PREVENTION FROM MALICIOUS PROGRAMS FOR HANDLING SECURITY ISSUES IN MOBILE CLOUD COMPUTING

[1]Adnan Shafiq, [2]Muhammad Aslam, [3]Adeel Ahmed, [4]Shahid Islam,

[1,2]Department of Computer Science and Engineering, University of Engineering and Technology, Lahore.
[3]Department of Computer Science, Virtual University of Pakistan
[4]Department of Computer Science and Engineering, Rachna College of Engineering and Technology, Gujranwala, Pakistan.
mr.adnan.shafiq@hotmail.com, maslam@uet.edu.pk, adeelahmed292@gmail.com , swains@gmail.com,

ABSTRACT—*Cloud Services are basically the resources provided through distributed computers using internet. Privacy issue is one of the main information security key notions. Malwares or malicious codes are auto downloaded having a payload and used for unauthorized access to information and disturb computer operations. Internet is the most common and well known pathway from hackers to users. 90% of the malwares spread through internet. From cloud adoption perception there are many challenges like Security, Charging model, Service level agreement and Costing model. Security problem is at the top priority. Mobile Cloud Computing (MCC) has its own troubles in Communication and Computing. Mobile communication mainly has the problems of Low Bandwidth, Availability and Heterogeneity. On the computing side Computing Offloading, Security and efficiency enhancement are most highlighted problems. As data in mobile environment broadcasts so there is a potential barrier in MCC with limitations as low bandwidth and battery timing due to which mobile devices are not able to run an anti-viruses as on desktop computers. The two new and fundamental problems in mobile cloud computing are multi-tenancy and fate- sharing which increase the malware threat. We study and analyze these problems to find the way to have better protection in mobile cloud computing. We use encryption and compression in our designed technique and make it* possible for data to be encrypted and compressed by utilizing various keys before sending on the cloud. Designed technique is tested by making a simulation and a detailed comparison with other techniques is also provided with better results.

Keywords: - Cloud Computing, Mobile Cloud Computing, Malicious Programs, Malwares, Security Issues

1. INTRODUCTION

Security is the major problem in mobile cloud computing perspective. Moving your records on someone else’s hard drive doesn’t seem to be fine. In cloud implementation challenges, top ranked issue is the security. Cloud made it probable to construct big data centers at little price for everybody. Might be it decrease the structure price but enlarge the networking price as you transfer data on the server might be on every deal. Anyone may require relating with dissimilar clouds throughout standard interfaces or API in order to allocate or assimilate diverse assets or data. As per cloud owner’s viewpoint, the suppleness feature of resources in shape of multi-tenancy or virtualization builds charge investigation much harder as compare to typical data center. In addition to this the virtual machine is prepared a price element rather that a corporal object (server etc.). Prior to a Cloud user transfer his central part of corporate info on cloud that demands rich enactment by the provider. Fundamental issues in cloud computing are Multi-tenancy and fate- sharing. Major asset of cloud computing is Multi-tenancy which means multiple users using the similar storage device, resources etc. This leads to two main security issues. One is, common assets (virtual machine, data) on alike physical machine might be origin of side channels (inactively observe information) or underground channels (aggressively transferring data). Second is, fate-sharing which means parts are yoked collectively causing probable joint failure. Such things will harm the status of good people who miserably giving out sources without illegal intentions [1]. Might be they both use alike network address.

To arrange and better appreciate present malware recognition systems, classification based on more than one distinctiveness of the uncovering techniques needs to be discussed. Cloud computing issues are discussed from diverse perspectives. There are lots of challenges from cloud acceptance viewpoint [5]. There are security and privacy issues as well because the data in mobile environment broad cast. When we talk about the malware detection in Mobiles, the conventional discovery engines (antivirus) are not reasonable due to control consumptions limits. On the other hand when we employ the cloud based solution of the problems then there are security and isolation factors get occupied. It is really challenging job to detect the malware in mobile environments. Until a little part of malware is inside, its discovery remains uncertain [9].

Cloud computing issues are discussed from different perspectives. There are many challenges from cloud adoption perspective. Mobile Cloud Computing (MCC) has its own troubles. It is divided into two parts Mobile Communication issues and Computing issues. A few challenges are from Mobile Multimedia Database (MMMDB). Multimedia includes imagery, auditory and videotape etc. It require fast transfer rate for storing and big storage space and organization of data. There are possible hurdles in MCC [7], In MCC all three service models Software As A Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) are supported but until now due to inadequate storage, battery, computing power and display only SaaS model is implemented. Android platform is open source and well known so warmly welcomes the third party software, which is one of the biggest reasons of malware spreading.

In mobiles there is addition of several vectors of malware spreading, as Bluetooth, WI-Fi, SMS, MMS and infrared etc. and limitations as low bandwidth and battery. So there is need of clear understanding to research about handling of such kind of issues. So, the objective is to carry out research on security issues that are arising theses day in mobile cloud environment and enhance the methods to identify the malicious programs that may harmful for data over the mobile cloud computing. Along the way, we discuss various techniques which are currently implemented to handle these security issues highlighting their pros and cons through a comparative study. We identify the shortcoming in the existing techniques and propose an improved method to detect and resolve malicious security threats. We plan to simulate the newly proposed technique and record the outcomes for the comparative analysis with existing techniques.

