Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 5, May-2016

Energy Efficient Cryptographic Tecchniques in Mobile Cloud Computing

Ms. Grishma Tamboli [1], Mr. Yask Patel[2]

[1]*Department of Computer Engineering, PIET Vadodara, grishmatamboli@gmail.com*
[2]*Department of Information Technology, PIET Vadodara, patelyask@gmail.com*

Abstract - *The Technology World, Mobile Devices such as Smart phones, Tablets are becoming important part of the Human life. They are facing some challenges in their resource such as battery life, bandwidth and storage. They also are facing some challenges of communication and security. It describes how securely mobile data to store in a cloud using various cryptographic technique with Symmetric Algorithm & Asymmetric Algorithm using Parameter Mean Processing time And Speedup ratio which related to this Parameters to find out Time Efficiency and increase security using Asymmetric algorithm.*

Keywords – *Cloud Computing, Mobile cloud computing, Energy Efficiency.*

I. INTRODUCTION

Cloud Computing is the network-based environment that concentrate on sharing computation or resources .Actually, cloud Internet based and it tries to guise complication for clients. Cloud computing refers to both the application provides as a services over the internet and the hardware and the software in the data center that provides that services [1].Here, Cloud provider, has a service that has private cloud part which only authorized by certified staff and protected by firewall from outside accessing and a public cloud environment which external users can access to it [1]. There are three major type of service in the cloud environment: SaaS, PaaS, and IaaS

Cloud Computing is described as a range of services which are provided by an internet based cluster system [2].such cluster system consists of the group of low cost servers or personal computers(PCs),organizing the various resources of the computers according to a certain management strategy, and offering safe reliable ,fast ,convenient and transparent services such as data storage, accessing and the computing the clients[2]

Meanwhile, Smartphone's are conceded as the representative for the various mobile devices as they have been connected to the internet with the rapid growing of wireless network technology [2].if we considered the smart phones which has a processors of limited capacity and limited amount of main memory, it restrict the smart phones to carryout operations that demand more processing power and memory[11].Another short comings of every Smartphone is its battery life as well which is very poor in all the cases. So in order to overcome these drawback mobile cloud computing can play an important role. with the help of computation offloading process we can offload the demanding task that demand for more processing power as well as memory to the resources rich cloud to get it processed there and the return the final output back to the device resulting in save the energy consumption as well [11].cloud computing the promising the technology which can offer many benefits of mobile cloud.

Mobile Cloud Computing offers to meet users increasingly functionality demands, as different servers execute all application logic and only user interface functionalities reside on the mobile [6].mobile cloud computing its separates the user interface from the application logic in such way mobile device executes only viewer component, operating as a remote display for the application running on different server in the cloud [6].

The rest of this paper is organized as follows. Section II presents basic architecture of Mobile Cloud Computing. Section III presents Mobile cloud offloading. Energy Consideration are discussed in section IV.

II. ARCHITECTURE OF MOBILE CLOUD COMPUTING

Figure 1 shows Mobile cloud computing can be divvied in to cloud computing and mobile computing such as devices can be laptops ,PDA, smart phones and so on which connect to the hotspot or base station by 3G,Wifi and GPRS.

Mobile computing and major data processing phases have been migrate to 'cloud' ,the capability requirement of mobile device is limited and some low cost mobile device or some non smartphones can also mobile cloud computing by using the cross platfrom midware[2].the clients in mobile computing is change from PCs and fix machine to mobile devices this is the main concept of mobile cloud computing.Mobile users send and recevices request to the cloud through a web browser or desktop application,then

the management componenet of the cloud allocates the resources to the request to established the connection ,while the monitoring and the calculating the function of mobile cloud computing will be implemneted to ensure the QOS until the connection will completed[2].

