ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 11(31), DOI: 10.17485/ijst/2018/v11i31/115060, August 2018*

Security Technique in Mobile Clouds to Ensure Malware Prevention

Abdul Shakoor, Adeel Ahmed and Muhammad Shahzad Sarfraz

Department of Computer Science, Faculty of C and IT, University of Gujrat, Pakistan;
shakoor009@yahoo.com,adeel.ahmed@uog.edu.pk, shahzad.sarfraz@uog.edu.pk

Abstract

Objectives: Major privacy issues in Mobile Cloud Computing (MCC) environment such as security of data are focused in this research. **Methods/Statistical Analysis:** Two major issues relating to the MCC, first issue is that the owners have no full control over the infra-structure. Therefore, they set up their own methods to control data security and make it reliable. Secondly, the cloud owners have maximum rights because cloud owners can change and manage the user's system and also make use of their data by implementing their rights. State the methodology adapted to meet your objectives. **Findings**: This study shows how data can be kept in confidentiality by maintaining necessary consistent relations in cloud. Prevention from Malware Technique is also being discussed that makes it probable for data to be compressed and encrypted by using a variety of keys prior to uploading on the cloud. It is uploaded in such a way that ending data could be decrypted and de compressed by a single key. **Application/Improvements:** The planed scheme empowers the user in performing utmost computation comprehensively and storage jobs which keep the users away from revealing the data guts and the personal/private information of users.

Keywords: Malware Prevention, Mobile Cloud, Security Technique, Threats

1. Introduction

The cloud computing gives benefits in the promotion of cost of investment, operating, computing and storage[1]. In some ways, cloud computing is considered a marketing umbrella which consists of utility computing, grid computing, distributed computing, Software As A Service (SAAS), Infrastructure As A Service (IAAS) and platform as a service (PAAS)[2]. Cloud computing facilitates in on call network approach to a common group of computing assets i.e. services, networks, applications, servers and storage. These can be swiftly released with little management exertion and interaction of cloud services provider[3].

Cloud service providers provide these services. All these topics have already covered lots of focus and many researchers conduct researches on it. In fact, lots of companies implement them. There are many other companies which are offering cloud computing services which are different from utility computing, grid computing, distributed computing. Somehow, they resemble but not completely. On clouds, when we use to send sensitive or private information, we strictly need some technique to protect our data. We need security for sending information between enterprise companies. Mobile computing, ubiquitous computing, pervasive computing, and dominant cloud computing are emerging areas in Information Technology. In June 2013, a new issue in news has been disclosed by Microsoft, Face book, Twitter and Google that FBI (Federal Bureau of Investigation) and NSA (National Security Agency) are demanding user's data from their servers. NSA and FBI are Sniffing data from

*Author for correspondence

servers on the name of criminal investigation. In this case, user's data and information is not secure[4]. In cloud computing fate sharing and multi-tenancy are the basic issues. Multi tenancy means that many users of cloud computing use the same storage devices, resources etc. This becomes the cause of two security issues. These security issues are regular resources the virtual data like physical machine is source of information observing passively or underground channels (transferring data aggressively)[5]. Other security issue is fate-sharing which an engineering design philosophy is where related parts of a system are yoked together, so that they either fail together or not at all. This can give harm to the position of good people by the people with illegal mind who are giving out the same sources. They could be using similar network address. In 2012 and 2013 android OS were focused, the selling IOS and android OS applications enhanced from thirty-eight to eighty-four millions. In 2011, the number of universal mobile is more than 1.6 billion devices.

For the better arrangement and appreciation of present malware recognition system, the classification which is related to more than one specialty of the visible techniques requires to be talked about. Issues of cloud computing may be discussed from different angles. Cloud acceptance view point demands many challenges[6]. Different comparative studies of antivirus and malware detection framework which are android platform based are discussed at the last but not least. There are certain securities and privacy issues exist when the mobile data is broad casted. In mobile when the malware detection is discussed, due to control uses limits the conventional discovering engines are not reasonable. On the other hand, during the employment of solution of problems, the security and isolation factor occupy. To detect the malware in mobile environment is a difficult and challenging task. Even a small part of malware is there, the discovery of its remains unsure[7].

2. Research Methodology

Till now cloud computing is not matured. Lots of issues are still associated with it. Here we shall discuss some of the significant issues linked with clouds. Main issues are security, confidentiality, integrity, availability and privacy; whereas Security is well-thought-out a main feature for cloud computing alliance as a strong and achievable multi-tenacity resolution[8]. Users view cloud as black box, they cannot view inside it, which keeps users away

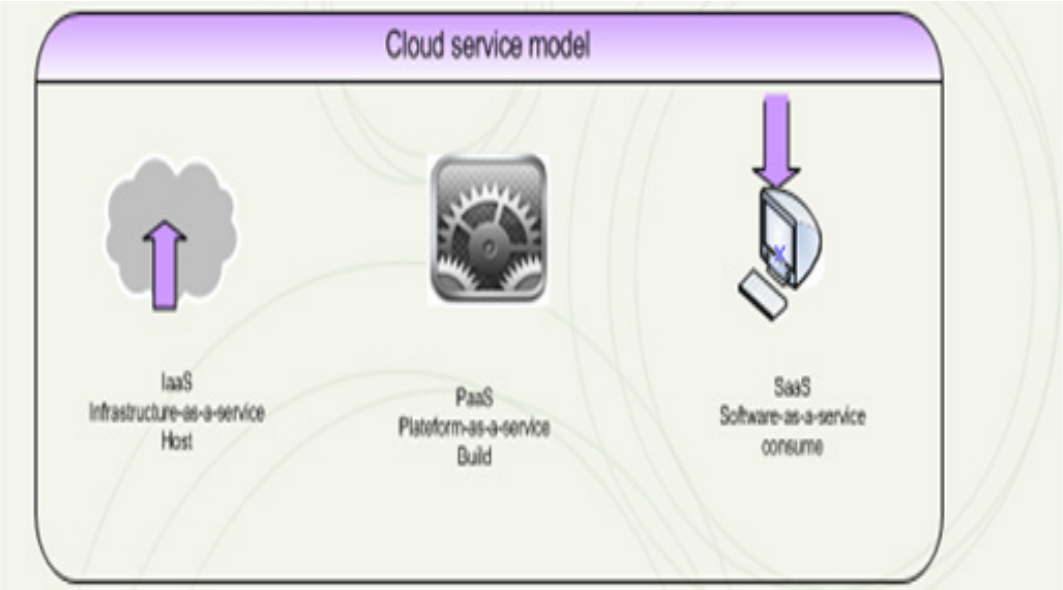

Figure 1. Cloud Service Models[12].

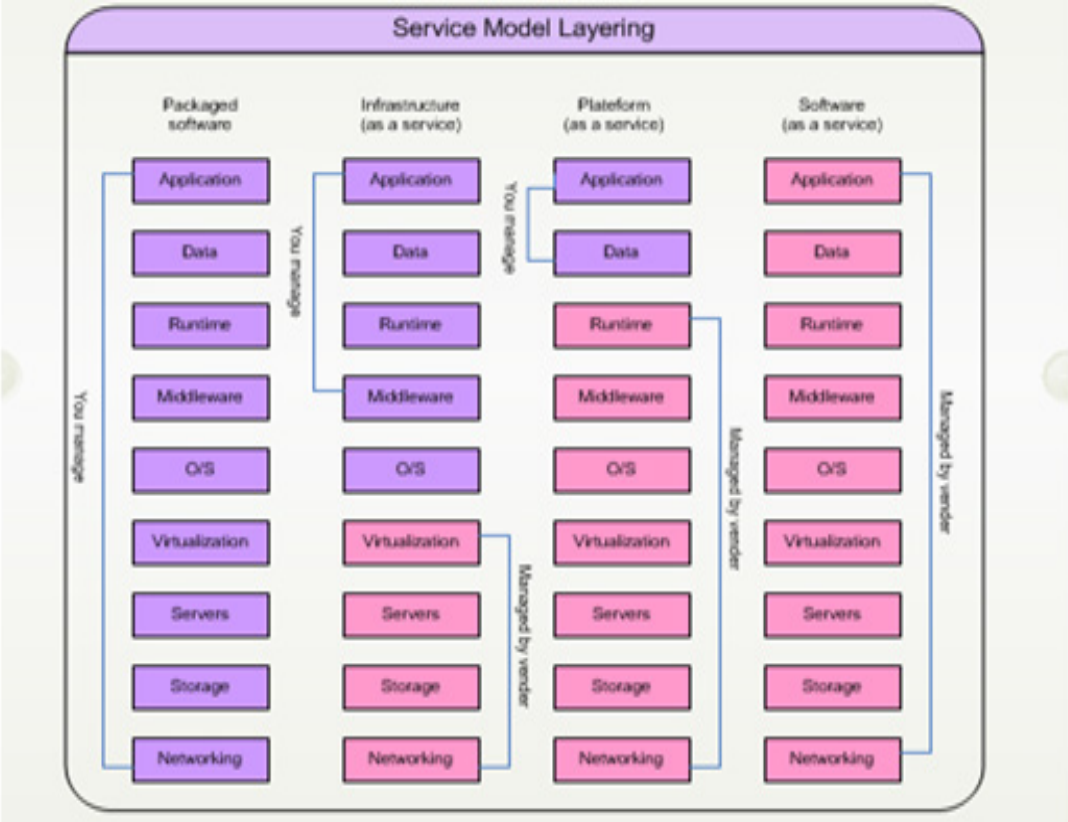

Figure 2. Service Model Layering12.

from clouds. This perspective is shared by university researchers, professionals[9] and government administrations. Zetta system provided by Zetta, its main task is to provide storage services[10]. Reliability and stability of data are of important concerns in cloud computing. This issue is covered mostly by making multiple instances of data, but there is still possibility that system could crash and companies could not be able to get their data[11]. Amazon S3 is an example of infrastructure which gives privacy and scalability[12]. Privacy is one of the big issue in cloud computing and many laws have been established for data protection but all are obsolete now. Now, new laws should be enforced for sake of privacy of user's data and there should be legal infrastructure for privacy. There are three service models which are given in Figure 1. Layered wise division is also given in Figure 2.