There are two major issues concerned with the mobile cloud computing. First is owner of data has only partial control on the infrastructure of IT; so they have to set up a method to command the implementation of their security plans to make certain data discretion and reliability. Second one is cloud owners or service providers have extreme rights. This lets cloud owners to alter and control user's system and use their data.

Above discussed two issues led straightly to incredibly minor belief on the maintaining and forwarding information to the mobile cloud as compare to conservative structures where operators have a definite amount of privilege on fundamental structures. This effort attempts to inaugurate a method to discourse this matter by letting consumers to prevent from malicious programs while sharing and storing data over the mobile cloud. So we proposed and implement a technique to overcome these security issues.

2. MATERIAL AND METHODS

To arrange and better realize existing recognition systems, a classification base on the subsequent several distinctiveness of the detection techniques is discussed. And at the last but not least different comparisons of ant viruses and android platform based malware detection frameworks are discussed. When we talk about the malware uncovering in Mobile, the conventional discovery engines i-e antivirus are not reasonable due to power usage limits. When we employ the cloud based results there are privacy and safety factor caught up. To identify a malware is actually difficult in mobile environment.

Lots of advantages are provided by service and pervasive computing in cloud computing [14].Mie. Though siani presents the solution of security and privacy breeching. They created a privacy manager it manages user data and keeps it private on the clouds. For sake of its defense, it uses the feature known as obfuscation it implements privacy where it is needed.

Many medium and small size businesses use Pay As You Go model in which organizations don't have to worry about hardware maintenance. Database normally comes with high price of hardware and software both so data management applications are good applications for use in the clouds [20]. According to this research, cloud computing is suggestive of the database-as-a-service (DaaS) paradigms and application service provider (ASP) .

Another good technique presented by Bo peng[1]and Dean[15].which is in map reducing form and Tplatform form. It is used to generate and process large data sets. Map reduction technique is used for managing database in clouds with different mappers. A key value is generated by a map function and use to generate other key values and another function is reduce function which is use to combine all generated key values related to the main key. Using this model with user defined map function permits us to compute large data easily and for fault tolerance we can re-execute the function. By using this model mostly programmers processes large quantity of data, like crawled documents. In mobile atmosphere broadcasting there is also a privacy and security issue. There are possible barriers in Mobile Cloud Computing [17].

An obvious separation and associations concerning service-oriented architecture, Grid computing, Cloud computing, and pervasive computing is given by Tharam Dillon [16]. In his research he mentioned entire relative knowledge and he presented some challenges in the field of cloud computing. Several scheduling issues are addressed by Young Choon Lee, in his research he concluded profit driven requests of two sets. Algorithm with best result is implemented after comparison [13].

According to [21] security is a basic problem and it will be extreme important in the future. Users from different regions make use of the distributed computing more easily and efficiently. Now cloud computing is a new source distributed computing. Proofs of Reteriveablity (POR) make sure the security of outsourced data by Ari Juels et al. [22]. This model attains the security of file retrievability and identifies data changes. A different scheme of POR is introduced by Shacham et al. [23]. It makes countless queries with less operating cost for verifiability. A theoretical Scheme improves the SW and JK model which is proposed by Kennadi D et al. All these schemes are single server schemes and weak security schemes. Further a HAIL protocol was defined by Kennadi Brow et al. [11]. It achieves availability and veracity of users' data in clouds, it extends multiple server schemes but it does not Katter all the security issues.

Provable Data Possession (PDP) is defined by Ateniese et al. to attain data integrity of outsourced data. It does not provide security but it can detect corruption. Scalable Data Possession (SDP) is proposed by R.D. Pietro et al. [23]. This model covers all security problems in PDP but the drawback is that it works only with single server.

Cloud computing is a day by day growing term. It includes the whole thing that is done concerning internet. Its growing and specific description divert from the main idea. It's another name of dispersed computing that meant capability to execute a solo program on a lot of linked systems at the similar occasion. It is the exercise of utilizing distant systems (servers) which are linked on the internet to manage, store up and execute data rather than on a limited system. Usually Cloud computing is a huge dispersed communication system on the internet base servers.

There are 3 major service models. Platform as a Service, Software as a Service and Infrastructure as a Service. Public clouds are reachable to common community or a huge industrial group. Service models are shown in the figure 1 and layered wise distribution is shown in the figure 2.

