International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 4 Issue 1 ǁ January. 2016 ǁ PP.36-45

Reduce Resources for Privacy in Mobile Cloud Computing Using Blowfish and DSA Algorithms

Tawfiq S. Barhoom, Mahmoud M. Abu Ghosh
Faculty of Information Technology Islamic University of Gaza (IUG) Gaza, Palestine
Faculty of Information Technology Islamic University of Gaza (IUG) Gaza, Palestine

Abstract: Mobile cloud computing in light of the increasing popularity among users of mobile smart technology which is the next indispensable that enables users to take advantage of the storage cloud computing services. However, mobile cloud computing, the migration of information on the cloud is reliable their privacy and security issues. Moreover, mobile cloud computing has limitations in resources such as power energy, processor, Memory and storage. In this paper, we propose a solution to the problem of privacy with saving and reducing resources power energy, processor and Memory. This is done through data encryption in the mobile cloud computing by symmetric algorithm and sent to the private cloud and then the data is encrypted again and sent to the public cloud through Asymmetric algorithm. The experimental results showed after a comparison between encryption algorithms less time and less time to decryption are as follows: Blowfish algorithm for symmetric and the DSA algorithm for Asymmetric. The analysis results showed a significant improvement in reducing the resources in the period of time and power energy consumption and processor.

Keywords: Mobile Cloud Computing, Security, Privacy, Blowfish, DSA***.***

I. INTRODUCTION

A. Cloud Computing

The Cloud Computing is gaining popularity with its main advantage of reducing the computational burden of the client and thus reducing the complexity and other infrastructure requirements at the client end. However, it is important to realize that the market is still deprived of cloud service providers because of following important issues [1]:

- Data replication
- Consistency
- Limited scalability
- Unreliability
- Unreliable availability of cloud resources
- Portability
- Trust
- Security
- Privacy

Data privacy is also important and is one of the main bottlenecks that restrict consumers from adopting mobile cloud computing. The users' data stored in the cloud may include emails, tax reports, personal images, salary and health reports etc, and may contain sensitive information. Therefore, the consumers cannot afford any privacy leakage as it may lead to financial loss and legal issues [2]. The European Union has passed some laws for the handling of data, according to which the data storage servers must reside in the countries that can provide sufficient protection. Moreover, in some cases the data storage location must be known. However, this is not always possible in a cloud environment due to the absence of standards, data privacy, and cloud security. Therefore, to gain consumers trust in the mobile cloud, the application models must support application development with privacy protection and implicit authentication mechanisms [2, 3].

The commonly accepted definition of Cloud computing is an IT service being provided to users on demand and being paid for depending upon amount of usage. It can also be termed as a dynamic service being provided to users that can add on to the available capacity and capabilities of user entity. Some of the key services of Cloud Computing as depicted in Fig. 1 are [1]:

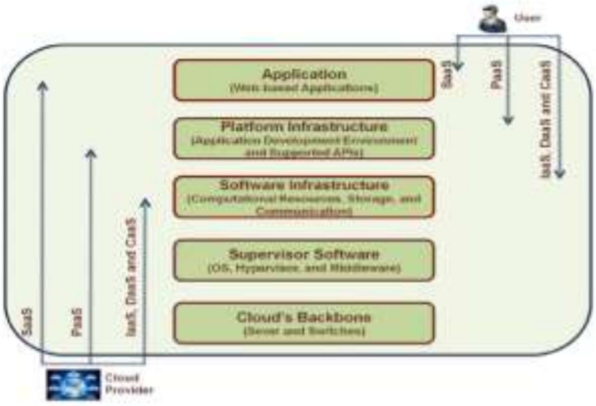

Fig. 1 Layered architecture of cloud computing [4]

Cloud computing providers offer their services according to several fundamental models:
1- Software as a Service (SaaS): The capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure with the possible exception of limited user-specific application configuration settings [2, 3, 5].

2- Platform as a Service (PaaS): The capability provided to the consumer to deploy onto the cloud infrastructure consumer created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations [2, 3, 5].

3- Infrastructure as a Service (IaaS): The capability provided to the consumer for provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g. host firewalls) [2, 3, 5].

B. Mobile Cloud Computing

The application of cloud is possible in many domains. One of the domains of our current interest is that of mobiles. Hence, we will be focusing on utility of cloud computing environment for mobile usage and how can a cloud add value to the overall functionality and performance of mobile devices? According to Khan et al [4] as depicted in Fig. 2, Mobile Cloud Computing is a service that allows resource constrained mobile users to adaptively adjust processing and storage capabilities by transparently partitioning and offloading the computationally intensive and storage demanding jobs on traditional cloud resources by providing ubiquitous wireless access.