From security point of view, the greatest risk is data leakage[13]. Ownership of data and rights of data can be lost, when data has been lost or stolen from cloud servers therefore cloud users hesitate to put their data on cloud servers[14]. Many cloud service providers are trying to resolve this issue by writing strong agreements and by applying laws. In cloud computing making data backup for reliability purpose could be expensive. But data could be more expensive[15]. So normally cloud service provides make backup of data by applying redundant techniques and by making dumps of data on user side by users wish. But still users are worried about their data because it can be lost. Cloud computing still contains lot of issues but we are emphasizing on privacy and security of data on clouds. Protecting data from passive attacks is a type of privacy[16]. Architectural design of MCC is shown in Figure 3. Authentication procedures taken place here and request brought to cloud through internet and dealt with 17. Virtualization, utility computing and service oriented design are the three milestones of this facility. Service models of MCC are shown in Figure 4.

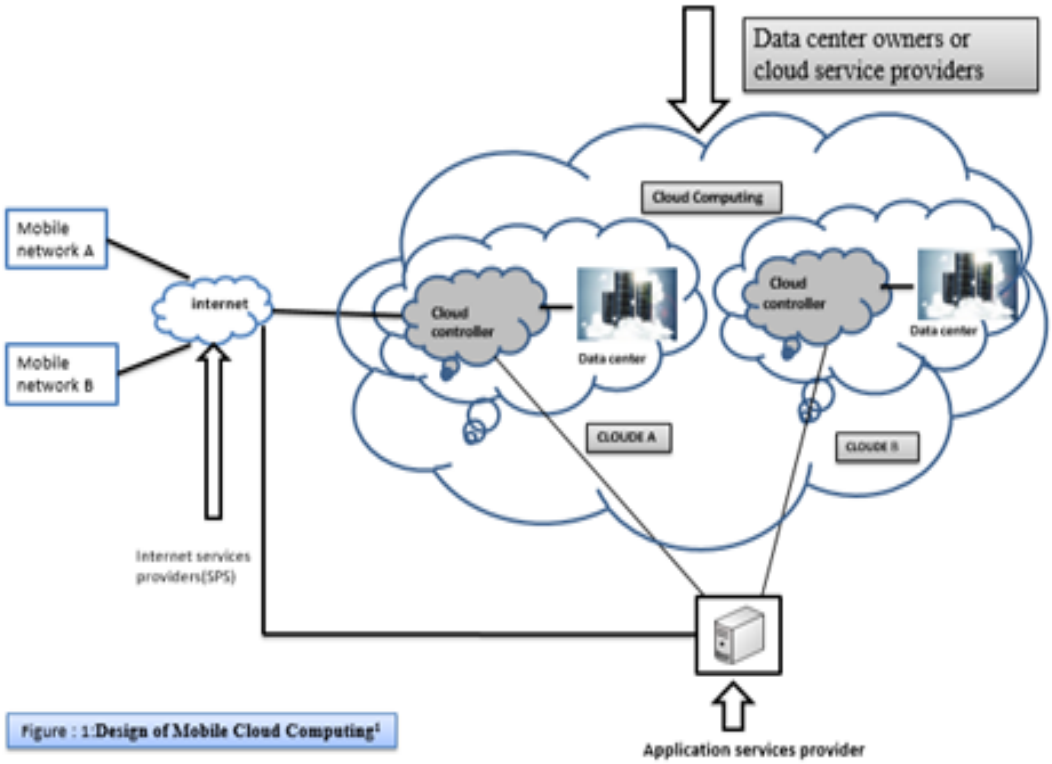

Figure 3. Design of Mobile Cloud Computing1.

Figure 4. Service Model of MCC1.

According to this model only the application configuration can be controlled by cloud user. For instance, Application programs as Amazon and Google is given in Figure 5.

In this model hosting environment will be handling by cloud's user. It also provides platform for application deployment and testing in simple and cost efficient way. Operating systems and middleware services are its

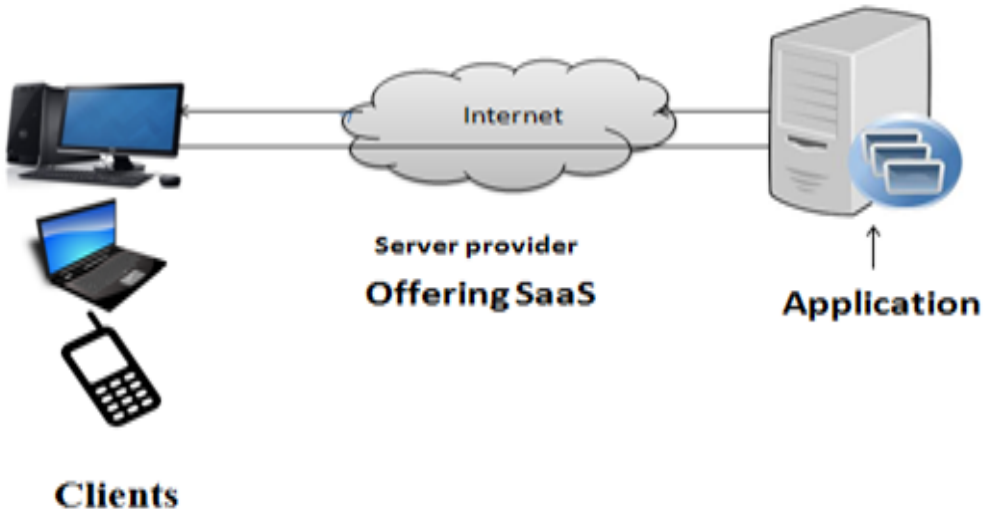

Figure 5. SaaS in Mobile Cloud Computing16.

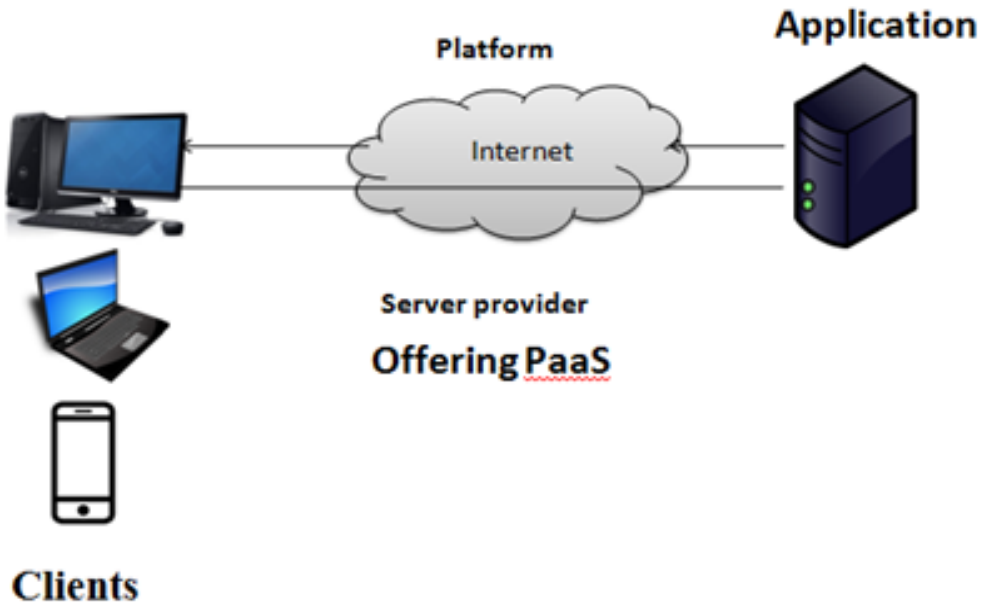

Figure 6. PAAS in Mobile Cloud Computing17.

examples shown in Figure 6. In this model all things are controlled by the user except data center infrastructure. It allows hardware, Servers, Storages and Network deliverance. Amazon elastic cloud computing is an example of IaaS. IaaS in Mobile Cloud Computing is shown in Figure 7.