"IaaS"
Infrastructure-as-a-Service
host
"PaaS"
Platform-as-a-Service
build
"SaaS"
Software-as-a-Service
consume

Figure 1: Service Model

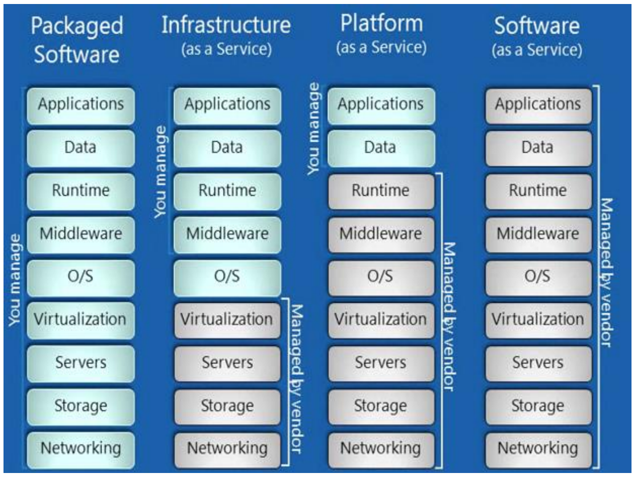


Figure-2: Layer wise Service Model

MCC is a mixture of cloud computing, Mobile computing and wireless network. MCC has turn into the latent platform for the mobile services and gorgeous user practice. In mobile cloud computing the processing and data is distant from the mobiles and shift on prevailing servers. Mobile cloud computing forum outlines it as "MCC talk about an structure where data processing and storage occurs exterior to the mobile phone device" [4]. Mobile cloud apps transfer the storage of data and computing power left from the mobile devices and put it into cloud, bring up Mobile cloud and applications to not only the Smart device user but to a larger collection of mobile users, by 2014 as per to the ABI research forecast there would be 1 billion users utilize cloud, some operators for example Orange, Verizon and Vodafone are in progress to present services of cloud computing for organization.

Mobile cloud computing common structural design is revealed in figure 3. Mobile phone devices are linked via base stations for example base transceiver position, satellite or entree point that first create and then control the link.

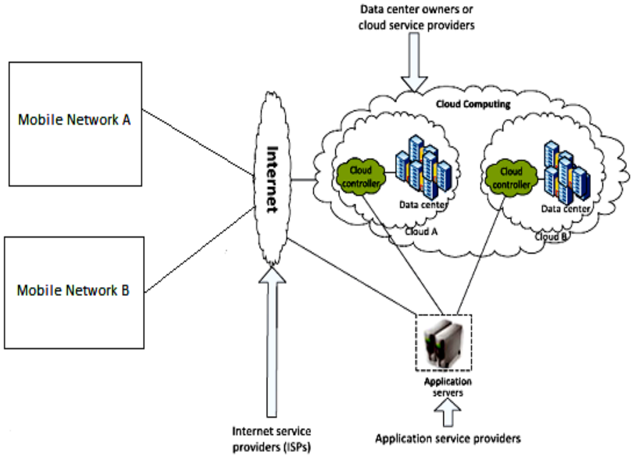


Figure-3: MCC Architecture

What features make a mobile phone smarts and greets malwares? Core variance between the terms 'Smart' and outdated 'Non-Smart' is the integration and welcome to the apps from third party from online marketplace. A vigorous aspect is participation of Cloud Computing that offers the liberty to device from storage and vigor limits. They both incline to uncertainty. In 2011 the consignment of worldwide mobiles is above 1.6 billion mobile devices (comprise of 472 smart mobile phones). As per the Nielsen analysis, between 2012 and 2013, only android IOS and OS rise 39 to 85 million [23]. Permission model for the main smart phone platform is given in the table1.

Table-1: Permission Models for the Major Smartphone Platform

Platform	Permissions	Control	Information	Interactivity
IOS	1	Low	Low	Low
Windows Mobile	15	Medium	Medium	Low
Black Berry OS	24	High	High	High
Android OS	75	Medium	High	Low

MCC issues = Mobile Communication issues + Computing issues

Android is permitted with adequate opportunity by the consumer. Due to its openness it is harmfully playing its role in malware phenomenon. We can see in Table 2 the detection rate of the most commonly used antivirus softwares. Here we can see that a comparison of detection rate is given w.r.t 3 months, 1 month and on weekly basis.

3. RESULTS AND DISCUSSIONS

When we talk about the malware recognition and handling in Mobiles, then the traditional antivirus softwares or other malware detection tools are not reasonable because of power consumptions restrictions. By using cloud based solution there are privacy and security issues get involved. Malware identification is certainly a challenging job in mobile atmosphere. Even if there is a tiny bit of malware its identification remains uncertain. Usually antivirus detects only 20-79 % of recognized viruses. AV-Test trainings completed with the limited set of data and indicate 90 % of

Table 2: Detection Rate of most popular Antivirus Soft wares

Antivirus Vencdo	Version	3 Months	1 Months	1 Week
Avast	4.8	63%	46%	40%
AVG	7.6	84%	79%	73%
BitDefender	7.2	84%	80%	79%
ClamAV	1.2	57%	49%	47%
CWSandbox	2.5	N/A	N/A	N/A
F-Port	6.4	71%	50%	46%
F-Secure	8.2	81%	75%	61%
Kaspersky	7.0.5	90%	84%	79%
Mcafee	8.5	71%	57%	54%
Norman	1.8	N/A	N/A	N/A
Symantec	15.0.0.65	61%	39%	43%
Trend MIcro	16.2	80%	75%	76%

the discovery percentage. Major security characteristics against the malwares in mobiles are application review, market level, remote management, platform level, application signing, permission, sandboxing and other security model.

