paradigm for mobile applications whereby the data processing and storage are moved from the mobile device to powerful and centralized computing platforms located in clouds. These centralized applications are then accessed over the wireless connection based on a thin native client or web browser on the mobile devices.

### B. Web services vs. Cloud

- Web Server Hosting is the service which has been provided and Cloud Computing is the technology which is in existence[6,8]

- Web Server basically consists of space which has been leased or purchased by the owner, whereas with cloud computing are used for applications (like email, word processing, spreadsheet, photo editing) that are located on a remote server somewhere[7].

## II.Mobile Applications with Security

### *A. Android-Development Platforms for Mobile Applications*

Content developers can work with audio, video, multimedia messaging, and Flash to create rich and compelling mobile content. Although the choice of development platform is largely market-driven, it also depends on the characteristics of available platforms and the requirements of particular applications. To illuminate the status and trends in current development platforms, we re- viewed and compared four popular mobile-application runtime environments with respect to various quantitative and qualitative criteria[4,5].

Android applications are primarily written in Java and compiled into Dalvik executable (DEX) format, a custom byte code. Each application executes on its own process, with its own instance of the Dalvik virtual machine.Dalvik runs DEX files, which are converted at compile time from standard class and JAR files. DEX files are more compact and efficient than class files.

- Developers have full access to all the frameworks and APIs that the core applications use and to Google-developed software libraries. Android's software architecture is designed to simplify component reuse. Any application can publish its capabilities, and any other application can then use those capabilities, subject to security constraints enforced by the framework. The Android software development kit (SDK) supports authoring applications with rich functionality. Compactibility: Android applications were easier to develop because of their improved compatibility with the full .NET and Java SE frameworks, respectively.
- Memory management: Automatic memory management handled by Dalvik's garbage collector, garbage collections might noticeably decrease performance.
- Runtime memory requirement: Minimum 32 Mbytes of RAM.
- Deployment speed (packaging, installing, testing) - Relatively fast.

### *B.Security Risks in Bank*

Some of the security risks faced by banks are

- Credit risk
- Market risk
- Interest risk
- Liquidity risk
- Operational risk
- Country risk
- Ownership / management risk

### *C.Types of operational risk events as having the potential to result in substantial losses for banks:*

**Internal fraud**. Intentional misreporting of positions, employee theft, and insider trading on an employee's own account.

- **External fraud**. robbery, forgery, cheque kiting, and damage from computer hacking.
- **Employment practices and workplace safety**. workers compensation claims, violation of employee health and safety rules, organized labour activities, discrimination claims, and general liability.
- **Clients, products and business practices**. Fiduciary breaches, misuse of confidential customer information, improper trading activities on the bank's account, money laundering, and sale of unauthorized products.
- **Damage to physical assets.** Terrorism, vandalism, earthquakes, fires and floods.
- **Business disruption and system failures**. Hardware and software failures, telecommunication problems, and utility outages.

## III. RELATED WORK

Cloud computing providers need to solve the common security challenges of traditional communication systems. At the same time, they also have to deal with other issues inherently introduced by the cloud computing paradigm itself. In this section, we have categorized the main cloud security issues as traditional and new cloud security challenges.

Homomorphic encryption [11] is a cryptography scheme where algebraic operations applied on the cipher text are directly reflected in the corresponding plaintext. Simply put, this allows a third party to compute the sum of two encrypted numbers, and when this encrypted result is returned to the user, it can be decrypted with the original key, and the result is the same as the sum of the two numbers in plaintext form. This allows multiple parties to cooperatively generate a piece of cipher text without knowing the plaintext that others work on.

Qiming Li et al.[12] Although a previous scheme based on homomorphic hash functions is applicable, it was mainly designed for server side coding only, and will be much less efficient when it is applied on random network coding. We propose a new on-the-fly verification scheme based on a faster homomorphic hash function, and proved its security. Described a homomorphism distributed verification scheme using Pseudorandom Data to verify the storage correctness of user data in cloud. This scheme achieves the guaranty of data availability, reliability and integrity. However, this scheme was also not providing complete protection to user data in cloud computing, since pseudorandom data would not cover the entire information.

Incremental encryption [15, 16] allows the computation of the final cipher text based on the initial cipher text and the change of the plaintext.

