Analysis of Mobile Techniques For Protection Of Data in Cloud Computing

Manik Kapoor[1]
Student
Amity University, Greater Noida
Uttar Pradesh , India – 201308

B.M. Sahoo[2]
Assistant Professor
Amity University, Greater Noida
Uttar Pradesh, India - 201308

Abstract : Along side the explosive boom of the cellular programs and up-raising cloud computing idea, cellular cloud computing seems to be a brand new capability technology for cell services. cellular cloud computing maps cloud computing ideas on top of the cellular surroundings, and overcomes boundaries that cope with performance (i.e. battery existence, CPU, garage, and bandwidth), environment (i.e. heterogeneity, scalability, availability) and security (i.e. reliability, privateness) mentioned in cell computing. in this function paper we're going to cognizance in depth on a Hadoop based totally framework for ad-hoc cell cloud computing – we specially confer with a research paper and the authors' choice to use and port Hadoop to build a digital Cloud Computing provider for cell devices. in the starting, we are going to define a quick creation and enumerate the demanding situations that we face imposing a framework for cell cloud computing. We finish this paper with a short example of other Map-lessen based totally MCC (mobile Cloud Computing) framework, which achieved higher performance using its personal custom implementation.

Keywords : Caching and Prefetching, QCMC,BB84 Protocol , Smart Load Balancing, Cloudlet, homomorphic code-based hash function, cloud storage

1. INTRODUCTION

The framework of Cloud Computing is many of the most relevant and efficient strategies in contemporary age of computing. The efficiency of cloud computing may be envisioned with the growth in the customers and additionally growing service carriers and operators.

The numerous techniques of implementation of cloud computing which offer severa strategies with

application with appreciate to actual world occasions. Cloud Computing is a completely unique technology which can be used to provide separate IT answers with an unequalled performance. Implementation of cloud related answer may be seen in 3 approaches :

- SOFTWARE USED AS A SOFTWARE(SAAS)
- PLATFORM USED AS A SOFTWARE (PAAS)
- INFRASTRUCTURE USED AS AN SOFTWARE (IAAS)

In the usage of software program mainly as utility version, cloud service vendors offer their offerings remotely with the assist of internet browser. Saas is owned and operated by means of others and customers may should installation , replace or maintain the software. The facts in Saas is stored in cloud so the facts is not completely lost. In Platform as a carrier the website hosting business enterprise may additionally offer the offerings by using constructing the complete surroundings required to assist functionality of web primarily based packages barring the requirement of buying and hidden hardware, software program facility as well as web hosting. This reduces middle complexity , the point of interest of developer shifts from maintaining the right surroundings required for the development of net packages. In Infrastructure used as service, the service provider bids offerings, considers payment as consistent with usage of existing centers. The maximum used model is IAAS due to the fact it's miles flexible and is fee efficient and innovative services also are available on call for. The Implementation of these provider models provided can be completed with the assist of 3 most important variations of deployment fashions that are :

- PUBLICLY FUNCTIONING CLOUD
- PRIVATELY FUNCTIONING CLOUD
- HYBRID FUNCTIONING CLOUD

Publicly rendered operated clouds are typically maintained by means of businesses that offer ready access to a publicly used network with affordable and worthwhile computing services. In offerings which are regulated as publicly controlled cloud utilities, clients may not want to lend in software hardware or any event that may be labeled into supporting framework at that given point of time, whose is ownership belongs to providers. high capabilities of public cloud are that it may provide a durable IAAS to shop and compute strategies in a short time frame. robust PAAS application improvement and deployment for cloud helping programs and innovative SAAS for small enterprise programs.

A personal cloud is an infrastructure maintained handiest for functions of a unit business enterprise, whether controlled by themselves or in accordance with a random service providing firm, and hosted for both internal or outside use. non-public clouds can gain the most top of the line advantage of cloud, at the same time as giving greater authority of assets at the same time as giving rest from multi-tenancy. non-public clouds additionally offer sure stage of abstraction to hold the statistics integrity when used garage as a provider. A self served interface might also manipulate carrier, additionally permit organisation team of workers to earmark and hand-over required IT resources in very brief period of time. massively automatic usage control of resources combines the entirety from relative computing capacity to facts garage.

standard safety parameters and gadget crafted for client's unique wishes a hybrid cloud uses both publically yet privately functioning attributes. In exercise, a privately operated cloud can't characteristic entirely with the final of the hosts resources and with publicly operating cloud. Many tech- giants with privately utilized clouds are evolving and are prepares to manipulate traffic across data storing places, the mixture of private public clouds—consequently main growing hybrid clouds. The Cloud of Hybrid nature lets in companies to keep the critical applications and inclined facts in a designated facts center like environment or a privately used cloud. Hybrid cloud ensures mobility of information, internet-apps and required offerings and more preference in phrases of deployment fashions.

The want of protection is requisite in the area of cloud computing with implementation growing invariably due to it's subsequent era architecture.

The latest assault on cloud offerings rendered by way of Tech-giant Apple leaked the non-public pics and breaches the confidentiality of many celebrities in hollywood in 2014.

