Secure and Energy efficient model with modified offloading algorithm in Mobile Cloud Computing using Advanced Diffie-Hellman Algorithm

Dr B.Anni Princy, A.Anto Crescentia, L.Charupreetha, S.Nivetha, S.Prathiba

Abstract— Mobile cloud computing is an evolving technology which is still unclear to many security problems and ensuring the security of data storage in cloud servers is one of the most challenging task. This paper proposes an algorithm which ensures to solve data protection and user authentication problems. In the proposed model an encryption and key exchanging mechanism has been described based on combination of Advanced Encryption Standard (AES), Triple Data Encryption Standard (DES) encryption algorithm and Advanced Diffie-Hellman algorithm which helps to enhance security in mobile cloud computing. Moreover, this paper focuses on to resolve the waste energy in the network and for this purpose offloading algorithm has been used. Since offloading algorithm has been used, data splitting can also be done in an efficient manner. In Advanced Diffie Hellman Algorithm, complex mathematical calculations have been applied on both sender side and receiver side in order to make communication more secure. Thus, it makes difficult for the intermediate person to decipher the code.

Index Terms—Authentication mechanism, Cloudlets, Cryptography, Key Exchange, Mobile Cloud Computing, Offloading Algorithm, Security

1. INTRODUCTION

Mobile Cloud Computing (MCC) originates from the concept of Cloud computing, it is fundamentally an integration of cloud computing and mobile networks to bring the services especially for the mobile users. It is an infrastructure which offers calculation and capacity assets on demand rather than maintaining large data storage on device**.** The cloud computing provides many resources to the customers using various technologies, such as Web services, virtualization, and multi-tenancy. The cloud services are distributed to the customer through the Internet whereas, the web applications are used to access and manage cloud resources that makes web applications an important component of the cloud computing . Based on the concept of cloud computing, mobile cloud computing is defined as a model which afford various IT resources and information services over the mobile network by the means of on-demand self-service. Mobile cloud computing is an application of cloud computing in combination with mobile devices Mobile cloud computing enables mobile clients to place their requests on the cloud servers through their mobile devices. The cloud servers handle those requirements and send the response back to the mobile devices. The vicinity of the cloud infrastructure neglect the need of inaugurating additional processing or memory unit to a mobile device. However, this convenient arrangement could be a threat to the system. Accessing cloud infrastructure by a mobile device through an entrusted channel or network leads to the compromise of the confidentiality of the data being transmitted. By outsourcing the information documents into the cloud, it gives numerous advantages to the extensive ventures and also singular clients because they can progressively expand the storage space as and when requires without buying their storage devices. The clients can get the remotely stored information anytime from anywhere and gives permission to approved clients to share the information. The clients can be alleviated from the burden of storage management at local device and it also leads to avoidance of capital consumption on equipment and programming costs and so forth. By using enable mobile cloud computing the complex data processing and the massive data storage are implemented in the cloud. So the burden of the calculation and storage on mobile equipment is reduced. Besides, it have intelligence to balance load and to save electricity, so the mobile cloud computing can resolve the sustain problem of the battery and improve the battery life of mobile equipment.

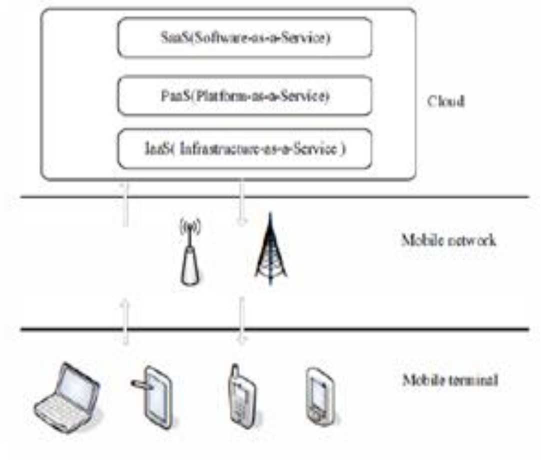

SaaS(Software-as-a-Service)
PaaS(Platform-as-a-Service)
IaaS(Infrastructure-as-a-Service)
Cloud
Mobile network
Mobile terminal

