Information Security using Surrogate Object based Encryption in Mobile Cloud Systems

DR. S. RAVIMARAN[1], A.N. GNANA JEEVAN[2], DR. M.A. MALUK MOHAMED[3]
[1],[2]&[3] Software System Group Lab, Department of Computer Science and Engineering
Affiliated to Anna University, Chennai
M.A.M. College of Engineering, Tiruchirappalli, Tamil Nadu.
INDIA.
[1] ssg_ravimaran@mamce.org, [2] ssg_jeevan@mamce.org, [3] ssg_maluk@mamce.org

Abstract: - The advancement in wireless technology and rapid growth in the use of mobile devices in cloud paradigm have the potential to revolutionize computing by the illusion of a virtually infinite computing infrastructure, namely the mobile cloud. However, the amount of unprotected data in mobile cloud platform will grow in the forthcoming year and this will leads to various security issues such as potential attack, authentication, faster accessing of data, challenges arise from data residency, accessing mechanism, mobility, bandwidth restrictions, number of wireless and wired access, number of communication messages. So, it is the right time to enhance, the existing mechanism to make the overall security more robust in this platform. This paper propose a new standardization for information security using Surrogate object that may store, gather private information and ensure that individuals' private information is kept and accessed in a secured manner. Thus, the Surrogate Object Based Encryption (SOE) model enhancing the privacy when business information is uploaded to the data centres. The performance of proposed models have been evaluated and compared with existing models in mobile cloud platform by simulation and proved that the proposed SOE scheme provides better protection for information in mobile cloud platform.

Key-Words: - Surrogate object, Information Security, Mobile Cloud Computing, Authentication, RSA Algorithm.

1 Introduction

Several computing paradigm such as Grid computing have promised to deliver utility computing vision. Computing is being transformed to a model, consisting of services that are commoditized and delivered in a manner similar to the utilities such as water, electricity, gas, and telephony (Voorsluys 2011), namely cloud [1]. This advancement in computing technology has enabled access to required services anonymously. Cloud computing is the most recent emerging paradigm promising to turn the vision of computing utilities into a reality. Cloud computing is a technological advancement that focuses on the way in which the design computing systems, develop applications, and leverage existing services for building software. It is based on the concept of dynamic provisioning, which is applied not only to the service, but also compute capability, storage, networking, and IT infrastructure in general. Cloud computing aggregates together a large amount of geographical and organizational dispersed and potential heterogeneous computing resources, such as processing power, storage, and bandwidth, in a scalable and a cost effective manner. Thus, cloud computing has been considered as a new computing paradigm which allows customers to utilize the computing resources hosted by multiple service providers (Xiangyu Zhang 2009), thus reducing the infrastructure and administrative cost of most of the service providers [2].

In addition, to that,, the recent technological advancement in computing, wireless communications, networking and electronics have embedded processing power, storage space and communication capabilities in electronic devices of day-to-day use, which lead to the era of ubiquitous computing (Weiser 1993).

This brings about a new paradigm of distributed computing in which mobile communication may be achieved through wireless networks and the users can communicate with other distributed static or mobile hosts even as they move from one environment to another (Sathyanarayanan 2001). As a result, a great amount of mobile data and computing resources resides on these devices in a distributed, non-integrated manner [4]. The environment for accessing and processing information is rapidly changing from stationary to

mobile with location independent, providing users a flexible.

Taken all together, advancement in wireless and mobile communication (Qureshi 2011) with cloud has the potential to revolutionize computing by the illusion of a virtually infinite computing infrastructure in day-to-day application, which leads to the era of mobile cloud computing [5]. It can be extended over multiple heterogeneous service providers and achieve portability and interoperability. Although cloud computing promises to eliminate obstacle due to management of various computing resources and reduce the infrastructure cost, however the realization of mobile cloud computing is still in its initial stage.

In general, Mobile cloud (Soebhaash Dihal 2013) is the collection of mobile devices over the cloud extended by mobility and a new ad-hoc infrastructure relying on single cloud service provider [6]. However, Expansion of the organizations in globally requires secure data communications among physically distributed mobile cloud systems.

The impact of the huge growth of these resources goes beyond the networking issues such as bandwidth, connectivity, security issues, loss of governance, lock-in, isolation failure, management interface compromise, data protection, insecure and incomplete data deletion, malicious insider, customers security expectations, availability chain and etc., So the traditional mechanism is not directly applicable for information security management in this context and hence the new paradigms are needed.