Another way of malware characterization is defined in which classification is completed on the base of discovery dissimilar to the native classification on the base of spreading technique. It's not supportive only in improved knowledge of the malwares, furthermore it support to recognize where to find the malware. Cloud computing offers the service for storage to its users that can be accessed to a big capacity of storage. We can also share cloud data by other users with the condition that data transferring is accredited by cloud data holders. Picture of protected sharing by preventing from malicious programs and an unauthorized person over the cloud is described in the figure 4.

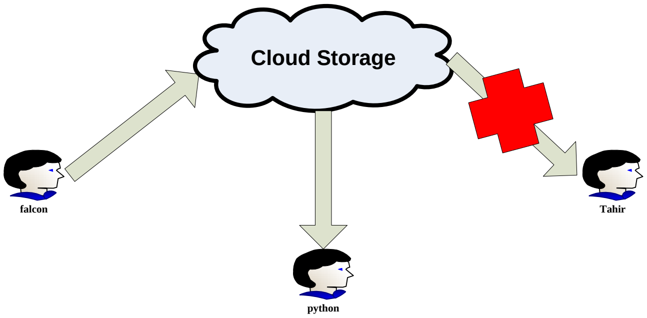


Figure-4: Secure Sharing Scenario on the Cloud

Falcon has some data that is retained on cloud. He wishes to send data to Python but at the same time he doesn't want Tahir to access this data. Tahir cannot reach to the data by snooping or obtaining authorized key of Python as the key is valid for Python only. We can summarize the definite security requirements as follows.

1) Data kept on mobile cloud must be stored safely. CSP offers storage facilities would not compromise on data confidentiality at any cost.

2) Data sharing can be attained after permission of the data owner. After getting permission, authorized users will be able to reach data stored over the cloud. However this permission and rights for accessing data would not give any right to cloud provider for data accessing.

3) When data owner gives you authorization then it would not be reassigned to anyone by authorization porter as the private key is only useful on the receiver machine. Those cloud users who do not have key, not capable to apply authorizations provided by owner of data for accessing data.

The challenge of requirements meeting in the overhead scenario is that protected data distribution demands to be attained under the mobile cloud computing atmosphere. It's essential that CSP supports to impose permission policy for accessing data but implementation would not disclose any kind of info to provider of cloud services. And it should not enable the cloud provider to have extreme rights so that it would be able to permit illegal access.

3.1 Design and Implementation of Malware Prevention Technique

This section presents a Malware Prevention Technique (MPT) that make it possible for data to be encrypted and compressed by utilizing various keys before sending on the cloud in a way that final data can be de compressed and decrypted by single key. Both encryption and decryption mechanisms are established on base of the RSA Encryption and the Elliptic Curve Cryptography techniques. Our MPT technique will work as below.

We assume that "U" is a set of users and "m" is a set of data. Such that For every $u_i \epsilon U$

u_i maintain a secret key k_i. Suppose 'q'is a randomly generated number which is accepted by all $u_i \epsilon U$. Then the encryption process is done in the sequence of $u_1, \ldots\ldots, u_N$. For $u_i \epsilon U$, it computes

$$m_i = m_{i-1} + qk_iG \tag{1}$$

Where $m_0 = m$

After while all $u \epsilon U$ will contribute in encryption procedure, then concluding encrypted data will be calculated as below.

$$\begin{aligned} m_e &= m_N && (2)\\ &= m_{N-1} + (qk_N G) && (3)\\ &= m_{N-t} + \sum_{i=N-t+1}^{N} (qk_i G) && (4)\\ &= m_0 + \sum_{i=1}^{N} (qk_i G) && (5)\\ &= m + \sum_{i=1}^{N} (qk_i G) && (6) \end{aligned}$$

Let $k_c = \sum_{i=1}^{N} k_i$, then m_e will be decrypted by a solitary operation as below.

$$\begin{aligned} m_p &= m_e - qk_c G && (7)\\ &= m_e - q\sum_{i=1}^{N} k_i G && (8)\\ &= m_e - \sum_{i=1}^{N} (qk_i G) && (9)\\ &= m && (10) \end{aligned}$$

With MPT technique, data will be compressed and encrypted several times by utilizing various keys, once by the owner itself and then during sharing data on the cloud. The last encryption creates a cipher text that could be decompressed and decrypted by utilizing a single key. To prevent data from malicious programs and for protected sharing of data on the cloud storage this technique is very helpful.

The step by step description of the technique is given in five steps as shown in the Figure 5.

1. Falcon encrypts and compresses the data and keeps it on a service delivered by the cloud provider.
2. While accessing data, Python directs a call to Falcon requesting for authorization to access data.
3. Falcon gives a permit to the cloud provider for the process of re encryption by sending encrypted data after compressing it.

4. At step 4 Falcon sends a permit for the Python to decompress and decrypt twicely encoded data with the private key.
5. Python gets re-encrypted data from cloud provider, decrypt and decompress it securely.