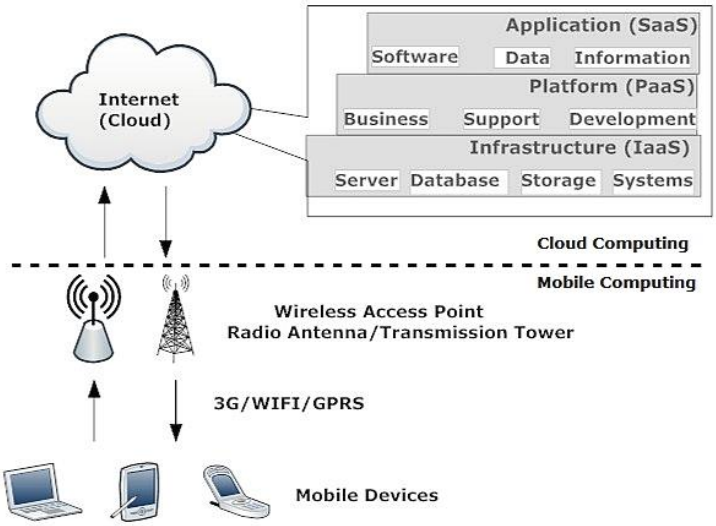

Figure 1. Architecture of Mobile Cloud Computing[2]

III. CRYPTOGRAPHIC APPROACH

The encryption algorithm is most commonly used technique to protect data within cloud environment. The data related to a client can be categorized as public data and private data[15]. The public data is sharable among trusted clients that provide an open environment for collaboration. Private data is client's confidential data that must be transferred in encrypted form for security and privacy[15].

We propose a suitable method that cryptographic algorithms with different key lengths are used in various environments. The number of mobile devices such as smart phones and smart pads grows rapidly recently[15]. End users can access easily to cloud computing environment thought these mobile devices we define that mobile cloud computing is one of specific services of cloud computing and it is a mobile service which is added a cloud computing service[15].

According to key characteristics, modern cryptosystem can be classified into symmetric cryptosystem, asymmetric cryptosystem and digital signature[15]. For a symmetric cryptosystem, the sender and receiver share an encryption key and decryption key. These two keys are the same or easy to deduce each other[15]. The representatives of symmetric cryptosystem are DES (Data Encryption Standard), AES (Advanced Encryption Standard). For an asymmetric cryptosystem, the receiver possesses public key and private key. The public key can be published but the private key should be kept secret[15]. The representatives of asymmetric cryptosystem are RSA (Rivest Shamir Adleman) and ECC (Elliptic Curve Cryptosystem). For Digital signature the representatives is MD5 and SHA1[15].

IV. PROPOSED WORK

The cryptographic algorithms used are Asymmetric key algorithms and Combination of these algorithm as a Hybrid Approach. Evaluation metrics for these algorithms are studied based on various previous research work. Encryption techniques will make the data more secure in the local system as well as on the remote cloud. Test has been executed in both the above environment using the following algorithms one at a time.

[1] RSA Algorithm[15]:

RSA has been widely used for establishing secure communication channels and for authentication the identity of service provider over insecure communication medium[15].

[2] Elliptic Curve Cryptography (ECC) with SHA-512[15]:

An elliptic curve is given by an equation in the form of the finite fields those are commonly used over primes (FP) and binary field (F2n)[15].

[3] Elgamal[16]:
In cryptography, the ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange[16]. It was described by Taher Elgamal in 1985[16]. ElGamal encryption is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems[16].

[4] Pailler Cryptosystem[17]:
The Paillier cryptosystem, named after and invented by Pascal Paillier in 1999, is a probabilistic asymmetric algorithm for public key cryptograph[17] .The problem of computing *n*-th residue classes is believed to be computationally difficult[17]. The decisional composite residuosity assumption is the intractability hypothesis upon which this cryptosystem is based[17].

[5] Cramer-Shoup[18]:
The Cramer–Shoup system is an asymmetric key encryption algorithm, and was the first efficient scheme proven to be secure against adaptive chosen ciphertext attack using standard cryptographic assumptions [24]. Its security is based on the computational intractability (widely assumed, but not proved) of the decisional Diffie–Hellman assumption[18]. Developed by Ronald Cramer and Victor Shoup in 1998, it is an extension of the ElGamal cryptosystem [24]. In contrast to ElGamal, which is extremely malleable, Cramer–Shoup adds other elements to ensure non-malleability even against a resourceful attacker[18]. This non-malleability is achieved through the use of a universal one-way hash function and additional computations, resulting in a ciphertext which is twice as large as in ElGamal[18].

