Creating Trust between Mobile and Cloud using Progressive Encryption

Neha Saini
Computer Science Engg Department,
Chd. College of Engg & Technology
Chandigarh, India

Mr. Mayank Arora
Chd. College of Engg & Technology
Chandigarh,India

Dr. Maitreyee Dutta
Professor & H.O.D
Computer Science & Engineering
NITTTR, Chandigarh, India

***Abstract*— Cloud computing is providing resources advent over a network which is benefiting almost all IT services. With software as a service and storage as service more and more enterprise applications are shifting towards Cloud platform making Smartphones their thin Clients and thus promoting Mobile Cloud Computing. Mobile cloud computing is a computing of data and storage of data outside the mobile device. The data storage and data processing happens on the cloud not on the mobile device. Thus mobile cloud computing provides the use of technology smartly and reserving the scarce resources of mobile. But as more and more sensitive information is passing the Mobile phones, the need of securing the information and creating a trust between the Mobile user and the Storage Cloud is emerging. This leads to the area to be focused that is security of mobile data, offloading to cloud for storage and processing. There are many encryption techniques used by researchers such as RSA, DES and AES for security purpose. These techniques have some loopholes. So, we are proposing a framework which will use ECC technique with progressive encryption to provide better security to the mobile data on cloud without creating much overhead on the Smartphone.**

Keywords:- Smartphone, Cloud Computing, Mobile Cloud Computing, Offloading, Encryption, Decryption, ECC, Progressive Encryption, PECE.

I. INTRODUCTION

Cloud computing means providing computing services (hardware & software) over the internet. The cloud computing model allows access to information and computer resources from anywhere, condition network connection should be available. Cloud computing provides a shared pool of resources including data storage space, networks, computer processing power and user applications. Cloud computing given a major change in how we store information and run applications. It has emerged as the great technology in term of scalability and portability. Cloud computing have different deployment models: a) Private cloud b) Public cloud c) Hybrid cloud d) Community cloud. Cloud computing has changed our view of carrying data and communication. Using cloud computing the user need not buy a powerful system, he just needs to connect to the internet through his tablet pc or smartphone and can use the computation power and memory of the cloud.

A. Mobile Computing

As a development and extension of Cloud Computing and Mobile Computing, Mobile Cloud Computing, as a new phrase, has been devised since 2009. Mobility has become a very popular word and rapidly increasing part in today's computing area. An incredible growth has appeared in the development of mobile devices such as, smartphone, PDA, GPS navigation and laptops with a variety of mobile computing, networking and security technologies. In addition, with the development of wireless technology like WiMax, Ad Hoc Network and WIFI, users may be surfing the Internet much easier but not limited by the cables as before. Thus, those mobile devices have been accepted by more and more people Mobile computing provides the ability to use the technology to wirelessly connect and use centrally located information through wireless computing and communication devices. Mobile cloud computing refers to an infrastructure where both the data storage and data processing happens outside the mobile devices.

B. Security in Cloud environment

Security in cloud environment is an important issue: security issues faced by their customer and security issues faced by cloud providers. There is a responsibility of cloud provider to ensure that their infrastructure is secure and their client's data and application while the user must ensure that the provider has taken the proper security measures to protect their information, and the user must take measures to use strong passwords and authentication measures. The given below are the various security concerns in a cloud computing environment.

- Access to server and applications
- Data Transmission
- Virtual Machine Security
- Network Security
- Data Security
- Data Privacy
- Data Integrity
- Data Location
- Data Availability
- Security Policy and Compliance

C. General cloud security Issues

In [12] Brodkin outlines seven security risks users need to consider in Cloud computing:

- Privileged user access: offloading sensitive data to the cloud would mean the loss of direct physical, logical and personnel control over the data.
- Regulatory compliance: the cloud service providers should be willing to undergo external audits and security certifications.
- Data location: the exact physical location of user's data is not transparent, which may lead to confusion on specific jurisdictions and commitments on local privacy requirements.
- Data segregation: since cloud data is usually stored in a shared space, it is important each user's data is separated from others with efficient encryption schemes.
- Recovery: it is imperative that cloud providers provide proper recovery mechanisms for data and services in case of technological failure or other disaster.
- Investigative support: since logging and data for multiple customers may be co-located, inappropriate or illegal activity should they occur may be very hard to investigate.
- Long-term viability: assurance that users data would be safe and accessible even if the cloud company itself goes out of business.

D. Mobile cloud security Issues

In addition to the aforementioned concerns, securing a mobile cloud introduces the following challenges as discussed in [12].

- Authentication between the weblets that would be distributed between the cloud and the device.
- Authorization for weblets that could be executing on relatively untrusted cloud environments to access sensitive user data.
- Establishment and verification of trusted weblet execution cloud nodes.