This paper propose a new standardization for information security among mobile cloud applications using Surrogate object that may store, gather private information and ensure that individuals' private information will be kept in a secured manner. So, the proposed model enhancing the privacy, when business information is uploaded to the data centers by using Surrogate Object Based Encryption (SOE), the performance of the proposed models has been evaluated and compared with the existing model by simulation and proved that the SOE scheme will provide better protection.

The rest of this paper is organized as follows: Section 2, presents Background and related work in cloud systems. Section 3 describes proposed SOE framework and Section 4 provides Performance Evaluation, finally Section 5 draws Conclusion of this paper.

2 Related Work

Abdul Nasir Khan et.al proposed the new scheme which offloads the frequently occurring dynamic credential generation operations on a trusted entity to keep minimum processing burden on the mobile device. To enhance the security and reliability of the scheme, the credential information is updated frequently on the basis of mobile-cloud packets exchange [7].

Kao Zhao et.al introduced the new scheme named Biometric Encryption (BE) in mobile cloud computing to solve the security problems related to mobile cloud and they analyzed the new critical issue to solve the critical situations by introducing the different Biometric Encryption methods to explore scenarios where each method shows its strengths and weaknesses. In particular, they address the problem of using BE to protect privacy for users in MCC [8].

Issa Khalil proposed a third-party security named Identity Management Systems (IDMs) to strengthen the information security. Which have the limitations of the state-of-the-art cloud IDMs with respect to mobile clients? Most importantly, they propose and validate a new IDM architecture dubbed Consolidated IDM (CIDM) that counter measures these attacks [9].

Zhiwei Wang et.al defined the new homomorphic signature for identity management in mobile cloud computing for storing the Sensitive Personal Information (SPI) with Trusted Third Party (TTP) for authenticate the users data to the cloud service provider. By using this, they give the formal secure definition of this homomorphic signature, and construct a scheme from GHR signature. We prove that our scheme is secure under GHR signature [10].

Saman Zonouz et.al proposed the new concept called Secloud, a cloud-based security solution for Smartphone devices. Secloud emulates a registered Smartphone device inside a designated cloud and keeps it synchronized by continuously passing the device inputs and network connections to the cloud. To perform a resource-intensive security analysis on the emulated replica that would otherwise be infeasible to run on the device itself.

Wei Ren et.al introduced the new schemes are lightweight in terms of computational overhead, resilient to storage compromise on mobile devices, and do not assume that trusted cloud servers are present. The algorithms are proposed in detail for guiding off-the-shelf implementation. The evaluation of security and performance is also extensively analyzed.

Jiun-Hung Ding et.al proposed an innovative Internet service and business model to provide a secure and consolidated environment for enterprise mobile information management based on the infrastructure of Cloud-based Virtual Phones (CVP). Our proposed solution enables the users to execute Android and web applications in the cloud and connect to other users of CVP with enhanced performance and protected privacy.[11].

A few other earlier research works (Qiming Chen 2010, ChatschikBisdikian 2011, OoiBeng Chin 2009, Daniel J 2009, Raghu Ramakrishnan 2009, Laura Cristiana Voicu 2010, Valentina Casola 2010, Rohan G 2010, Sudipto Das 2009) had discussed the challenges in managing the information in cloud platform but not in mobile cloud. To the best of our knowledge, only our research work has proposed for Information Security in Mobile Cloud (SOE).

The emerging mobile computing in association with cloud, offers growing business market in developing the world economy. However, the information security playing a vital role in this paradigm, because of the necessity to store data at remote locations seem to be a critical one for both business and an individual customer.

In general, the variety of mobile devices involved in the mobile paradigm is difficult to ensure a standard, credential protection to information stored in the remote locations. They are also suffered by various limitations such as battery powered, limited processing power, low storage, and unpredictable internet connectivity. Due to these limitations in the mobile environment, most of the computational and storage related tasks should be migrated to cloud platform. However, the careful designed planning is required to migrate the tasks to the cloud by considering the network conditions. In order to provide a better information security solution, cloud is used to avoid communication.

The proposed model suggest a lightweight secure framework called SOE, which provides security for information stored in this emerging platform with minimum communication, less failure rate, less cost, minimum energy usage and minimum processing overhead. The proposed Surrogate Object Encryption (SOE) model describes a different approach for information security in distributed mobile cloud systems. The prime focus of this paper is on developing a Surrogate Object Encryption model for various applications as well as protocols in distributed mobile cloud platform. The surrogate object Encryption model presented in this paper provides a new perspective for designing a distributed mobile cloud system.