Google App Engine[19]:

Google App Engine (often referred to as GAE or simply App Engine) is a platform as a service (PaaS) cloud computing platform for developing and hosting web applications in Google-managed data centers [25]. App Engine offers automatic scaling for web applications—as the number of requests increases for an application, App Engine automatically allocates more resources for the web application to handle the additional demand[19].

Google App Engine is free up to a certain level of consumed resources[19]. Fees are charged for additional storage, bandwidth, or instance hours required by the application[19].

Advantages:

- Scale Automatically
- Start quickly, Build faster
- Automatic scaling
- Automated security scanning

Cloud architecture is designed by combining cryptographic algorithms with Mobile device environment. The cryptographic algorithms to be used are selected based on comparative study from previous researches. So the symmetric, asymmetric and digital signature algorithms AES, DES, RSA, ECC, and MD5 are selected and used for cryptographic application.
The cryptographic application is used to encrypt and decrypt data, provides options to application user whether to use asymmetric with digital signature or symmetric algorithm.
Steps Performed:

- Create some input data samples of sizes 25kb, 50kb, 75kb, 100kb, 125kb and 150 kb.
- Run the cryptographic algorithms with all input data sizes in mobile device.
- Make a cloud server instance on application tool and then make a dynamic web project.
- Run the encryption algorithms on cloud server input data sizes and note all observations
- Compare both the results.

Results are compared based on the performance metrics Mean Processing Time and Speed-Up Ratio.

Mean Processing Time:
Mean processing time is the difference between the starting time taken to encrypt the data and the endingvtime. It is also evaluated both on single system and on cloud network. It is the difference between the time taken to encrypt the data.

Speed-Up Ratio:
It is defined as the difference between the mean processing time of single system and the cloud network. It will give us the idea about speed of encryption.

Speedup Ratio = Processing Time in Local − Processing Time in Cloud

Time Efficient based on Energy:
Energy Efficiency Formula, Energy=Power*Time. Assume, total Power=2500mAh Here, 10Hr Battery full Discharge

1 Hr=250, 1 Min=4.16,1 Sec=0.069 So that time power is constant for 0.069
Ex. Power=0.069 & Time=0.003
Energy=Power*Time =0.069*0.003 =0.000276 =0.0276%
Now, Time Efficient based on Energy is 0.02%

V. RESULT ANALYSIS

Table 1: Mean processing time in Local

Local				
Encryption				
Size	**PAILLER**	**ELGAMAL**	**RSA**	**CRAMER-SHUOIP**
25kb	0.210	0.300	0.190	0.299
50kb	0.400	0.390	0.378	0.501
75kb	0.598	0.610	0.579	0.799
100kb	0.793	0.835	0.789	0.878

Local				
Decryption				
Size	**PAILLER**	**ELGAMAL**	**RSA**	**CRAMER-SHUOIP**
25kb	0.100	0.156	0.189	0.213
50kb	0.356	0.366	0.356	0.400
75kb	0.589	0.567	0.578	0.678
100kb	0.856	0.789	0.878	0.989