E. Progressive Elliptic Curve Encryption

Progressive elliptic curve encryption (PECE). The PECE scheme [1] allows a piece of data to be encrypted multiple times using different keys such that the final cipher text can be decrypted in a single run with a single key. The encryption and decryption are both based on Elliptic Curve Cryptography.

II. FINDING FROM SURVEY

A number of researchers proposed that the privacy of the data could be maintained if the data is encrypted before storing it on the cloud. This proposal gave birth to the idea of encrypting the data on the smartphone before sending it to the cloud.

- Researchers proposed that the data from the smartphone needs to be encrypted using the two encryption techniques RSA and DES [2]. These techniques have following limitations:

(a) The key size used for encryption using RSA is quite higher. Thus making it an extra overhead for the smartphone.

(b) In [2] the proposed scheme the data needs to be decrypted at the cloud side before second round of encryption. Thus making the whole point of encrypting the data at the smartphone side is useless.

- ECC (Elliptic curve cryptography) is a relatively better approach for public key cryptography. It uses shorter length key than other public key cryptosystems offering the same security level. For e.g. ECC 163-bit key offers the same security level as RSA with 1024- bit key. This implies less space for key storage and faster arithmetic operations. Further it has been shown [4] that ECC's security is higher than that provided by RSA. Using Progressive Encryption with ECC makes the technique stronger.

- A new scheme has been proposed which is highly suitable for the mobile cloud environment. According to which a piece of information could be encrypted multiple times at different points using different keys. But decryption could be done using single key in a single step.

III. PROBLEM DEFINITION

According to a survey, presently only 17% enterprise applications are on mobile devices and by 2018 almost 98% enterprise applications will be mobile. As of now with only 17% enterprise applications on the mobile devices, the data leakage is through mobile devices (mobile theft is very high). Moreover as the enterprise applications are shifting to mobile, the mobile devices are facing a crunch in the memory, thus shifting the mobile data to the external cloud storage providers.

In this scenario, the security needs to be provided from two different perspectives i.e. firstly, the data stored in the smartphone needs to be secured and secondly, the data to be stored in the cloud needs to be secured. According to the literature survey, the data stored on the Cloud by the smartphone could be secured by using certain approaches such as RSA, DES. But they have certain drawbacks such as they create heavy load on memory and processor of smartphone due to large key size and they are not much powerful against brute force attack and side channel attack. Moreover the data is decrypted at the Cloud side before re-encrypting the data, thus making the data vulnerable to compromise the privacy. To store the enterprise data on to the cloud requires high amount of trust between the cloud storage provider and the enterprise because it is possible to have highly sensitive data to be stored by the employees.

So there is a need of better approach to be used to ensure the security and privacy of smartphone and cloud data such as ECC using progressive encryption for mobile cloud environment.

IV. PROPOSED SOLUTION

It is proposed that we had developed a framework which is used by the Smartphone user and thus encrypted data is transferred from the smartphones user to cloud to perform progressive encryption with ECC to have more privacy and confidentiality

.It is also proposed that the framework will not impose much extra overhead on the smartphone as by the earlier proposed schemes. The proposed scheme will reduce the overhead by performing ECC encryption once on the required information, at the Smartphone side making the application lighter than RSA before uploading it to the Cloud storage.

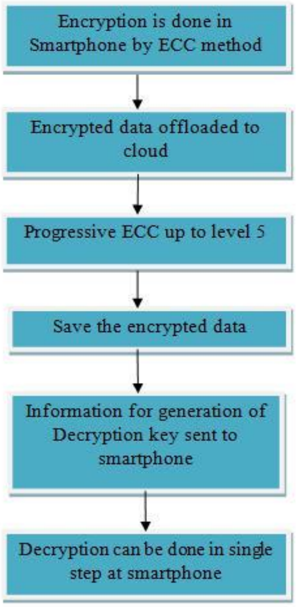

Encryption is done in Smartphone by ECC method
Encrypted data offloaded to cloud
Progressive ECC up to level 5
Save the encrypted data
Information for generation of Decryption key sent to smartphone
Decryption can be done in single step at smartphone

Fig.1. Flowchart for proposed methodology

To ensure the encrypted data cannot be misused, few more encryption steps may be performed on the Cloud side making it even more effective than the currently available encryption schemes such as AES or DES.

The decryption could be done by the authorized smartphone user's using a single decryption key provided by the owner of the data in a single step.

A. Encryption Process

As shown in figure 2, the plain text reaches the user smartphone, it is encrypted using ECC encryption before pushed towards the storage cloud.