Fig. 1 Model of Mobile Cloud Computing

Figure 1 explains the basic model for mobile cloud computing. Whereas, it is composed of three major components including mobile terminal, mobile network and cloud. Mobile terminal refers to the mobile devices to access the cloud, such as smart phones, tablet PC's. The cloud includes the infrastructure centres and servers providing the IT resource or information service, e.g. Infrastructure-as-a-Service (IaaS, including all kinds of servers, databases, storage devices, parallel and distributed computing systems), Software-as-a-Service (SaaS, including all kinds of software, data and information), Platform-as-a-Service (PaaS, including operation platform, support platform and development platform).

One of the biggest obstacles in the extensive approval cloud computing is security. Several business and research organization are hesitant in completely trusting the cloud computing to move computerized assets to the third-party service contributors. The ordinary IT infrastructure keeps the computerized resources in the administrative field of the organizations. All of the processing movement and management of data/application are performed inside an organizational administrative domain. On the other hand, organizations do not enjoy administrative control of cloud services and infrastructure. The security measures taken by the cloud service providers (CSP) are generally transparent to the organizations. The vicinity of huge extent of clients that are not related within the organizations, aggravate the concerns further. The users might be trusted by the CSP but they may not be of trust to each other. The aforementioned reasons keep the customers under uncertainties about their digital assets located at the cloud resulting in reluctance to adopt cloud computing.

1.1 Cloudlets

With the emerging cloud computing and the explosive growth of mobile applications, mobile cloud computing (MCC) has become a promising technology for mobile services. In MCC, mobile devices, such as smart phones and tablets, can offload data storage and computational task on to the cloud through wireless communications, thereby overcoming their limited capabilities regarding processing power, storage capacity, and battery lifetime.

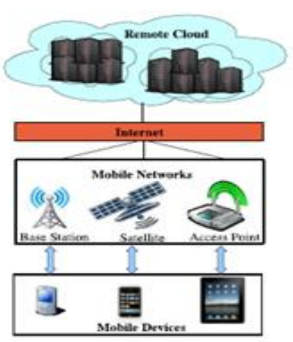


Figure 2 Remote cloud in MCC

The *remote cloud* provides data storage and computing service while mobile devices are clients to access the service through wireless networks, mainly cellular and WLAN (Wireless Local Area Network). When accessing a remote cloud is costly due to long WAN (Wide Area Network) latencies, a mobile user can exploit nearby Computers that are well-connected to the Internet and uses cloud service over a high-bandwidth WLAN. The vast computation resources on remote cloud servers can enable computation intensive applications, such as image processing for video games, optical character recognition (OCR), and augmented reality, run on mobile devices.

