ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 8, October 2012

A Perspective Approach on Mobile World Propelling Security for Entity Cloud

Bhavya Boggavarapu

Department of Computer Science and Engineering, K L University, Andhra Pradesh, India

Abstract—***The arena of cloud computing is still in its earlier state of growth as far as implementation and usage, partly because it is heavily promoted by technology advancements. Mobile Cloud Computing is the advancement done on the basis of involvement from basic cloud computing in which mobile device plays a key role for the ensuring of data storage. MCC clasps the potency to extinguish the requirements for coiffuring up of high-cost computing infrastructure for the solution and even by providing several operational facilities and services that the industries uses. MCC even stands ahead to provide multifarious security and privacy challenges. MCC access data from shared pool of entropy, thereby it increases the service providing interaction and removes risks associated with the society to reach all sorts of application goals. This paper concludes providing security tasks in dealing up with sharing of data with the accessible world linked up in MCC. This extensive survey paper aims to elaborate and analyze the numerous unresolved issues threatening the cloud computing adoption and diffusion affecting the various stake-holders linked to it by providing security mechanism by even ciphering the data through several implementation cryptic techniques.***

Index Terms *- **Mobile cloud computing(MCC), security issues, mobile services, Interoperability, Platform of mobile application for privacy.***

I. INTRODUCTION

Cloud Computing which is now focused as a hot topic in the present scenario of the enriching technological implementation applications is now excelling its way towards the greater world through the access of mobile devices as their main feature of implementation done to its storage, access, application aspects. MCC higher up the cloud computing by minimizing its backdrops and intruding as the work efficiency growth to excel into mobile environment – heterogeneity, scalability and availability, related to the performances like battery life, storage capacity and bandwidth and security-reliability, non-replication of entropy and privacy. In application, using MCC the user can access their resources virtually by means of using internet for lightweight portable devices and do not need to carry their entropy anywhere and also reduces the monetary value by sharing computing and increased storage resources, merged together with an on-demand provisioning. It also helps performing the operations facilitating the comforts of remote execution, which increases the process capacity, capability existing and new software increases. The advantageous tasks acquired on implementing this phenomena are – hardware percentage utility can be reduced and perfect low limit of cost can be maintained, provides accessibility around the globe, flexibility and the highly automated processes can be indulged efficiently to be put forth. The opportunities provided by cloud services available to enterprises of all levels that enable them to deliver more scalable and resilient services to employees, partners and customers at lower cost and with higher business agility for the sustain increment in the growth aspects. Through the application of mobile implementation in the cloud security of data aspect do not need a powerful configuration - CPU speed and memory capacity since all the data which are complex natured in computing modules can be processed in the clouds.

So, due to this efficient and effective usage through this implementation can be eventually higher up to a greater extent. On usage, there may be a change put forth as they become vulnerable to attacks and threats the internet has to offer. This may reduce capital expenses for some extent, somehow. But, a variety of information security risk for computing need to be concentrated upon as there are dealing under the risky environments. If the data is found to be sensitive in nature, then the risks associated to it may be high and vice versa. So,

in order to process the data, cloud provider has to be chosen and implemented to provide its own security services. In this paper, we discuss about the security and privacy issues that are needed to be deal for providing secure data surety. Thus,

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 8, October 2012

drawing and realizing the security risks the cloud environment has to offer. Even the access associated.

II. DEPLOYMENT FRAMEWORKS FOR MOBILE CLOUD APPLICATIONS

Irrespective of the services models of the cloud data, there exist four main ways through cloud services can be deployed depending upon the customer's requirements –

- Public Cloud
- Private Cloud
- Community Cloud
- Hybrid Cloud

A. *Public Cloud*

If the cloud infrastructure managed by the third party service provider, which is intern provided to numerous customers. Form this we can accomplish that, there exist many enterprises in lot more number can work on the infrastructure provided, at a same instance of time duration. Even if the wastages occurred at any sort of location, they can be checked as the user pays, for what we access.