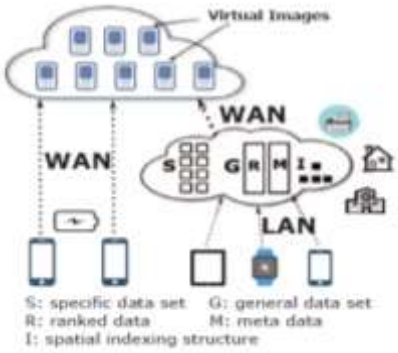
whilst the assault on Yahoo! in 2014 become more treacherous in nature because the impact of the assault turned into realised at a later time, and no longer detected at an early stage.

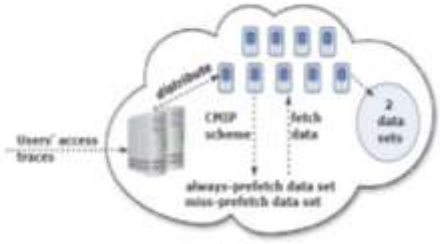
The employer changed into breached in 2014,15 as well as 2016 with facts from over 500 million user accounts.

2. LITERATURE REVIEW

A) USING CACHING AND PREFETCHING (CAFE) SCHEME

To evaluate the effectiveness of CAFE scheme, we have conducted a sequence of simulation experiments. In our evaluation, we've got as compared the proposed CAFE towards a baseline, which did now not gift any caching or prefetching techniques inside the information access of Cloud services.





For our simulations, we use the OMNET++ simulator to model the simulations situations; we've got implemented the proposed structure and a basic model in it. With the assist of INET framework, we've got configured the network in experiments as IdealWireless pattern: the best and most suitable mode to avoid the interference of the community. UDP programs are used to trans it information between a Cloudlet and cell gadgets.The objective of this evaluation includes displaying that our structure can lessen the latency and improve the performance of information get right of entry to; therefore, the experiments found the time taken to request needed records from a Cloudlet, as well as the quantity of acquired facts inside the same time c language. in the simulations, the full quantity of statistics information we set in the Cloudlet is 6000. inside the fundamental model, all of these information are saved together in the Cloudlet cache. alternatively, in our structure, we classify those data into particular and widespread information facts. these document entries are then disbursed to Cloudlet and mobile devices as a result. The distribution of unique data facts comprises copying them to every bulk in Cloudlet. despite the fact that facts statistics in every bulk of precise facts set are similar, this does not affect the functioning of both evaluated algorithms seeing that facts bulks are distinguishably separated. On the general facts set, we had to simulate that users have a distinctly excessive possibility to get entry to the top of the records in a Cloudlet; this determines the popularity of such information in the coverage area. The records request includes the records kind, specific or standard, and facts wide variety document, which is between 1 to 6000. parent 4a indicates the first set of results, which examine the variety of received facts information inside the same simulation time of the two evaluated models. in this scenario, we restricted the simulation time from 1s to 500s and recorded the range of the received records information in the cellular tool.

Algorithm 2 Specific Data Access

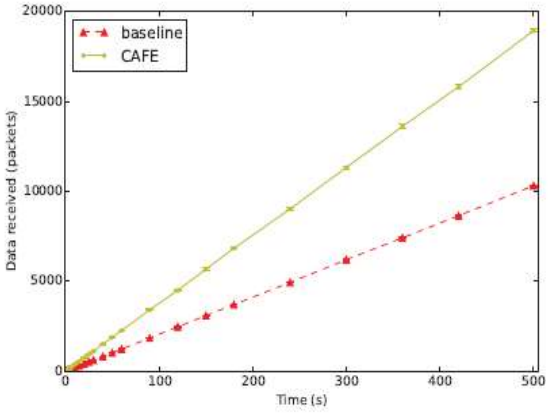
Input: req_{spec}
Output: $data_p$
1: **if** $req_{spec} \in cache_{l_i}$ **then**
2: $return \leftarrow data_p$
3: **else**
4: $send(req_{spec}, cloudlet_j)$
5: **end if**
6: **if** $req_{spec} \in data_{set_{spec}}$ **then**
7: $return \leftarrow data_p$
8: **else**
9: $send(req_{spec}, Cloud)$
10: $receive(data_p)$
11: $return \leftarrow data_p$
12: **end if**

Algorithm 3 General Data Access

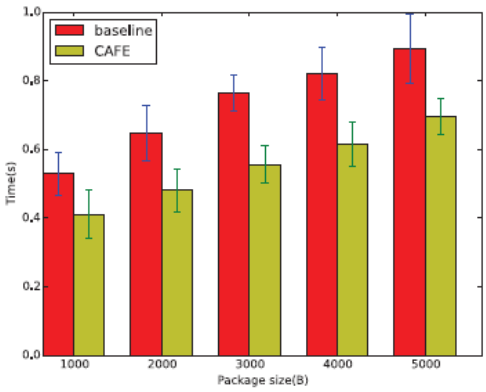
Input: req_{gen}
Output: $data_p$
1: $send(req_{gen}, cloudlet_j)$
2: **if** $req_{gen} \in data_{set_{rank}}$ **then**
3: $return \leftarrow data_p$
4: **else**
5: **if** $req_{gen} \in data_{set_{meta}}$ **then**
6: $dev_{mob_x} \leftarrow search(dev_{mob_i}, SIS_j)$
7: $connect(dev_{mob_i}, dev_{mob_x})$
8: $return \leftarrow data_p$
9: **else**
10: $send(req_{spec}, Cloud)$
11: $receive(data_p)$
12: $return \leftarrow data_p$
13: **end if**
14: **end if**