Let D be a piece of data, U be a set of N users. For each u_i є U, u_i has the secret key k_i. Let q be a random number agreed by all u_i єU. The encryption is performed in the order of $u_1, \ldots, u_N$, it computes

$$D_i = D_{i-1} + qK_iG \text{ ………………… } (1)$$

Once the data has been encrypted the cipher text is pushed out of the phone toward the storage cloud. A random number q agreed upon by the smartphone and the computational cloud is also pushed along with the data with the cipher text.

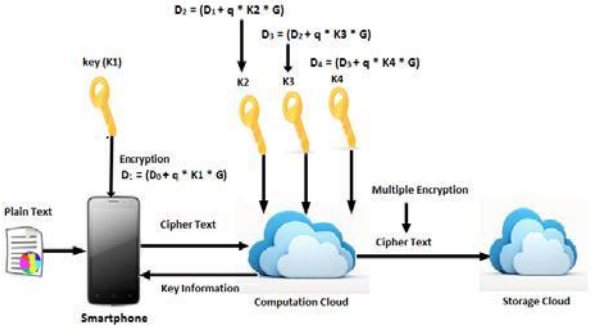


Fig.2. Encryption Process

Before reaching the storage cloud, the cipher text and the random number is received by the computational cloud which in term runs multiple rounds of re-encryption using different keys generated by it.

Where D_0 = D.

When all u ϵ U has participated in the encryption process, the final encrypted data is as follows.

$$\begin{aligned} D_\varepsilon &= D_N \text{ ……………………………… } (1) \\ &= D_{N-1} + (qK_NG) \text{ ……………… } (2) \\ &= D_{N-t} + \textstyle\sum_{i=N-t+1}^{N}(qk_iG) \text{ ……… } (3) \\ &= D_0 + \textstyle\sum_{i=1}^{N}(qk_iG) \text{ …………… } (4) \\ &= D + \textstyle\sum_{i=1}^{N}(qk_iG) \text{ …………… } (5) \end{aligned}$$

The multiple encryption cipher text is sent over the storage cloud for storage and the keys used for the encryption process by the computational cloud are sent back to the smartphone.

B. Decryption Key generation process

The decryption key as shown in figure 3 is generated by the smartphone using the key information from all the encryption process.

$$\text{Key} = K_1 + K_2 + K_3$$

Where K_1 is the key for encrypting the cipher text coming from smartphone, K_2 is the key for encrypting the cipher text resulted from before encryption and K_3 is the key for encrypting the cipher text resulted from third time encryption.

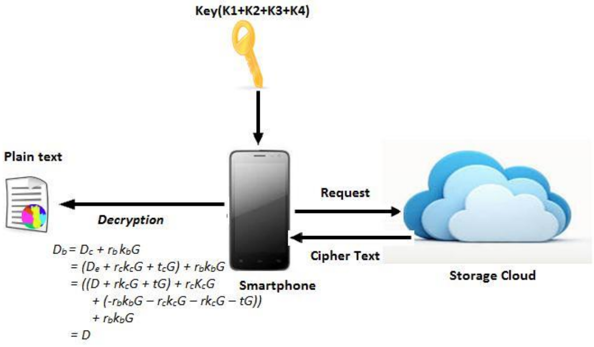

Key(K1+K2+K3+K4)
Plain text
Decryption
Request
Cipher Text
Smartphone
Storage Cloud
$D_b = D_c + r_b k_b G$
$= (D_e + r_c k_c G + t_c G) + r_b k_b G$
$= ((D + rk_c G + tG) + r_c K_c G$
$+ (-r_b k_b G - r_c k_c G - rk_c G - tG))$
$+ r_b k_b G$
$= D$

Fig.3. Decryption process

For security reasons the decryption process could only be performed by the smartphone which started the encryption process or by some other user to which a key is provided by the original smartphone user.

C. Decryption process

If the data earlier encrypted by the user is required by the user, he will send request to the storage cloud for the same. The data received by the smartphone would be multiple encrypted cipher text. This time the decryption process could directly take place on the smartphone by omitting the computational cloud in the way and decrypting the cipher text in the single go.

Let k_c = ∑ (i=1) ^N k_i then D_e can be decrypted by a single operation as follows.

$$\begin{aligned} Dp &= D_\varepsilon - qk_cG \\ &= D_\varepsilon - q\textstyle\sum_{t=1}^{N} k_iG \\ &= D_\varepsilon - \textstyle\sum_{t=1}^{N}(qk_iG) \\ &= D \end{aligned}$$

With PECE scheme, a piece of data can be encrypted multiple times using different keys. The final encryption produces a cipher text that can be decrypted using a single key with a single round of decryption.

V. RELATED WORK

Cloud computing provides computing resources as a service via the internet. Smartphones are feature rich phones with a recognized operating system which have strong internet connectivity and little processing capabilities.