3 Surrogate Object Encryption (SOE)

The benefits of Surrogate object based encryption are numerous, including improved efficiency, reduced costs and greater accessibility and flexibility. When business move their(more sensitive) data's from on-premise to cloud-based and it is accessed by mobile devices, challenges arise from data residency, accessing mechanism, mobility, bandwidth restrictions, number of wireless and wired access, number of communication messages and privacy in order to protect sensitive information. The primary solutions for these problems include encryption of data stored in the cloud. New SOE based solution has been proposed for improving information security and protecting sensitive data and important applications while accessing these data through mobile devices in mobile cloud scenario. The surrogate object can serve as a proxy "entry" to a cloud application, replacing sensitive data with encrypted values with the help of Surrogate Object Authentication Manager for transmission and storage in the cloud.

A typical Surrogate Object based Encryption Architecture (SOE) structure is shown in Figure 3.1. The structure includes various components: (1) mobile end users; (2) a mobile support station (MSS) that controls and create surrogate object for end users; (3) a surrogate object that is created on MSS to act on behalf of each mobile end users. The surrogate object of each mobile end user generates an access key requesting to access the information; then this information are retrieved and stored in their local cache of surrogate object. The cache is a non-volatile storage that supports transactions execution in both normal and disconnected mode; (4) Surrogate Authentication Manager (SAM) is an administrator which controls all over authentication and authorization. The Surrogate Authentication Manager is Two Factor Authentication which identifies the access token key generated by mobile user and check for the authenticated user by the Surrogate Object Encryption Algorithm which generates encrypted token similar to mobile user access token for identify authenticated user; (5) Surrogate Object Encryption (SOE) that generate the encrypted access key by using the RSA algorithm.

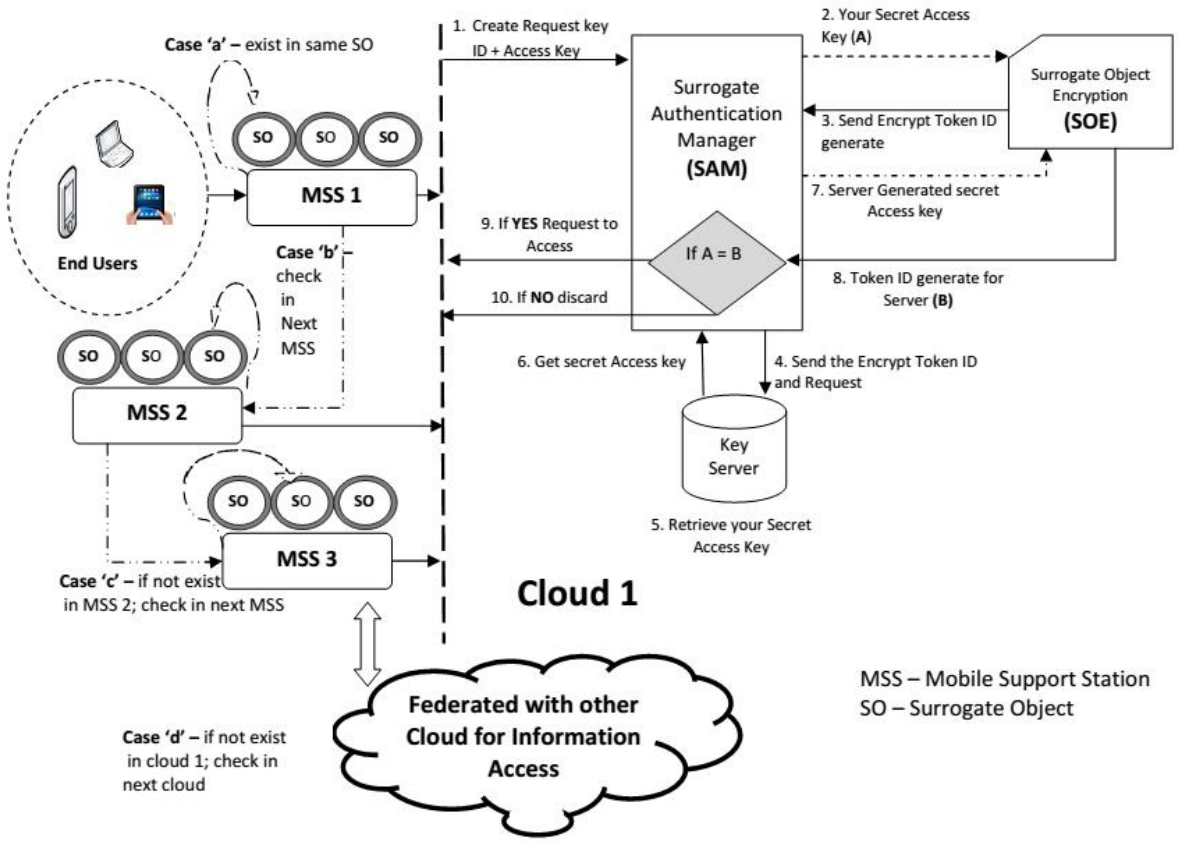

Fig. 3.1: Surrogate Object Encryption Architecture

The same algorithm accepts the matched access key which was generated by key server and produces the token identifier and handover to SAM. The SAM check the token identifier and access key are same it will permit to access the mobile user to access the information in a secured manner.