Every time, we ran the simulation for 10 instances and got the common variety that is extra correct. To report end result readily, we set the number of cell devices as 1. From the determine, it may be discovered that the number of acquired information data in our architecture is more than the wide variety of statistics furnished by way of the baseline. This distinction is originated from the truth that once a mobile tool requests a specific facts document in its cache, the time spent may be very brief with just searching time. another cause is that after the cellular tool requests a popular records document within the fashionable records, only a few rows need to be searched. but, in terms of the non-ranked information set of the basic version, the identical document may be within the backside of all statistics, so the time spent to retrieve facts is long.

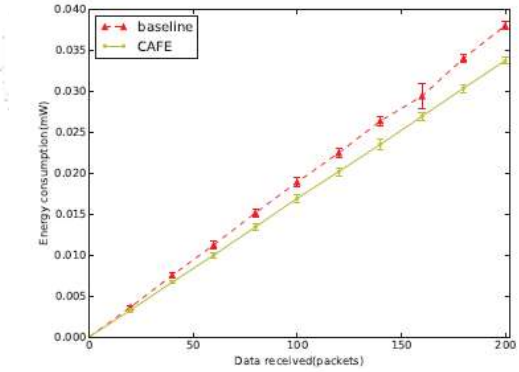
parent 4b affords the outcomes of the time spent to fetch extraordinary size programs from the Cloudlet. We defined package deal size as 1000, 2000, 3000, 4000 and 5000 Bytes. in this scenario, we set the records request type as always widespread to examine the one of a kind request times between ranked records and non-ranked information. From the effects in the parent, the time spent in our architecture is much less than that in the baseline. On a 1000B-records, our architecture desires 0.4s to fetch the records, and the baseline needs about 0.5s, the difference of zero.1s appears to be small. but, when the data size is 5000B, we will notice that the distinction turns into to about 0.3s that money owed for a extraordinarily big share of total time. additionally, the 2 evaluated schemes presented a comparable variety of oscillations within the result values that shows the CAFE scheme can mitigate the latency at the same time as maintaining the steadiness in having access to statistics.



(a) Received data packets by simulation time



(b) Request time by different data sizes



(c) Energy in mW by received data packets

determine 4c shows the energy intake analysis wherein on the factor of two hundred, CAFE consumes approximately 0.033mW and baseline 0.038mW. The distinction among those 2 schemes mainly consequences from the electricity consumption combination. in the primary model, while

requesting a data effectively, the aggregate can just be sending a packet and receiving a packet with power(sendpacket + receivepacket). whilst in CAFE, the combination can be electricity(finddatalocally) and electricity(finddatalocally+sendpacket+receivepacket) and energy(sendapacket + receiveapacket). accordingly, the common intake is (2×(finddatalocally +sendpacket+ receivepacket))/three wherein energy ate up by using domestically finding data is less than other forms, which results in much less strength intake in CAFE evaluating with baseline.

In this paper, we proposed an architecture based totally on the Cloudlet version to lessen latency and improve utilization of confined bandwidth whilst getting access to information supplied by way of Cloud offerings. With pre-fetching and caching techniques, data access behavior patterns may be described, facts types can enable more green remedy at the retrieval, and data may be stored within a spatial indexing shape. In our experiments, we compared our structure with a baseline. we've analyzed the performance of our scheme in a 3-tire structure by means of caching facts in cell gadgets and rating statistics in Cloudlets. via distributing the same amount information in these studied fashions, with distinctive techniques, our architecture confirmed greater green records get entry to and lower latency. As a future work, we will behavior further experiments to assess CAFE scheme towards other previous works, reading controlled situations in which only caching or prefetching are gift. we will also enlarge the structure to include dynamic modifications primarily based on hit prices and demand.

B. USING QUANTUM CRYPTOGRAPHY IN MOBILE COMPUTING (QCMC MODEL)

Experimental environment is shown as in Fig4. We have transformed three TNRN nodes in the campus network for distributing the quantum keys. 1550nm single-mode optical fiber is adopted; the optical fiber distances are 5km, lOkm and 15km respectively. The quantum key vendor devices are Quantum-Ctek QGW, 40MHz.