Data center layer provides the infrastructure facility and hardware capabilities for cloud. These build with short occupied spaces, immense power reliability and small hard time risk. In mobile phones devices battery time is most vital. Some solutions to increase the battery life requires amendment in architecture or to add another hardware are in practice but not feasible. Off-load techniques may be used by flowing data and control to cloud. Moreover, many procedures are in trend to keep data local and which data move to cloud. Storage is a

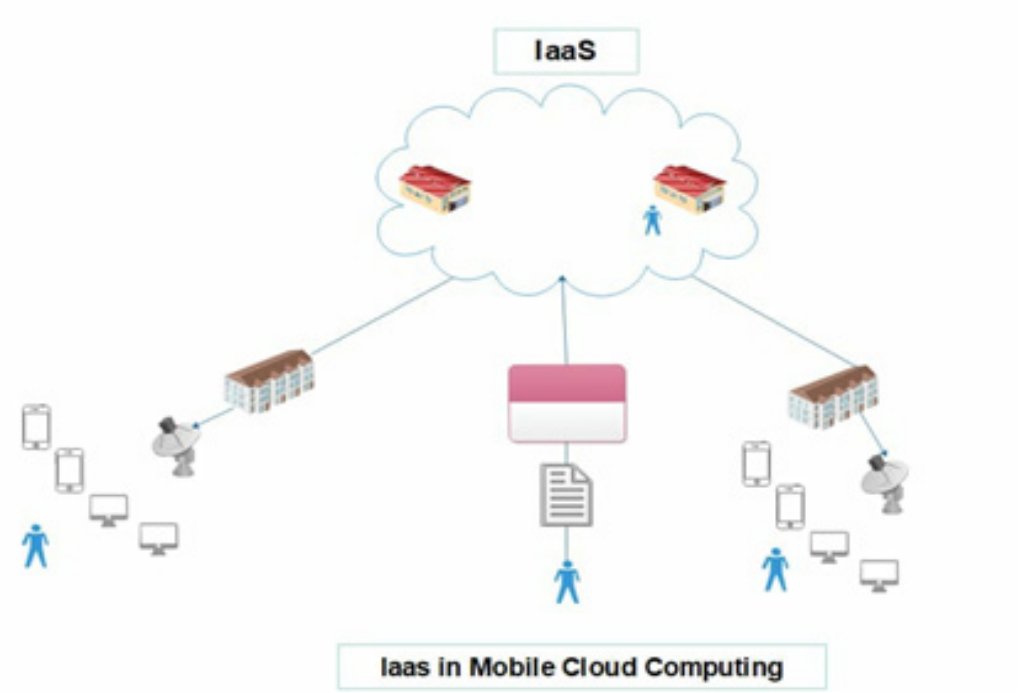

Figure 7. IaaS in Mobile Cloud Computing16.

grand restraint obstacle in mobile devices. MCC is helpful to user in shifting processing and data on cloud e.g. Amazon. In addition, user may share texts, images and videos over the media and through Flicker like applications. Because of the fact that applications and data are backup and stored on many computers under security observance, very small amount of assets i.e. smaller power and low price mobile devices to get required practices by users on mobile. Advantages of Mobile Cloud Computing are shown in Figure 8.

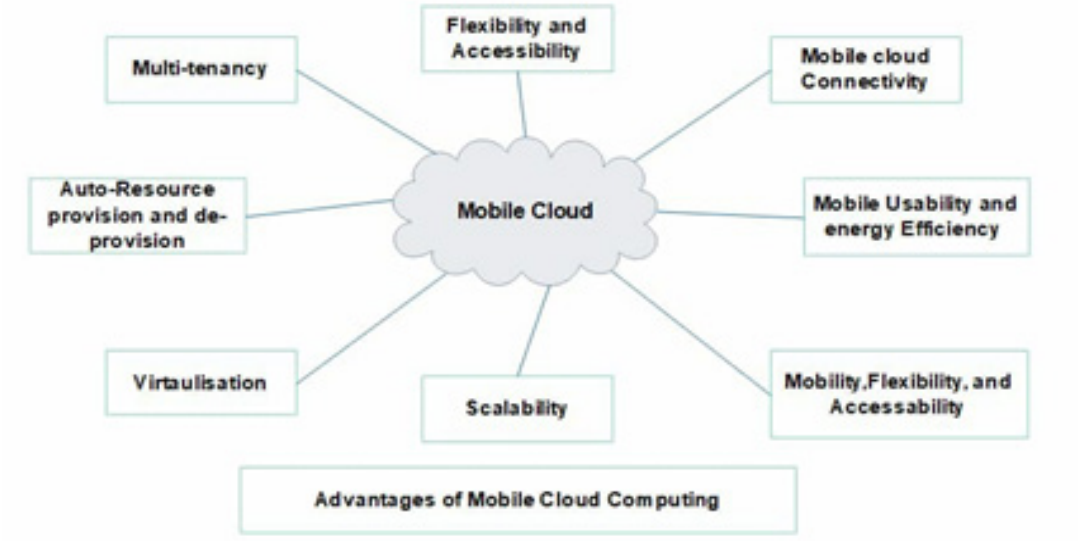

Figure 8. Advantages of Mobile Cloud Computing9.

Cloud users focus on the promise of the cloud service supplier concerning strength of their service in avoiding data from illegal entry within public surroundings[17]. Cloud service provider organizes clouds in such a manner that they can compensate, where ever it is possible. Cloud users establish a contract mostly with consideration to its physical verification. Both of the client and the cloud service provider share the accountability for protection. At present the major problem in cloud computing is security and privacy issues[16]. Mostly enterprises are deploying application on public, private and hybrid clouds. Private clouds are built especially for enterprises and for their applications to fulfill their security needs. Third parties keep up public clouds. Hybrid clouds are mixture of both public and private clouds. A new platform is launched by SUN, named as the Sun-Open-Cloud-Platform[18].

If a user is trying to get data at some new location, then he may compromise on his privacy. Organizations require new different ways to protect user data. A method is used for security is authentication techniques[19]. It works with secured credentials or username and passwords. Authorization, privacy and security are the major terms in cloud computing. Now a day's Risk management is attained by encryption of data[20,21]. While decrypting it, we ensure that certificate of authority is verified and the communication is totally safe. There is also self- repeating virus software, which is called Trojan virus. It only damages the computer after completely installing in your systems. Mobile database problems also exist there. Images, audio and video are the parts of multimedia. Multimedia database computing demands vast storage capacity, fast speed for the organization of data and transfer rate[22]. Privacy challenges along with security issue also exist within mobile atmosphere broadcasting. There are possible difficulties in MCC[19]. Discussion is made while concluding the several uniqueness of detection techniques as base, classification is made to arrange and understanding or realizing existing recognition systems in better way. Analysis of anti-viruses with Android based malware finding programs also talked about at the last but not least[23].

In mobile environment identifying a malware is a difficult job in fact. In cloud computing service and pervasive computing provides lots of advantages[24]. The solution is discussed by[25] in security and privacy breeching. They managed user data and also kept it private on clouds by creating a privacy manger. For the purpose of privacy and the sake of its defense, it uses obfuscation feature which implements the privacy when the need arises. Private data was to store in an encrypted form on cloud instead of data's normal form remained the focus[25]. Mostly "Pay as you go" cloud computing model is used by small and medium size businesses. This model eliminates the worry or hardware maintenance. Data management applications are the best solution in clouds to minimize or cover up the price factor of hardware and software attached with database[26].

