# A Survey on Security of Android devices over Cloud

Pankajkumar S Thakre, Dr.Vaishali M. Deshmukh

**Abstract**— The growth of mobile phone users increasing in millions, as per as the user data and storage demands increases rapidly, the future of cloud need more attention to manage all the layers like network, service and whole infrastructure. The one of the important area where cloud need to focus is the security in all the layers. In this paper we have reviewed various issues related to security of data for mobile in cloud also discussed the various work ethics done for cloud to enhance the security.

**Index Terms:** Cloud; Security; Android

## 1 INTRODUCTION

The growing field of cloud computing supply mobile users the ability to store data in the cloud Such as google Drive, Drop box etc. By using this application user can uploads their data and download their data from the cloud at any time. It simplifies the limited storage capacity problem of the user. As cloud storage facilitates the user but also increase certain risk to the security of their data because user have to surrender the full control of their data. Most of the user uses mobile device which uses android application. Each data transferred using these types of apps which leads to solve the issue area of cloud Security in android. In reality cloud may not guarantee's the data security and confidentiality of user private data. Generally, there are two ways to guarantee user not to be destroyed: one is to encrypt user data by some popular algorithm or standards in the user mobile terminal, the another way is to provide the safety of the storage devices in the cloud by all kinds of security mechanisms such as firewalls, virtual private networks , intrusion detection system and other security policies and technical ways . But user trust himself only rather than service provider hence by encrypting the data before uploading in the cloud provides the security of data.

## 2 LITERATURE SURVEY

### 2.1 Cloud computing

Cloud computing [1]-[2] is a model generally defined asthe clusters of scalable and virtualized resources likedistributed computers, storage, and system software etc. which makes use of internet to provide on demandservices to the user. Cloud Computing refers to both the applicationsdelivered as services over the Internet and thehardware and systems software in the datacenters thatprovide those services (Software as a Service - SaaS).The datacenter hardware and software is what we willcall a Cloud. When a Cloud is made available in a payas-you-go manner to the public, we call it a PublicCloud; the service being sold is utility Computing.

Cloud computing [4]-[5], indeed, is a wide-ranging term that transmits hosted services over the Internet. These hosted services are generally separated into three broad categories:

1) *Infrastructure as a Service (IaaS)*
Also referred as Resource Clouds generally provide resources which are managed and can easily be scaled up, as services to a variety of users. They essentially supply superior virtualization capabilities. Consequently, diverse resources may be offered via a service line: Data and storage clouds have to offer a dependable access to data of a potentially large size

2) *Platform as a Service (PaaS)*
It supplies computational resources via a platform upon which applications and services can be urbanized and hosted. In other way, it supplies all the needed resources to build an application and service via the internet, without downloading or installing it.

3) *Software as a Service (SaaS)*
It is also referred to as Application or a Service Clouds. SaaS is the model which hosts the application as a service to its various cloud users via internet. The user utilizes the software.

According to [6]-[7] the network architecture of cloud consist of user, Cloud service provider (CPA) and third party auditor (TPA).The users store his data to cloud storage servers through the use of cloud service provider. User need to get assure about storage of data .In case that users do not necessarily have the time, feasibility or resources to monitor their data, they can delegate the tasks to an optional trusted TPA of their respective choices out of the box without any integration or patching up with any infrastructure.

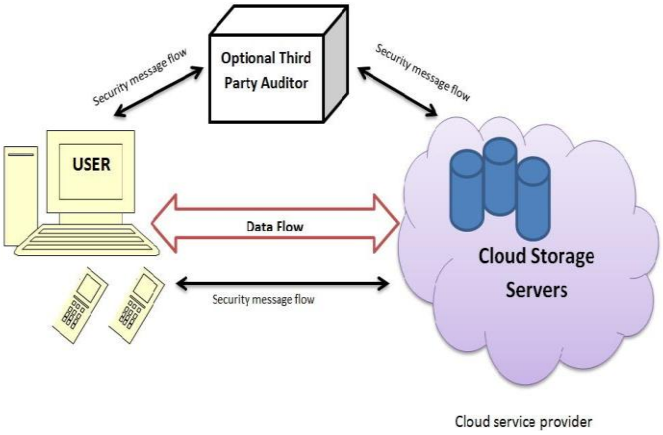

Figure 1.Network Architecture of Cloud

## 2.2. Security Issues

The issues related to Cloud with advantages and disadvantagesare [2]-[3];

1) *Private Cloud*

- Most control over data and platform
- Latent for multi-tenancy of business units to cause fulfilment and defense risk
- May not have convulsive abilities when added performance or capacity is required.