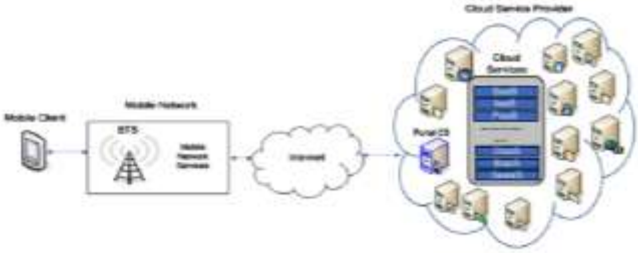

Fig. 2 Mobile Cloud Computing Architecture [4]

Some of the limitations of mobile devices which drive use of Cloud Computing for mobile devices are [1]:

- Limited battery
- Limited processing power
- Low storage
- Less security
- Unpredictable Internet connectivity

- Less energy

The mobile cloud applications execute in two ways. In the first case, the applications execute on the nearby infrastructure that acts as a (virtual) cloud, for instance, personal computers, laptops, and servers. In the second case, the applications execute in a real cloud, for instance, Amazon EC2, Google App Engine, and Microsoft Live Mesh. Therefore, the mobile cloud application models may support execution of the applications on either nearby infrastructure, cloud or both [1]. Execution resource significantly affects the scalability and availability of the application models. For instance, the availability of a nearby infrastructure is an unrealistic assumption, particularly when the user is on the move. Therefore, the assumption may be valid only for home and office environments, where the personal computers or nearby servers are available. However, some application models may require heavy software installations on the infrastructure to support computational offloading [2]. In principal, the personal computers do not promise virtually unlimited resources like real cloud platforms. Moreover, keeping the personal computers always in the ready state, just for the sake of computation offloading is not an energy efficient solution. Therefore, to make the application models scalable and capable of utilizing virtually unlimited resources with guaranteed availability; shifting the task of computation from the nearby infrastructure to the real cloud platforms is an appealing choice. Nevertheless, cloud computing is more energy efficient and the researchers have proposed different energy efficient techniques, that can get maximum output from the cloud based servers [2, 3].

TABLE I. CLOUD COMPUTING AND MOBILE CLOUD COMPUTING COMPARISON [2]

Issues	Cloud Computing	Mobile Cloud Computing
Device energy	┘	╮
Bandwidth utilization cost	┘	╮
Network connectivity	┘	╮
Mobility	┘	╮
Context awareness	┘	╮
Location awareness	┘	╮
Bandwidth	┘	╮
Security	╮	╮

An aim is a solution to the problem of privacy using encryption on fragmentation of the file with saving reducing resources. such as the time, processor, power energy, processor and memory.

II. RELATED WORK

Many researches have been done related to this field: -

A. Security and privacy issues of Mobile Cloud Computing have been discussed by many researchers.

Somani, Lakhani et al. in [6] have described the cloud storage methodology and proposed algorithm and Implementing the RSA algorithm through Digital Signature. And proposed the gradually process consumed in Digital Signature with RSA algorithm. If these implementing algorithms are combined in other encryption techniques (i.e. DES, AES etc) then it's became stronger and secure for cloud computing.

Naser, Ghosh et al. in [3, 5] have described a system called Secure Mobile Cloud Computing for sensitive data: Teacher Services for Palestinian Higher Education Institutions (MCCTSs) which is a mobile application to facilities access. and proposed the using RSA algorithm to encrypt the data which send and receive through Cloud computing application.

Zhou and Huang in [7] have described present a comprehensive security data inquiry framework for mobile cloud computing. solution focuses on the following two research directions: First, present a novel Privacy Preserving Cipher Policy Attribute-Based Encryption (PP-CP-ABE) to protect sensing data. using PP-CP ABE, light-weight devices can securely outsource heavy encryption and decryption operations to cloud service providers, without revealing the data content. Second, propose an Attribute Based Data Storage (ABDS) system as a cryptographic group based access control mechanism.

Jia, Zhu et al. in [8] have described design a secure mobile user-based data service mechanism (SDSM) to provide confidentiality and fine-grained access control for data stored in the cloud. the core idea of SDSM is that SDSM outsources not only the data but also the security management to the mobile cloud in a trust way. explored identity based proxy re-encryption scheme to make mobile users easily implement fine-grained access control of data and also guarantee the data privacy in the cloud.

Yang, Wang et al. in [9] have described proposes a novel public PDP scheme, in which the trusted third-party agent (TPA) takes over most of the calculations from the mobile end-users. by using bilinear signature and Merkle hash tree (MHT), the scheme aggregates the verification tokens of the data file into one small signature to reduce communication and storage burden. MHT is also helpful to support dynamic data update. mobile terminal devices only need to generate some secret keys and random numbers with the help of trusted platform model (TPM) chips, and the needed computing workload and storage space.

Current research initiatives seem to address only one or two parameters of security from the comprehensive set of authentication, integrity, confidentiality and privacy. These research approaches favor static security algorithms without considering changing demand for security, quality of service, and resource usage of mobile.