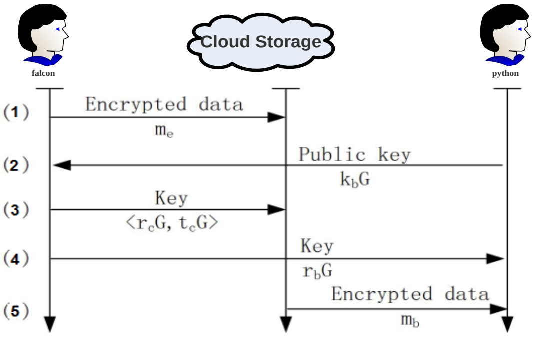


Figure -5: Secure Sharing over Cloud Storage

By supposing that

Falcon has	**Python has**
Private key = "k_a"	Private Key ="k_b
Public key ="k_aG",	Public key ="k_bG"

CSP has a shared public key "k_cG" and private key "k_c" with Falcon as

1) Falcon chose two numbers randomly such as 't' and 'r', and encodes "m", for example

$$m_e = m + rk_cG + tG \qquad (11)$$

Falcon compresses and saves the data in encrypted form "m_e" on the server.

2) Python requests to Falcon with the public key k_bG.

3) Falcon selects the random number r_c and r_b. Falcon calculates

$$t_cG = -r_bk_bG - r_ck_cG - rk_cG - tG \qquad (12)$$

4) Falcon sends (r_cG; t_cG) to cloud storage provider, and r_bG to Python.

5) Cloud storage provider will again encrypt the data m_e as below.

$$m_c = m_e + r_ck_cG + t_cG \qquad (13)$$

6) Python receives m_c from cloud storage provider and performs the calculation given below to produce m_b.

$$m_b = m_c + r_bk_bG \qquad (14)$$

The concluding text m_b produced by Python is in fact alike to m. It can be proofed as follow.

$$m_b = m_c + r_bk_bG \qquad (15)$$

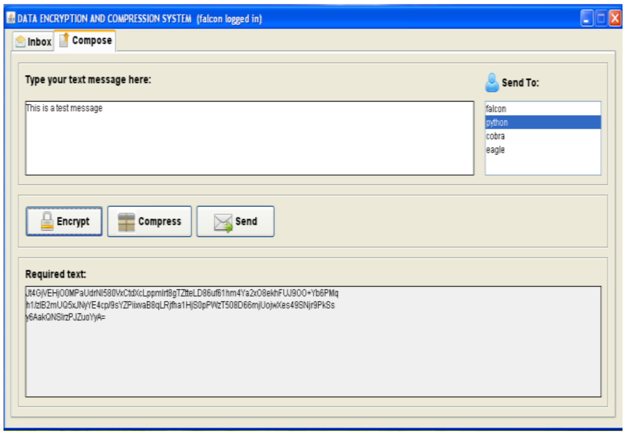
$$=(m_e + r_ck_cG + t_cG) + r_bk_bG \qquad (16)$$

$$=((m + rk_cG + tG) + r_ck_cG + (-r_bk_bG - r_ck_cG - rk_cG - tG)) + r_bk_bG \qquad (17)$$

$$=m \qquad (18)$$

The MPT technique allows secured transferring of data on the cloud storage. This data transferring is dependent on the access rights provided by the owner of the data and will not reveal any info to CSP. Implemetation details of the proposed idea is illustrated. we make a simulation of the proposed idea by using Netbeans and MS Access.

Encryption of text message "This is a test message" for user "python" is shown in the figure 6.



Type your text message here:

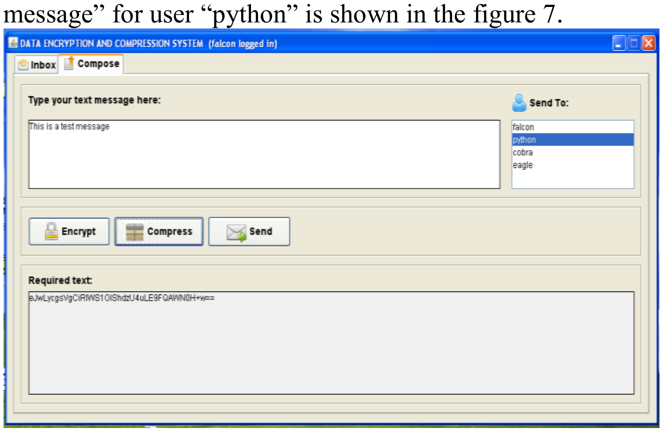
This is a test message

Required text:

```
Jt4GjVEHjO0MPaUdrNI580VxCtdXcLppmlrt8gTZtteLD86uf61hm4Ya2xO8ekhFUJ9OO+Yb6PMq
h1/zlB2mUQ5xJNyYE4cp/9sYZPiixvaB8qLRjfha1HjS0pPWzT508D66mjUojwXes49SNjr9PkSs
y6AakQNSlrzPJZuoYyA=
```

Figure -6: Encryption of Message

Compression of encrypted text message "This is a test message" for user "python" is shown in the figure 7.