Rong et al. [17, 18] propose an incremental encryption scheme based on elliptic curve cryptography which is different than that presented by Bellare et al. The mechanism allows users to have trusted data storage and sharing over untrusted cloud storage providers. Being able to implement trusted services on untrusted cloud storage providers allows users to manage their data on any cloud storage provider, eliminating the required trust on the providers. The general idea is to encrypt the data before storing it in the cloud. On sharing the data, the encrypted data will be re-encrypted without being decrypted first. The rencrypted data will then be cryptographically accessible only to the authorized user with the corresponding token.

Ateniese et al. [14] proposed a secure distributed storage scheme based on proxy re-encryption. The data owner encrypts blocks of content with symmetric content keys. The content keys are all encrypted with a master public key. The data owner uses his master private key and user's public key to generate proxy re-encryption keys, using which the semi-trusted server can then convert the cipher text into plaintext for a specific user. The issue with this scheme is that collaboration between a malicious server and any single malicious user would expose decryption keys of all the encrypted data and compromise data security of the system.

## IV. PROPOSED WORK

### A. 3-WAY AUTHENTICATION FOR DATA SECURITY IN CLOUD

This paper is deals with creating an application using android. Mobile cloud computing is accessing the application in cloud through mobile. Banking is an art of striking a balance between Risk and Revenue. [Swiss Banking Corporation's Credit Manual].Fig. 1 represents the user name, password and mobile no to login the application defense against intruders on your computer, for very little time and effort. However, your data is only really as secure as your username and password. So, everyone can take steps to improve their password security.

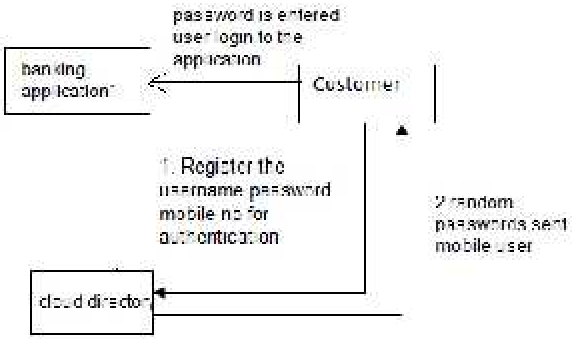


Fig. 1 Customer register in the cloud

It's generates the random password and sent to the mobile. Each time it's creating when the user login to application. Random passwords are valid for few seconds. After that it's invalid.

### B.Creation of application

While user wants to create the new account, the user wants to add the details like

Name
Bank name
Branch name
Address
Current balance
Remarks
IFSC (Indian Financial System Code)
MICR(Magnetic character ink Recognition)

Click the Add account button. Details are added to the Cloud. The Indian Financial System Code (IFSC) is an alphanumeric code that uniquely identifies a bank-branch participating in the two main electronic funds settlement systems in India.

In account transaction chooses the account holder and selects the transaction type, deposit or withdraw. Its shows the recent transaction of the details like account no, Transaction date, Transaction type, Transaction amount and remarks.everal other approaches also have been presented. Chow et al. [13] propose to extend control measures from the enterprise into the cloud through the use of Trusted Computing and applied cryptographic techniques.

### C.Classification of data

After classification of data, three entity is considered, first one is cloud provider itself, second is bank whose data resides at cloud and last one is user who request for access of cloud data.

Appling proposed formula the value of Criticality raring is calculated. Now allocation of data on the basis of Cr is done in three levels of location. This suggests that internal three levels of location is very critical and it require more security technique to ensure confidentiality. After classification of data in above step, three entity is considered, first one is cloud provider itself, second is Bank whose data resides at cloud and last one is employee or anonymous user who request for access of cloud data.

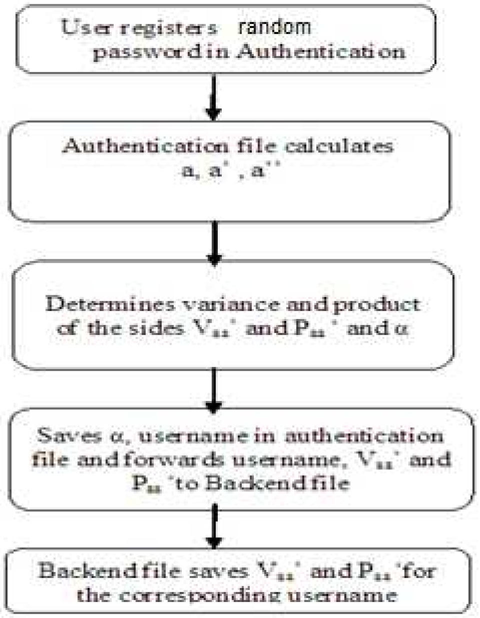

User registers random password in Authentication
Authentication file calculates a, a' , a''
Determines variance and product of the sides V_aa' and P_aa' and α
Saves α, username in authentication file and forwards username, V_aa' and P_aa' to Backend file
Backend file saves V_aa' and P_aa' for the corresponding username