2) *Public Cloud*

- Likely for better cost savings if infrastructure owned and controlled by public providers
- Failure of control and data loss.
- Possible for multi-tenancy with former organizations to reason security risk
- Third party safety controls possibly not clear and may cause unidentified risks.

3) *Hybrid Cloud*

- Potential for difficulty to cause unfamiliar vulnerabilities and indefinite risks.

Also there are many security challenges [4]-[5] with respect to service models SaaS, PaaS and IaaS like backup and storage, dataleakage, maliciousattack. Apart from service cloud framework establishes the network which leads to security issues to solve like browser security, SQL injection, flooding attack, locks in etc.

Also the study of authors Cong Wang, WenjingLou [8] and framework represented by Xiao Zhang and Lei-jieZeng [9] shows that the cost of maintaining a data center is increasing rapidly, especially for the medium data center. An economic choice is to use cloud computing and cloud storage instead of manage data center by itself. Small companies buy compute and storage service just like water and electronic. The difficulty is how to ensure their data safe in cloud storage. Cloud storage provider claims that they can protect the data, but no one believes them. The decentralized data storage by cloud is a big problem as the data of user placed in different places to get the backup mechanism succeed. But in real world if the data placed in number of centers then it increases the risk of data stolen.

## 2.3. Various Mobile data security technics for Cloud

1) *Adaptive and dynamic data encryption method*

There are various technics available and the work is going on to enhance the security issues concerned with cloud data and mobile transmitted data, according to authors CAO Wanpeng and BI Wei2[10] works on adaptive and dynamic data encryption method to encrypt user data in the mobile phone before it is uploaded. In this method for each encryption by user mobile device the algorithm is adaptively and dynamically selected from the algorithm set which is already added in advance in the mobile phone encryption system. The method uses mobile phone hardware information and key selection module responsible to make a dynamic encryption key for data in mobile. And further the modules responsible for dynamically and adaptively selecting the encryption algorithm from set of new high-performance encryption algorithm and generating the encryption key based on the output from the mobile phone hardware information and user personalization information collection module and the input pseudo-random number.

2) *Modern Encryption Standard (MES-I) version-I*

According to authors Somdip Dey and Asoke Nath[11]in present world we need a high security for transmitting any digital information from client to another client. Hence the Authors proposes the new cryptographic method called as Modern Encryption Standard (MES-I) version-I. It is the amalgamation of two different algorithms developed by Nath et al. namely TTJSA and DJSA [14] in randomized fashion. The method is achieved by splitting the file which is to be encrypted and encrypting the split sections of the file in various ways using TTJSA and DJSA cipher methods. Further according to author there are two types of cryptography one is symmetric key and other is public key. And author proposes the symmetric key cryptography which is combination of above given methods. HereTTJSA [13] method is a combination of three distinct, methods namely Generalized modified vernam cipher, MSA and NJJSA [13].This first method requires text key with randomized number as input.

Table1.
Comparison of execution time(in sec)

| *File size* | *TTSA* | *DJSA* | *MES-I* |
|---|---|---|---|
| *1024 bytes* | 1 | 2 | 4 |
| *2048 bytes* | 2 | 2 | 6 |
| *4096 bytes* | 2 | 3 | 6 |

3) *Modern Encryption Standard (MES-II) version-II*

In the new proposed technic [12] Rahul sircar,Gunjansekhon and Asoke Nath strengthened previous MES-I[11] algorithm by using Modified generalized vernam cipher method with feedback called as MES-II[12] with different block size from left to right and after that entire content is divided into two files and then combine them by taking 2nd half first and the 1st block. The generalized modified vernam cipher method again applied from left to right with different block sizes.Here authors have modified the method using variable block size and variable key. After completion of encryption in forward direction then the entire file is divided in two parts and the two parts interchanged and again applied the modified vernam cipher method with feedback and new key.Author tested the given method, the result shows that the method is free from standard cryptography attack such as known plain text attack, brute force attack and differential attack.