G. Zhao et al. [1] proposed that Cloud computing, as associate rising computing paradigm, permits users to remotely store their knowledge during a cloud, thus on relish services on-demand. With fast development of cloud computing, additional and additional enterprises can source their sensitive knowledge for sharing during a cloud. To stay the shared knowledge confidential against untrusted cloud service suppliers (CSPs), a natural approach is to store solely the encrypted knowledge during a cloud. The key issues of this approach embody establishing access management for the encrypted knowledge, and revoking the access rights from users after they are not any longer licensed to access the encrypted knowledge. A progressive encoding theme supported elliptic curve encoding theme permits knowledge to be encrypted multiple times with completely different keys and produces a final cipher text that may be decrypted with one decoding key during a single decoding operation. This theme permits ever-changing the encoding key while not decrypting the info initial, so permits the re-encryption of information in associate Untrusted atmosphere. For secure sharing on the cloud encoding theme, permitting an information owner to store its encrypted data on a cloud and share with completely different users. The sharing is achieved by re-encrypting the info to the licensed users by the cloud supplier, sharing policies nominative by knowledge house owners, and preventing unauthorized access to knowledge.

In year 2013, Md. AI-Hasan et al. [2] followed with a work that Cloud computing architecture provides a proper management to share distributed resources and services throughout the world via computer network. A new data security approach for smartphone in cloud computing architecture, which ensures secured communication system and hiding information from others. Security level is maintained using the Global Positioning System (GPS) and network provider which ensures strong user-authentication to secure our cloud.

Year 2012 witnessed the proposal of Autonomous Computation Offloading Framework for Android using Cloud by M. Arora et al [3].They proposed a framework for making the applications of smartphones intelligent enough, to offload their compute intensive part from the smartphone to the virtual image of the smartphone on the cloud thus using the unlimited resources of the cloud.

A research by S. Maria Celestin Vigila and K. Muneeswaran [4] come up with the explosion of networks and the huge amount of data transmitted along, securing data content is becoming more and more important. This research presents the implementation of stream cipher, where the key stream is generated based on the properties of Linear Feedback Shift Register and cyclic Elliptic Curve over a finite prime field. In this research they proposed the process of encryption/decryption of an image in spatial domain and also encrypt key file parameters needed for generating the Key stream to other parties using Elliptic Curve Cryptography. Therefore the encrypted Key file parameters are only transmitted and not the entire full-length Key. Since Elliptic Curve Cryptography is replacing RSA for key exchange and Elliptic Curve based stream cipher offers a good choice for encryption in real time application.

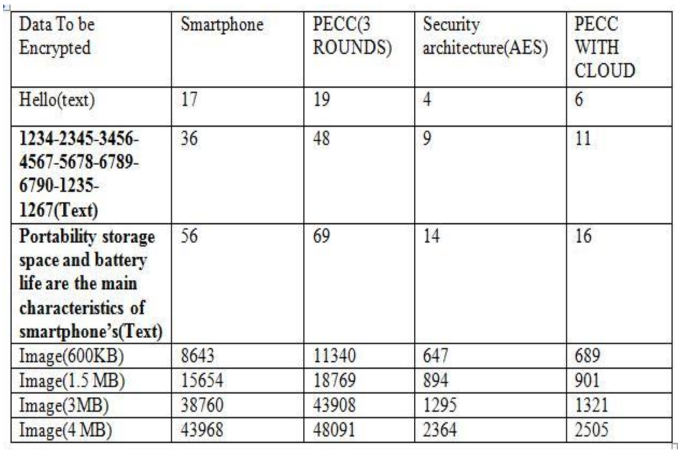
L. Subramanian et al. [12] proposed a generic architecture for providing security services in the cloud for smartphones within a corporate environment. Due to the resource constraints of smartphones, realizing security services for smartphones in the form of cloud services seem to be a natural fit. Researchers propose a generic architecture for providing security services in the cloud for smartphones within a corporate environment.

P. Teufl et al. [13] researched that high usability of smartphones and tablets by consumers as well as the corporate and public sector. The researchers proposed different encryption systems for android's that are assessed and their susceptibility to different attacks is analyzed in detail. Deploying Android in security-critical environments is a complex task, as confidential data might get compromised when being accessed, processed, and stored by insecure mobile devices.

VI. RESULTS AND DISCUSSION

MEASUREMENT OF EXECUTION TIME FOR THE ENCRYPTION PROCESS

To demonstrate the proposed work we developed an android application to encrypt data using AES encryption scheme on a smartphone. We encrypted certain text strings as given in the table below, as well as different images of different sizes. The applications develop by us showed the time consumed to encrypt the data. We used AES encryption scheme to create a benchmark for our comparisons as AES is the most commonly used/ robust encryption scheme being used now days. We implemented PECC as proposed in the base paper [1] for encrypting data on an android phone having three rounds of encryption. After comparing the results from the AES and three round of PECC showed that even after three round of encryption PECC proved to be taken only a fraction of time greater than the AES.