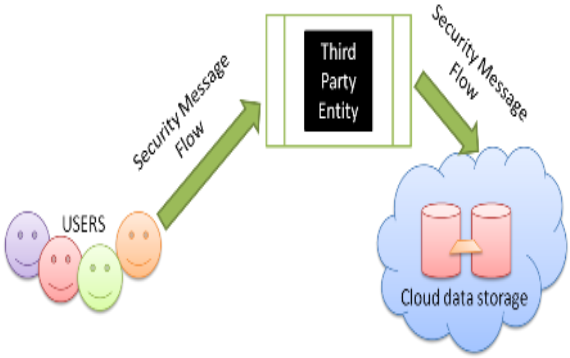

Figure 1. Public Cloud

B. *Private Cloud*

These are client dedicated and are built for the exclusive use of one client, providing the at most control over data, security and quality of service. Concept of virtualization can be implemented here.

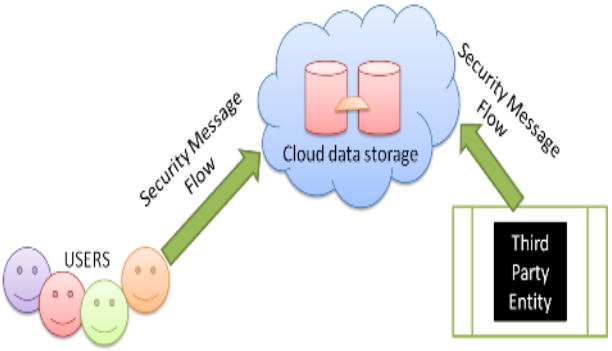

Figure 2. Private Cloud

C. *Community Cloud*

Infrastructure shared by several organizations for a shared cause and may be managed by them or a third part entity service provider. It involves a private cloud that is shared by several organizations and a need to store or process data of similar sensitivity.

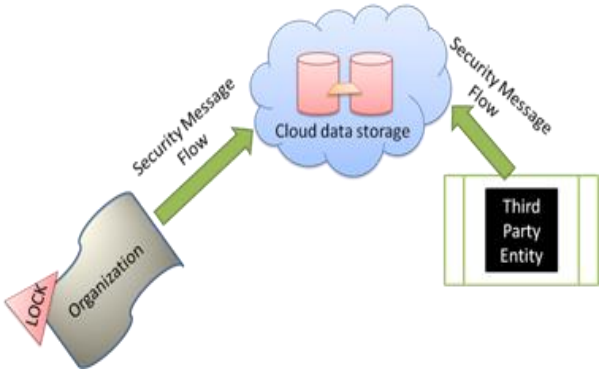

Figure 3. Community Cloud

D. *Hybrid Cloud*

These involve a relation of combining the public cloud and private cloud. This help in providing on-demand,

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 8, October 2012

externally provision scale. The comparison of two or more clouds deployable models linked in a way that data transfer takes between them without effecting each other.

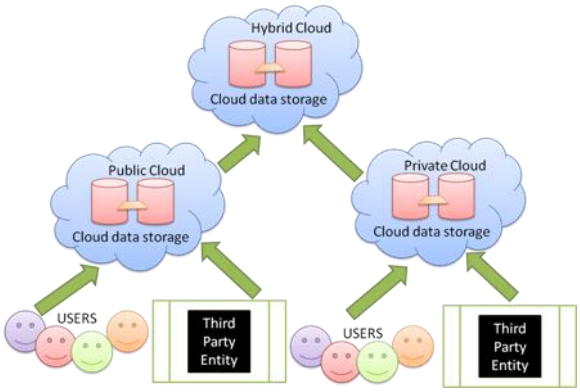

Figure 4. Hybrid Cloud

III. ROAD BLOCKS TO MOBILE CLOUD COMPUTING

The main issue of ensuring data through mobile cloud computing technology do have certain limitations and boundaries for proceeding transformational aspects on implementation of operations. Certain loopholes arose in the architecture have made computing vulnerable to various security and privacy threats. They are –

- Privacy and Security
- Performance
- Latency
- Reliability
- Probability and interoperability
- Data breach through fiber optic network
- Storage of data on internet networks

IV. ENSURING SECURITY FOR MOBILE CLOUD COMPUTING

As mobile cloud computing is the combination of mobile networks and cloud computing. The aspects which are related to security issues can be found in many types. All these types can be categorized based upon their efficiency, effectiveness and implementation criteria into two forms of their existence.