The study also discusses the limitations of the data management issues installing and opportunities in the changing phases of the cloud computing. Rather than operative and transactional database systems, DSS[26], Large-scale, mission application specific data, data analysis and more for the benefits of cloud computing possibly provide than the transactional database. The main focus in this research is on these challenges. Map reducing form and T Platform is another efficient technique presented by [27,28]. This technique is used to process data sets in huge amount. By the use of this form with the user defined mapping enables us to calculate huge data simply and can re-execute the function for fault tolerance. Large quantity of the data like crawled documents are processed by programmers mostly by using this model. According to an extreme important and basic problem in future will be security. Due to the evaluation of electricity from last decade, large organizations have changed their focus on business rather than power generation for their business, easily switching to new and advanced working resources on network, and cloud computing as developing Information Technology. Security of outsourced data is made using Proofs Of Irretrievability (POR)[29]. This model (POR) achieves the file irretrievability security, also recognizes changes in data. A HetNet mobile cloud computing architecture that is different from traditional static cloud computing and existing mobile cloud computing was proposed. The new architecture consists of two layers, a GSC and an MDC[30,31]. Up till now the all

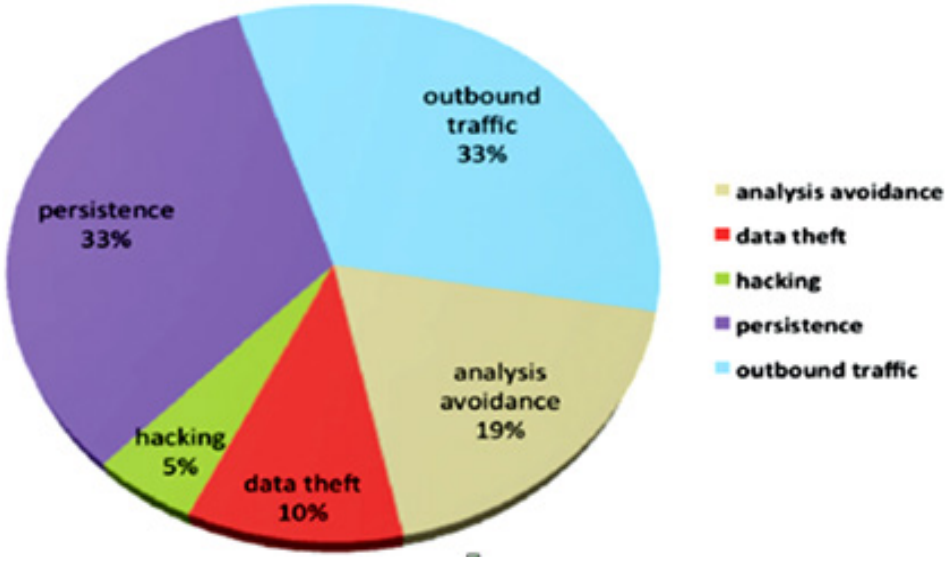

Figure 9. Usually experiential malware behaviors34.

Schemes are weak safety measures schemes and work as a single server. Gives definition of PDP (Provable Data Possession) to achieve data integrity of outsourced data. PDP can sense corruption but not gives safety. Planned Scalable Data Possession (SDP)[32]. SDP overcomes all safety issues in PDP but the problem is that it facilitates to one server. Through the web browsers 90% of unseen malwares were extended. Web is boundary line of challenge in conflict to anonymous malware. In the Figure 9 experiential malware behaviors are revealed. Antivirus can inspect that what a file will be carried out by running it in the sandbox. State cost on base of act execute by the

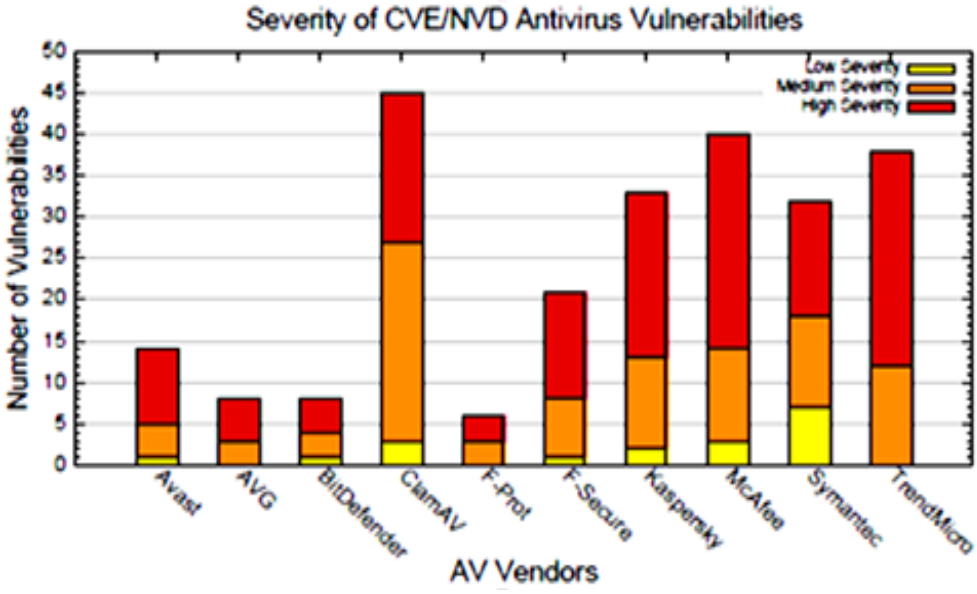

Figure 10. Detection Rate of each antivirus vendor35.

file. National Vulnerability Database counted some issue for ten antivirus vendors is shown in the Figure 10.

For the mobile workplace it's a technique for malware detection on cloud. It consists of many pay backs as enhanced detection method, power diminution of mobiles. It consists of a host agent and a network service may be having a few antivirus software, moreover they enlarge the finding means. Security can be considered as a big setback in mobile cloud computing point of view. When you move your record on other hard drives, it is not secure. Security could be a top rank issue in cloud implementation. It is possible to establish huge data center on very low cost to everyone. It can reduce overall infrastructure price but it can enlarge network price. If one requires different clouds in typical interfaces or API's in sequence to allot or insert different resources or data, according to the view point of the cloud provider, the flexible assets likewise multi-tenancy or virtualization make the charge investigation stronger than a distinctive data center. Further the virtual machine is a cost enhancing element. It is a dire demand from the cloud customer before shifting his central part of his organizational information over to the cloud to avail this facility. It needs high performance by the supplier[33].

2.1 Problem Statement

Many cloud users use the similar storage device, resources wirelessly it is called multi-tenancy. It may cause two security issues. Universal assets the virtual machine, data like physical machine is source of side channel (information observed passively) or dissident channels (flowing data aggressively). Other security issue is fate sharing which shows that parts are joined together and may or may not fail jointly. This can cause sabotage the position of good people unwontedly sharing the same resources with bad people as both are using the same network address.

There are two main issues relating to the MCC; first, the possessor has no full power infra-structure. Users only have limited rights to access and interpret his data stored on the cloud. There is no facility provided to secure the data rather than traditional security measures. Therefore, users need to set up their method to control to implement their own security plan to make data reliable. User needs to take measures to secure his data before uploading on the cloud. Second, the cloud owners have maximum rights because cloud owners can change and manage the user's system and also make use of their data by implementing their rights. So it reveals that cloud owner can access your personal data at any time and if you have not taken any measure to secure your data then you are at risk. These two issues give us a small belief on managing and sending data on mobile cloud as compared to old structures where the user privilege on fundamental structure. This can allow the consumer to avoid from wicked programs while storing and sharing data on mobile cloud. To solve these security flaws a technique is proposed that provides us the way to secure out data before uploading it on the cloud and that will be based on the security keys to pack and unpack the secured data on both ends i.e. sender and receiver.

3. Results and Discussions

Whenever in Mobiles we discuss regarding the Malware detection and management, then conventional anti viruses or further malware discovery tools are not practical due to the power consumptions limitations. By means of answers based on clouds there are securities and privacy problems are concerned. Recognition of malware is surely a demanding work in the mobile environment. If there is a small fragment of malware its recognition leftovers unsure. Typically, antivirus identifies only 21 to 80 percent of known viruses. AV-Test finished with restricted group of data and point to Ninety percent of detection proportion. Main Security distinctiveness beside viruses in the Mobiles is Apps evaluation, Remote Management. Other method of Malware classification is elaborated in which categorization is accomplished on foundation of detection unlike to local organization on stand of dispersal method. It is not helpful simply in enhanced facts of malwares, additionally it helps to be familiar with where discover malware. The service for storage to its users is offered by the cloud computing that could be reached to a large amount of storage space. Cloud data by other users

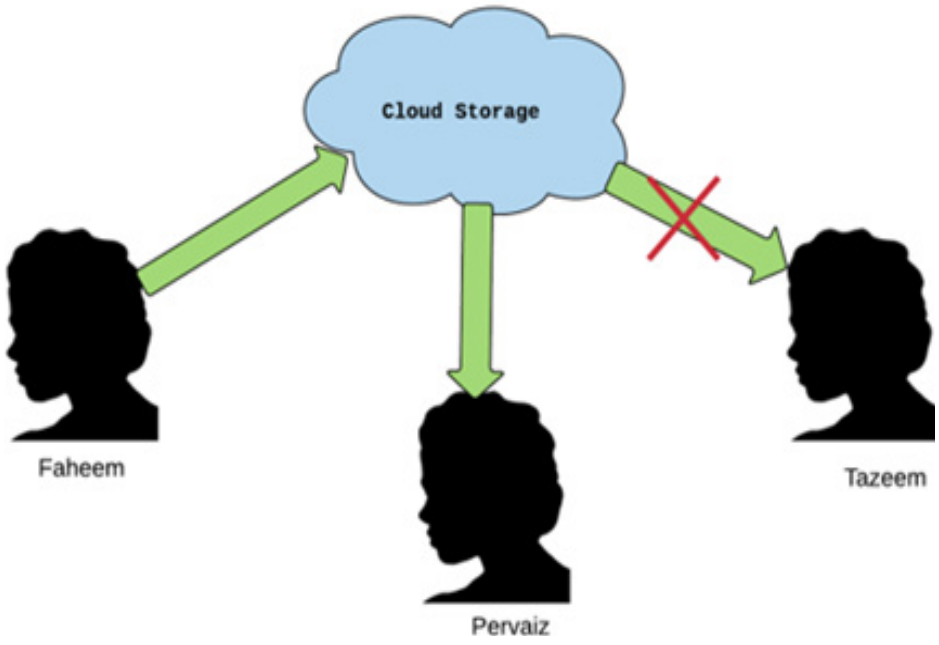

Figure 11. Secure Sharing using Cloud Computing.

can also be splitter by means of state that data transfer is credited by holder of data on cloud. Depiction of confined distribution by prevention from wicked software and an illegal person on cloud is shown in Figure 11.