The proposed Surrogate Authentication Manager (SAM) in mobile cloud makes it more efficient model in executing secure information access during disconnection period and ensures minimum wireless access and achieves the low abort probability and short response time for executing the transactions. Whenever a new mobile user is joined to the mobile environment, the MSS-s assigns a access key for the mobile user object and creates the surrogate object which is act as a object reference for that host and assigns an unique access key for the same and the Surrogate Authentication manger (SAM) updates these entries into object reference which is flushed into key server resides in the same. The Surrogate Authentication manager maintains a separate key server to store all these objects and object references are correct it will generate a secret access key. The key server search the entries for the access key generated by mobile users surrogate object which was encrypted and reply to SAM.

The SAM also maintains the log data structure which stores the various records for ongoing transactions. In general, the SAM makes appropriate entries then and there in the secure information during the disconnection period.

The proposed Surrogate Object Encryption (SOE) algorithm, in which a mobile end user entered into Mobile Support Station (MSS) it, checks for the authentication and authorization for accessing the secured information. The SOE algorithm was proposed to check and create the access key by using the RSA algorithm for standard encryption and decryption to access the secured information. The SOE algorithm namely soe () method is common for all mobile end users which resides in the Surrogate Authentication Manager (SAM) which checks and control all over the authentication and authorization of the end users for allowing the end user to access the information through the Mobile support Station (MSS) and surrogate object (SO).The surr_encrypt() method provides the additional requirements for accessing the secured information which is located in SAM.

This method is common to all end users who are all connected to MSS by surrogate object. The detailed encryption algorithm is shown in Table 1.

Table 1: surr_encrypt() method

surr_encrypt(access key, timestamp)
{
secret access key ID ← MSS(access key, timestamp);
where: access key is single use code, timestamp is used for session expire
The SAM sends the access key to soe () algorithm method:
soe (secret access key ID)
{
By using the standard RSA algorithm this method generate and return the encrypted Token ID to the surr_encrypt() method as public key for user access.
{
data access (m)= access key as public key;
select two prime number p and q;
compute e,d,n and $\phi(n)$;
generate encrypt Token ID = Encrypt with public key as (access key) ^{e} mod n;
return(encrypt token ID);
}
}

Now, the SAM sends the encrypted Token ID to the key server which holds the private key. The key_server() method is shown in Table 2.

Table 2: key_server() method

key_server (encrypt Token ID)
{
search for the respective token ID ;
return (secret access key) as private key;
}

SAM gets the secret access key from key server as private key to sod () algorithm method for decrypt. The sod() method is described in Table 3.

Table 3: sod() method

sod (secret access key)
{
token ID = (secret access key) ^{d} (mod n);
where : token ID is the original data, d and n are the computed value while encryption
return(token ID);
}
Now SAM check the token ID and secret access key
If (token ID == secret access key)
{ Allow to access the information; }
else
{ Discard the user; }
}

information through the MSS 1, that information if it is available in the same surrogate object, the MSS 1 check the end user whether he/she is authenticated user or not, for that the MSS 1 had a common Surrogate Authentication Manager (SAM) with Surrogate Object Encryption (SOE) algorithm. This SAM identifies the authentication of user and authorized the user to access the secure information.

Case 'b': From the case 'a'; if the end users search information is not available in their own MSS and Surrogate object. It checks to next MSS 2 and their surrogate objects of the same cloud 1. If this MSS 2 has the information the MSS 2 check for authentication and authorization through SAM. After SAM verification only the end user allow to access the information.

Case 'c': From the case 'b'; the end users search information is also not available in MSS 2, it check to the next MSS 3 and their surrogate objects of the same cloud 1. If this MSS 3 has the information the MSS 3 check for the authentication and authorization through SAM.

Case 'd': If the case 'c'; is failed i.e. from the case 'c' the end users search information is also not available in cloud 1 MSS's , it federated to next Cloud 2 for accessing the information, each cloud has the SAM and SOE for authentication and authorization the secured information.