They are as follows -

- External Security with the user views of the mobile networks
- Internal Security as Cloud data Protection

A. *External Security with the user views of the mobile network*

I. Security for mobile applications

The merest ways to detect security threats will be installing and running security software and anti-virus programs on mobile devices. For the processing and power limitations, protecting constraints. These certain applications develop transferring threat detection and security mechanisms to the cloud. Before mobile users could use a certain apps, it should grow through some level of threat applications. All file activities to be sent to mobile devices will be verified if it is malicious or not. Therefore, instead of running anti-virus software or threat detection program locally, mobile devices only performs lightweight activities such as – Execution traces transmitted to cloud security servers.

II. Privacy

Providing private information like indicating your current location and users important information create scenarios for private issues. Threats for exposing private information could be minimized through selecting and analyzing the enterprise needs and require only specified services to be acquired and moved to the cloud.

III. Data Ownership

Another issues that arise from mobile cloud computing relates to the ownership of acquired digital media. Using the application of cloud computing methodology it becomes possible to store purchased media files such as –

- Audio
- Video
- E-books

remotely rather than locally. This can lead concerns regarding the true ownership of the data.

IV. Data Access and Security

Issues of access and security are significant to applications that rely on remote data storage and internet access in order to function.

V. DNS Attacks

A domain name server performs the translation of a domain name to an IP address. Since, the domain names are much easier to remember. Hence, DNS servers are needed. Domain Name System security extensions reduces the effects of DNS threats but still there are cases when these security measures prove to be inadequate when the path between a sender and a receiver gets rerouted through some evil connections.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 8, October 2012

VI. Sniffer Attacks

These sort of attacks are launched by applications that can capture packets flowing in a network. If the data that is being transferred through these packets is not encrypted, it can be viewed and there are chances that vital information flowing across the network can be traced and captured.

VII. HIJACKING

Prefix Hijacking is a type of network attack in which a wrong announcement related to the IP address associated with an autonomous system is made and hence malicious parties get access through the untraceable IP address.

B. *Internal Security as Cloud Data Protection*

i. Integrity

Every mobile cloud user must ensure the integrity of their information stored on the cloud. Every access that make must be authenticated and verified. This can be the access which on ensuring that it their own information and thus verifying its integrity.

ii. Authentication

Different authentication mechanisms have been presented and proposed using cloud computing to secure the data access suitable for mobile environments. Some uses the open standards and even support the integration of

various authentication methods like the use of access of login IDs, passwords or pins, authentication request etc….

iii. Digital Rights Management

Illegal distribution and privacy of digital contents such as –

- Video
- Audio
- Image

- E-book
- Programs

Become more and more popular. This can also be done by providing the encryption and decryption keys to access these contents. So, as to perform the above required criteria, A coding or decoding platform must be done before any mobile user can have access to such digital contents.

V. PROVIDING KEY SECURITY CONSTRAINTS

A. *Compliance and Risk Management*

Enterprises the shift to the cloud are responsible for compliance, risk and risk management.

B. *Service Integrity*

Cloud based services should be engineered and operated with security in mind. Operational processes should be integrated into organization's security management.

C. *Information Protection*

Cloud services require reliable process for protecting information before, during and after the transaction.

This can be achieved by providing the security by implementing the cryptic views to the data store.

D. *Security Concerns with the Hypervisor*

Various types of attacks can be launched by targeting different components of the hypervisor. Based on the various components in the hypervisor architecture behave, an advanced cloud protection system can be developed by monitoring the activities of the virtual machine and inter communication among the various infrastructure components.

E. *Cookie Poisoning*

It involves changing or modifying the contents of cookie to make unauthorized access to an application or to a webpage. Cookie basically contains the users identity related credentials and once the cookies are accessible, the content of these cookies can be forged to impersonate an authorized user.

VI. SECURITY MECHANISM

In the modern scenario it has been a routine for the usage of secure data by accessing them without proof. In order to overcome these problems we need to make the unsecure data hidden perfectly. This can be approached by applying cryptic methods. In mobile network, each peer for his user requirements needs to register with an identity in the system, thus obtains the secret key corresponding to his identity. Mobile users explore different types of encryption algorithms to encrypt the data which provides guarantee for the maintenance of data secrecy of the cloud service. Accordingly it generates cipher text as its next step which can be transformed to another person who can decrypt the

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 8, October 2012

data determining particular required destination. Let the considered data, D is divided into n-blocks, where

$$D = (d1, d2, d3, d4, \ldots\ldots dn)$$

For each entity of D, considered d_i, data owner encrypts the data under his selected secret key. At the same time data owner should generate enciphering key to the authorized user on the destination side. The size of enciphering is as same as that off. The d_i selected. Now, on using this key, the destination side authorized person can get back his data without loss in the secure format.