Data To be Encrypted	Smartphone	PECC(3 ROUNDS)	Security architecture(AES)	PECC WITH CLOUD
Hello(text)	17	19	4	6
1234-2345-3456-4567-5678-6789-6790-1235-1267(Text)	36	48	9	11
Portability storage space and battery life are the main characteristics of smartphone's(Text)	56	69	14	16
Image(600KB)	8643	11340	647	689
Image(1.5 MB)	15654	18769	894	901
Image(3MB)	38760	43908	1295	1321
Image(4 MB)	43968	48091	2364	2505

Table 1: Time consumption Comparison during encryption

As the results shown in the table below depict that AES proves to be a faster encryption scheme as compared to PECC as no encryption is taking place on the smartphone side and the whole encryption process is being offloaded to the cloud.

As shown in the graph below it is clear that PECC with cloud shown in purple color is a clear winner over AES running on the smartphone shown in Blue color. The amount of encryption done in both cases is same as only one round of PECC is being done on the Smartphone as in the case of AES.

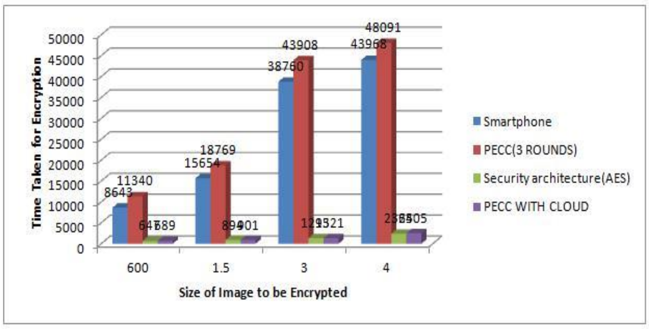
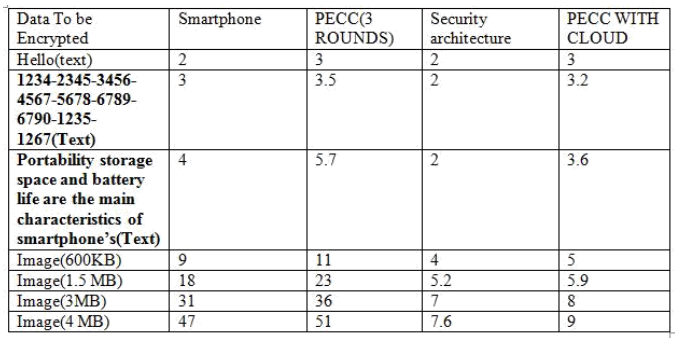


Figure 4: Graph showing comparison between time consumption by the encryption processes

MEASUREMENT OF EXECUTION ENERGY FOR THE ENCRYPTION PROCESS

The energy consumption of all the different architectures running on the smartphone as well as cloud is captured using a third party application named power tutor. Most researchers use this application for measuring the energy constraints. Power tutor is a research project [28, 29]. The energy consumed by an application is shown in Jules by the power tutor application.



Data To be Encrypted	Smartphone	PECC(3 ROUNDS)	Security architecture	PECC WITH CLOUD
Hello(text)	2	3	2	3
1234-2345-3456-4567-5678-6789-6790-1235-1267(Text)	3	3.5	2	3.2
Portability storage space and battery life are the main characteristics of smartphone's(Text)	4	5.7	2	3.6
Image(600KB)	9	11	4	5
Image(1.5 MB)	18	23	5.2	5.9
Image(3MB)	31	36	7	8
Image(4 MB)	47	51	7.6	9

Table 2: Energy consumption Comparison during encryption

As it is clearly visible in the graphs shown below the energy consumed by the PECC with cloud is slightly higher than the security architecture using AES.

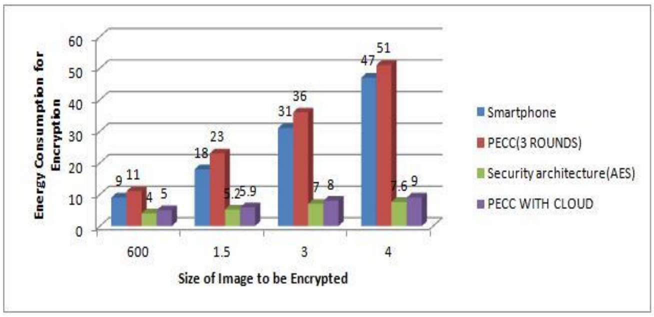
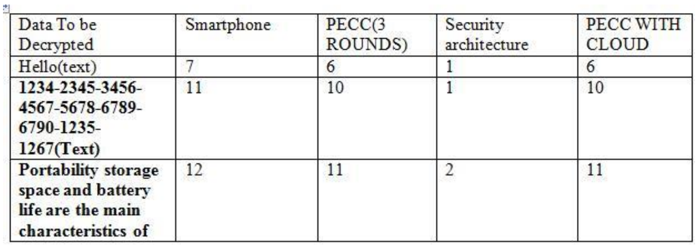


