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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

Adapting Efficient Software Requirement Engineering model to implement AES Algorithm for Mobile Cloud Computing

Manjunath A E[1], Pavithra H[2], Swarnalatha K. S[3], Sharadhadevi S K[4]

Assistant Professor, Department of Computer Science and Engineering, RVCE, Bangalore, India [1]

Assistant Professor, Department of Computer Science and Engineering, RVCE, Bangalore, India [2]

Assistant Professor, Department of Computer Science and Engineering, RVCE, Bangalore, India [3]

Assistant Professor, Department of Computer Science and Engineering, RVCE, Bangalore, India [4]

Abstract: Mobile cloud computing provides network access to a shared group of computing resources like services, storage applications, network and servers on demand basis as and when required. In mobile cloud computing, mobile devices can depend on cloud computing and information storage resources to perform computationally intensive operations such as multimedia processing and searching. In spite of the hype achieved by the mobile cloud computing the growth of the cloud computing subscribers is still below expectations due to risks associated with the security and privacy. The mobile user's private data and sensed information must be processed and stored in a secure manner in order to protect user's privacy in the cloud. In traditional approaches where user's data is stored in single big data base and same unique encryption keys are used to secure each mobile user's data. Traditional approaches have several following drawbacks; first in terms of scalability it is not scalable when the database is large. Secondly data encrypting keys for mobile users are maintained in a centralized location which leads to single point of failure. In this framework, cryptographic keys are maintained by cloud service providers.

Keywords: Attribute-Based Encryption, Advanced Encryption Standard, cryptographic keys, Extended shadow images

I. INTRODUCTION

Cloud computing can be defined as the trend in which resources are provided to a local client on demand basis, usually by means of the internet connection. One of the main advantages of cloud computing is reducing and wasted expenditure for computer equipments and servers. Cloud computing can be termed as model of information processing, storage, delivery in which clients can request cloud computing resources as when they required [1].To set up infrastructure organizations need physical devices, services, storage or any networking equipments instead of purchasing above mentioned resources clients can request these resources from cloud service providers as outsourced resources [2] [3] on demand basis. Mobile devices have some significant constraints like resource constraint mobile devices, ubiquitous wireless infrastructure, longer battery life, less storage capability. Cloud computing provides a ground for a new computing rule called Mobile Cloud Computing (MCC) [4]. The mobile devices battery powered have limited processing power, low storage, The limitations of mobile devices mentioned above are obstacles for computationally intensive and storage demanding applications on a mobile. Computationally intensive and storage demanding jobs should be moved to cloud to improve the capability, capacity and battery time of the mobile devices. On the basis of the above discussion, mobile cloud computing can be defined as protocol allows resource constrained mobile users to adaptively adjust processing and storage capabilities by partitioning and offloading the computationally intensive and storage demanding jobs on traditional cloud resource by providing wireless access.

Therefore secure mobile cloud service architecture is necessary to address the requirements of users. The secure mobile cloud data processing framework for mobile cloud application model includes the following three main components described as follows. Mobile Cloud Trust Management: This model of mobile cloud includes identity management, security policy enforcement and key management. Managing security keys and certificates for mobile users are the responsibilities of trusted authority (TA).Multi – Tenant

Secure Data Management: In this model services for all mobile devices and Extended Semi Shadow Images (ESSI) are provided by the cloud public service and storage domain. Mobile devices can request services from storage

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

domain and from the public service and also it can request services through ESSI's. ESSI Data Processing Model: In the ESSI data processing model, the advantage of the user root includes maintaining user's data in a storage called secure storage and encryption, decryption and verification associated processes. Maintenance functions of ESSI are performed by cloud root and it does not have the access to secure storage and associated security functions. The auditing root can be used to list the activities of both cloud root and user root. The listed data is maintained by a third trusted authority. User's private information and security credentials are stored in secure repository managed by the ESSI that are mapped to the user's mobile device.

II. LITERATURE SURVEY

In spite of the hype achieved by mobile cloud computing, the growth of the mobile cloud computing subscribers is still below expectations due to the risks associated with the security and privacy. This study is based on existing literature, highlights the current state of the work proposed to secure mobile cloud computing infrastructure.