3.1 Performance Analysis

In this section, we analyze the performance of SOE by comparing it with the other models proposed in related work. Most of the existing methods provide less security, waste uplink bandwidth for both wired and wireless accesses. The performance metrics employed are the average response time of service requests, the number of failures of service request, and the number of wired and wireless access to the database servers and between the surrogate objects from mobile nodes for the final validation.

The performance was measured by a simulation by varying the number of service requests. The scheme also presents a simulation study about the potential benefit in a service provider, when doing federation in object level, outsourcing and in sourcing their database server during the over load and less load period. The entire simulation work was supported by Aneka cloud simulator which is .Net based service oriented management platform. It provides the minimum functionality needed for a Mobile node in cloud platform and provides the base infrastructure that consists of services for persistence, authorization, authentication and auditing, message handling and dispatching. The simulation prototype has been created for the proposed SOE technique using Aneka Configuration wizard. The sample prototype consist of 15 nodes which are created, configured and monitored properly through the node selection module, advanced setting module, data store setting, security and service setting modules. The nodes are grouped

into different clouds. The different Clouds such as Cloud1, Cloud2 and Cloud 3 nodes were created as simulation prototype using advanced setting module. After a successful creation of nodes for different clouds, a surrogate object, and its cache in the respective nodes were created by using management tool and data base setting tools and finally the application was implemented over this setup.

3.1.1 The Effect of Information Security

In this section we study about the information security in cloud environment for mobile users to use their services. As shown in Figure 3.1.1, the top five choices are secure mobile cloud, Identify management system, homomorphic signature, secloud-lightweight security, and virtual phones. From these factors we study the cloud computing security risks that have been cited in the security literature along with our Surrogate Object Encryption (SOE). With respect to these five risk areas, our SOE providers are most confident about their ability to ensure recovery from significant information failures and ensure the physical location of data assets are in secure environments. Our SOE have highly confident in their ability to restrict privileged end user access to sensitive data and ensure proper data segregation requirements are met.

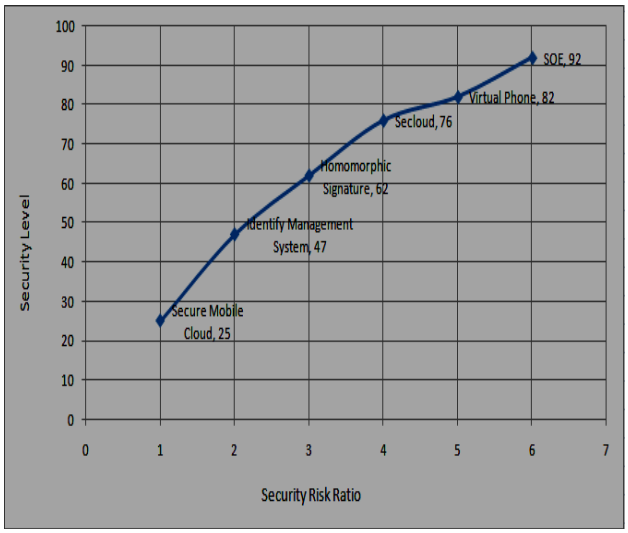

Fig 3.1.1: Effect of Information Security

3.1.2 The Effect of Data Access

In this section, we investigate the database access implication during the peak time. For instance, the service consumer request database access through his mobile device from Cloud 1. Assume there are other two clouds existing in the environment namely Cloud 2 and Cloud 3 and Cloud 1 is federated with Cloud 2 and Cloud 3. Cloud 1, Cloud 2 and Cloud 3 have surrogate objects for their mobile devices in the respective mobile support stations. If requested data item exist in the cache of respective surrogate object in Cloud 1, the data items are immediately given for access. When database access request is not satisfied by Cloud1 due to cache miss and overloaded status, either Cloud 2 or Cloud 3 can provide supports for data access with the help of their surrogate objects. The interaction between Cloud 2 and Cloud 3 is completely hidden from the Cloud 1 consumer. Due to this, the scheme is assured that even with increase in database access and cache miss status, it will be able to provide database access. The rate of database access during peak time is shown in Figure.3.1.2.