B. Security and privacy issues and Reduce Resources of Mobile Cloud Computing have been discussed by many researchers.

Khan, Kiah et al. in [10] have described an improve the resource limitation of mobile devices, mobile users may utilize cloud-computational and storage services. a light-weight security scheme is proposed for mobile user in cloud environment to protect the mobile user's identity with dynamic credentials. scheme offloads the frequently occurring dynamic credential generation operations on a trusted entity to keep minimum processing burden on the mobile device. to enhance the security and reliability of the scheme, the credential information is updated frequently on the basis of mobile-cloud packets exchange. the credentials are encrypted with the mobile user public key that ensures the confidentiality.

Khan, Kiah et al. in [11] have described an incremental version of proxy re-encryption scheme for improving the file modification operation and compared with the original version of the proxy re-encryption scheme on the basis of turnaround time, energy consumption, CPU utilization, and memory consumption while executing the security operations on mobile device. the incremental version of proxy re-encryption scheme shows significant improvement in results while performing file modification operations using limited processing capability of mobile devices.

Othman, Khan et al. in [12] have described article proposes a mobile cloud application development model, named MobiByte, to enhance mobile device applications' performance, energy efficiency, and execution support. MobiByte is a context-aware application model that uses multiple data offloading techniques to support a wide range of applications. The proposed model is validated using prototype applications and detailed results are presented.

Khan, Kiah et al. [13] in have described article Cloud-Manager-based Re-Encryption Scheme (CMReS) that combines the characteristics of manager-based re-encryption and cloud based re-encryption for providing the better security services with minimum processing burden on the mobile device. the proposed cloud-manager-based re-encryption scheme shows significant improvement in turnaround time, energy consumption, and resources utilization on the mobile device as compared to existing re-encryption schemes. in the CMReS, most of the encryption, decryption, and re-encryption operations are offloaded on trusted entity and cloud that improve the resource utilization on the mobile device.

Current research initiatives seem to address only parameters of security from the comprehensive set of authentication, integrity, confidentiality and privacy. and these research approaches favor static security algorithms with considering changing demand for security, quality of service, and reduce resource usage Such as (time, processor and power battery) of mobile.

An aim is to leverage cloud computing capabilities for augmenting resource-constraint mobile devices, this approach is the base for this research.

III. A PROPOSED REDUCE RESOURCES FOR PRIVACY IN MOBILE CLOUD COMPUTING

The proposed solution to the problem of privacy with saving and reducing energy and resources. the resources such as the processor and Memory, in mobile cloud environment with minimum processing burden, communication delay, and energy loss on the mobile device.

To achieve the requirements of the Privacy encryption algorithms using and there are a lot of them. It was a choice of two of each type of algorithms symmetric and asymmetric according to their popularity in the experiment are as follows [14, 15]:

- symmetrical algorithms (Blowfish, AES)
- asymmetric algorithms (RSA, DES)

The components used in the system model are (a) Public Cloud service provider, (b) mobile users, and (c) trusted entity called Private Cloud service provider as illustrated in Fig. 3.

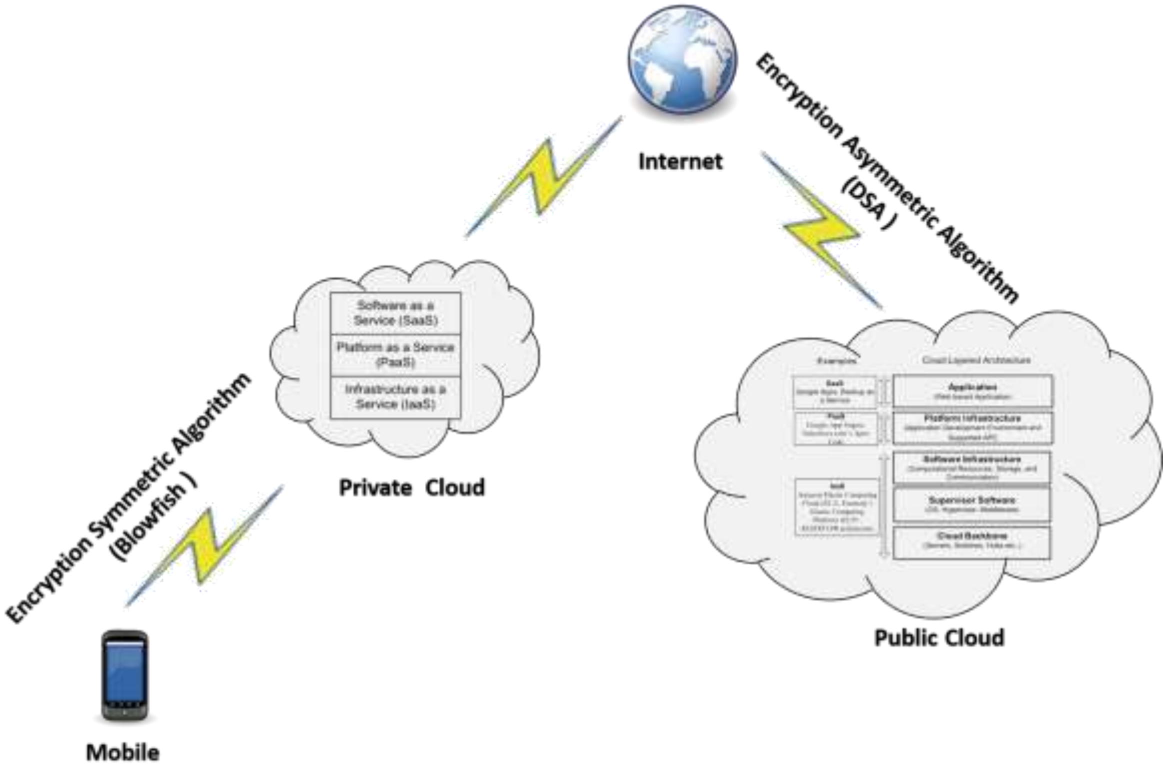
Internet
Encryption Asymmetric Algorithm (DSA)
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
Private Cloud
Examples
Cloud Layered Architecture
SaaS
PaaS
IaaS
Application
(Web based Application)
Platform Infrastructure
Software Infrastructure
Supervisor Software
Cloud Backbone
Public Cloud
Encryption Symmetric Algorithm (Blowfish)
Mobile