Faheem has data which is stored on the cloud. He needs to dispatch data to Pervaiz however at similar occasion he does not wish for Tazeem to reach at the data. Tazeem cannot arrive at data by probing or getting authoritative 'key' of Pervaiz as 'key' is applicable only for Pervaiz. Specific security necessities can be summed up the as follows.

- Data should be stored securely which is placed on mobile cloud. Cloud Service Provider offers storage services will not conciliation on the data privacy at any price.

- Data sharing can be obtained subsequent to authorization of the owner of that data. When permission received, approved user would be capable to attain stored data on the cloud. Though this authorization and privileges for data access will not provide any privilege to the cloud provider for the access of data.

- When owner of data gives you permission then it will not be reused by anybody through permission porter because private key is functional only on recipient computer. Users of cloud, who does not encompass the key, will not able to be valid authentication given by data owner for access of data.

Requirements congregation challenge in the overhead circumstances is that secure data sharing burden to be attain beneath the MCC impression. It is necessary that Cloud Service Provider helps to oblige authorization strategy for data access however execution will not reveal any type of information to cloud services provider. Cloud provider should not allow having tremendous privileges so that it will be capable to allow prohibited entrance. Proposed solution is elaborated in the Figure 12.

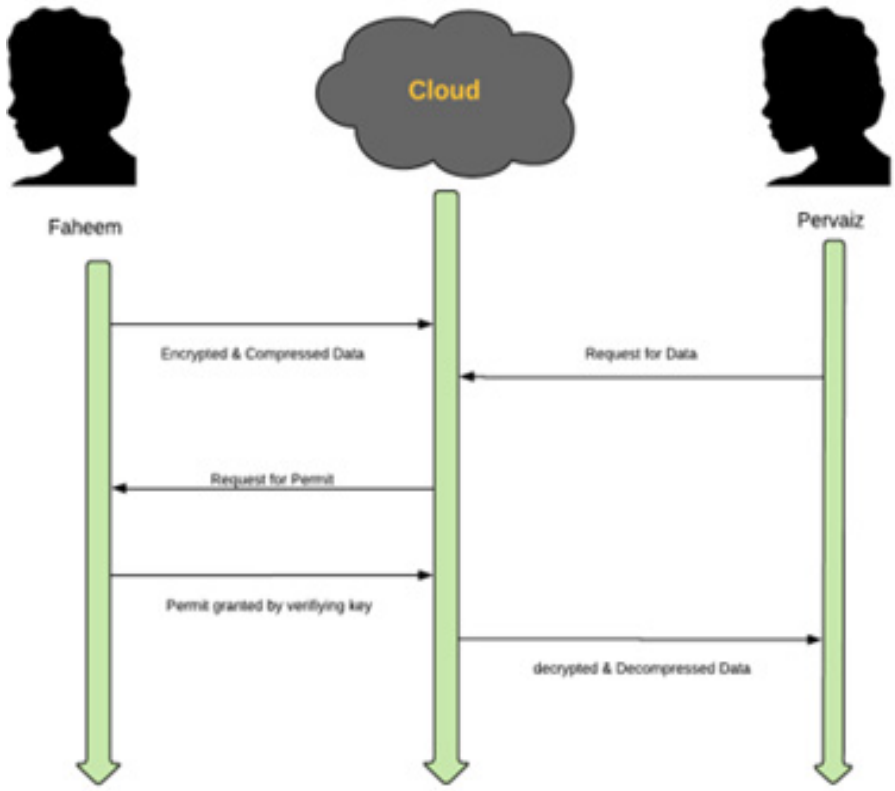

Figure 12. Sequence diagram of protected sharing.

3.1 Actual Working of the Technique

We discuss prevention from malware technique that makes it is probable for data to be compressed and encrypted by using a variety of keys prior to uploading on the cloud. It is uploaded in such a move that ending data could be decrypted and de compressed by a solo key. Encrypt and decrypt methods are recognized on basis of Elliptic Curve Cryptography and RSA Encryption. Our prevention technique will proceed as follow.

It is assumed that "V" is the group of users while "m" is the group of data.

For each $v_i \in V$, v_i keeps a hidden key named 'k_i'. Assume 'q'is a number that is created randomly and it is acknowledged by every $v_i \in V$. After this acknowledgment encryption procedure is finished in succession of $v_1 \ldots v_N$ where, 'G' is the general number. For $v_i \in V$, it calculates

$$\mathbf{m_i = m_{i-1} + qk_iG} \quad \textbf{(i)}$$

where, $m_0 = m$

Subsequent to that all $v \in V$ will donate in encrypt process, then final data in encryption form will be designed as under.

$$\mathbf{m_e = m_N} \quad \textbf{(ii)}$$

$$m_e = m_{N-1} + (qK_NG) \quad \text{(iii)}$$

$$= m_{N-t} + \sum_{i=N-t+1}^{N} (qK_iG) \quad \text{(iv)}$$

$$= m_0 + \sum_{i=1}^{N} (qK_iG) \quad \text{(v)}$$

$$= m + \sum_{i=1}^{N} (qK_iG) \quad \text{(vi)}$$

In equation (ii) m_e donates the encrypted data which is substituted with m_N. In equation (iii) we break the m_N data by value 1 and append a key combination with this data which is qk_NG. In equation (iv) we make the summation of the key combination and denote the 'm' data with m_{N-t} which is the one value subtracted from the original data m_N. In equation (v) we represent the data 'm' with the initial value 'm_0' and set the equation to the initial value "1" to the "N" and in equation (vi) we have substituted the "m_0" with the 'm'.

Let

$$\mathbf{k_c} = \sum_{i=1}^{N} K_i$$

Afterward m_e will be decrypted by a single process as under. Now we start the decryption process from equation (vii) where m_p denotes the decrypted data and it is calculated by subtracting the key combination from the encrypted data m_e. In equation (viii) we put the value of k_c and insert the summation value. Further in equation (ix) we apply the rule of multiplication and append 'q' within the summation. Ultimately we get the original encrypted value that was generated at the start of the encryption process.

$$\mathbf{m_p = m_e - qk_cG} \quad \textbf{(vii)}$$

$$= m_e - q\sum_{i=1}^{N} K_i G \quad \text{(viii)}$$

$$= m_e - \sum_{i=1}^{N} (qK_i G) \quad \text{(ix)}$$

$$= \mathbf{m} \ \textbf{(x)}$$

By using our prevention technique, data is compressed and encrypted numerous times by using a variety of keys, formerly by the owner and after that throughout distribution of data on cloud. The final encryptions create a code text that might be decompress and decrypt by using a solo key in. This technique is extremely supportive to secure data from malevolent software and for sheltered data distribution over cloud storage.

Complete procedure of this technique is specified in 5 major steps as given in Figure 4, 8.

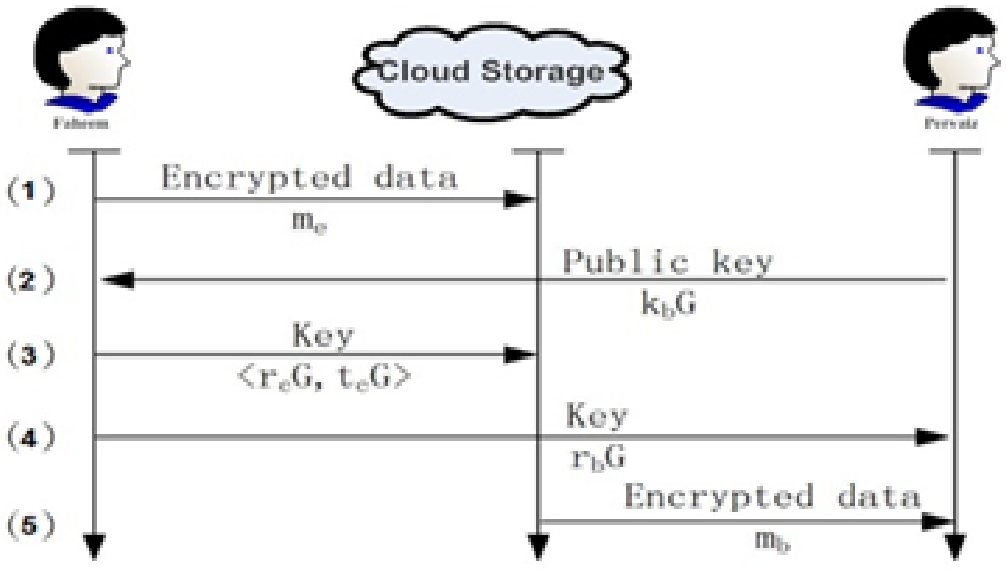

Figure 13. Protected sharing over cloud storage.