4) *Location-Dependent Data Encryption*

According to [15]-[16],author proposed a technic called Location-Dependent Data Encryption in which the mobile client transmits a target latitude/longitude coordinate for dataencryption to information server. Then, the serverencrypts the message and sends the ciphertext back tothe mobile client. The client can only decrypt theciphertext when the coordinate acquired form GPSreceiver matches with the target coordinate. The above technic uses TD(Tolerance Distance) to make accurate coordinate matching because there is no guarantee that the target coordinate matches every time.

5) *Self-Encryption scheme*

Statistics [18]-[19] shows that 22% of PDA owners have lost their devices, and 81% of those lost devices had no protection. Even worse, 37% of PDAs have sensitive information on them, such as bank account information, corporate data, passwords, and more. For this reason, some companies do not allow employees to use PDAs or similar mobile devices to store company data hence there is need ofeffective protection of device sensitive data even if it is stolen or losses.Hence the author proposes a Self-Encryption scheme [18] for mobile data security.In this scheme the sensitivedata is broken into two parts using our self-encryptionstream cipher scheme. The major part (Part A: ciphertext) isstored in the mobile device carried by the companyemployee, and the minor part (Part B: keystream + otherparameters) is protected in the secure server of thecompany.Part A is encrypted using part B.When the userneeds to access the data; he or she has to input a correct PINto pass the authentication procedure. Then the server willsend part B to decrypt part A and merge them together torecover the original plaintext. When a mobile device is lost, at most the adversary can access the part A, from which it iscomputationally infeasible to get meaningful information.

6) *Multiservice authorization over Mobile Cloud*

Mr. Falesh M. Shelke, Prof. Pravin D. Soni[20] proposed the enhanced work on authentication strategy for Multiservice authorization overMobile Cloud in which both the user and the server verify each other's identity by means of token. First the registered user will request to Authentication server by logging in, after this user will get token, then the user will request for the service to server. It sends same ticket to the Service Server for accessing the service, service Server will check this ticket and grant the service if it matches.

7) *Homomorphic encryption*

According to [21] the top 74% challenges in cloud computing is security. There are many security issues in mobile cloud computing like data ownership, privacy, data security and data segregation. Author proposes a scheme called Homomorphism which is an encryption schemes which allow computing with encrypted value without decrypting them. Because the data in a homomorphic encryption scheme retains the same structure, identical mathematical operations whether they are performed on encrypted or decrypted data will yield equivalent results.

8) *Attribute-based encryption mechanism*

According to authors Sebastian Zi ckau,Felix Beierle and Iwailo Denisow[22] recent headlines shows that the access to private information is often not sufficiently secured on the service level. Hence author presented a prototype which aims to use attribute-based meta-information to secure data on the level of files without relying on additional functionality of third-party services. A mobile device app is used to access and alter the Meta information. Attribute-based encryption mechanisms secure the private data and define access policies for friends and other users simultaneously. The author work on the attributes like ABE information, general Meta information, application-specific Meta information, access history and file content. The system shows the client is an Android device which provides functionality of Master key, private key and also encryption and decryption. Also as per performance evaluation the system works on mobile devices very well but not on Laptop or PC.The system can be accessed by anonymous user or authorized user but only authorized user can generate his own private key from Master key in his/her device.

### 2.4. Android devices and security

M Tiwari and N Gupta [23] reviewed that Android has the biggest market share among all Smartphone operating system. Android is a Google operating system for mobile platforms with the basic functionality of system utilities, middleware in form of Virtual Machine (VM) and some core application like browser, dialer, calculator and some others as well. The large number of applications is available for user. But the user need trust full applications, which do not harm their privacy and security issues, so it is mandatory for every application to ask for permissions from the user during the time of installation. User has only two choices, either to grant all the required permissions and the application will be installed. And once the permissions are granted, Android does not provide any facility to revoke those permissions, unless the user uninstalls the application.