Fig. 3 The model proposed for Architecture Mechanism

This is done through data encryption in the mobile cloud computing by symmetric algorithm and sent to the private cloud and then the data is encrypted again and sent to the public cloud through Asymmetric algorithm as illustrated in Fig. 3.

During the experiment is to switch between the selected algorithms in encryption between mobile and private and public cloud, either symmetric or asymmetric, then compare the results and choose the least the time it takes the algorithm and processor power, memory and energy consumption.

Experimental setup

In the experiment it was installed the same private and public cloud to calculate the most accurate results, as in the specification Table I. the experiments are performed on private and public cloud using Samsung Galaxy S3 smartphone to evaluate the energy consumption and turnaround. The Samsung Galaxy S3 JDE 7.0.0 and Android SDK tools are used for the development of the mobile client applications. The mobile client applications interact with the manager and Public cloud service provider through socket programming and http post request/response methods, respectively. implemented using JDK 1.6, which updates the cloud and mobile secrets on behalf of the cloud service provider and mobile device. A single frontend web instant of class F4 having 1 GB of memory and 1.5 GHz of CPU capacity is hosted on the Google App Engine (GAE). The mobile client application interacts with the web instant hosted on GAE through the Private Cloud service provider. The hardware specifications of the smartphones and Cloud are presented in the Table II.

TABLE II. HARDWARE SPECIFICATIONS OF SMARTPHONES AND CLOUD

Specifications	**Device type**		
	Mobile	***Private Cloud***	***Public Cloud***
CPU	Dual-core 1.5 GHz	2 NO. Of Processors	4 NO. Of Processors
Memory	1 GB	4 GB	16 GB
Storage	8 GB	100 GB	500 GB
OS	Android OS v4.3	Linux	Linux
Battery	mAh1750	-	-
Internet	Wi-Fi	Lan	Lan
HTTP	Yes	NO	NO

IV. RESULTS & DISCUSSION

Experimental Results:-

The schemes are evaluated on the mobile device and (Private, Public) Cloud while performing encryption, decryption on the basis of as follows:

- Total turnaround time in seconds as illustrated in Fig. 4.
- Total power energy consumption in percentage as illustrated in Fig. 5.
- Total CPU utilization in percentage as illustrated in Fig. 6.
- Total memory consumption in megabytes as illustrated in Fig. 7.