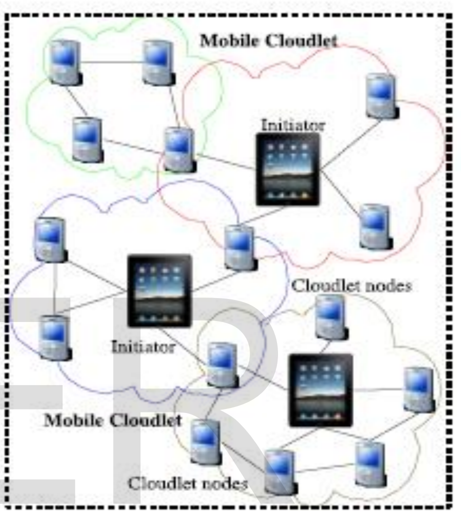


Fig. 3 Mobile cloudlet in MCC

Fig. 3, *a group of nearby mobile devices can connect by WiFi or Bluetooth to form a mobile cloudlet*, in which mobile devices (referred to as cloudlet nodes) can be computing service providers as well as clients of the service. By dividing the task among cloudlet nodes, the initiator mobile device could speedup computing and conserve energy. Users can get direct cloud computing access instantly through interactions among one another, eliminating the communication latency and data roaming charges introduced by the cellular networks. Mobile cloudlet is appealing to users pursuing a common goal in group activities, such as multimedia sharing for audience at an event and language translation for a group of tourists in a foreign country. The major concern of using mobile cloudlet resides in the limited computing power of mobile devices and the unstable connections between cloudlet nodes due to node mobility.

1.2 Green Cloud Computing

The use of Green Cloud Computing has increased substantially in the recent past. A lot of research has been done to incorporate and enhance the applicability of Green Cloud in real life scenarios with these help of various parameters. Usage of energy is dramatically increases in data centres.

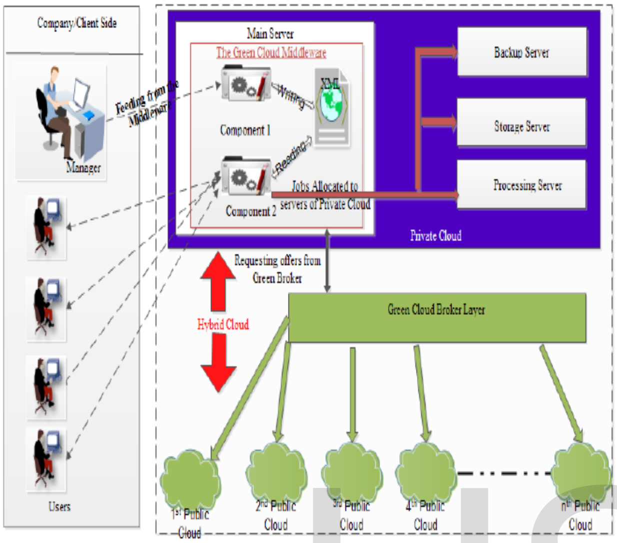


Fig 4. Integrated green Cloud architecture

This architecture has two elements; one is the client and second is the server side. In the client side the manager and the users are present, which deals with the execution destination of the job and in the server side includes the green cloud middleware, green broker and sub servers like processing servers , storage servers etc. The directory concept is used in the green broker layer of IGCA for organizing all the information of the public cloud and provides the best green service to the user.

The green cloud middleware has two components. The manager is the main head that deals with one component and stores all the information of the middleware. The usage of the user's PC, the servers present on the private clouds all the information. The frequencies of each sever like high, medium and low. The energy usage, storage capacity and other information also exist in the component of middleware.

When the manager got request from the client. The request is dividing into jobs and distributed among the users meanwhile they also stores the information about job into the component. The carbon emission and energy used for the execution of job on the private cloud by servers, on the public cloud by using green broker or on the client's PC is calculated and show to the users. The best green offer is selected by the manager by taking into consideration the security level of the job also. When the decision is making out by the manager then this information is store in the XML file for future usage.

The second component is accessed by all the users for reading the XML file. This file stocks all the information of the execution of job. The locations of the jobs are registered in the file and according to the addresses, they will execute. If the job entry is not in the file then the job will be executed either on the PC of the client or in the private cloud. The execution of job is takes place in three places. First if the job is executed LOCALLY (on the requester side) then this information is stored in the client side so next time when the request arrives it will not get through will middleware. If the job is executed in the private cloud the location as well as the server name is fetched from the file. Or if it is in public cloud, we will take help from the green broker to know the most excellent green decision for the execution of the job. The middleware know all the information about the three places. Energy used by the workers working in the company is also calculated by the middleware for taking further decisions.