Type your text message here:

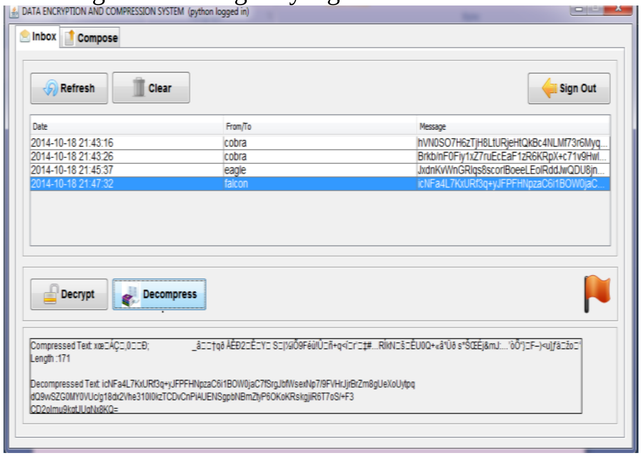
This is a test message

Required text:

```
eJwLycgsVgCiRlWS1OlShdzU4uLE9FQAWN0H+w==
```

Figure -7: Compression of Encrypted Message

Inbox view of a received message by user "python" from user "falcon" after decompression is shown in the figure 8. Green flag indicates digitally signed document.



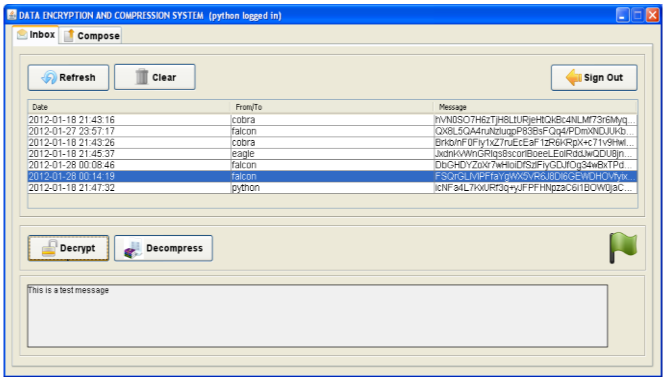
Date	From/To	Message
2014-10-18 21:43:16	cobra	hVN0SO7H6zTjH8LtURjeHtQkBc4NLMf73r6Myq...
2014-10-18 21:43:26	cobra	Brkb/nF0Fiy1xZ7ruEcEaF1zR6KRpX+c71v9Hwl...
2014-10-18 21:45:37	eagle	JxdnKvWnGRlqs8scorlBoeeLEolRddJwQDU8jn...
2014-10-18 21:47:32	falcon	icNFa4L7KxURf3q+yJFPFHNpzaC6i1BOW0jaC...

```
Compressed Text: xœ□ÂÇ□,0□□Ð;          _â□□†qð ÂÈÐ2□Ê□Y□ S□|½Õ9Féü!Û□ñ+q<Í□r□‡#...RlkN□š□ÊU0Q+«â'Üð s*ŠŒÉj&mJ:...'ôÕ'}□F–)<u]ƒä□žo□
Length :171

Decompressed Text: icNFa4L7KxURf3q+yJFPFHNpzaC6i1BOW0jaC7fSrgJbfWsexNp7/9FVHrJjrBrZm8gUeXoUytpq
dQ9wSZG0MY0VUc/g18dx2Vhe310I0kzTCDvCnPiAUENSgpbNBmZtyP6OKoKRskgjiR6T7oS/+F3
CD2olmu9kqtJUqNx8KQ=
```

Figure -8: Inbox View after decompression

Inbox view of a received message by user "python" from user "falcon" after decompression and decryption is shown in the figure 9.Green flag indicates digitally signed document



Date	From/To	Message
2012-01-18 21:43:16	cobra	hVN0SO7H6zTjH8LtURjeHtQkBc4NLMf73r6Myq...
2012-01-27 23:57:17	falcon	QX8L5QA4ruNzlugpP83BsFQq4/PDmXNDJUKb...
2012-01-18 21:43:26	cobra	Brkb/nF0Fiy1xZ7ruEcEaF1zR6KRpX+c71v9Hwl...
2012-01-18 21:45:37	eagle	JxdnKWnGRlqs8scorlBoeeLEolRddJwQDU8jn...
2012-01-28 00:08:46	falcon	DbGHDYZoXr7wHloiDfSzlFiyGDJfOg34wBxTPd...
2012-01-28 00:14:19	falcon	FSQrGLMPFfaYgWX5VR6J8DI6GEWDHOVfyix...
2012-01-18 21:47:32	python	icNFa4L7KxURf3q+yJFPFHNpzaC6i1BOW0jaC...

This is a test message

Figure -9: Inbox View after decompression and decryption

3.2 Analysis

Security occurrences to the offered technique contain retrieving data deprived of permission, revealing info throughout distribution, and sharing of information with others deprived of getting permission from the data owner.

The suggested secure sharing scheme approves users to get entree into data by allotting authorizations to only legal users. Dispensing of authorizations could be showed by owner of the data. Deprived of identifications, neither CSP nor the user will be able to get entrance into data. As contact to data rest on owner of data delivering of approval authorizations, however cloud server is uncontrollable by the owner of data and it's yet malevolent and not trustable; application of access control rule is definite.