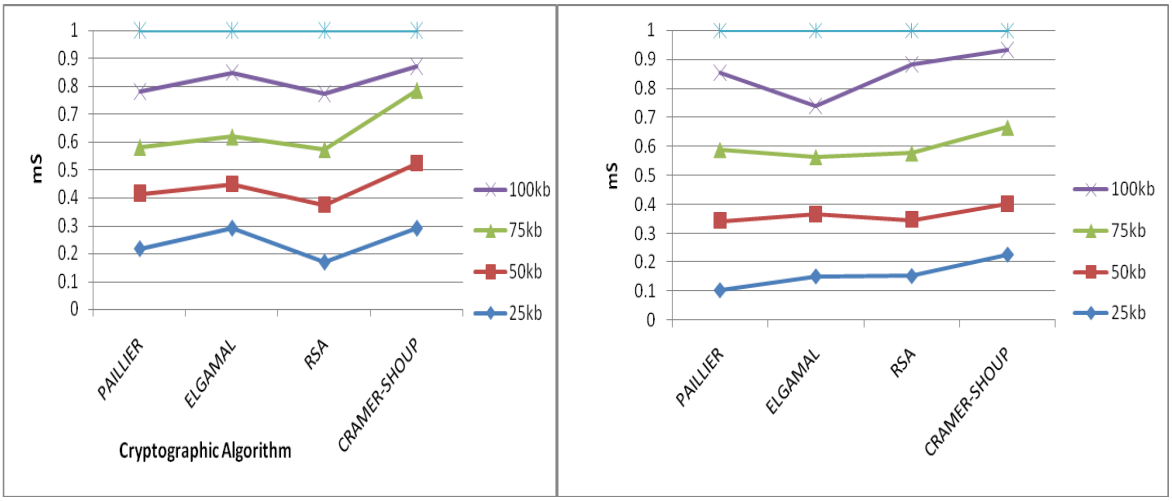

Fig 2: Mean Processing time in Local

Table 2: Mean processing time in Cloud

Cloud				
Encryption				
Size	**PAILLER**	**ELGAMAL**	**RSA**	**CRAMER-SHUOIP**
25kb	0.190	0.300	0.104	0.245
50kb	0.402	0.450	0.304	0.500
75kb	0.568	0.590	0.534	0.800
100kb	0.787	0.777	0.760	0.846

Cloud				
Decryption				
Size	**PAILLER**	**ELGAMAL**	**RSA**	**CRAMER-SHUOIP**
25kb	0.100	0.123	0.100	0.234
50kb	0.389	0.300	0.314	0.423
75kb	0.610	0.534	0.578	0.701
100kb	6.845	0.700	0.902	0.934

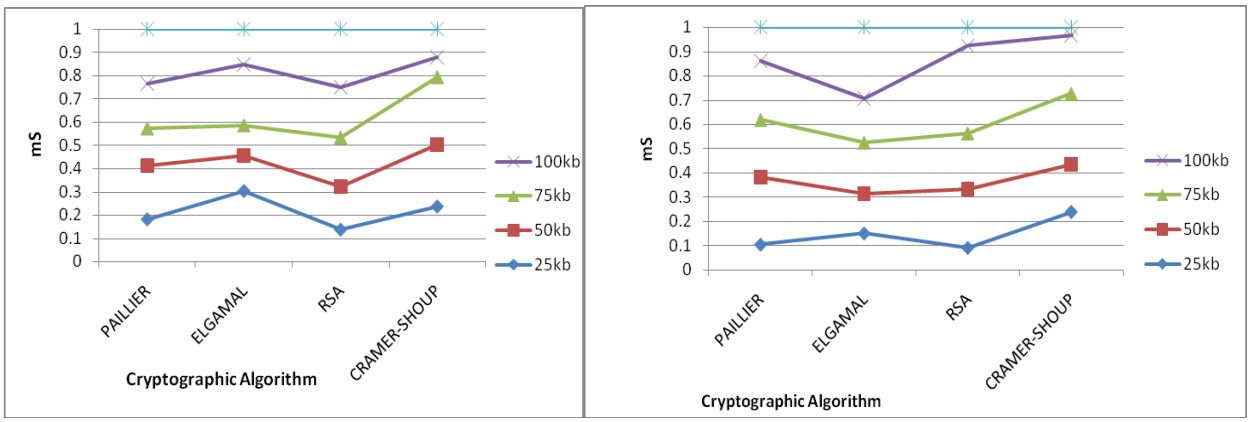

Fig 3: Mean Processing time in Cloud

Table 3: Speedup ratio in Local

Speedup ratio				
Encryption				
Size	**PAILLER**	**ELGAMAL**	**RSA**	**CRAMER-SHUOIP**
25kb	0.239	0.300	0.578	0.345
50kb	0.431	0.590	0.700	0.555
75kb	0.590	0.700	0.800	0.788
100kb	0.879	0.820	0.900	0.888
Speedup ratio				
Decryption				
Size	**PAILLER**	**ELGAMAL**	**RSA**	**CRAMER-SHUOIP**
25kb	0.239	0.300	0.578	0.345
50kb	0.431	0.590	0.700	0.555
75kb	0.590	0.700	0.800	0.788
100kb	0.879	0.820	0.900	0.888