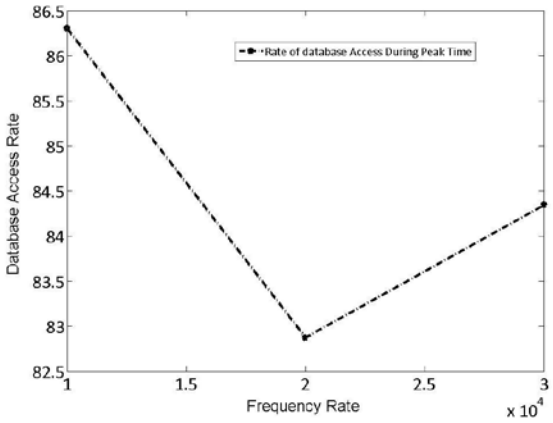

Fig. 3.1.2. Rate of Database access during Peak Time

3.1.3 The Effect of Average Latency

Figure 3.1.3 shows the average latencies (in terms of response times) of transaction requests in the MSS federated over the presence of the surrogate objects. In the graph, the data access response time variance is plotted against simulation time for different probabilities. The graph shows better response time which is achieved for data access in the presence of surrogate object than in the existing federation model. The reason for this significant improvement in the performance of the new model is due to data caching at the surrogate object through object level federation and replication. As a result, lower average response time is achieved through this proposed technique.

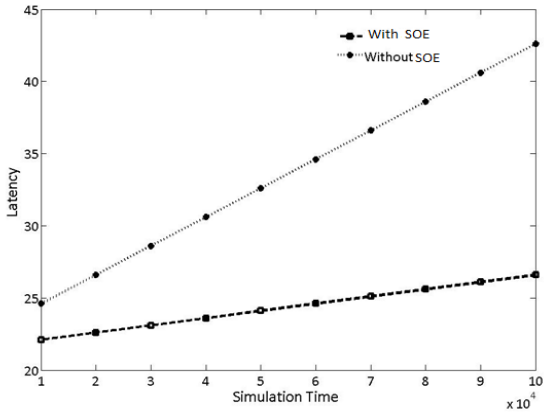

Fig. 3.1.3. Latency Comparison

3.1.4 The Effect of the number of failures of Service request

The Figure 3.1.4 shows the number of aborts of transactions request against simulation time for different probabilities and different transaction request size in order to show the improvement in the network life time and fault tolerance in our simulations. The proposed approach is compared with the existing approaches which are implemented based on two of the closely related works [17] and the simulation shows that the lifetime improves with the support of surrogate objects and its cache. This also leads to a better bandwidth utilization and only 5 percent of abort (implies 95 percent of Success achieved) because of more data items are cached into the surrogate objects. Due to this, most of the time the data access requests are sent to the surrogate objects instead of database server located in different service provider in different clouds, which ensure minimum abort rate.

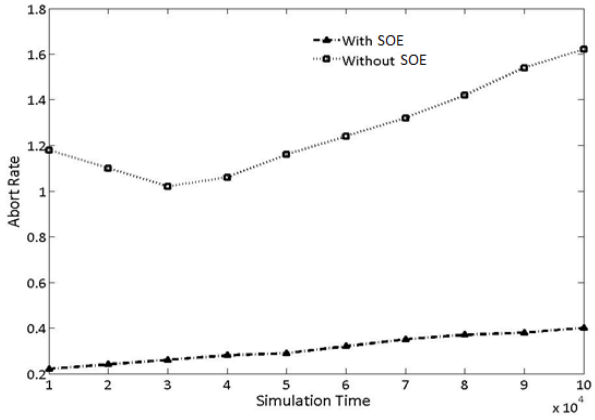

Fig.3.1.4. Rate of Transaction Abort

3.1.5 The Effect of the number of Wired and Wireless Access

Figure 3.1.5 and 3.1.6 shows the comparison of wired and wireless access to perform the data access with and without SOE techniques. The graph shows the network traffic in terms of number of wireless and wired access versus simulation time for various move frequencies. It can be seen that in the SOE, it involves more data accesses over the wireless and wired network, whereas, the proposed model reduces the number of data access over the wired and wireless network and consequently, the impact of pocket loss probability during disconnection period of mobile device is much lesser. As a result, SOE method can avoid sending data access requests to database server located in different clouds and save the usage of uplink communication bandwidth and reduce both the wired and wireless access across various clouds