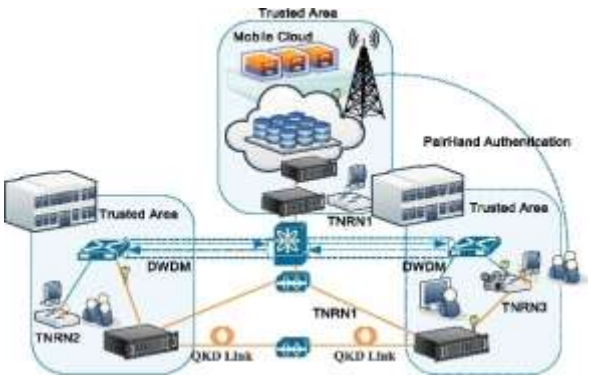
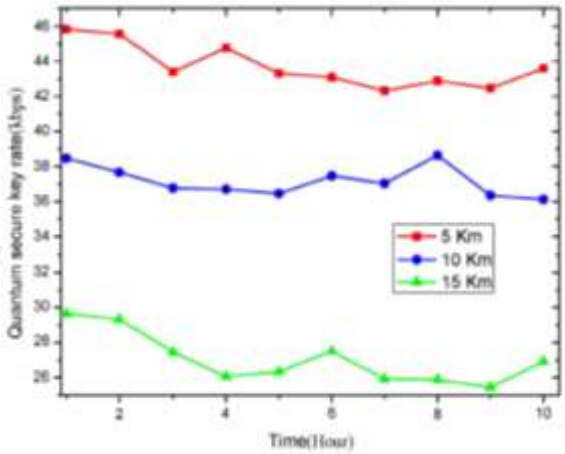
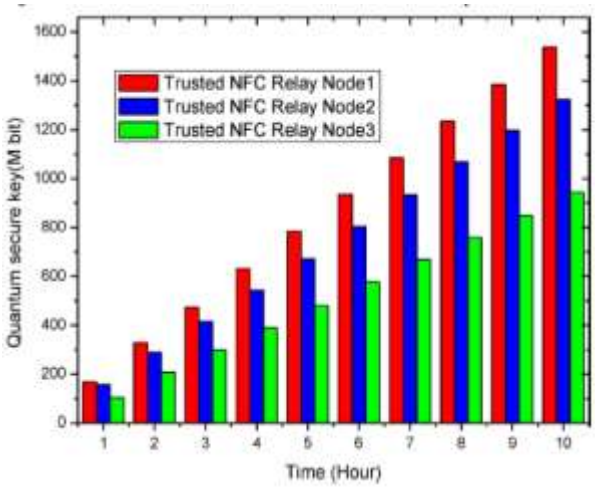


Figure. Experimental finding of QCMC model

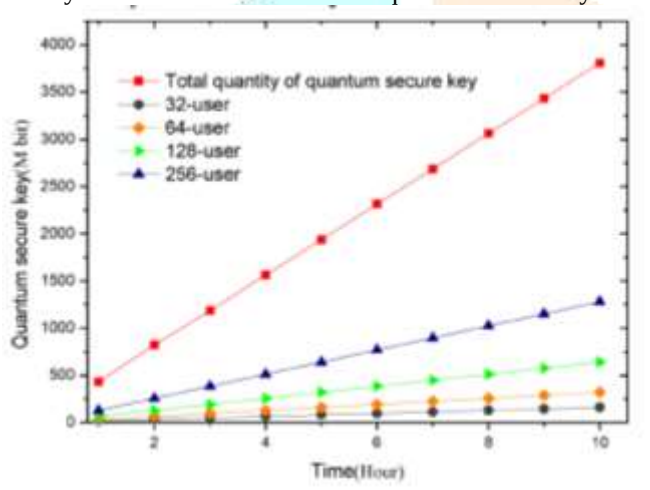
Within the cellular cloud computing experimental surroundings based on the quantum cryptography, we have upgraded the quantum cryptography for community in a campus in line with QCMC version. three get admission to nodes of quantum key distribution were set up, lengths of which are 5km, 10km and 15km respectively, as shown in Fig. throughout the system operation, technology price could be amassed every hour at the quantum secret keys.



As indicated in Fig. after a period of distributing quantum keys, amount of secret keys in each TNRN (depended on NFC Relay Node) is regularly growing, achieving the purpose of dispensing the quantum keys securely to the depended on vicinity and transmitted them into the cell users' telephone. considering that mobile customers undertake AES-256 set of rules and use quantum keys to access the encrypted facts at the cloud, plus with using 64 bits for using quantum authentication token QTT one-time-pad even as traveling the cloud authentication whenever, users best need to have 320-bit mystery keys consumption for every session. For those data with unique security requirements of statistics, they can use "One-Time-Pad" completely primarily based on bit. each TNRN node adopts SMC532 module with packing of Libnfc for improvement. every TNRN and nodes support 10 cellular phones to carry out quantum secret keys transmission on the identical time via significant generation of the serial port. It desires just numerous mins every to transmit the quantum mystery



keys to customers' phones. As quantum secret keys are generated constantly, sufficient phone customers can be supported after gathering. If use technique of paper, no need to carry out accumulating section of secret keys, however directly to realise the distribution of quantum secret keys.



As irrespective of which TNRN node is used by users to receive quantum keys, quantum key management carrier on the cloud are assigned the quantum mystery keys in keeping with the team spirit of users' sick. as a result, the greater QKD gadgets used, the most important quantity of quantum mystery keys is to be had at the cloud. In Fig, graph in red represents the whole amount of quantum mystery keys after collecting quantum mystery keys generated by 3 pairs of QK D links at the cloud. four different graphs are used for calculating the intake of quantum mystery keys according to the records of 32 users, sixty four, 128 customers and 256 customers respectively. For smooth contrast, it describes the common fee of the entire quantity of quantum mystery keys 401 fed on by using these customers in 10 hours. 5Mbit of quantum mystery keys is transmitted to cellular telephone users every time. Transmission into users' phones is taken into consideration the quantum mystery keys fed on. From what we see from the figure, the model can properly help the utilization requirements on the quantum
mystery keys for mobile users, making sure that cellular customers can use the quantum keys and the cloud application to get entry to information in encryption.