Fig. 2 Trigonon based Encryption

```
Algorithm: Trigonon based Encryption
1. Input: Data, three levels of location, D[] array
of n integer size.
2. Output: categorized data for corresponding
        ring. For i 1 to n
        C [i] = Value of
        Confidentiality. I [i] = Value
        of Integrity.
A [i] =Value of Availability.
Calculate
            S [i] = (C[i] +
        (1/A[i])*10)/2 For j 1 to
                10
                    For k 1 to n
                IF S [K] = = 1||2||3 then
        R[k] =3 /* public access allotted to D[k]th
            data. IF S [K] = = 4||5||6 then
        R[k] =2 /* limited access allotted to D[k]th
            data. IF S [K] = = 8||9||10 then
        R[k] =1 /* private access allotted to D[k]th
                    data.
```

In above algorithm the first job of the user is to categories it on the basis of confidentiality, integrity and availability. After if a user is customer want to access the data if it belongs to limited access then user have to register itself (if he is already registered need not require further registration), if the data belongs to private it require strong authentication, if the data belongs to Public then it is public need not require any authentication. Now suppose the user registered itself for accessing data, Bank will provide username and password for authentication. At the same time Bank sends the username to cloud provider

D.*Steps for Trigonon based Encryption*

1. Split PW into 2 components – Authen & BE server
2. PW into its corresponding ASCII value.
3. Calculate the three-fourth of total digits of the ASCII value modulo 180, which results the first three digits of PAI.
4. Append the remaining one-fourth of the ASCII digits to PAI.
5. Vaa'=a-a'; Paa' = a * a'; α = 2P aa' − a„ ** 2
6. Pi is taken as the angle between the two the two sides of the trigon a and a' – PAI * 10 ** (n-2) (> 180) or PAI * 10 ** (n-3)
7. AI (i) = Pi / 2 – Authen server
8. AT(i) = αi + Vaa' * 2Paa„ from BE server
9. Verify Sin AI(i) = ( 1- ATi / 2 ) ½

It's generate authentication token.

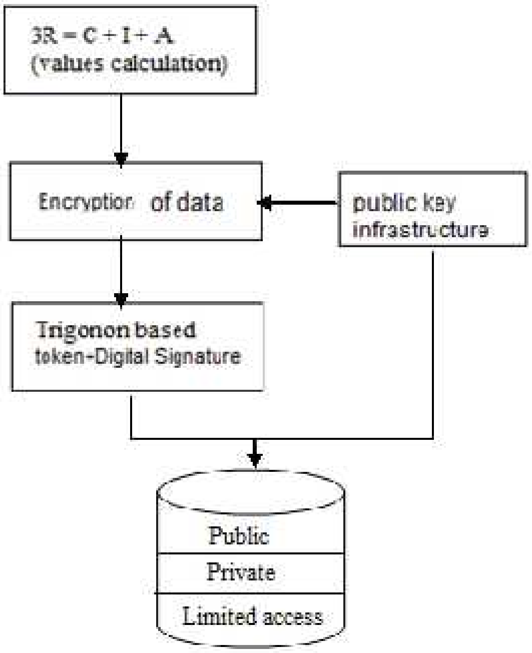


Fig. 3 Data stored in cloud

Fig. 3 represents PKI allows you to know that a given public key belongs to a given user PKI builds off of asymmetric encryption. . Each entity has two keys: public and private. The private key is known only to the entity The public key is given to the world encapsulated in a X.509 certificate[16]. Encryption of data is attached with the key value of public key infrastructure and it's goes into nextlevel encryption.

Digital Signature also ensures that no alterations are made to the data once the document has been digitally signed. A DSC is normally valid for 1 or 2 years, after which it can be renewed with trigonon based token. Based on that classification of data its stores in the cloud. While retrieving the data decryption will follow the same manner of encryption.

## V. Experimental Result

Android is a Open source software which it's used to support device Interoperability.Application results are shown in below.

**Fig. 4 Add Transaction**

Fig. 4 represents the transaction details.We accessing the application in mobile through cloud it's arises some security problems.

**Fig. 5 Recent Transaction**

While storing and retrievals of data from the cloud we apply Cryptographic encryption is certainly the best practice in worldwide, It's avoid the vulnerability and unauthorized acess of data is reduced using 3-Dimensional Encryption for data security in cloud.Fig. 5 represents the recent transaction details.