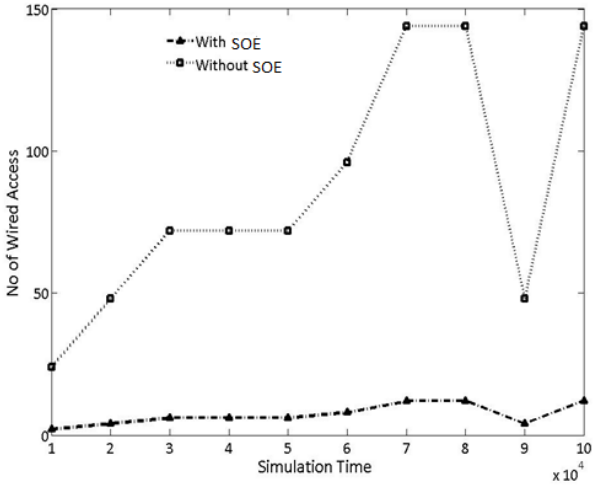

Fig. 3.1.5. Effect of Wired Access

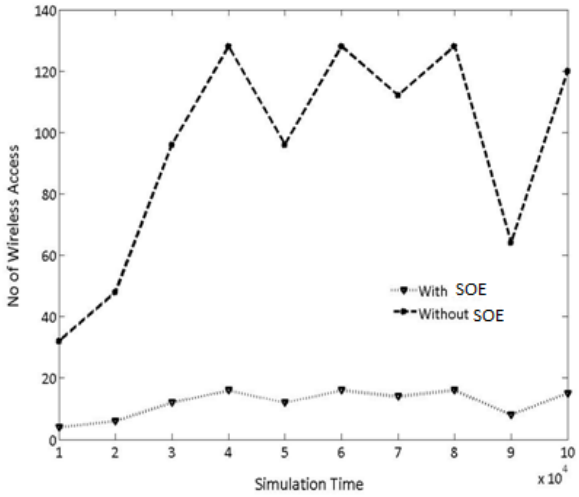

Fig. 3.1.6. Effect of Wireless Access

4 Conclusion

The feature of the proposed model is proved by handling information security for the mobile users for reducing the communication overhead and wireless communication. Thus the proposed model tolerates failures and limitations of the mobile devices and provides a significant reduction in wireless access, abort probability and response time with authentication and authorization. Thus, the performance of SOE has been evaluated and compared with an existing security mechanism. The result of the evaluation shows that the proposed Surrogate object Encryption based mobile cloud model enables to solve computationally intensive task for data secure and transaction processing by pooling the cloud resources to surrogate objects located in multiple clouds through federation techniques. This model provides reliable integration of SAM and SOE to mobile cloud platform through object encryption and decryption for data secure which federation and replication techniques and provides elegant support for various constraints of the mobile devices and cloud environment such as poor computational resources, limited energy power, low bandwidth, unpredictable consumer request, limited services facility offered by the cloud, overloaded consumer request during peak time, and problems due to mobility under various conditions.

References:

[1] Voorsluys, W., Broberg, J. and Buyya, R. (2011) *Introduction to Cloud Computing, in Cloud Computing: Principles and Paradigms* (eds R. Buyya, J. Broberg and A. Goscinski), John Wiley & Sons, Inc., Hoboken, NJ, USA. doi: 10.1002/9780470940105.ch1

[2] Xiangyu Zhang, Jing Ai, Zhongyuan Wang.: *An efficient multi-dimensional index for cloud data managemen*t. CloudDB'09, proceeding of the ACM first international workshop on cloud data management (2009) ISBN: 978-1-60558-802-5 doi:10.1145/1651263.1651267

[3] Weiser M., Hot Topics : *Ubiquitous computing*, IEEE Computer, October 1993

[4] Sathyanarayanan M., *Pervasive Computing: Vision and Challenges*, IEEE personal Communications, pp. 10-17,2001

[5] Qureshi, S.S.; Ahmad, T.; Rafique, K.; Shuja-ul-islam, "Mobile cloud computing as future for mobile applications - Implementation methods and challenging issues," *IEEE International Conference on* , vol., no., pp.467,471, 15-17 Sept. 2011

[6] SoebhaashDihal, Harry Bouwman, Mark de Reuver, MartijnWarnier, ChristerCarlsson, (2013) "*Mobile cloud computing: state of the art and outlook*", info, Vol. 15 Iss: 1, pp.4 – 16

[7] Abdul Nasir Khan, M.L. Mat Kiah, Samee U. Khan, Sajjad A. Madan , "Towards secure mobile cloud computing: A survey" *Original Research Article Future Generation Computer Systems*, Volume 29, Issue 5, (2013), 1278-1299

[8] Kao Zhao, Hai Jin, Deqing Zou, Gang Chen, Weiqi Dai, "*Feasibility of Deploying Biometric Encryption in Mobile Cloud Computing*", IEEE ,110 to 130, 978-0-7695-5058-9/13 (2013)

[9] Issa Khalil, Abdallah Khreishah, Muhammad Azeem ,"Consolidated Identity Management System for secure mobile cloud computing" *Original Research Article Computer Networks*, Volume 65, (2014) , 99-110