C. CODE BASED SCHEME FOR INTEGRITY AND VERIFICATION IN CLOUD

Firstly, we examine the overall performance value of each degree in provable records ownership. We convert all of the exponentiation operations into multiplication operations. We denote the multiplication cost in * p Z as MultCost(p). For calculating yx , we want 1 five. x instances multiplications using Iterative rectangular technique. First step to calculate 2z i y , build a list for 2z i y (1) p ≤ z ≤λ , want |x| instances multiplications, secondly to look for a listing desires |x|/2 multiplications. during the manner of calculating hash fee, all of us need to search for a list 2z i y . So the list is constructed inside the Setup degree. To simplify the performance analysis, we are able to ignore the computation cost in the course of the following analysis. in the Setup level, producing parameters G of homomorphic hash feature, relates to the random range
era and modulus exponentiation. For parameters p and q, they mainly use a random wide variety generator and
top testing. For parameter g, it wishes m(p-1)/2q mod p multiplications, its value is 1 ( ) 2 p q m(λ −)MultCost p / λ . however, these parameters are handiest generated one time. For any method of provable data possession, these parameters are vital and their price is nearly the identical. in the TagBlock stage, the size of the facts block is 16KB, the output of homomorphic hash function is 1024 bits, so the hash function reduces the garage space of file to its authentic λp/β=1024/(16×1024×eight)=1/128. This manner of generating tag may be very helpful in lowering garage redundancy. We want to compute hash fee of every data block, which pertains to nm|p|/2 mod p multiplications, its cost is nm λpMultCost(p)/2. inside the mission degree, the fee is two random numbers. within the ProofGen level, the fee is okay instances mod q additions, additionally has okay instances mod p multiplications, here the cost of multiplication is cMultCost(p)/2. within the ProofVerify level, the fee is one time homomorphic hash calculation, relating to m times mod p multiplications, its price is m λpMultCost(p)/2.

Setup $(\lambda_p, \lambda_q, m, s) \rightarrow G = (p, q, g)$
seed PRNG R with s.
do
$q \leftarrow qGen(\lambda_q)$
$p \leftarrow pGen(q, \lambda_p)$
while p=0 **done**
for(i=1 **to** m) **do**
do
$x \leftarrow R(p-1)+1$
$g_i \leftarrow x^{(p-1)/q} \pmod p$
while $g_i = 1$ **done**
done
return (p,q,g)
$qGen(q, \lambda_q)$
do
$q \leftarrow R(2^{\lambda})$
while q is not prime **done**
return q
$pGen(q, \lambda_p)$
for(i=1 to 4 λ_p) **do**
$X \leftarrow R(2^{\lambda_p})$
$c \leftarrow X \pmod{2q}$
$p \leftarrow X - c + 1$
if p is prime **then return** p
done
return 0

TagBlock(G,F)
G=(p,q,g),$F = (b_1, b_2, \cdots, b_n)$
for(j=1 to n) **do**
$x_j = H_G(b_j) = Hc_j^r$
$r_j = R(seed)$
done
then Tag= $[x_1 \cdot r_1, x_2 \cdot r_2, \cdots, x_n \cdot r_n]$
return Tag= $[t_1, t_2, \cdots, t_n]$, $t_j = x_j \cdot r_j$
the client sends F,Tag,p,q to the server
saves G and seed

In sensible use of cloud storage, performance is constantly restricted by way of network bandwidth. Modular multiplication set of rules may be optimized, the optimization approach refers to literature [10]. Optimized overall performance can improve more than 4 instances. Zhao et al. [13] proposed the usage of images processing unit [14,15] to boost up the performance of homomorphic hash characteristic. We also can use this technique to enhance the overall performance in our scheme.

This paper proposes a PDP scheme primarily based on homomorphic hash feature in keeping with the troubles
current within the above algorithms. This approach permits customers to verify facts integrity within the server for unlimited wide variety of instances. It also provides provable facts possession inside the server and statistics integrity protection. customers handiest need to save parameters G, transmission statistics is little at some stage in the verification technique, and the verification of provable statistics possession is just one time homomorphic hash calculation. via protection analysis and overall performance analysis, we prove that the technique is viable. The scheme can attain information restoration. we will use errors-correcting codes or erasure codes to encode records earlier than calculating hash value.