1. Faheem compresses and encrypts data and maintain it on service deliver by Cloud Service Provider (CSP).

2. Whenever needs to access data, Pervaiz forwards a call to Faheem and requests for permission to get data.

3. Faheem handover an authorization to the Cloud Provider (CP) for the course of re encrypts by transferring data in encrypt form subsequent to compression.

4. In step four Faheem dispatches an authorization for Pervaiz to decrypt and decompress doubly programmed data with help of private key.

5. Pervaiz get doubly encrypt data from the CP and decrypts and decompress it safely.

This protected sharing procedure in detail on the Cloud Storage is revealed in the Figure 13.

let suppose that Faheem has Private Key = "k_a" and Public key ="k_aG", Pervaiz has Private Key ="k_b" and Public key ="k_bG". Cloud Service Provider has a private key "k_c" and mutual public key "k_cG" with Faheem as

1. Faheem select 2 no's arbitrarily for example't' and 'r', and encoded "m", for instance

$$\mathbf{m_e = m + rk_cG + tG} \qquad \textbf{(xi)}$$

Faheem firstly compress and then save data in encrypted structure "m_e" on server.

2. With public key k_bG, Pervaiz send request to Faheem.

Table 1. Results of different attempts

Sr. No	Attempts	Success	Success Ratio	Failure	Failure Ratio	Time/Sec.
1	5	2	40	3	60	8.9×10^5
2	10	8	80	2	20	1.04×10^4
3	15	6	40	9	60	8.9×10^5
4	20	11	55	9	45	7.5×10^5
5	25	15	60	10	40	1.04×10^4
6	30	14	46.67	16	53.33	7.2×10^5
7	35	18	51.43	17	48.57	9.2×10^5
8	40	19	47.5	21	52.5	8.8×10^5
9	45	26	57.78	19	42.22	9.1×10^5
10	50	23	46	27	54	9.7×10^5

3. Faheem chooses the random number r_b and r_c. Faheem calculate

$$t_cG = -r_bk_bG - r_ck_cG - rk_cG - tG \quad \text{(xii)}$$

4. Faheem dispatch, r_bG to the Pervaiz and (r_cG; t_cG) to CSP.

5. CSP would once more encrypt data m_e as under.

$$m_c = m_e + r_ck_cG + t_cG \quad \text{(xiii)}$$

6. Pervaiz get m_c from the CSP and perform the computation provided underneath to make m_b.

$$m_b = m_c + r_bk_bG \quad \text{(xiv)}$$

Final text m_b shaped by Pervaiz is actually similar to m. which can be verified as below.

$$m_b = m_c + r_bk_bG \quad \text{(xv)}$$

$$= (m_e + r_ck_cG + t_cG) + r_bk_bG \quad \text{(xvi)}$$

$$= ((m + rk_cG + tG) + r_ck_cG + (-r_bk_bG - r_ck_cG - rk_cG - tG)) + r_bk_bG \quad \text{(xvii)}$$

$$= m \quad \text{(xviii)}$$

This prevention technique permits protected sharing of data over the cloud. Data transfer depends on accessibility privileges offered by possessor of data and would not disclose any information to Cloud Storage Provider. The proposed technique allows protected distribution of data store over the cloud. Data allocation is reliant on the admission privileges offered by data owner and would not disclose any information to the Cloud Service Provider. Implemetation particulars of our plan is described. By using MATLAB we develop a simulation of the planned idea. We have implemented the proposed technique by using the MATLAB simulation and recorded the results of different iterations. Following are the results taken during different iterations of the simulation. In Table 1 simulation results of different attempts are shown.

In Table 1 we have ten iterations and in each iteration numbers of attempts are varied. We note the success and failure rate of each attempt. In Figure 14 success ratio of different attempts is given which shows that how many

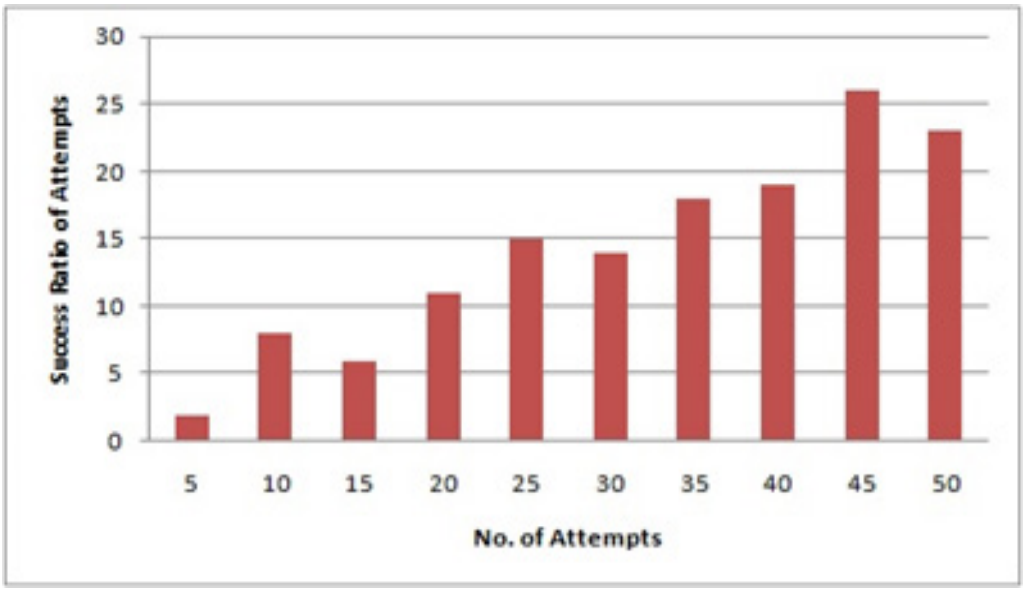

Figure 14. Success ratio of attempts.

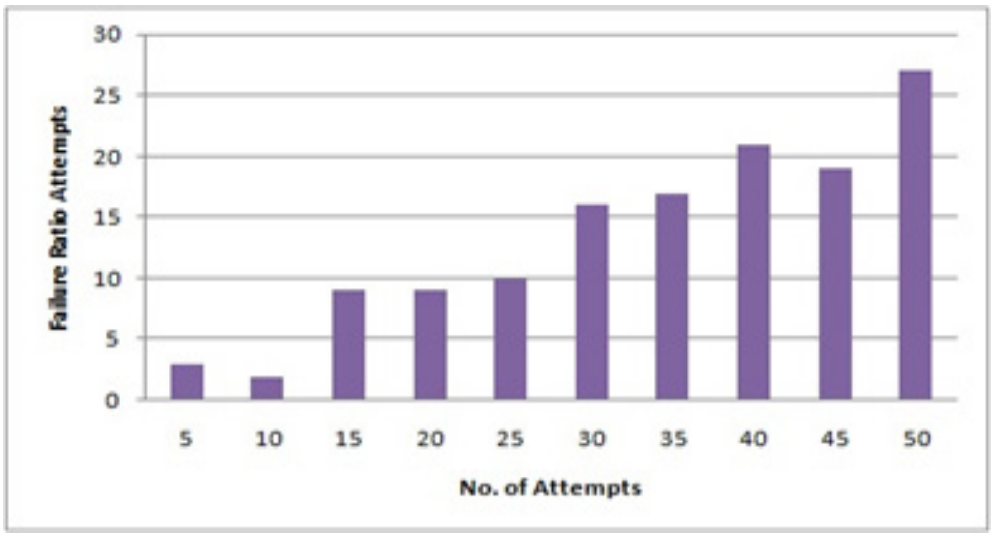

Figure 15. Failure ratio of attempts.