The processing speed, energy consumption, bandwidth or others factors are responsible for deciding the best location for the execution of the job. By considering all the factors the middleware will compute and judge the place from the three places. The IGCA provides the balance in the job execution and provide the security and quality of service to the clients. The manager divides the task and top quality green solution by considering all the places (public, private, local host).

In this architecture the manager plays the central coordinator work which allocates the job to the users and does all decision making. But at the same time the manager is the weakest point in this architecture as it is the central point of failure, as if the manager fails everything in the architecture collapses.

2. PROBLEM STATEMENT

Organizations can use services and data stored as and when required at any physical location outside their own control. This facility raised the various security issues like privacy, confidentiality, integrity etc., and demanded a trusted computing environment wherein data confidentiality can be maintained. To get rid of the same and to induce trust in the computing, there is need of a system which provides authentication, verification and encrypted data transfer, hence maintaining data confidentiality.

3. PROPOSED SYSTEM

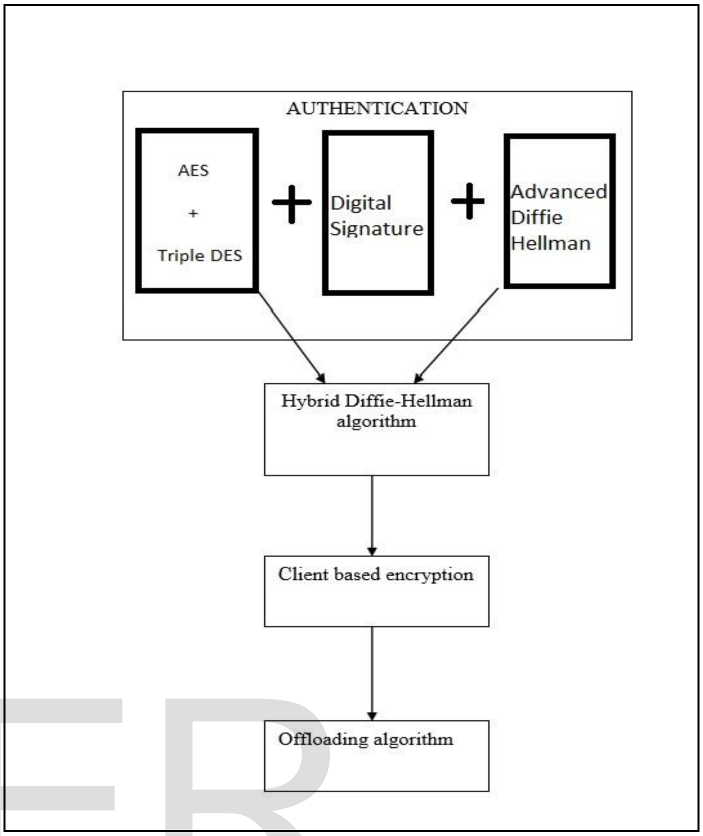
In the proposed architecture, we are using three ways of protection scheme. Firstly, to generate keys for key exchange step, Advanced Diffie Hellman algorithm is used.

Then digital signature is used for authentication, there after user's data file is encrypted or decrypted using AES and Triple DES Algorithm. With this algorithm data will be uploaded into cloud server by double encryption .Initially data will be encrypted using AES algorithm and again re encryption will be done by 3DES and similar lily data will be downloaded from the cloud server by decrypting the file as exactly reverse of encryption process. All this is implemented to provide trusted network at the server end. For the same reason two separate servers are maintained, one for encryption process known as (trusted) computing platform and another known as storage server for storing user data file. When a user wants to upload a file to the cloud server, first key are exchanged using Advanced Diffie Hellman key exchange at the time of login, then the client is authenticated using digital signature. Finally user's data file is encrypted using hybrid encryption algorithm and only then it is uploaded to Cloud Storage server. The client can download the same file, from Cloud server. When a user logins, first encryption keys are exchanged, file to be downloaded is selected, authentication takes place using digital signature and AES and 3DES algorithm is used to decrypt the saved file and client is allowed to access the file.