1) *Android Inter Component Communication* [27]

- **Activity:** Provides GUI for interaction of user with the application. Depends upon design, an application may consists of one or more activities,
- **Service:** It is a background process that fetches data from the network,
- **Broadcast receiver:** Receives broadcast announcements and response to them according to the situation.
- **Content provider:** is a SQLite database, which supports the sharing and accessing of data among applications.

2) *Automatic backup and restore of data*

With respect to author P Nayadkar[24]-[25], there is need to make secured backup and restore of data on Android devices as every person uses it.Here author proposes the system which provide automatic backup and restore of data from mobile online using AES 128 algorithm which is suited at the transmission level. The encrypted file is generated after backup. The system provides online backup and privacy of data in scheduled basis like daily, weekly or monthly. The system developed using Java eclipse and supports backup of bookmarks, contacts, call log, phonebook, SMS, images, videosetc. The author talks about various types of backup technics like Full backup, Incremental backup, Online backup and offline backup etc. Also as per survey by author it is easy to back up our contacts to Google account with Android phone.

3) *Four issues are in Android* [28]

- User must grant all permissions to install any application.
- No way for restricting the granted permissions to an application.
- As all permissions are based on install time checks, access to resources cannot be restricted based on dynamic constraints.
- Hence the only way of revoking permissions are to uninstall the application.

4) *Android has two basic methods of security enforcement* [26]

Firstly, applications run as Linux processes with their own user IDs and thus are separated from each other. This way, vulnerability in one application does not affect other applications. Since Android provides IPC mechanisms, which need to be secured, a second enforcement mechanism comes into play. Android implements a reference monitor to mediate access to application components based on permission. If an application tries to access another component, the end user must grant the appropriate permissions at installation time. Hence the Android provides more security than other mobile phone platforms. Different levels of data security for different users. It does also embody the concept of cloud computing on-demand services.

## 3 Conclusion

Cloud storage increases rapidly and future is to face the challenge of security of information over cloud. Hence we need to focus on the data of devices when it goes to cloud so that we can have the control on it.Android devices provides all security features, also millions of peoples using it.Hence we need work on security of data when android device comes to contact with cloud by means of transmission of data on it.

## References

[1] John Viega, "Cloud Computing and the Common Man", Computer, vol.42,no.8,pp. 106-108, August 2009, doi:10.1109/MC.2009.252.

[2] ENISA: Cloud Computing: Benefits, Risks and Recommendations for Information Security. Tech Rep., European Network and Information Security Agency[EB/OL]. [2009-11-20]. http:// enisa.europa.eu.

[3] Molnard D, Schechter S. Self-Hosting vs. Cloud Hosting: Accounting for the Security Impact of Hosting in the Cloud[C]// Proceedings of Workshop on the Economics of Information Security (WEIS 2010): June 7-8, 2010.Harvard University, MA, USA, 2010.

[4] Ms. Disha H. Parekh, Dr. R. Sridaran , "An Analysis of Security Challenges in Cloud Computing"(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No.1, 2013

[5] Subashini, and V. Kavitha. "A survey on security issues in service delivery models of cloud computing."Journal of Network and Computer Applications 34.1 (2011): 1-11.

[6] CSA: Cloud Security Guide. Tech. Rep., Cloud Security Alliance[EB/OL].[2009-04].http://www.cloudsecurityalliance.org/csaguide.pdf.

[7] Reddy, A. Rama Mohan. "Data Security in Cloud based on Trusted Computing Environment."

[8] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou "Ensuring Data Storage Security in Cloud Computing",978-1-4244-3876-1/09/$25.00 ©2009 IEEE

[9] Xiao Zhang, Hong-tao Du ,Jian-quan Chen, Yi Lin, Lei-jie Zeng," Ensure Data Security in Cloud Storage"2011 International Conference on Network Computing and Information Security

[10] CAO Wanpeng1, BI Wei2, "Adaptive and Dynamic Mobile Phone Data Encryption Method", Communications, China (Volume:11 , Issue: 1 ),IEEE, May 2014.