Table -3: Comparison of MPT with other Security Management Techniques

Features	Credential Management	Adaptability	Expandability	Interoperabilit	Adoption to Security	Platform Indene pence	Identity Management	Attribute Management	Privilege Management	Digital Policy Management	IA Config. Management	Crypto Key Management	IA Meta Data Management	IA Audit Management
Security Providers														
CA-Enterprise IT management	0	10	10	10	10	10	10	10	10	10	0	0	0	10
Check point software Blades	0	10	10	10	10	10	10	0	0	10	10	0	0	10
CISCO security management suit	0	10	5	5	10	0	0	0	0	10	5	0	0	10
Evidian Identity & access management suit	10	10	10	10	10	10	10	5	10	10	0	5	0	5
IBM-Tivoli suit	0	10	10	10	10	10	10	10	10	10	10	10	0	10
NetIQ- Security and Contro management	0	10	10	5	10	0	0	0	0	0	0	0	0	10
Novell-Identity and Access management	0	10	10	10	10	5	10	10	10	10	0	0	0	10
Oracle-Identity and Access management	0	10	10	10	10	10	10	10	10	10	0	0	0	10
RSA-Security Suite	10	10	10	10	10	10	0	0	10	5	0	10	0	10
MTP	5	10	10	10	10	10	10	10	10	5	0	0	0	5
Symantec-Control suit	0	10	10	5	10	5	0	0	0	5	0	0	0	10

0 Not Support; 5 Partial Support; 10 Full Support

Line chart of the comparison is shown in the figure 10.

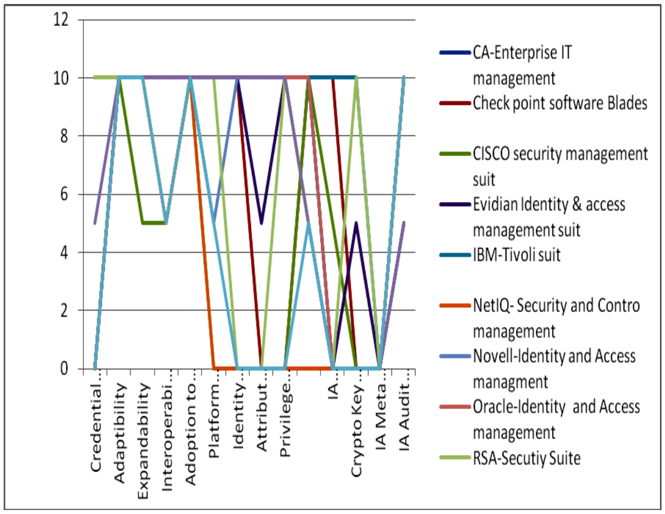


Figure -10: Comparisons Graph chart

Illegal entrance to data could be realized by two scenarios given below. Attacker demands a permit that can decrypt data with the assist of CSP. To get this permit, attacker should have the awareness of r_b, k_b, or the information of r_bk_bG. As r_b is deliver to Python in the shape of r_bG, it is not probable for the attacker to calculate r_b from r_bG. k_b is a furtive that is reserved in concealed by Python, for this reason the attacker cannot attain k_b. In short, it's not probable for the attacker to get permit that could decode data with assistance of CSP.

Throughout transferring of data it is forever in the encrypted shape, although at diverse phase it might be encoded with dissimilar keys. It's not a solitary phase that information is decoded in its obvious shape afore it is delivering to certified users. It will make sure that the entire process of transferring data will not reveal info to anybody. To obtain the data throughout sharing process attacker should contain a decryption key for me, mc or m_b. The Above conversation shows that attacker will not be able to decrypt me or m_b. For decrypting mc, the attacker wants the information of rckcG. As kc is the confidential secret reserved by the CSP, the attacker could be capable to compute rckcG from r_cG.

Comparison of MPT is given with other security management approaches in the table 3.

4. CONCLUSION AND FUTURE WORK

Mobile Cloud Computing inherits a few characteristics of clouds for the mobile services. MCC apps entail software that execute on mobile device and accomplish confident jobs for mobile phone user. Mobile cloud computing encompasses numerous research fields and subjects are discussed. Mobile banking device is getting famous now a days. It permits a customer to do business dealings over a mobile. In a cloud anti malware software, each node will execute a procedure to sense each runnable and dispatch it over cloud and execute it on the basis of outcomes resumed by cloud. There are numerous antivirus softwares on the cloud which are executed to sense malwares. We proposed and implement a technique to prevent from malicious programs on the cloud. We do comparative study of the developed technique with the other security techniques against different features and it shows more effectiveness against these techniques in prevention from the malicious programs.

MCC includes numerous fields of research. A few interesting research fields are engineering for Mobile Cloud Computing, Networking for MCC, Infrastructure for Mobile Cloud, Mobile Cyber Security in MCC and Green Computing in MCC. There are also some open research topics in malwares regarding MCC that we will consider in the future are malwares in other smart devices, Automatic malware analysis and classifications, trusted software and cooperative security for the smart devices.