Figure 5: Graph showing comparison between energy consumption by the encryption processes

MEASUREMENT OF EXECUTION TIME FOR THE DECRYPTION

PROCESS

This makes the data vulnerable to threats. The architecture proposed in this paper sends data in encrypted format i.e. one round of PECC takes place on the smartphone preceding a couple of more rounds on the Cloud.



Data To be Decrypted	Smartphone	PECC(3 ROUNDS)	Security architecture	PECC WITH CLOUD
Hello(text)	7	6	1	6
1234-2345-3456-4567-5678-6789-6790-1235-1267(Text)	11	10	1	10
Portability storage space and battery life are the main characteristics of	12	11	2	11

Table 3: Time consumption comparison during decryption

The decryption process takes more time as compared to the AES running on the Cloud as no processing is being done at the smartphone side in case of AES and the whole decryption process is being done on the smartphone in case of the proposed architecture. Again as data at the Cloud is in the Plain Text format the issue of trust arises preventing smartphone users from using the Cloud.

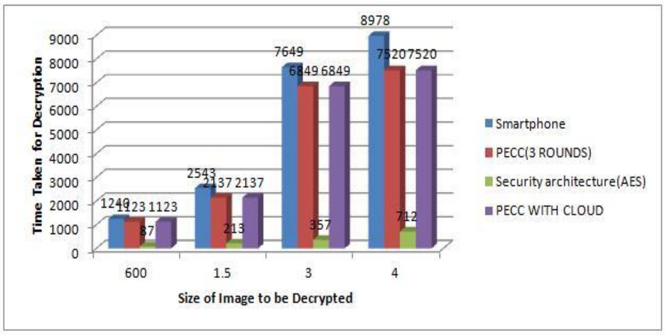
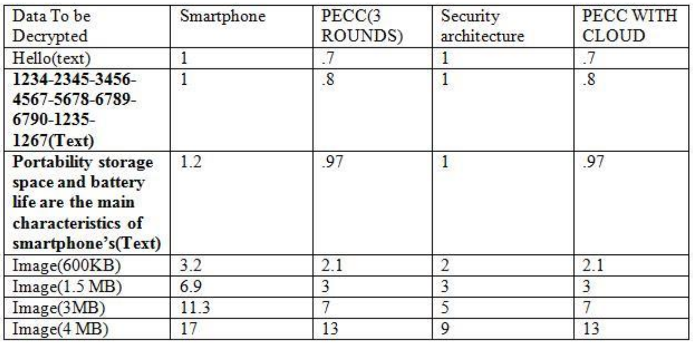


Figure 6: Graph showing comparison between Time consumption by the decryption processes

The proposed architecture ensures that the data is never in the Plain text format when going out of the smartphone or coming into the smartphone.

MEASUREMENT OF EXECUTION ENERGY FOR THE DECRYPTION PROCESS

While decrypting the text or images the PECC running on the smartphone and via the architecture consumes the same amount of energy as in both the cases only a single round of decryption is required which is taking place on the phone itself to ensure privacy. The key in the first case is with the smartphone and in the second case a part of key is with the smartphone user and rest of the part is sent to it by the computational cloud running the subsequent processes.



Data To be Decrypted	Smartphone	PECC(3 ROUNDS)	Security architecture	PECC WITH CLOUD
Hello(text)	1	.7	1	.7
1234-2345-3456-4567-5678-6789-6790-1235-1267(Text)	1	.8	1	.8
Portability storage space and battery life are the main characteristics of smartphone's(Text)	1.2	.97	1	.97
Image(600KB)	3.2	2.1	2	2.1
Image(1.5 MB)	6.9	3	3	3
Image(3MB)	11.3	7	5	7
Image(4 MB)	17	13	9	13

Table 4: Energy consumption comparison during decryption

As shown in the graphs below the energy consumed by the proposed scheme is slightly higher than the AES using cloud.