D. FRAMEWORK OF SECURE MOBILE CLOUD COMPUTING WITH SMART LOAD BALANCING

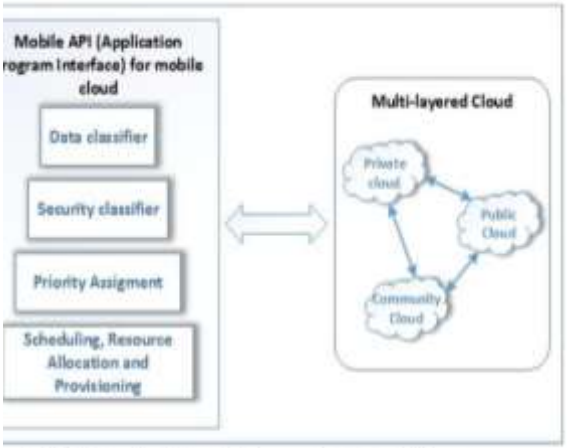
The framework proposed in this studies is in the main developed the usage of simulation based totally software program. but, a hardware replication is also currently being advanced. A. Simulation basis because the aim of the mobile cloud is to reduce the burden of computing strength and cellular storage from cell gadgets, it's far vital to switch mobile facts from these gadgets to the cell cloud and method them in the cloud. There are numerous previous steps prior to sending cellular records from cellular gadgets to the mobile cloud. the foremost step is to confirm the information whether or not there are any security worries.For this model, information are divided into five exclusive security lessons in line with its severity and shareability from elegance-1 to elegance-five. class-1 is categorised with the top secret information, and the subsequent categories include less secrete information respectively (table 1).

TABLE I. DATA SECURITY CLASSES

Class	Data severity	Examples
Security Class-1	Top Secret Data	Very personal information without sharing, e.g. personal notes, text messages, some pictures etc.
Security Class-2	Secret Data	Data shareable with very specific people or specific group of people.
Security Class-3	Confidential Data	Data shareable with certain group of people including friends and family, co-workers, people of certain community, etc.
Security Class-4	Restricted Data	Data shareable with almost everyone but not certain limited group.

records can be processed otherwise consistent with its magnificence. as an instance, very touchy information that belong to magnificence-1should no longer be sent from cellular devices to cellular cloud, but rather to a private area of the cellular cloud through a at ease encryption technique. it is also cautioned to have a cloud that helps multi-layer structure, which may also beautify a layer of security and proportion the processing capacity in addition to storage load. The multilayer cloud structure refers to a cloud infrastructure cconsisting public cloud, non-public cloud, hybrid cloud and network-based totally cloud. In Fig., the proposed approach of records processing in multilayer cloud shape in step with security elegance is proven. as soon as the ascertainment of the safety troubles is completed, statistics from all 3 categories (person Generated records, software statistics and system information) are required to be separated in step with its call for (Fig.). cell cloud API is
a accepted cellular software that is chargeable for interfacing from the mobile device to the cellular cloud. in the course of this manner, mobile API is needed to perform a number of vital obligations, which include classifying the facts, assigning safety flag based totally on the security classifier, scheduling,

assigning the priority of the statistics and useful resource control. cell API permits a unified platform for all operation structures. whilst cellular API takes the responsibility to shop and method information from cell cloud, the applications of the cloud will be operation machine impartial, consequently enhancing the mobility of cell packages.

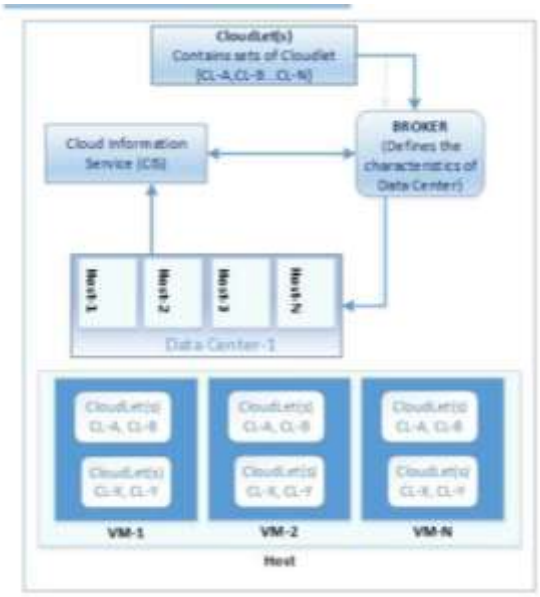


Mobile Cloud Application Program Interface Architecture

Data categories located within the Data Classifier Layer

Security Class levels

To assemble a model of a cloud computing and simulate the environment, the JAVA based toolkit CloudSim gives the framework for cloud infrastructures and offerings. This tremendous simulation toolkit makes available the primary cloud additives, inclusive of Cloud statistics provider (CIS), data middle, broker, CloudLet, Host, digital system (VM), and so on. Fig. illustrates the simple version of CloudSim.