Itani et al. [7], proposed an energy efficient integrity verification scheme for mobile clients to verify the integrity of the files stored on a cloud server using an incremental message authentication code. The proposed scheme offloads most of the integrity verification jobs on a cloud service provider and trusted third party to minimize the processing overhead on the mobile client. The cloud service provider redirects the stored files towards the coprocessor when instructed by a mobile client. The coprocessor computes incremental MAC on received files for integrity verification.

Jia et al. [8], proposed a secure data service that outsources data and security management on cloud without disclosing any user information with the help of proxy re-encryption and identity based encryption schemes. Although the proposed secure data service has removed security management overhead from mobile users, still mobile users have to perform cryptographic operations before uploading a file on cloud. The cryptographic operations involve massive pairing evaluations and exponential calculations. The cryptographic operations consume a considerable amount of energy that needs to be considered while designing a secure framework for mobile cloud computing. Secondly, the cloud is responsible for performing the security management and re-encryption on behalf of the mobile user. Hsueh et al. [9] proposed a scheme for smart phones that ensures the security, integrity, and authentication of mobile user data. The mobile user encrypts the files using traditional asymmetric encryption techniques. The encrypted files are stored on cloud servers along with mobile user name, signature, and password. The encrypted files along with user credentials may be stored on a cloud server hosted by an adversary. The adversary can utilize credentials to impersonate the user later on. Secondly, the proposed scheme ignored the processing and storage limitations of the device. The encryption and decryption and even hash function applied on an entire file are performed on the mobile device. Yang et al. [10] proposed a public provable data possession scheme for a resource constrained mobile device that ensures privacy and confidentiality. Trusted third party is responsible for handling encoding/decoding, encryption/decryption, signature generation, and verification on behalf of the mobile user. Although the offloading of mobile user's jobs on trusted third party saves energy, an increase in the number of mobile users results in performance degradation. Huan et al. [11] proposed a new mobile cloud computing framework that not only provides conventional computation services but also improves the functionality of MANET in terms of risk management, trust management, and secure routing. In spite of the advantages provided by the MobiCloud to MANET, the MobiCloud framework did not consider the trust worthiness of the cloud node. There should be a mechanism to store mobile user information on cloud servers in a secure manner.

III. SYSTEM ARCHITECTURE

The system architecture shows the blocks required for the project. Large systems are decomposed in to sub systems that provide some related set of services. The initial design process of identifying these sub systems and establishing a framework for subsystem control and communication is called architecture design and the output of this design process is a description of the software architecture. The architectural design process is concerned with establishing a basic structural framework for a system. It involves identifying the major components of the system and communications between these components. Design is one of the most important phases of software development. The design is a creative process in which a system organization is established that will satisfy the functional and non-functional system requirements. The figure below shows the complete architecture:

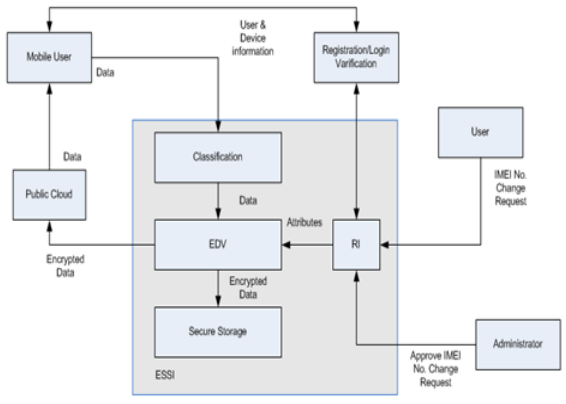

Figure: System architecture

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

The secure mobile cloud data processing model in the above figure include following components:

1. Registration/login verification
2. Classification
3. Encryption/ Decryption module.

A user's private information and security credentials are stored in the security repository managed by the ESSI mapped to the user's mobile device. Data flow is inspected by the classification model that classifies the data as critical data or normal data. If the data is classifies as normal, the normal data will be sent to the public cloud storage through a masking procedure. The Encryption/ Decryption/verification (EDV) module is then used on the critical data and stores the processed data in secure storage (SS).

IV. HIGH LEVEL DESIGN

ESSI data processing model in the level-1 data flow diagram is divided into classification and EDV modules. A user's private information and security credentials are stored in the security repository managed by the ESSI mapped to the user's mobile devices. When the user uploads the data, the data enters into the ESSI data processing model.