The main aim of this research is used to improve the security as well as energy efficiency and resolve the waste energy in the mobile cloud computing. It proposes the secure authentication for the user anonymity, in order to provide secure mobile clouds. It is used to resolve the additionally energy consumption in the wireless communication, by proposing the energy aware model in the dynamic cloudlet with secure authentication method and it reduces the latency delay and provides the user authentication and authorization. To minimize the energy consumption in the mobile devices, we propose the offloading algorithm with the energy aware model for resolving additional unwanted energy in the MCC and for security, enhanced client access based user authentication method is incorporated in this proposed design. In proposed offloading algorithm, we incorporate the data caching mechanism and improve task management strategies with dynamic energy scheduling algorithm with time constraints for improving the energy optimization while performing the task in the dynamic cloudlet, which ultimately improves the overall performance of the mobile cloud computing.

3.1 Authentication

Authentication is an absolutely essential element of a typical security model. It is the process of confirming the identification of a user or a machine that is trying to log on or access resources. There are a number of different authentication mechanisms, but all serve this same purpose. While authentication verifies the user's identity, authorization verifies that the user in question has the correct permissions and rights to access the requested resource.



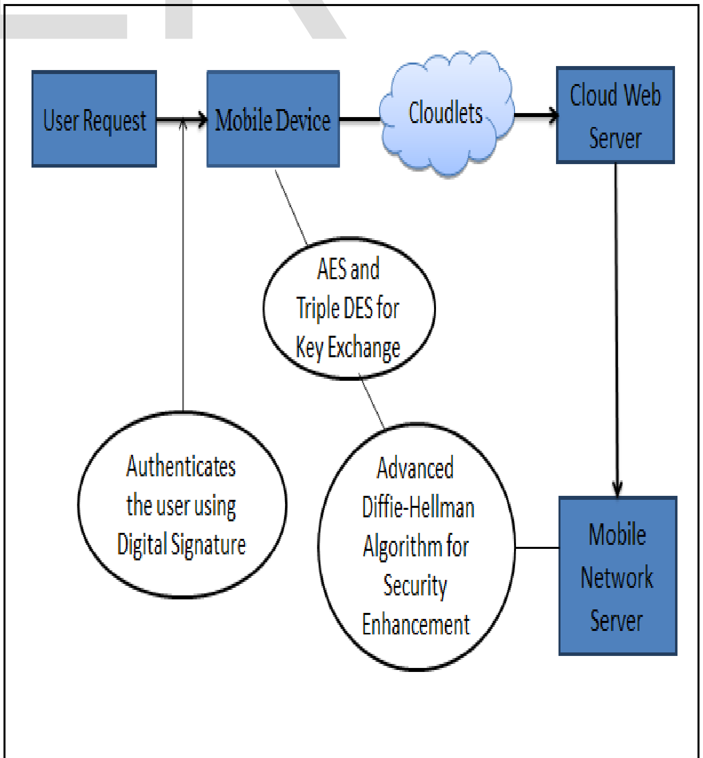

User Request
Mobile Device
Cloudlets
Cloud Web Server
AES and Triple DES for Key Exchange
Authenticates the user using Digital Signature
Advanced Diffie-Hellman Algorithm for Security Enhancement
Mobile Network Server

Figure 6 Architecture Diagram of the proposed system

3.2 Concepts of AES and 3 DES

The idea of a hybrid based AES-3DES can be constructed with reference to basic DES Feistel equations. The repetition of these equations is based on the number of rounds as adapted by the Feistel network, which in the case of DES was standardized for 16 rounds. However, by incorporating the AES within this yields the following results.