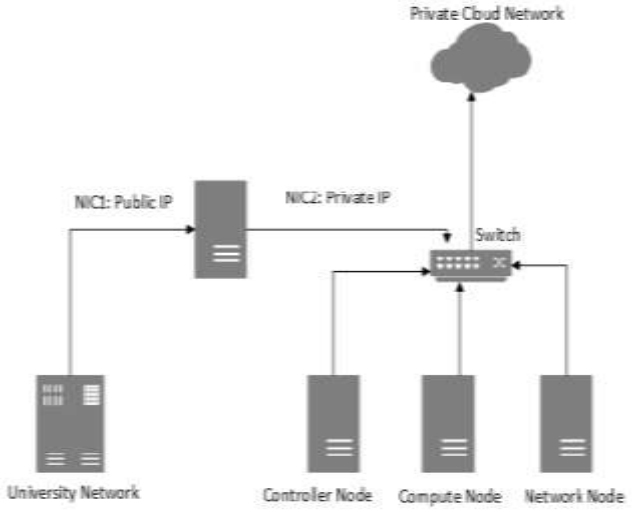


Research Tasks

The 2 fundamental obligations of this research are: the layout of a private cloud community that operates inside the university community and the layout of an algorithm so that it will dictate how sources will be allotted and processed. The testbed will allow us to simulate a multi-user cloud environment and examine the accessibility of numerous sorts of customers. This surroundings affords the capacity to analyze feasible security troubles in mobile cloud, which include however not limited to safety of noticeably exclusive records, reasons of sluggish request rates, maximum ability of requests at height times and typical availability of the machine to the customers.

Experimental Framework

Every machine inside the implementation runs Ubuntu Server 14.04 and has OpenStack cloud software established with a view to shop and provision virtual machines. in this model, the lead node is the controller, which continues the communications among database storage of the users, software and permissions some of the nodes. the principle manipulate station uses the Ubuntu metallic As A service (MAAS) as a method to install software and updates.MAAS permits for very clean scale-up and scale-down of physical machines, thanks to the truth that any server linked is truely visible as clusters of virtual machines. One cluster incorporates the nodes and in each node runs the desired software for the cloud. The community topology of the experimental framework is validated in Fig.



It's been shown that mobile devices will need to access the cellular cloud to order processing strength and battery existence. A proposed testbed for the clever load balancer is supplied. A simulated framework became then created to describe how the network will handle resources and a physical machine has been implemented. destiny paintings will then bring to use a smart load balancer to address huge statistics of varying ranges of protection and necessity to assist mobile devices function greater efficiently.

3. CONCLUSION

In this research article, we review and evaluate the big obstacle in data security in cloud computing operations, that can also be a differentiated model due to fragmentation of information for security purposes. To achieve guaranteed purity and reliability of data present in cloud, we must strain on quality of services so that users are able to avail reliable cloud computing and storage options, a durable,cost-efficient and flexible arrangement is sufficed.

Our review concludes that all of the above discussed methods for storage and security in cloud computing offer efficient solutions and can be used in place of the conventional RSA that is highly used for storing data securely by virtue of cloud computing.

4. ACKNOWLEDGEMENT

Expressing my gratitude to all the persons who were helped me in all times, I would also like to sincerely thank my professors as well as college authorities for granting resources in my Endeavour.

5. REFERENCES :

[1] E. Koukoumidis, D. Lymberopoulos, K. Strauss, J. Liu, and D. Burger, “Pocket cloudlets,” in ACM SIGPLAN Notices, vol. 46, no. 3. ACM, 2011, pp. 171–184.

[2] H. Falaki, R. Mahajan, S. Kandula, D. Lymberopoulos, R. Govindan, and D. Estrin, “Diversity in smartphone usage,” in Proceedings of the 8th international conference on Mobile systems, applications, and services. ACM, 2010, pp. 179–194.

[3] S. Acharya and S. Zdonik, Broadcast disks: dissemination-based data management for asymmetric communication environments. Brown University, 1998.

[4] H. Song and G. Cao, “Cache-miss-initiated prefetch in mobile environments,” Computer Communications, vol. 28, no. 7, pp. 741–753, 2005.

[5] C.-Y. Chow, H. V. Leong, and A. Chan, “Peer-to-peer cooperative caching in mobile environments,” in Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference on. IEEE, 2004, pp. 528–533.

[6] C.-Y. Chow, H. V. Leong et al., “Grococa: Group-based peer-to-peer cooperative caching in mobile environment,” IEEE Journal on Selected Areas in Communications, vol. 25, no. 1, pp. 179–191, 2007.

[7] N. Dimokas, D. Katsaros, and Y. Manolopoulos, “Cooperative caching in wireless multimedia sensor networks,” Mobile Networks and Applications, vol. 13, no. 3-4, pp. 337–356, 2008.

[8] Y.-C. Hu and D. B. Johnson, “Caching strategies in on-demand routing protocols for wireless ad hoc networks,” in Proceedings of the 6th annual international conference on Mobile computing and networking. ACM, 2000, pp. 231–242.

[9] C. M. Procopiuc, P. K. Agarwal, and S. Har-Peled, “Star-tree: An efficient self-adjusting index for moving objects,” in Workshop on Algorithm Engineering and Experimentation. Springer, 2002, pp. 178–193.

[10] S.Saltenis, “Indexing the positions of continuously moving objects,”in Encyclopedia of GIS. Springer,2008,pp.538–543.

[11] R. Alleaume, c. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Lfinger, N. Liitkenhaus, C. Monyk, P. Painchault, M. Peev, A. Poppe, T. Pornin, 1. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, and A. Zeilinger, "Using quantum key distribution for cryptographic purposes: A survey," Theoretical Computer Science, vol. 560, pp. 62-81,2014

[12] B. FrOhlich, 1. F. Dynes, M. Lucamarini, A. W. Sharpe, S. W. B. Tam, Z. Yuan, and A. 1. Shields, "Quantum secured gigabit optical access networks," Scientific Reports, vol. 5, pp. 18121-18127, December, 2015.