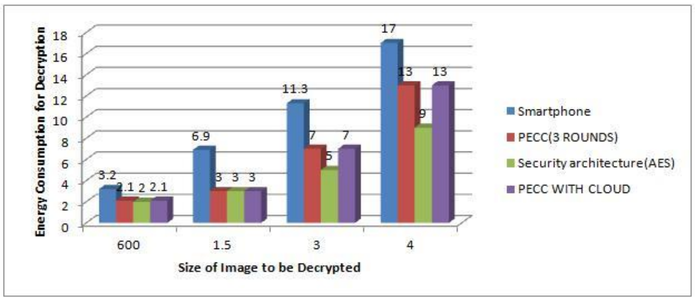


Figure 7: Graph showing comparison between Energy consumption by the decryption processes

CONCULSION

The enterprise applications are shifting to mobile; the mobile devices are facing a crunch in the memory, thus shifting the mobile data to the external cloud storage providers. In this scenario, the security needs to be provided from two different perspectives i.e. firstly, the data stored in the smartphone needs to be secured and secondly, the data to be stored in the cloud needs to be secured. There are different techniques used in literature survey such as RSA and DES which has certain drawbacks i.e. they create heavy load on memory and processor of smartphone due to large key size. Moreover the data is decrypted at the Cloud side before re encrypting the data. So there is a need of better approach to be used to ensure the security and privacy of smartphone and cloud data such as ECC using progressive encryption for mobile cloud environment.

The future scope of this research could lay a foundation to many new ideas such as issues in provisioning of a computational virtual Smartphone with the actual smartphone while a smartphone is purchased. Another approach is to devise a searching algorithm to search files in encrypted format, encrypted using PECC. A robust and secure key distribution method could also be clubbed with this research making the key distributable among several users of a common enterprise.

REFERNCES

[1] G. Zhao, C. Rong, Jin Li, F. Zhang and Yong Tang,“Trusted data sharing over untrusted cloud storage providers”, in 2nd *IEEE International Conference on Cloud Computing Technology and Science*, Page(s): 98 – 103, 2010.

[2] Md. AI-Hasan, K. Deb and M. O. Rahman, “User-Authentication approach for data security between smartphone and cloud”, in 8th *International Forum on Strategic Technology (IFOST),* Vol.2, Page(s): 2 – 6, 2013.

[3] M. Arora, M. Kalra and Dr. S. Singh, “Autonomous computation offloading framework for android using cloud” in 2nd *International Conference on Information Management in the Knowledge Economy,* 2013.

[4] S. Maria Celestin Vigila, K. Muneeswaran, “Elliptic curve based key generation for symmetric encryption” in *International Conference on Signal Processing, Communication, Computing and Networking Technologies , Page(s):* 824 – 829, 2011.

[5] M. M. Sandoval, C. F. Uribe, “A hardware architecture for elliptic curve cryptography and lossless data compression”, in 8th *International Conference on Electronics, Communications and Computers,* Page(s): 113 – 118, 2005.

[6] D. Mukherjee, H. Wang, A. Said, S. Liu, “Format independent encryption of generalized scalable bit-streams enabling arbitrary secure adaptations” in *IEEE International Conference on Acoustics, Speech and Signal Processing , Vol.* 2, Page(s): 1033 - 1036, 2005.

[7] S. Govindarajan, P. Gasti, K. S. Balagani, “Secure privacy- preserving protocols for outsourcing continuous authentication of smartphone users with touch data” in *IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS),* Page(s): 1 – 8, 2013 .

[8] P. Ragunathan, K. Sambath, V. Karthik, “Accessing a network using a secure android application” in *International Conference on Advanced Networking and Applications,* Vol. 4, Page(s):1503-1508, 2012.

[9] A. Tripathi and P. Yadav, “Enhancing security of cloud computing using elliptic curve cryptography” in *International Journal on Computer Applications*,Vol.57, Page(s): 1-8, 2012.

[10] G. Portokalidis, P. Homburg, K. Anagnostakis and H. Bos, “Paranoid Android: Versatile Protection for Smartphones,” in *Proceedings of the 26th Annual Computer Security Applications Conference*, Page(s): 347-356, 2010.

[11] E. Cuervo, A. Balasubramanian, D.K. Cho, A. Wolman, S. Saroiu, R. Chandra and P. Bahl, “MAUI: Making smartphones last longer with code offload,” in *Proceedings of the 8th international conference on Mobile systems applications and services*, Page(s): 49-62, 2010.

[12] L. Subramanian, Gerald Q. Maguire Jr. and P. Stephanow “An architecture to provide cloud based security service for smartphones”,[Online].Available:http://www.divaportal.org/smash /get/diva2:509785/FULLTEXT01.pdf.

[13] P. Teufl, A. Fitzek, D. Hein, A. Marsalek, A. Oprisnik and T. Zefferer “ Android encryption system”, in *Proceedings of the 8th internationalconference*,2014.[Online].Available:http://www.asit.a t/pdfs/Technologiebeobachtung/Android_Encryption_Systems_Pa per_1569918947.pdf.