REFERENCES

[1] T. Dillon, C. Wu and E. Chang, "Cloud Computing: Issues and Challenges", 2010 24th IEEE International Conference on Advanced Information Networking and Applications.(2010).

[2] Y. Chen, V, Paxson and R. H. Katz, "What’s New about Cloud Computing Security?” Electrical Engineering and Computer Sciences University of California, Technical Report No. UCB/EECS-2010,http://www.eecs.berkeley.edu/Pubs/TechRpt s/2010/EECS-2010-5.html, January 20, (2010).

[3] Khan and K. Ahirwar, "MOBILE CLOUD COMPUTING AS A FUTURE OF MOBILE MULTIMEDIA DATABASE", International Journal of Computer Science and Communication, Vol. **2**(1), 219-221 (2011).

[4] H. T. Dinh, C. Lee, D. Niyato and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches" RESEARCH ARTICLE, School of Computer Engineering, Nanyang Technological University (NTU), Singapore, Published online in Wiley Online Library (wileyonlinelibrary.com).DOI: 10.1002/wcm.(2013).

[5] H. Suo, Z. Liu, J. Wan and K. Zhou, "Security and Privacy in Mobile Cloud Computing", 978-1-4673-2480-9/13, IEEE, 655-659. (2013).

[6] R. S. Chang, J. Gao, V. Gruhn, J. He, G. Roussos and W. T. Tsai, "Mobile Cloud Computing Research – Issues, Challenges, and Needs", 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering,,442 453.(2013)

[7] D. Weerasinghe, V. Rakocevic, M. Rajarajan, "Security Framework for Mobile Banking", City University London, United Kingdom, MoMM Proceedings, 421-424 (2010).

[8] J. Oberheide, E. Cooke, F. Jahanian, "Rethinking Antivirus: Executable Analysis in the Network Cloud", Electrical Engineering and Computer Science Department, University of Michigan, Ann Arbor,MI48109.

[9] http://en.wikipedia.org/wiki/Antivirus_software, (2013).

[10] D. J. SanokJr, "An Analysis of How Antivirus Methodologies Are Utilized in Protecting Computers from Malicious Code", Kennesaw State University 1000 Chastain Road Kennesaw, GA 30144, USA 404-514- 9052, 142-144.(2013).

[11] G. Suarez-Tangil, J. E. Tapiador, P. P. Lopez and A. Ribagorda, "Evolution, Detection and Analysis of Malware for Smart Devices", IEEE COMMUNICATIONS SURVEYS & TUTORIALS,ACCEPTEDFOR PUBLICATION, (2013).

[12] M. Sikorski and A. Honig, "PRACTICAL MALWARE ANALYSIS - The Hands-On Guide to Dissecting Malicious Software", Publisher: William Pollock, (2012).

[13] J. Li, D. Gu, Y. Luo, "Android Malware Forensics: Reconstruction of Malicious Events", 32nd International Conference on Distributed Computing Systems Workshops, 552-558, (2012).

[14] K. Dunham, S. Abu-Nimeh, M. Becher, S. Fogie, B, Hernacki, J. A. Morales and C. Wright, "Moble Malware Attacks and Defence", PUBLISHED BY Syngress Publishing, Inc.Elsevier, Inc. 30 Corporate Drive Burlington, MA 01803, Copyright by Elsevier, Inc, (2009).

[15] "The Modern Malware Review", Palo Alto Networks™, Analysis of New and Evasive Malware in Live Enterprise Networks | 1st Edition, (2013).

[16] S. S. Qureshi, T. Ahmad, K. Rafique, S. islam, "MOBILE CLOUD COMPUTING AS FUTURE FOR MOBILE APPLICATIONS - IMPLEMENTATION METHODS AND CHALLENGING ISSUES", Proceedings of IEEE CCIS2011, 467-471, (2011).

[17] R. Hunt and S. Zeadally, "Network Forensics: An Analysis of Techniques, Tools, and Trends", the IEEE Computer Society, 36-43, (2012).

[18] E. Fernandes, B. Crispo, M. Conti, "FM 99.9, Radio Virus: Exploiting FM Radio Broadcasts for Malware Deployment", In (IEEE) Transactions on Information Forensics & Security, **8**(6): 1027-1037 (2013).

[19] V. Rastogi, Y. Chen and X. Jiangy, "DroidChameleon: Evaluating Android Anti-malware against Transformation Attacks", Information Forensics Security, IEEE Transactions on Volume:**9**(1), (2013).

[20] K. D. Bowers, A. Juels, and A. Oprea, “Proofs of Retrieve ability: Theory and Implementation,” Cryptology ePrint Archive, Report 2008/175, (2008) http://eprint.iacr.org/.

[21] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson,and D. Song, “Provable Data Possession at Untrusted Stores,” Proc. Of CCS ’07, pp. 598–609 (2007).

[22] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, “Scalable and Efficient Provable Data Possession,”Proc. Of Secure Comm ’08,1–10 (2008).

[23] Mowbray, M., Pearson, S.: A client-based privacy manager for cloud computing. In: COMSWARE 2009. ACM, New York, (2009).