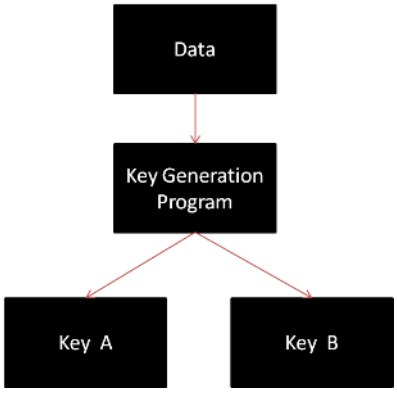

Fig. 5. Security Mechanism

The method should be in such a way that the selected entity of the data or the entire data when subjected for encryption using the secret key, there should obtain a cipher text, on enciphering it by the authorized user on the destination side can collect his data.

Launching:

Select key for message or required data as 'k'

$$D = (d1, d2, d3, \ldots\ldots , dn)$$

Secret key for user A : (A, parameters, k)

$$k_A = D(A)^k$$

VII. ENCRYPTION METHOD

The data, D is divided into n number of fragments, therefore

$$D = (d1, d2, d3, \ldots\ldots , dn)$$

For, di is subjected for encryption algorithm, which generates –

$$D' = E_k(D_i) \;;\; \text{for } 1<= i<=n$$

⇨ D' = (d1, d2, d3, d4, …… , dn)' to the cloud
⇨ $D' = E_k(d_1)\, E_k(d_2)\, E_k(d_3) \ldots\ldots\ldots\ldots E_k(d_n)$

Algorithm:

```
Encryption(parameters, A, d)
{
 // To encrypt data under user A, as public key

        D' = Ek (D(A))^k ;
}
```

Key for user B :

```
KeyB(parameters, kA, A, B)
{
      kA -> B = ( D(A)^k, D(B)^k ) ;

 }
```

VIII. DECRYPTION METHOD

The ciphered data now can be enciphered backed using its corresponding enciphered key.

$$D_k(D') = D_k(E_k(Di))$$

⇨ $D_k(D') = D_k(d1, d2, d3, \ldots\ldots , dn)'$
⇨ $= D_k(d1', d2', d3', \ldots\ldots\ldots , dn')$
⇨ $= D_k(E_k (d1, d2, d3, \ldots\ldots\ldots.., dn)$
⇨ $= D_k(E_k(d1), E_k(d2), E_k(d3), \ldots\ldots.. , E_k(dn))$
⇨ $= D_k(E_k(d1))\, D_k(E_k(d2))\, D_k(E_k(d3)) \ldots\ldots\ldots$
$\ldots\ldots\ldots\ldots\ldots.. D_k(E_k(dn))$
⇨ d1 d2 d3 d4 …… Dn
⇨ D_i ; $1< = i < = n$.

Enciphering:

```
Enciphering(parameters, kA -> B, CA)
{
 // To re – encrypt the data we need to generate the re-ciphering key by the user B, to apply it on as a private key generation
  CB = ( C1, C2, C3, …….. Cn ) ;
}
```

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 8, October 2012

Decryption:

```
Decryption(C1, C2, C3, ……,Cn)
{
 // We obtain d by computing

    d = C_{n-k}/ (E_k(D_i)) ;     }
```

D = (d1, d2, d3, …… ,dn) is obtained.