Data flow arriving at the ESSI is processed as follows: (i) Data flow is inspected by the classification model that classifies the data as critical data or normal data. (ii) If the data is classified as normal, the normal data will be sent to the public cloud storage through a masking procedure. (iii) The EDV module is then used on the critical data and stores the processed data in secure storage. In the following figure level-2 data flow diagram the EDV module encrypts the user's uploaded data by using Attribute-Based Encryption scheme [13][14] by taking user's attributes that are stored in the Repository Information (RI).

The encrypted data is then stored in the Secure Storage (SS). The masking procedure is used to remove private information associated with the user and anonymize the data content. The masking procedure can be configured differently according to the level of the criticality of the data. It is up to the user's preference and it is operated through the trust manager.

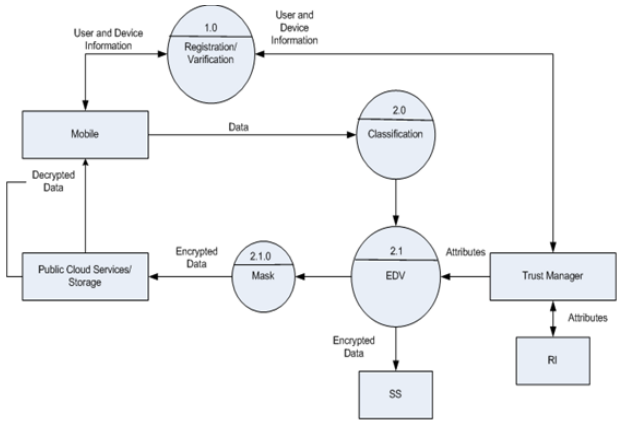

Figure: Data Flow Diagram

The sequence of execution steps is as follows.

1. In order to use cloud storage services mobile user's has to register to the cloud by providing username, password, first name, last name, address, pin code, device model, mobile number, and IMEI number.
2. If the registered IMEI number is already present in the repository information then response this device is already registered is send to the mobile user (client).
3. If the registered IMEI number is not registered earlier then all user attributes will be stored in repository information and registered successfully message is send to the user.
4. User has to enter details like username, password and IMEI number.
5. Request is sent to the web service, web service will check the validation of user. If the user is valid then it will send logged in process response to client and critical manager logged screen open.
6. If the validation of user fails then web service sends login failed response to the mobile user.

CONCLUSION

The aim of the framework is to design and implement a secure data processing framework for mobile cloud applications. The proposed framework utilizes decentralized approach and the proposed multi-tenant data management divides the data in to two security levels critical data and non-critical or normal data. In this framework, attribute-based encryption scheme with the Advanced Encryption Standard (AES) -128 bits is used for encrypting the mobile user's data in the cloud. AES is a symmetric block cipher that is intended to replace Data Encryption Standard (DES) for a wide range of applications. Anything less than 128-bits is considered weak encryption, and would not sufficiently protect data from brute force attacks. The proposed method has a number of advantages over the traditional approaches example scalability, computation is distributed between ESSI and a mobile device and no single point of failure.

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

AES is definitely more secure due to larger-size key and AES with 128-bit cipher key needs 2128 tests to find the key this would be impossible. Advanced Encryption Standard not only assures security but also improves the performance in a variety of settings such as smartcards, hardware and software implementations etc. Data operations like data retrieval, data indexing etc are also distributed to ESSI and computation overhead is distributed to multiple processors in the cloud. Extended semi shadow images (ESSI's) enhance the user's security by adding one additional layer of security in which critical data are stored in each ESSI. As a result composition one ESSI will not impact the other ESSI.

REFERENCES

[1] Jadeja, Y. ; Modi, K., Cloud Computing - Concepts, Architecture And Challenges ,International Conference on Computing, Electronics and Electrical Technologies(ICCEET), Kumaracoil, 2012,DOI:10.1109/ICCEET.2012.6203873, 978-1-4673-0211-1,pp 877 - 880.

[2] Shaikh, F.B. ; Haider, S.,Security Threats In Cloud Computing, International Conference For Internet Technology And Secured Transactions (ICITST), Abu Dhabi ,2011, 978-1-4577-0884-8 , pp 214 – 219.