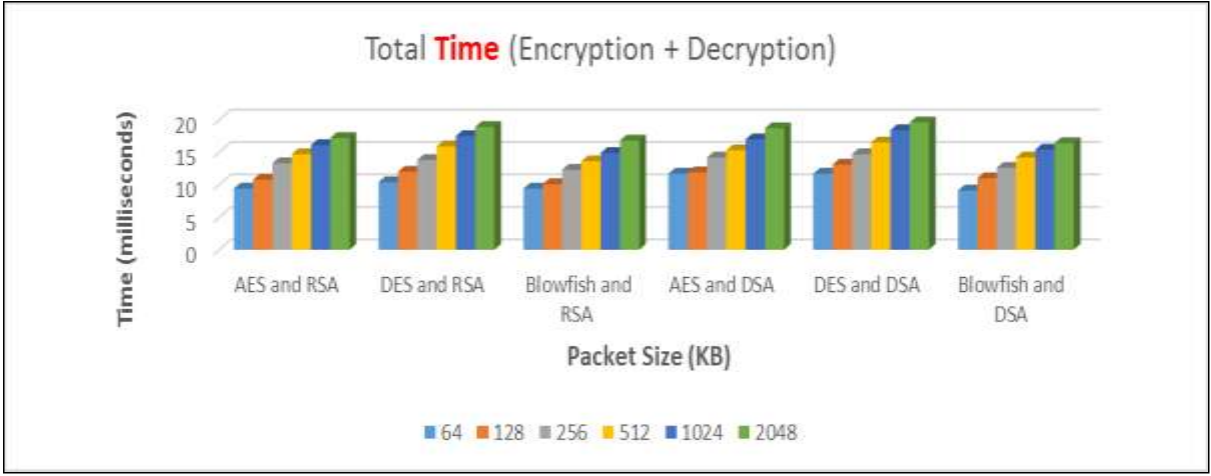

Fig. 4 Total Turnaround time according to type encryption

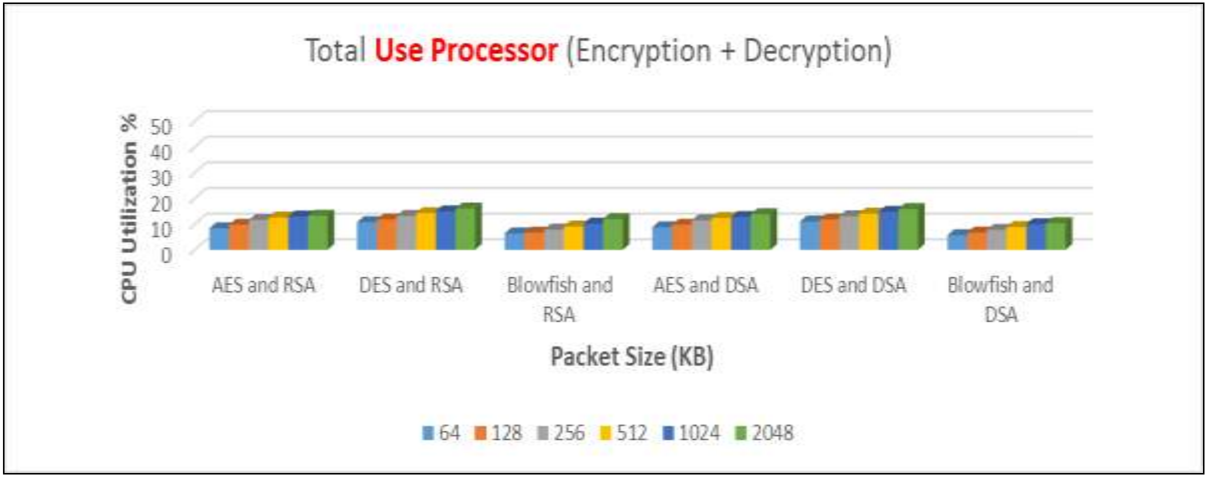

Fig. 5 Total Processor Utilization according to type encryption

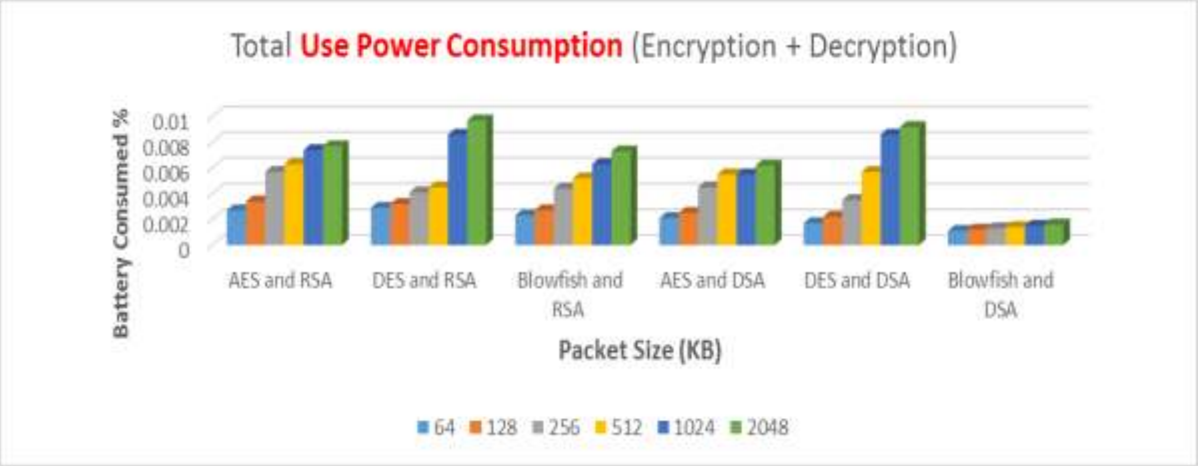

Fig. 6 Total Power Energy Consumption according to type encryption

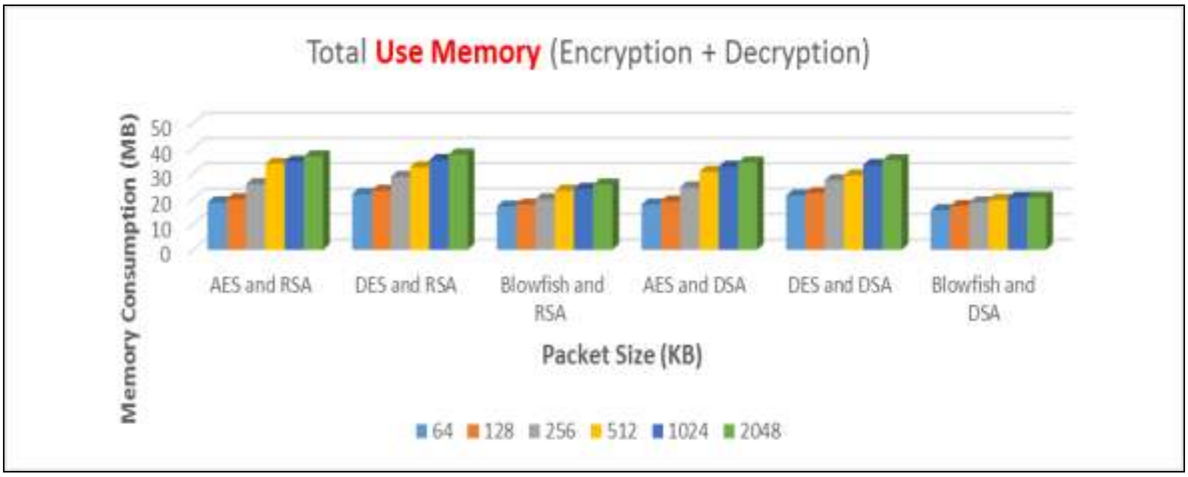

Fig. 7 Total Memory Consumption according to type encryption

The final results showed that the following algorithms are Blowfish and DSA least in the total time encryption and decryption Moreover least in the processor, memory and power energy consumption.

So, it has been adopted in this model they make the privacy clause and with the least resources such as time and processor, memory and power energy consumption.

The data is encrypted in the mobile by symmetry algorithm (Blowfish) and send public key to the private cloud and are decryption versa as in Fig. 8.