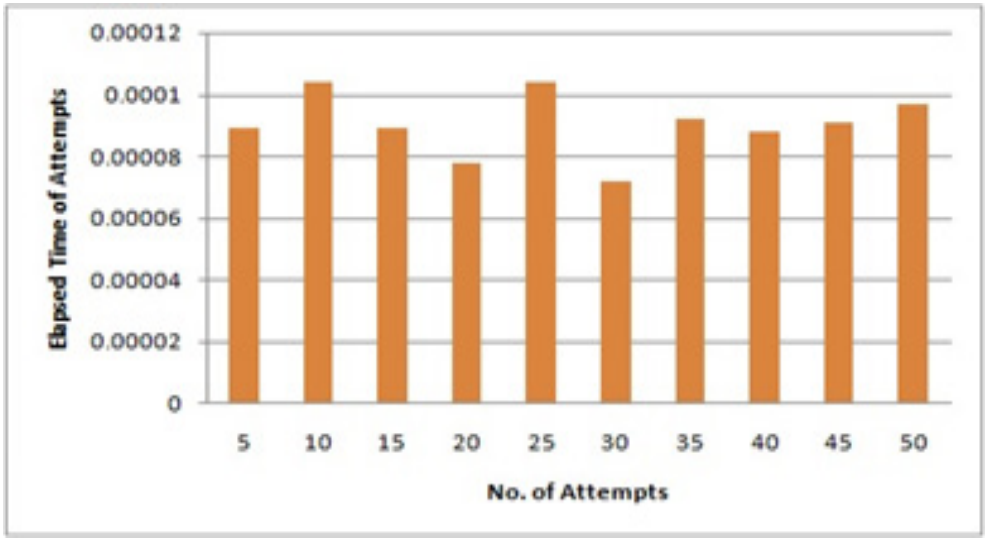

Figure 16. Elapsed time of attempts.

attempts were succeeded during the execution of the simulation. In Figure 15 failure ratios of different attempts is given which shows that how many attempts were failed during the execution of the simulation. It shows the unauthorized accesses and the prevention from those accesses. Ratio of each access is given in the Figure 15. During the execution of each iteration we measure the elapsed time of the iteration and calculate the average time of the elapsed time which is shown in the Figure 16. The elapsed time shows the execution performance of each iteration which is required to highlight the performance overhead.

3.2 Comparative Analysis

Security threats to our presented technique hold accessing data without authorization, illuminating information during sharing and distribution of data with others without receiving permit from the holder of data. We have sum-

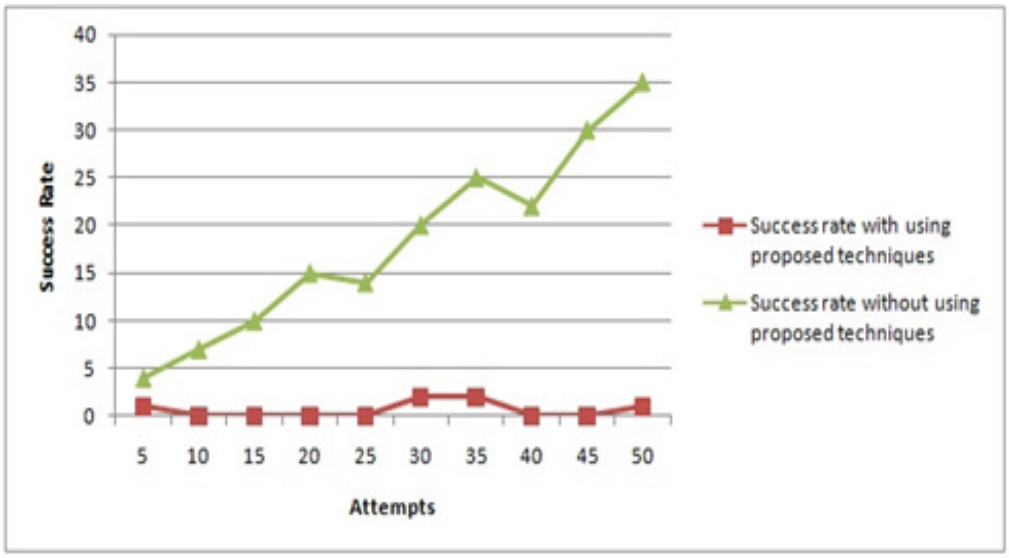

Figure 17. Graph comparison with and without using proposed technique.

marized a detailed comparison of our proposed technique with the conventional approach and list down the success ratio against un-authorized accessibility of data. Some exceptions in unauthorized attempts were got. When unauthorized attempts were made and compared, minor authorized attempts also included. In Table 2 we have

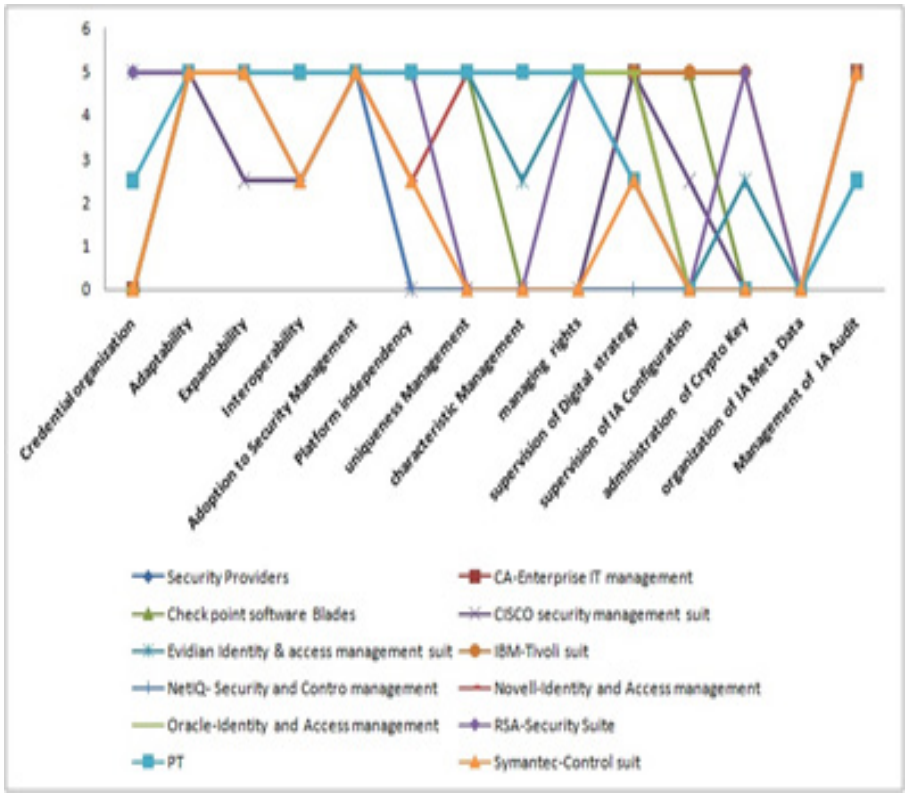

Figure 18. Comparisons chart of different techniques.

noted the number of unauthorized attempts and success rate with using technique and without using the technique. Graph of the comparison is shown in the Figures 17, 18. Proposed sharing method verifies users to acquire entry into the data by allot of authority to just authorized users. Provision of authorizations can be shown by data owner. Without identifications, neither Cloud Service Provider nor user would be capable to obtain entry into the data. Cloud server is unrestrained by data proprietor and it is so far malicious and not trustworthy; function of access management law is specific. Prohibited entry to data can be identified by two scenario specified beneath. Invader needs a consent that could decrypt the data by means of Cloud Service Provider. To obtain this authorization, attacker must contain the consciousness of k_b, r_b, or info of $r_b k_b G$. $r_b$is conveyed to Pervaiz in form of $r_b G$, it's not possible for invader to compute r_b from $r_b G$. k_b is a secret that is kept in hidden by Pervaiz, for this cause the attacker could not reach k_b. In brief, it is not possible for attacker to acquire authorize that can interpret data with help of Cloud Service Provider. During data transfer it's eternally in encrypted form, though at varied stage it may be encoded by means of different keys. It is not a retiring stage that info is decoded in its clear form before it is dispatching to proficient user. It is certified that the whole procedure of dispatching data would not disclose data to anyone. To get data during transferring procedure invader should include a decryption key for, m_b m_c or m_e. So far discussion reveals that attacker would not be talented to decrypt m_b or m_e. The attacker requires the info of $r_c k_c G$ for decrypting m_c. k_c is the secret info kept by Cloud Service Provider; invader will be able to calculate $r_c k_c G$ from the value of $r_c G$. In Table 3 comparison of Prevention Technique is given with other security techniques.

Table 2. Success rate with and without using technique

Sr. No	Unauthorized Attempts	Success Rate with using Proposed Technique	Success Rate without using Proposed Technique
1	5	1	4
2	10	0	7
3	15	0	10
4	20	0	15
5	25	0	14
6	30	2	20
7	35	2	25
8	40	0	22
9	45	0	30
10	50	1	35

Table 2 Continued

Attributes / Security Providers	Credential organization	Adaptability	Expandability	Interoperability	Adoption to Security Management	Platform Independency	Uniqueness Management	Characteristic Management	Managing Rights	Supervision of Digital strategy	Supervision of IA ConFig. ration	Administration of Crypto Key	Organization of IA Meta Data	Management of IA Audit
CA-Enterprise IT management	0	5	5	5	5	5	5	5	5	5	0	0	0	5
Check point software Blades	0	5	5	5	5	5	5	0	0	5	5	0	0	5
CISCO security management suit	0	5	2.5	2.5	5	0	0	0	0	5	2.5	0	0	5
Evidian Identity & access management suit	5	5	5	5	5	5	5	2.5	5	5	0	2.5	0	2.5
IBM-Tivoli suit	0	5	5	5	5	5	5	5	5	5	5	5	0	5
NetIQ- Security and Control management	0	5	5	2.5	5	0	0	0	0	0	0	0	0	5
Novell-Identity and Access management	0	5	5	5	5	2.5	5	5	5	5	0	0	0	5
Oracle-Identity and Access management	0	5	5	5	5	5	5	5	5	5	0	0	0	5
RSA-Security Suite	5	5	5	5	5	5	0	0	5	2.5	0	5	0	5
PT	2.5	5	5	5	5	5	5	5	5	2.5	0	0	0	2.5
Symantec-Control suit	0	5	5	2.5	5	2.5	0	0	0	2.5	0	0	0	5