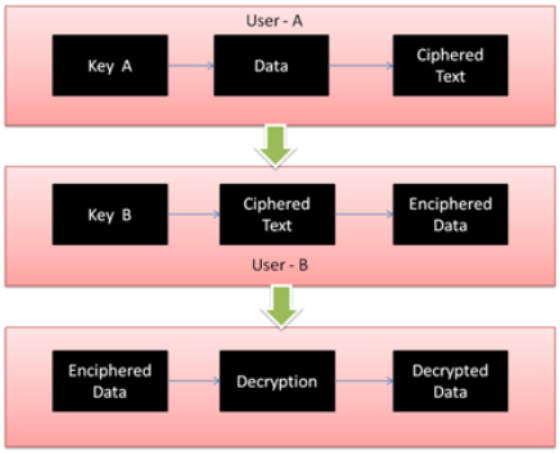

Figure 6. Decryption Method

IX. METHODOLOGY FOR ERROR RECOVERY BY VERIFICATION TECHNIQUE

```
public static String encrypt(String str)
    {
        byte b[] = new byte[str.length()];
        byte result[] = new byte[str.length()];
//          byte mod[] = new byte[str.length()];
        b=str.getBytes();
      for(int i=0;i<str.length();i++)
        {
          result[i] = (byte) ((byte) b[i] -(byte) 4);


 //   mod[i]=(byte) ((byte) b[i] % (byte) 4);

        System.out.println(b[i]+"-"+result[i]);
        }

    return ( new String(result) );
    }

public static String decrypt(String str)
    {
    byte b[] = new byte[str.length()];

    byte result[] = new byte[str.length()];

    b=str.getBytes();
    for(int i=0;i<str.length();i++)
        {
        result[i] = (byte) ((byte) b[i]+(byte) 4);
        System.out.println(b[i]+"-"+result[i]);
     }

    return ( new String(result) );

    }
```

X. CONCLUSION

Cloud computing as a transformative technology holds a considerable promise that can change the very nature of computing specifically to business enterprises. Building applications on on-demand infrastructures instead of building applications on fixed and rigid infrastructures was provided by cloud computing providers. By simply tapping into the cloud, enterprises can gain fast access to business applications or infrastructure resources with reduced Capital Expenditure (CAPEX). Mobile cloud computing provides an optimal services for mobile users as one of the mobile technology trends in the future since it combines the advantages of both mobile computing and cloud computing. This paper have discussed security considerations concerning mobile cloud computing. Securing mobile cloud computing user's privacy and integrity of data or applications are the key issues that most cloud providers must have given considerations. The mobile cloud computing is a combination of mobile networks and cloud computing, the security related issues are then divided into two categories: mobile network user's security; and mobile cloud security.

REFERENCES

[1] H. Liang, D. Huang, L. X. Cai, X. Shen and D. Peng, "Resource allocation for security services in mobile cloud computing," in Proc. IEEE INFOCOM'11, Machine-to-Machine Communications and Networking (M2MCN), pp. 191-195, April 10-15, 2011, Shanghai, China.

[2] Ruiping Lua and Kin Choong Yow, "Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network," IEEE Network, vol. 25, no. 4, pp. 28-33, July-August, 2011.

[3] Gaoyun Chen, Jun Lu and Jian Huang, Zexu Wu, "SaaAS - The Mobile Agent based Service for Cloud Computing in Internet Environment," Sixth International Conference on Natural Computation, ICNC 2010, pp. 2935-2939, IEEE, Yantai, Shandong, China, 2010. ISBN: 978-1-4244-5958-2.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 8, October 2012

[4] Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks," ICPPW '10 Proceedings of the 2010 39th International

Conference on Parallel Processing Workshops, IEEE Computer Society, pp. 280-284, Washington DC, USA, 2010. ISBN: 978-0-7695-4157-0.

[5] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing," Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

[6] NEC Company, Ltd. and Information and Privacy Commissioner, Ontario, Canada. "Modelling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach, (2010), http://www.ipc.on.ca/images/Resources/pbd-NEC-cloud.pdf.

Biography

Ms. Bhavya Boggavarapu currently studying in the Department Of Computer Science and Engineering, K L University. She currently secured the top rank and stud as the topper of the Department of CSE with a grading point of 9.7 for 10 in the current semester. She has received two Gold Medals for the position of AIR-162 in National Science Olympiad (NSO) in 2007 and in National Interactive Maths Olympiad (NIMO). She has also got selected in AMTI – Association Of Math Teachers Of India. She has published paper in National Conference. She has done a Summer Internship in the name of Summer Student Program 2012 held at Indian Institute of Science, Education and Research (IISER)Pune, Maharastra in the area of Mathematics which can be applied in Cryptography, topic of Computer Networks. She became Microsoft Technology Associate in 2012 in the area of .Net as a Qualified Professional. She has exhibited her project titled- " Encryption and Decryption through Message Flasher in IEEE national level project expo 2012.