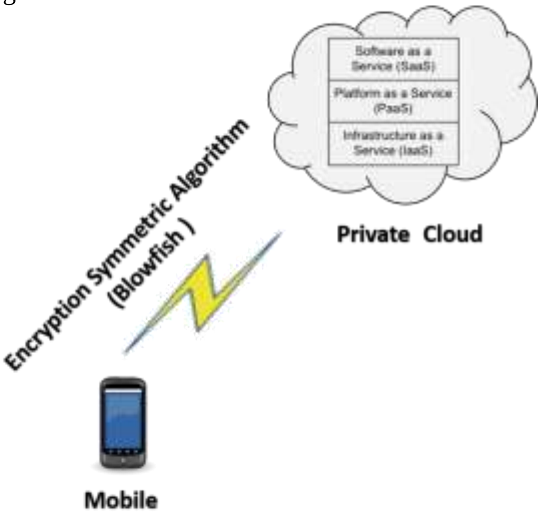
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
Private Cloud
Encryption Symmetric Algorithm (Blowfish)
Mobile

Fig. 8 Encryption and decryption Architecture Mechanism between the mobile and the private cloud

TABLE III. BLOWFISH OF ENCRYPTION (FROM MOBILE TO PRIVATE CLOUD) AND DECRYPTION TIME (FROM PRIVATE CLOUD TO MOBILE)

Size Packet (KB)	*Time Encr. (Sec)*	*Decr. Time (Sec)*	*CPU (%)*	*Memor y(MB)*	*Power (%)*
64	0.6	0.3	5.4	12.9	0.0011
128	0.8	0.5	6.2	14.2	0.0012
256	1	0.9	7.3	15	0.0013
512	1.1	1.1	8.2	15.9	0.0014
1024	1.2	1.3	9.1	15.3	0.0015
2048	1.4	1.5	9.3	15.08	0.0016

The data is encrypted in the private cloud by symmetry algorithm (DSA) and send public key to the public cloud and are decryption versa as in Fig. 9.