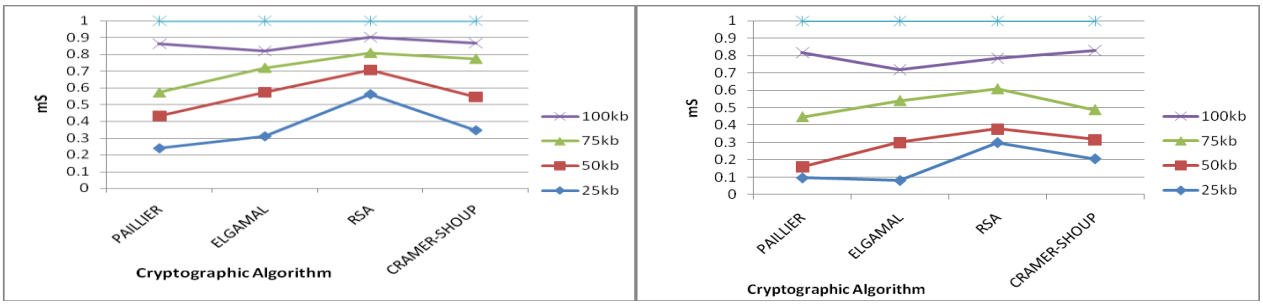

Fig 3: Speedup Ratio in Local

Table 4: Time Efficient in Local

Time_efficient_Local				
Encryption				
Size	**PAILLER**	**ELGAMAL**	**RSA**	**CRAMER-SHUOIP**
25kb	2.762	3.9246	1.483	2.782
50kb	4.614	5.511	3.580	5.812
75kb	5.518	7.538	5.556	7.209
100kb	7.621	9.383	7.566	8.214

Time_efficient_Local				
Decryption				
Size	**PAILLER**	**ELGAMAL**	**RSA**	**CRAMER-SHUOIP**
25kb	2.762	3.9246	1.483	2.782
50kb	4.614	5.511	3.580	5.812
75kb	5.518	7.538	5.556	7.209
100kb	7.621	9.383	7.566	8.214

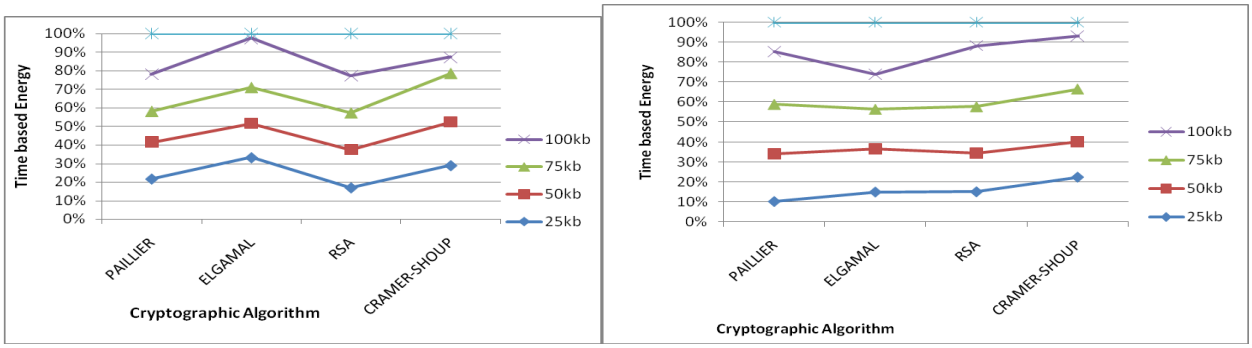

Fig 4: Time efficient in local

VI. CONCLUSION

Cryptographic algorithms works in a single system environment to store the mobile data in cloud which increases the security in local environment and also cloud environment. RSA Asymmetric Algorithm is qualifies better than other algorithm in mean processing time and Elgamal Algorithm is in speed up ration. So the main concern to improve Security using Local and cloud. Other two parameter like turnaround time & throughput consider as a future.