[10] Zhiwei Wang, Guozi Sun, Danwei Chen ,"A new definition of homomorphic signature for identity management in mobile cloud computing" *Original Research Article Journal of Computer and System Sciences*, Volume 80, Issue 3, (2014) , 546-553

[11] Saman Zonouz, Amir Houmansadr, Robin Berthier, Nikita Borisov, William Sanders, "Secloud: A cloud-based comprehensive and lightweight security solution for smartphones", *Original Research Article Computers & Security*, Volume 37, (2013), 215-227

[12] Qiming Chen, Palo Alto, Data stream analytics as cloud service for mobile applications, Proceeding of OTM'10 Proceedings of the 2010 international conference on On the move to meaningful internet systems: Part II Pages 709-726

[13] ChatschikBisdikian,BernhardMitschang, Dino Pedreschi, Vincent S. Tseng, audio Bettini, *Challenges for Mobile Data Management in the Era of Cloud and Social Computing*, Proceeding MDM '11 Proceedings of the 2011 IEEE 12th International Conference on Mobile Data Management - Volume 01 Page 6

[14] OoiBeng Chin, *Cloud Data Management Systems: Opportunities andChallenges*, Proceeding of Fifth International Conference on Semantics, Knowledge and Grid, 2009

[15] Daniel J. Abadi, New Haven, *Data Management in the Cloud: Limitations and Opportunities*, published in Bulletin of the IEEE

Computer Society Technical Committee on Data Engineering, 2009

[16] Raghu Ramakrishnan, *Data Management in the Cloud*, proceedings of IEEE International Conference on Data Engineering, 2009

[17] M.A. Maluk Mohamed, D. Janaki Ram and Mohit Chakraborty, "*Surrogate Object Model: A New Paradigm for Distributed Mobile Systems*", Proceedings of the 4th International Conference on Information Systems Technology and its Applications (ISTA'2005), May 23-25, 2005 - New Zealand, pp.124-138.

[18] ValentinaCasola, MassimilianoRak, Umberto Villano, Identity Federation in Cloud Computing, proceedings of *Sixth International Conference on Information Assurance and Security*, 2010

[19] Rohan G. Tiwari, Shamkant B. Navathe, Gaurav J. Kulkarni, *Towards Transactional Data Management Over The Cloud*, Proceedings of Second International Symposium on Data, Privacy, and E-Commerce, 2010

[20] Sudipto Das, DivyakantAgrawal, Amr El Abbadi, ElasTraS: *An Elastic Transactional Data Store in the Clou*d, 2009

[21] Xiangyu Zhang, Jing Ai, Zhongyuan Wang, An efficient multi-dimensional index for cloud data management:, CloudDB'09, proceeding of the *ACM first international workshop on cloud data management*, ISBN: 978-1-60558-802-5 doi:10.1145/1651263.1651267, (2009).

[22] Bogdan Nicolae, Gabriel Antoniu, Luc Bouge,. BlobSeer: Next generation data management for large scale infrastructure:, *Journal of Parallel and distributed computing*, volume 71 issue 2, February 2011, doi : 10.1016/j.ipdc.2010.08.004, (2011)

[23] Chen Gang, Data Center Management Plan in Cloud Computing Environment:, *Proceedings of IEEE 3rd International conference on information management*, Innovation Management and industrial Engineering, doi: 10.1109/ICIII.2010.575, (2010).

[24] Anton Beloglazov, Rajkumar Buyya,. Energy Efficient Resource management in virtualized cloud data centers:, Proceedings of 2010 10th *IEEE/ACM international conference on cluster, cloud and grid computing*,2010, doi:10.1109/CCGRID.2010.46, (2010).

[25] Hoon Jeong, Euiin Choi, User Authentication using Profiling in Mobile Cloud Computing, *AASRI Conference on Power and Energy System*s, Elsevier, 2012

[26] Soeung-Kon(Victor) Ko, Jung-Hoon Lee, Sung Woo Kim, Mobile Cloud Computing Security Considerations, *Journal of Security Engineering*, 2012

[27] Abid Shahzad , Mureed Hussain, Security Issues and Challenges of Mobile Cloud Computing, *International Journal of Grid and Distributed Computing*, Vol.6, No.6 (2013),pp.37-50

[28] Nancy J. King, V.T. Raja, Protecting the privacy and security of sensitive customer data in the cloud, 0267-3649,Elsevier Ltd. doi:10.1016/j.clsr.2012.03.003, 2012