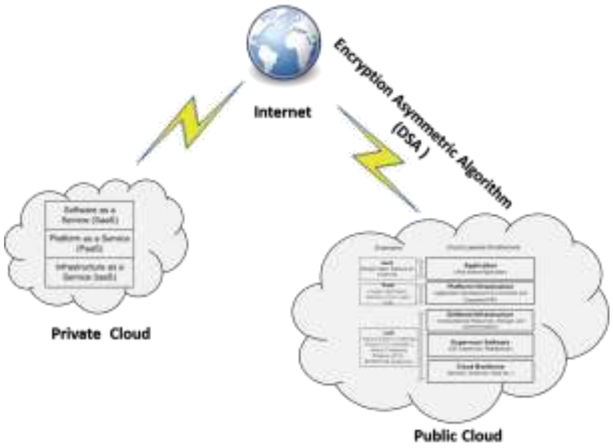
Internet
Encryption Asymmetric Algorithm (DSA)
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
Private Cloud
Public Cloud

Fig. 9 Encryption and decryption Architecture Mechanism between the private cloud and the public cloud

TABLE. IV DSA OF ENCRYPTION (FROM PRIVATE CLOUD TO PUBLIC CLOUD) AND DECRYPTION TIME (FROM PUBLIC CLOUD TO PRIVATE CLOUD)

Size (KB) Packet	***Time Encr. (Sec)***	***Decr. Time (Sec)***	***CPU (%)***	***Memory(MB)***
64	4.7	3.5	0.3	2.8
128	5.6	4.1	0.5	3.1
256	6.4	4.3	0.5	3.7
512	6.5	5.5	0.7	3.8
1024	6.8	6.1	0.9	5.3
2048	7.1	6.4	1.1	5.6

The results showed on the basis of turnaround time in seconds, energy consumption in percentage, CPU utilization in percentage, and memory consumption in megabytes on the mobile device to private cloud as in Fig. 8 while performing encryption, decryption Using Blowfish encryption and decryption, and Private Cloud to Public Cloud as in Fig. 9 while performing encryption, decryption Using DSA encryption and decryption.
Show that with increased package size with double the number 2 (X^2) there is a significant increase in the time, CPU, memory and Power Energy consumption gradually in the Table III, Table IV.

Difference Between two Algorithms:-

The Table V Blowfish and DES algorithms also shows the difference between the Table VI Blowfish and RSA algorithms in less resources such as time and processor, memory and power energy consumption.
The results showed on the basis of turnaround Total of time in seconds, energy consumption in percentage, CPU utilization in percentage, and memory consumption in Megabytes on the mobile device, Public and Private Cloud while performing encryption, decryption Using Blowfish and DSA encryption and decryption in the Table V, and Using Blowfish and RSA in the Table VI.
Show that with increased package size with double the number 2 (X^2) there is a significant increase in the time, CPU, memory and Power Energy consumption gradually in the Table V, Table VI.

TABLE V. TOTAL BLOWFISH AND DSA OF ENCRYPTION TIME (FROM PRIVATE CLOUD TO PUBLIC CLOUD) AND DECRYPTION TIME (FROM PUBLIC CLOUD TO PRIVATE CLOUD*)*

Size Packet (KB)	***Time Encr. (Sec)***	***Decr. Time (Sec)***	***Total Time (Encr + Decr) (Sec)***	***CPU (%)***	***Memor y(MB)***	***Power (%)***
64	5.3	3.8	9.1	5.7	15.7	0.0011
128	6.4	4.6	11	6.7	17.3	0.0012
256	7.4	5.2	12.6	7.8	18.7	0.0013
512	7.6	6.6	14.2	8.9	19.7	0.0014
1024	8	7.4	15.4	10	20.6	0.0015
2048	8.5	7.9	16.4	10.4	20.68	0.0016

TABLE VI. TOTAL BLOWFISH AND RSA OF ENCRY.TIME (FROM PRIVATE CLOUD TO PUBLIC CLOUD) AND DECR. TIME (FROM PUBLIC CLOUD TO PRIVATE CLOUD*)*

Size Packet (KB)	***Time Encr. (Sec)***	***Decr. Time (Sec)***	***Total Time (Encr + Decr) (Sec)***	***CPU (%)***	***Memory (MB)***	***Power (%)***
64	5.2	4.2	9.4	6.4	17.1	0.0023
128	5.7	4.4	10.1	6.7	17.8	0.0027
256	6.9	5.4	12.3	7.9	20	0.0044
512	7.5	6.1	13.6	9.1	23.3	0.0052
1024	8.1	6.8	14.9	10.2	24.1	0.0063
2048	8.9	7.9	16.8	12	25.8	0.0073

Experimental Results of the Performance:-

After selecting Blowfish and DES Algorithms encryption and decryption, the results show that with increased package size with double the number 2 (X^2) there is a significant increase progressively in the Turnaround time, Processor Utilization, Memory and Power Energy Consumption as in Fig. 10,11,12,13.