[3] K.Kumar, Y.H. Lu, Cloud Computing for Mobile Users: Can Offloading Computation save Energy? , IEEE journal on cloud computing, 2010, Issue: 4, Volume: 43, pp 51 - 56, West Lafayette, PA, USA.

[4] Crago S, Dunn K, Eads P, Hochstein L, Heterogeneous Cloud Computing, IEEE International Conference on Cluster Computing (CLUSTER), 2011, pp 978-1-4577- 1355-2.

[5] B.P. Rimal, E. Choi, I. Lumb, A taxonomy and survey of cloud computing systems, in:Proc .5th Int. Joint conference of INC,IMS and IDC,NCM '09,Seoul,Korea,Nov 2009.

[6] H. Canepa, D. Lee, A Virtual Cloud Computing Provider For Mobile Devices, in: Proc, 1st ACM workshop on Mobile Cloud Computing and Services Social Networks and Beyond, MCS 10,San Francisco, USA, June 2010.

[7] W.Itani, A. Kayssi, A. Chehab, Energy-Efficient Incremental Integrity For Securing Storage In Mobile Cloud Computing, in: Proc. Int. Conference on Energy Aware Computing, ICEAC '10, Cario, Egypt, Dec. 2010.

[8] W. Jia, H. Zhu, Z. Cao, L. Wei, X. Lin, SDSM: A Secure Data Service Mechanism in Mobile Cloud Computing. In: Proc. IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS, Shanghai, China, and Apr. 2011.

[9] S.C. Hsueh, J.Y. Lin, M.Y. Lin, Secure Cloud Storage For Conventional Data Archive Of Smart Phones, in: Proc. 15th IEEE Int. Symposium on Consumer Electronics, ISCE '11, Singapore, June 2011.

[10] J. Yang, H. Wang, J. Wang, C. Tan, D. Yul, Provable Data Possession Of Resource Constrained Mobile Devices In Cloud Computing, Journal of Networks ,China,6(7) (2011),pp 1033-1040.

[11] Fei Li, Rahulamathavan, Y. Rajarajan, M. ,Low Complexity Multi-authority Attribute Based Encryption Scheme for Mobile Cloud Computing, IEEE 7th International Symposium on Service Oriented System Engineering (SOSE),2013, 10.1109/SOSE.2013.12 ,pp 573-577.

[12] Rewagad, Prashant,Pawar, Yogita ,Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing ,International Conference on Communication Systems and Network Technologies (CSNT), 2013, 10.1109/CSNT.2013.97 ,pp 437-439.

[13] ElBadawy, E.-S.A.-M,Mokhtar, A.,El-Masry,W.A Hafez, A New Chaos Advanced Encryption Standard (AES) Algorithm For Data Security , International Conference on Signals and Electronic Systems (ICSES),Egypt,2010, 978-83-9047-4-2 ,pp 405- 408.

[14] Zhao Yun, Si Huayou, Ni Yulin and Qi Hengnian; "A Service-Oriented Analysis and Design Approach Based On Data Flow Diagram", International conference on Computational Intelligence and Software Engineering, Lin'an, China, 2009. Issue Date: 11-13 Dec. 2009, Digital Object Identifier: 10.1109/CISE.2009.5365568,pp.1- 5.

[15] Song Luo, Jianbin Hu .Zhong Chen, Implementing Attribute-Based Encryption in Web Services, IEEE International Conference on Web Services (ICWS), 2010,10.1109/ICWS.2010.82 ,pp 658-659.

BIOGRAPHIES

Manjunath A E is working as Assistant Professor in RV College of EngineeringBangalore. His areas of interest are Device Drivers,Context Aware computing, Adhoc Networks, Mobile Computing, Java / J2EE and Java native interface (JNI).

H Pavithra is working as Assistant Professor in RV College of EngineeringBangalore. Her areas of interest are Cloud Computing and sensors.

Swarnalath K S is working as Assistant Professor in RV College of EngineeringBangalore. Her areas of interest are Cloud Computing and Software Engineering

Sharadhadevi S Kaganurmath is working as Assistant Professor in RV College of Engineering Bangalore. Her areas of interest are Cloud Computing and sensor Network.