References

[1] Anantkumar A.kanwale1, Prof.Mr.O.V.Chandure "REVIEW PAPER ON CLOUD COMPUTING"IJRISE-International Journal of Research In Science & Engineering e-ISSN: 2394-8299|Volume: 1 Special Issue: 1 p-ISSN: 2394-8280

[2] Han Qi,Abdullah Gani"Research on Mobile Cloud Computing: Review, Trend and Perspectives"Faculty of Computer Science and Information TechnologyUniversity of MalayaKuala Lumpur, Malaysia,Faculty of Computer Science and Information TechnologyUniversity of Malaya Kuala Lumpur, Malaysia

[3] Karthik Kumar and Yung-Hsiang Lu"CLOUD COMPUTING FOR MOBILE USERS: CAN OFFLOADING COMPUTATION SAVE ENERGY?",confrence paper Published by the IEEE Computer Society,APRIL 2010

[4] Eli Tilevich and Young-Woo Kwon,"Cloud-Based Execution to Improve Mobile Application Energy Efficiency"confrence paper Published by the IEEE Computer Society,JANUARY 2014

[5] Niroshinie Fernando , Seng W. Loke , Wenny Rahayu"Mobile cloud computing: A survey"artical of Future Generation Computer Systems 29 (2013) 84–106

[6] Pieter Simoens, Filip De Turck, Bart Dhoedt, and Piet Demeester"Remote Display Solutions for Mobile Cloud Computing"confrence paper Published by the IEEE Computer Society,0018-9162/11/$26.00 © 2011 IEEE

[7] Karthik Kumar,Jibang Liu,Yung-Hsiang Lu,Bharat Bhargava"A Survey of Computation Offloading for Mobile Systems"© Springer Science published online 10 April 2012

[8] Frank H. P. Fitzek,Joerg Widmer"Survey on Energy Consumption Entities on the Smartphone Platform" CONFERENCE PAPER · JUNE 2011 DOI: 10.1109/VETECS.2011.5956528 · Source: IEEE Xplore

[9] Milindkumar H. Tandel, Vijay S. Venkitachalam,"Cloud Computing in Smartphone: Is offloading a better-bet?"Department of Electrical Engineering and Computer Science Wichita State University Wichita, Kansas 67260-0083mhtandel@wichita.edu, vxvenkitachalam@wichita.edu >CS837-F12-MW-04A

[10] Mushtaq Ali, Jasni Mohamed Zain, Mohammad Fadli Zolkipli, Gran Badshah"Mobile Cloud Computing & Mobile Battery Augmentation Techniques: A Survey" IEEE Publication 978-1-4799-6428-4/14/$31.00 ©2014

[11] Siddiqui Mohammad Saad et al, "Energy Efficient Mobile Cloud Computing"IJCSIT-International Journal of Computer Science and Information Technologies|Vol. 5 (6) , 2014, 7837-7840

[12] Eemil Lagerspetz,Sasu Tarkoma"Mobile Search and the Cloud: The Benefits ofOffloading"IEEE publication 2011

[13] Antti P. Miettinen,Jukka K. Nurminen"Energy efficiency of mobile clients in cloud computing"Nokia Research Center

[14] Alexander W. Min, Ren Wang, James Tsai, Mesut A. Ergin, Tsung-Yuan Charlie Tai"Improving Energy Efficiency for Mobile Platforms by Exploiting Low-power Sleep States"Circuits and Systems Research, Intel Labs CF'12, May 15–17, 2012, Cagliari, Italy.

[15]Sujithra Ma, Padmavathi G b, Sathya Narayananc" Mobile Device Data Security: A Cryptographic Approach by Outsourcing Mobile data to Cloud" Procedia Computer Science 47 (2015) 480 – 485

[16] https://en.wikipedia.org/wiki/ElGamal_encryption

[17] https://en.wikipedia.org/wiki/Paillier_cryptosystem

[18] https://en.wikipedia.org/wiki/Cramer%E2%80%93Shoup_cryptosystem

[19] https://en.wikipedia.org/wiki/Google_App_Engine