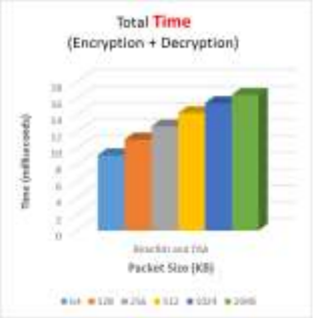

Fig. 10 Processor Utilization

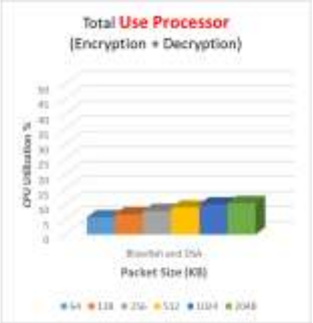

Fig. 11 Turnaround time

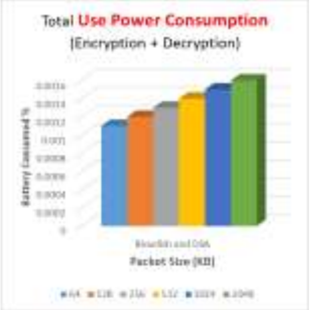

Fig. 12 Power Energy Consumption

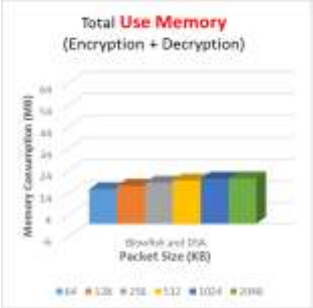

Fig. 13 Memory Consumption

V. CONCLUSIONS

In this paper, we presented a system called: reduce resources for privacy in mobile cloud computing using blowfish and DSA algorithms, which to reduce resources such as the time it takes the processor, memory and battery power. Also, a discussion of various symmetric encryption algorithms and asymmetric that can support dramatically privacy. This is done through data encryption in the mobile cloud computing by symmetric algorithm and sent to the private cloud and then the data is encrypted again and sent to the public cloud through Asymmetric algorithm. The experimental results showed after a comparison between encryption algorithms less time and less time to decryption are as follows: Blowfish algorithm for symmetric and the DSA algorithm for Asymmetric. The analysis results showed a significant improvement 34.12% from the previous in reducing the resources in the period of time and energy consumption and processor. It was proposed to apply the program of Mobile cloud computing services in the Palestinian academic institutions of higher education (MCCAS) who added privacy and safety while reducing the time in encryption and decryption, power energy consumption and processor significantly from its predecessor, where the increase in time by 17%, which is reasonable and acceptable for the end user. Furthermore, it has been compared most of the time until the peak time, which was not affected on a large which proves the effectiveness of the proposal.

Acknowledgment

We would like to thank all people who provided any type of help in this paper.

References

[1.] Chaturvedi, M., et al., Privacy & Security of Mobile Cloud Computing. Ansal University, Sector, 2011. 55.

[2.] Khan, A.R., et al., A survey of mobile cloud computing application models. Communications Surveys & Tutorials, IEEE, 2014. 16(1): p. 393-413.

[3.] Naser, S.S.A., M.A. Ghosh, and R.R. Atallah, Mobile Cloud Computing: Academic Services for Palestinian Higher Education Institutions (MCCAS). International Journal of Research in Engineering and Science (IJRES), 2015.

[4.] Khan, A.N., et al., Towards secure mobile cloud computing: A survey. Future Generation Computer Systems, 2013. 29(5): p. 1278-1299.

[5.] Naser, S.S.A., M.A. Ghosh, and R.R. Atallah, Secure Mobile Cloud Computing for Sensitive Data: Teacher Services for Palestinian Higher Education Institutions. International Journal of Advanced Science and Technology (IJAST), 2016.

[6.] Somani, U., K. Lakhani, and M. Mundra. Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. in Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on. 2010. IEEE.

[7.] Zhou, Z. and D. Huang. Efficient and secure data storage operations for mobile cloud computing. in Proceedings of the 8th International Conference on Network and Service Management. 2012. International Federation for Information Processing.

[8.] Jia, W., et al. SDSM: a secure data service mechanism in mobile cloud computing. in Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on. 2011. IEEE.

[9.] Yang, J., et al., Provable data possession of resource-constrained mobile devices in cloud computing. Journal of networks, 2011. 6(7): p. 1033-1040.

[10.] Khan, A.N., et al., Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing. The Journal of Supercomputing, 2013. 66(3): p. 1687-1706.

[11.] Khan, A.N., et al., Incremental proxy re-encryption scheme for mobile cloud computing environment. The Journal of Supercomputing, 2014. 68(2): p. 624-651.

[12.] Othman, M., et al., MobiByte: An Application Development Model for Mobile Cloud Computing. Journal of Grid Computing, 2015: p. 1-24.

[13.] Khan, A.N., et al., A Cloud-Manager-Based Re-Encryption Scheme for Mobile Users in Cloud Environment: a Hybrid Approach. Journal of Grid Computing, 2015: p. 1-25.

[14.] Chaudhari, M.P. and S.R. Patel, A Survey on Cryptography Algorithms. International Journal, 2014. 2(3).

[15.] Ebrahim, M., S. Khan, and U.B. Khalid, Symmetric algorithm survey: a comparative analysis. arXiv preprint arXiv:1405.0398, 2014.