[11] "Modern Encryption Standard (MES) Version-I: An Advanced Cryptographic Method", Somdip Dey, Asoke Nath, Proceedings of IEEE 2nd World Congress on Information and Communication Technologies (WICT- 2012), pp. 242-247.

[12] Gunjan Sekhon,Asoke Nath, "Modern Encryption Standard (MES) Version-II", Proceedings of IEEE International Conference on Communication Systems and Network Technologies,April 2013.

[13] Symmetric key Cryptosystem using combined Cryptographic algorithms - Generalized modified Vernam Cipher method, MSA method and NJJSAA method: TTJSA algorithm, proceeding of information and Communication Technologies(WICT),2011 held at Mumbai Dec 2011,Pages:1175-1180.

[14] Advanced Symmetric key Cryptography using extended MSA method: DJSSA symmetric key algorithm: , Jounal of Computing, Vol 3, issue-2, Page 66-71,Feb(2011).

[15] LIAO H C, LEE P C, CHAO Y H, et al. A Location-Dependent Data Encryption Approach for Enhancing Mobile Information System Security[C]// Proceedings of the 9th International Conference on Advanced Communication Technology:February 12-14, 2007. Gangwon-Do,Korea, 2007: 625-628.

[16] LIAO H C, CHAO Y. H. A New Data Encryption Algorithm Based on the Location of Mobile Users[J]. Information Technology Journal, 2008, 7(1): 63-69.

[17] BAO Haiyong, WEI Guiyi, SHAO Jun, et al. Efficient Signature-Encryption Scheme for Mobile Computation[C]// Proceedings of 2011 International Conference on System Science and Engineering (ICSSE): June 8-10, 2011. Macao, China, 2011: 390-393.

[18] Yu Chen and Wei-Shinn Ku "Self-Encryption Scheme for Data Security in Mobile Devices" Manuscript submitted, Oct. 2, 2008 to CCNC'09, Las Vegas, NV,USA, Jan. 10 – 13, 2009.

[19] GASTI P, CHEN Yu. Breaking and Fixing the Self Encryption Scheme for Data Security in Mobile Devices[C]// Proceedings of 2010 18th Euromicro Conference on Parallel, Distributed and Network-Based Processing (PDP): February 17-19, 2010. Pisa, Italy, 2010: 624-630

[20] Mr. Falesh M. Shelke , Prof. Pravin D. Soni ,"An Enhanced Authentication Strategy for Multiservice Authorization over Mobile Cloud" International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 3 Issue:3

[21]"Homomorphic Encryption in Mobile Multi Cloud Computing" by Maya Louk and Hyotaek Lim 978-1-4799-8342-1/15/$31.00 ©2015 IEEE.

[22] Sebastian Zickau, Felix Beierle, and Iwailo Denisow ,"Securing Mobile Cloud Data with Personalized Attribute-based Meta Information" 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering 2015

[23] "Review on Android and Smartphone Security", Tiwari Mohini, Srivastava Ashish Kumar and Gupta Nitesh NRI Institute of Information Science and Technology, Bhopal,Madhya Pradesh, INDIA, Received 25th October 2013, revised 4th November 2013, accepted 19th November 2013

[24]Pratap P.Nayadkar, Balu L.Parne. "A Survey on Different Backup and Restore Techniques Used in Mobile Devices" IJCSIT issue 6,vol 5,issn:0975-9646.

[25] Pratap P.Nayadkar ,"Automatic and Secured Backup and Restore Technique in Android",IEEE International Conference on Innovations in Information Embedded and Communication Systems (ICIIECS'15),March 2015

[26] Kaur S. and Kaur M., Review Paper on Implementing Security on Android Application, Journal of Environmental Sciences, Computer Science and Engineering & Technology, 2(3), (2013)

[27] Powar S.,Meshram B. B., Survey on Android Security Framework, International Journal of Engineering Research and Applications, 3(2), (2013)

[28] Bing H., Analysis and Research of Systems Security Based on Android, Intelligent Computation Technology and Automation, 581–584 (2012)

[29] Tim Mather,Subra Kumarasawmy,Shahed Latif,"Cloud Security and Privacy",Mike Loukides,Ed.,America,O'Reilly,2011

[30] http://www.salesforce.com/eu/cloudcomputing/#what