## VI. Conclusion

This paper also presented a proof of concept implementation of the cryptographic algorithms in a cloud computing environment for banking application.. Providing security in a distributed system requires more than user authentication with passwords or digital certificates and confidentiality in data transmission by using 3-way authentication for data security in cloud. We also intend to research and improve cloud computing security.

## References

[1] Weiguang SONG, Xiaolong SU Review of Mobile cloud computing

[2] http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031

[3] Zhang, Q., Cheng, L., Boutaba, R., Cloud Computing: state-of-the-art and research challenges, Journal of Internet Services and Applications, 2010, 1:7-18.

[4] http://www.onlinesbi.com/osbi_rtgs_faq.html

[5] www.scribd.com/doc/Risk-Management-for-Banking-Sector.

[6] T.Rajendran and P.Balasubramanie, "An Efficient Architecture for Agent-Based Dynamic Web Service Discovery with QOS", Journal of Theoretical and Applied Information Technology, Vol 15. No. 2, pp 86-95, May 2010.

[7] T.Rajendran and P.Balasubramanie, "An Optimal Broker-Based Architecture for Web Service Discovery with QoS Characteristics", International Journal of Web Services Practices, Vol. 5, No.1, pp. 32-40, July 2010.

[8] S.Gowri,T.Gnanaprakasam,A..NaveenKumar,M.Sasitharagai"Improved security system In Mobile Cloud Access Through Fuzzy Intrusion Detection Technique, International Journal of Internet Computing ISSN No: 2231 – 6965, VOL- 1, ISS- 4 2012.

[9] H. Takabi, J. Joshi, and G. Ahn. SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing Environments.

[10] <http://crypto.stanford.edu/craig/craig-thesis.pdf>

[11] Qimig Li, johnon the Security and Efficiency of Content Distribution via Network coding IEEE transactions on dependable and secure computing, vol. 9, no. 2, march/april 2012

[12] Chow R, Golle P, Jakobsson M, Shi E, Staddon J, Masuoka R. et al. Controlling data in the cloud: outsourcing computation without outsourcing control. CCSW 2009.

[13] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc.of NDSS'05, 2005. [retrieved 21.04.11].

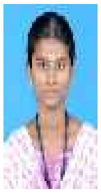
[14] Bellare Mihir, Goldreich Oded, Goldwasser Shafi. Incremental cryptography: the case of hashing and signing. In: Advances in cryptology –CRYPTO'94. Springer; 1994. p. 216–33.

[15] Bellare Mihir, Goldreich Oded, Goldwasser Shafi. Incremental cryptography and application to virus protection. In: Proceedings of the 27th annual ACM symposium on theory of computing. ACM; 1995. p. 45–56.

[16] Zhao Gansen, Rong Chunming, Li Jin, Zhang Feng, Tang Yong. Trusted data sharing over untrusted cloud storage providers. In: Proceedings of the 2nd IEEE international conference on cloud computing technology and science (CloudCom 2010); 2010.

[17] Rong Chunming, Zhao Gansen. Incremental encryption. Norwegian Patent No. P3683NO00-DT

## AUTHORS BIOGRAPHY



**Ms. S.Gowri** received B.E degree in Computer Science and Engineering from Anna University, Coimbatore and pursuing her M.E degree in Computer Science and Engineering from Anna University, Chennai. She has published 4 papers in National Conferences. Various Seminars, Workshops to enhance her knowledge. She is a life time member of IAENG.

**Mr. T. Gnanaprakasam** received M.E degree in Computer Science & Engineering from Anna University, Coimbatore. Now pursuing his Ph. D in Open Source Mobile Cloud Computing from Anna University, Chennai. He is the Open Source Club in charge of Angel College of Engineering and Technology. He attended more than 15 national and international level workshops. Also he has organized two national level conferences.

**Dr. T.Rajendran** completed his PhD degree in 2012 at Anna University, Chennai in the Department of Information and Communication Engineering. Now he is working as a Dean for Department of CSE & IT at Angel College of Engineering and Technology, Tirupur, Tamilnadu, India. His research interest includes Distributed Systems, Web Services, Network Security, SOA and Web Technology. He is a life member of ISTE & CSI. He has published more than 51 articles in International/ National Journals/Conferences. He has visited Dhurakij Pundit University in Thailand for presenting his research paper in International conference. He was honored with Best Professor Award 2012 by ASDF Global Awards 2012, Pondicherry.