Table 3. Assessment of prevention technique with other security method

0	Not Existed
2.5	Partially Existed
5	Fully Existed

4. Conclusion and Future Work

In this research a security technique has been proposed and implemented to save data from viruses and malicious programs over cloud. Proportional study of proposed method with other security techniques was conducted. This comparative study is about dissimilar features of the new and old techniques. The proposed new technique results show that it is more efficient than the old one in terms of safety from the malwares. Mobile cloud computing applications involve software that implements on mobile devices and achieves certain jobs for the users of mobile phones. There are many anti viruses on cloud which are implemented to intellect malwares. Now a day's Mobile Banking is becoming well-known. It allows a customer to carry out business transactions on the mobile from everywhere during 24 hours. In a cloud anti malware, every machine will implement a process to intellect every executable and transmits it on cloud and implement it on the base of outputs resume by cloud. We are unable to deploy this technique on a real cloud based environment it is suggested that this technique should be deployed at two different cloud based organizations and then issues and problems can be resolved in parallel. Our future plan is to explore mobile cloud computing in several areas of research including Infrastructure for Mobile Cloud, engineering for MCC, Networking for Mobile Cloud Computing, Green Computing and Mobile Cyber Security in Mobile Cloud Computing.

5. References

1. Hoang T, Chonho L, Dusit N. A survey of mobile cloud computing: architecture, applications, and approaches. Wireless communications and mobile computing. 2013; 13(18):1587–611. https://doi.org/10.1002/wcm.1203.
2. Fernando N, Seng W, Wenny R. Mobile cloud computing: A survey. Future Generation Computer Systems. 2013; 29(1):84–106. https://doi.org/10.1016/j.future.2012.05.023.
3. Dipali S. Yadav H, Kanchan D. Mobile cloud computing issues and solution framework. International Research Journal of Engineering and Technology. 2016; 3(11):1115–18.
4. Ahmed E. Seamless application execution in mobile cloud computing: Motivation, taxonomy, and open challenges. Journal of Network and Computer Applications. 2015; 52(1):154–72. https://doi.org/10.1016/j.jnca.2015.03.001.
5. Shiraz M, Abolfazli S, Abdul G. A study on virtual machine deployment for application outsourcing in mobile cloud computing. 2013; 63(1):946–64.
6. Abid S, Mureed H. Security issues and challenges of mobile cloud computing. International Journal of Grid and Distributed Computing. 2013; 6(6):37–50. https://doi.org/10.14257/ijgdc.2013.6.6.04.
7. Aminzadeh N, Zohreh S, Siti H. Mobile storage augmentation in mobile cloud computing: Taxonomy, approaches, and open issues. Simulation Modelling Practice and Theory. 2015; 50(1):96–108. https://doi.org/10.1016/j.simpat.2014.05.009.
8. Abolfazli S, Aasd E. Mobile cloud computing: The-state-of-the-art, challenges, and future research. Encyclopedia of Cloud Computing. 2015; 1(1):123–9.
9. Chang J, Gao V, Gruhn J, Roussos G. Mobile cloud computing research – issues, challenges, and needs. IEEE Seventh International Symposium on Service-Oriented System Engineering; 2013. p. 442–53. https://doi.org/10.1109/SOSE.2013.96.
10. Zetta. Zetta: Enterprise cloud storage on demand [Internet]. [cited 2008 Mar]. Available from: http://www.zetta.net/.
11. Wang X. Mobile cloud computing in 5g: Emerging trends, issues, and challenges. IEEE Network. 2015; 29(2):1234–40. https://doi.org/10.1109/MNET.2015.7064896.
12. Ali M, Samee U, Vasilakos AV. Security in cloud computing: Opportunities and challenges. Information Sciences. 2015; 30(5):357–83. https://doi.org/10.1016/j.ins.2015.01.025.
13. Liu J. Application partitioning algorithms in mobile cloud computing: Taxonomy, review and future directions. Journal of Network and Computer Applications. 2015; 48(1):99–117. https://doi.org/10.1016/j.jnca.2014.09.009.
14. Shant D, Pinku S. Computation offloading frameworks in mobile cloud computing: A survey. IEEE International Conference on Current Trends in Advanced Computing (ICCTAC); 2016. p. 123–30.
15. Sujithra M, Sathya N. Mobile device data security: A cryptographic approach by outsourcing mobile data to cloud.

Procedia Computer Science. 2015; 47(1):480–5. https://doi.org/10.1016/j.procs.2015.03.232.
16. Anirudh P, Mohammad S, Mais N. Survey on three components of Mobile Cloud Computing: offloading, distribution and privacy. Scientific Research an Academic Publisher. 2017; 5(6):4236–43.
17. Nurmi D, Wolski R, Grzegorczyk C, Obertelli G, Soman S, Youseff L, Zagorodnov D. The eucalyptus open-source cloud-computing system. 9th IEEE/ACM International Symposium on Cluster Computing and the Grid; 2009. p.124–31. https://doi.org/10.1109/CCGRID.2009.93
18. Sun Microsystems Unveils Open Cloud Platform [Internet]. [cited 2009 Mar 18]. Available from: https://www.businesswire.com/news/home/20090318005374/en/Sun-Microsystems-Unveils-Open-Cloud-Platform. Date accessed: 18/03/2009.
19. Dipayan D, Krishna L. A review and research towards mobile cloud computing. 2nd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering; 2014. p. 1–5.
20. Mascolo C. The power of mobile computing in a social era. IEEE Internet Computing. 2010; 14(6):76–9. https://doi.org/10.1109/MIC.2010.150
21. Fernandes E, Crispo B, Conti M. FM 99.9, Radio Virus: Exploiting FM radio broadcasts for malware deployment. IEEE Transactions on Information Forensics & Security. 2013; 8(6):1027–37. https://doi.org/10.1109/TIFS.2013.2259818.
22. Xing T, Huang D, Ata S, Medhi D. Mobicloud: A geo-distributed mobile cloud computing platform. Network and Service Management (CNSM). 8th International Conference on Network and Service Management (CNSM) and, Workshop on Systems Virtualiztion Management (SVM); 2012. p. 164–8.
23. Li J, Gu D, Luo Y. Android Malware Forensics: Reconstruction of malicious events. 32nd International Conference on Distributed Computing Systems Workshops. 2012, pp. 552-558. https://doi.org/10.1109/ICDCSW.2012.33.
24. Lijun M, Chan K, Tse H. A tale of clouds: Paradigm comparisons and some thoughts on research issues. IEEE Asia-Pacific Services Computing Conference; 2008. p. 464–9.
25. Siani P, Yun S, Miranda M. A privacy manager for cloud computing. HP Labs. Long Down Avenue, Stoke Gifford, Bristol BS34 8QZ, UK; 2009. p. 90–106.
26. Rastogi V, Chen Y, Jiangy X. DroidChameleon: Evaluating android anti-malware against transformation attacks. Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security; 2013. p. 329–34. https://doi.org/10.1145/2484313.2484355.
27. Jeffrey D, Sanjay G. MapReduce: A flexible data processing tool. Communications of the ACM. 2010; 53(1): 12–19.
28. Bo P, Bin C, Xiaoming L. Implementation issues of a cloud computing platform. Bulletin of the IEEE Computer Society Technical Committee on Data Engineering. 2009; 8:59–66.
29. Jiawei Y, Shucheng Y. Proofs of retrievability with public verifiability and constant communication cost in cloud. Cloud Computing. 2013; 4(2):1234–50.
30. Jo M. Device-to-device-based heterogeneous radio access network architecture for mobile cloud computing. IEEE Wireless Communications. 2015; 22(3):50–8. https://doi.org/10.1109/MWC.2015.7143326.
31. Satyanarayanan M, Bahl P, Caceres R, Davies N. The case for VM-based cloudlets in mobile computing. IEEE Pervasive Computing. 2009; 8(4):14–23. https://doi.org/10.1109/MPRV.2009.82.
32. Giuseppe A, Roberto D. Scalable and efficient provable data possession; 2008. p. 1–11.
33. Shiraz M and Gani A. Mobile cloud computing: Critical analysis of application deployment in virtual machines. Proceedings, International Conference Information and Computer Networks (ICICN'12). 2012; 27(1):123–30.
34. Sikorski M, Honig A. Practical Malware Analysis - The hands-on guide to dissecting malicious software; 2012.
35. Jon O, Evan C, Farnam J. CloudAV: N-version antivirus in the network cloud. Proceedings of the USENIX security symposium; 2008. PMCid:PMC3131111