[13] O. K. Jasim, S. Abbas, E.-S. M. EI-Horbaty, and A.-B. M. Salem, "Cryptographic cloud computing environment as a more trusted communication environment," International Journal of Grid and High Performance Computing, vol. 6, pp. 38-51, January, 2014.

[14] V. Thayananthan and A. Albeshri, "Big Data Security Issues Based on Quantum Cryptography and Privacy with Authentication for Mobile Data Center," Procedia Computer Science, vol. 50, pp. 149-156,2015.

[15] M. Fujiwara, T. Domeki, S. Moriai, and M. Sasaki, "Highly secure network switches with quantum key distribution systems," International Journal of Network Security, vol. 17, pp. 34-39, 2015.

[16] W. Xin, H. Sun, and Z. Chen, "Analysis and design of distancebounding protocols for RFlD," Jisuanji Yanjiu yu FazhaniComputer Research and Development, vol. 50, pp. 2358-2366, 2013.
[17] 1.W. Han, Y.H. Liu, X. Sun, and L.J. Song, "Quantum key management algorithm based on sliding window," Journal of Jilin University (Engineering and Technology Edition), vol. 46, pp. 535-541,2016.
[18] Wang C, Chow S S M, Wang Q, et al. Privacy-Preserving Public Auditing for Secure Cloud Storage. IEEE Transactions on Computers, 2013, 62(2):362-375.
[19] Juels A,Kaliski B S,Por S. Proof of rerievability for large files. Proc of the 14th ACM Conf on Computer and Communications Security. New York: ACM, 2007: 584-597.
[20] Giuseppe Ateniese, Randal Burns, Reza Curtmola, et al. Provable Data Possession at Untrusted Stores. 2015, in press, http://cs.njit.edu/~crix/publications/pdp.pdf.
[21] Johnson R, Molnar D, Song D, et al. Homomorphic Signature Schemes. the Cryptographers Track at the Rsa Conference on Topics in Cryptology. Springer Berlin Heidelberg, 2002:244-262.
[22] Sebe F, Domingo-Ferrer J, Martinez-Balleste A, et al. Efficient Remote Data Possession Checking in Critical Information Infrastructures. IEEE Transactions on Knowledge & Data Engineering, 2008, 20(8):1034-1038.
[23] Ateniese G, Pietro R D, Mancini L V, et al. Scalable and Efficient Provable Data Possession. Proceedings of the 4th international conference on Security and privacy in communication netowrks. ACM, 2008:1--10.
[24] Erway C, , Alptekin, Papamanthou C, et al. Dynamic Provable Data Possession. Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2008:213-222.
[25] Chen B, Curtmola R. Robust Dynamic Provable Data Possession 2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops. IEEE, 2012:515-525.
[26] Zhou E, Zhoujun L I, Guo H, et al. Cooperative provable data possession scheme for multicloud storage. Journal of Tsinghua University, 2013.
[27] S. Khan, A. Gani, A. Wahid, et. Al. Towards an Applicability of Current Network Forensics for Cloud Networks: A SWOT Analysis. IEEE Access, vol 4, pp. 9800-9820, 2016.
[28] N. Chalaemwongwan and W. Kurutach, "Mobile Cloud Computing: A Survey and Propose Solution Framework" in 13th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), Chiang Mai, 2016.
[29] S. Thamarai Selvi, C. Valliyammai, G. P. Sindhu and S. Sameer Basha, "Dynamic resource management in cloud," in Sixth International Conference on Advanced Computing (ICoAC), Chennai, 2014.
[30] H. Hu, Y. Wen, H. Wang and A. Begen, "Cloud mobile media," in *China Communications*, 2016.
[31] Yuan Zhang, Jinyao Yan and Xiaoming Fu, "Reservation-based resource scheduling and code partition in mobile cloud computing," in *IEEE Conference on Computer Communications Workshops*, San Francisco, CA, 2016.
[32] "OpenStackOpen Source Cloud Computing Software", OpenStack, 2016. [Online]. Available: http://www.OpenStack.org/software/sampleconfigs. [Accessed: 13-Sep- 2016].
[33] "Chapter 1. Architecture -OpenStack Installation Guide for Ubuntu 14.04 - juno", Docs.OpenStack.org, 2016. [Online]. Available: http://docs.OpenStack.org/juno/installguide/ install/apt/content/ch_overview.html. [Accessed: 14-Sep- 2016].
[34] "OpenStackDocs: Overview", Docs.OpenStack.org, 2016. [Online]. Available: http://docs.OpenStack.org/liberty/install-guideobs/ overview.html. [Accessed: 14- Sep- 2016].
[35] Z. Su, Q. Xu, M. Fei and M. Dong, "Game Theoretic Resource Allocation in Media Cloud With Mobile Social Users", *IEEE Transactions on Multimedia*, vol. 18, no. 8, pp. 1650-1660, 2016.