[14] K. Bhardwaj and S. Chaudhary “Implementation of elliptic curve cryptography in ‘C’”, in *International Journal on Emerging Technologies*, Vol. 2, Page(s): 38- 51, 2012.

[15] A. Dabholkar and K. C. Yow “Efficient implementation of elliptic curve cryptography (ECC) for personal digital assistants (PDAs)” in *Journal on Wireless Personal Communication*, Vol. 29, Page(s): 233 – 246, 2004.

[16] A. Saarinen, M. Siekkinen, Y. Xiao, J. K. Nurminen, M. Kemppainen and P. Hui, “SmartDiet: Offloading popular apps to save energy,” in *Data Communications Conference on Association for Computing Machinery's Special Interest Group* , Page(s): 297-298, 2012.

[17] W. SONG and X. SU, “Review of mobile cloud computing,” in *IEEE 3’rd international conference on Communication Software and Networks*, Page(s): 1-4, 2011.

[18] J. Peng, X. Zhang, Z. Lei, B. Zhang, W. Zhang and Q. Li, “Comparison of several cloud computing platforms” in *Proceedings of IEEE international conference on Information Science and Engineering*, Page(s): 23-27, 2009.

[19] National Institute of Science and Technology, "The NIST,".Available: http://csrc.nist.gov/publications/nistpubs/800- 145/SP800-145.pdf. Last accessed on July 2014.

[20] R. Buyya, J. Broberg and A. Goscinski. Introduction to Cloud Computing in Cloud Computing: Principles and Paradigms, Wiley Press [Online], Page(s):1-44, 2011.

[21] Android Open Source Project. Philosophy and Goals. Available: http://source.android.com/about/philosophy.html. Last accessed on July 2014.

[22] M. A. Vouk, "Cloud Computing - Issues, Research and Implementations", in *Journal of Computing and Information Technology* - CIT 16, Vol. 4, Page(s): 235-246, 2008.

[23] Y. Hu, Wong, G. Iszlai, M. Litoiu "Resource provisioning for cloud computing", in *Proceedings of the Center for Advanced Studies on Collaborative Research*, Page(s): 101-111, 2009.

[24] Y. Tang, P. P. C. Lee, J. C. S. Lui, and R. Perlman, "FADE: Secure overlay cloud storage with file assured deletion", in *Proceedings of Secure Communication*, 2010.

[25] T. S. Kar, M. A. P. Mahmud, "A newer secure communication, file encryption and user identification based cloud security architecture" in *International Journal of Computer Applications*, Vol. 52, 2012.

[26] N. Fernando , Seng W. Loke , W. Rahayu, " Mobile cloud computing : A Survey" in *International Journal of Future Generation Computer Systems*, Page(s): 84-106, May 2012.

[27] K. Divya, N. Sadhasivam, “Secure data sharing in cloud environment using multi authority attribute based encryption” in *International Journal of Innovative Research on Computer and Communication Engineering* , Vol.2, Page(s): 24-29, March 2014.

[28] Power tutor application. Feb 2013. Available: http://ziyang.eecs.umich.edu/projects/powertutor/

[29] Mian Dong and Lin Zhong, “Self-constructive, high-rate energy modeling for battery-powered mobile systems,” in Proc. ACM/USENIX Int. Conf. Mobile Systems, Applications and Services(MobiSys), June 2011.

[30] J. Dean and S. Ghemawat, “MapReduce: simplified data processing on large clusters,” Commun. ACM, Vol. 51, 2008, Page(s). 107–113.

[31] G.F. F. Berman and T. Hey, Grid Computing: Making the Global Infrastructure a Reality, New York: Wiley, 2003.

[32] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, “The Eucalyptus Open-Source Cloud-Computing System,” In Proceedings of the 2009 9th IEEE/ACM International Symposium on Cluster Computing and the Grid, Washington, DC, USA: IEEE Computer Society, 2009, Page(s). 124–131.

[33] L.M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, “A break in the Clouds: towards a Cloud definition,” in Proceedings of SIGCOMM Comput. Commun. Rev., Vol. 39, 2009, Page(s). 50– 55.

[34] S. Perez, Mobile Cloud Computing: $9.5 billion by 2014, http://exoplanet.eu/catalog.php, 2010.

[35] E. E. Marinelli, “Hyrax: Cloud Computing on Mobile Devices using MapReduce,” Master Thesis, Carnegie Mellon University, 2009.

[36] H.Y. Kung, C.H. Chen, H.H. Ku, “Designing intelligent disaster prediction models and systems for debris-flow disasters in Taiwan,” Expert Systemswith Applications 39 2012, Page(s). 5838–5856.

[37] Weiguang SONG and Xiaolong SU, “Review of Mobile Cloud computing,” in proceedings of 3rd International Conference on Communication Software and Networks, 2011, Page(s).1-4.