L1 =f (R0) --------------------------------- (1)

R1 =AES (f (L0) XOR f (R0)) --------- (2)

The user gives the plain text where the plain text is divided into two halves L0 and R0 of 128 bits each. Each half is then again divided into two halves i.e. LL0 and LR0 from L0 and from R0 we get RL0 and RR0 of 64 bits each respectively. DES algorithm is then applied to all the halves which are generated that is LL0, LR0, RL0 and RR0 using the key given by the user. There is also a provision of using two different keys. If the user selects two keys option at the time of encryption the two different keys are used, one key is used DES encryption and the other key is used for AES encryption. If the user selects one key option at the time of encryption then the same key is used for 3DES and AES encryption. The output of 3DES encryption text is of 192 bits each. Since DES encryption is applied on four quarters each quarter generates an output of 192 bits. The output of LL0 and LR0 is clubbed together to form f (L0) and the output of RL0 and RR0 is clubbed together to form f (R0). The length of f (L0) and f (R0) is 384 bits each. Once we have got f (L0) and f (R0) they both are then XOR with each other i.e. f (L0) XOR f (R0). The length of the output will be same as the length of the input that is 384 bits. The result is then given to the AES algorithm where the result is encrypted using the key provided by the user. The key can be same or different as mentioned above. The output length of the AES encrypted text is 704 bits. The f (R0) can be termed as L1 and the AES encrypted text can be termed as R1. Both L1 and R1 are then clubbed together to give the cipher text of 1088 bits. The Decryption process is exactly reverse of the encryption process.

3.3 Digital Signature Algorithm

Digital signatures are used to achieve **Authentication**, **Non-repudiation**, and **Authorization**.

Authentication is a technique by which a process verifies that its communication partner is who it is supposed to be and not an intruder, and deals with the question of whether or not you are actually communicating with a specific process. Non-repudiation is a mechanism which provides a way to prevent the author from falsely claiming that he or she isn't the author. Authorization is concerned with what that process is permitted to do.

3.3.1 Key generation

Key generation has two phases. The first phase is a choice of *algorithm parameters* which may be shared between different users of the system, while the second phase computes **public** and **private keys** for a single user.

3.3.2 Per-user keys

Given a set of parameters, the second phase computes private and public keys for a single user:

- Choose a secret key x by some random method, where $0 < x < q$.
- Calculate the public key $y = g^x \bmod p$

3.4 The Advancement in Diffie-Hellman Algorithm

The Advanced Diffie Hellman algorithm has been proposed in order to make the original Diffie Hellman algorithm more secure. Our main aim here is to compute the values of secret number chosen by the two organizations using certain mathematical algorithm. This would ensure the confidentiality of the chosen values of 'a' and 'b;, that is the secret number. Our next aim would be to secure the data sent from one organization to another. Alice sends the value (g^amodp) to Bob in the original Diffie Hellman, but here we have cubed this value and then sent to Bob. This would make man in the middle attack more difficult. With this as the area of focus, we hereby propose the Advanced Diffie Hellman.

3.4.1. Advantages of the Advance Diffie-Hellman Algorithm

Complexity - The complexity of the algorithm is increased. Values of the chosen number 'a' and 'b' are made complex. If a cryptanalyst tracks down the values of the chosen numbers, it would be difficult to decrypt and find 'a' and 'b'. The cryptanalyst would be finding only a1 and b1. Man in the middle attack - If an attacker finds the data being sent from Alice to Bob, he would be capturing (a1^3) or (b1^3). It would make the task difficult to arrive at the actual value since the actual values are cubed and then sent. Security - The Diffie Hellman code had no security over the chosen secret key 'a' and 'b'. If the cryptanalyst deciphered the values of and b, the secret key would be obtained. In advanced diffie-hellman, the values of 'a' and 'b' has been encrypted. Even if the values of 'a' and 'b' are deciphered, this algorithm would make the values more secure. Reverse process - Reverse engineering or reverse process would be very difficult for the cryptanalyst. The major advantage of this algorithm is that the users are making their own secret numbers more secure by performing algorithms at their own end.

The following table shows how advanced Diffie-hellman algorithm works.

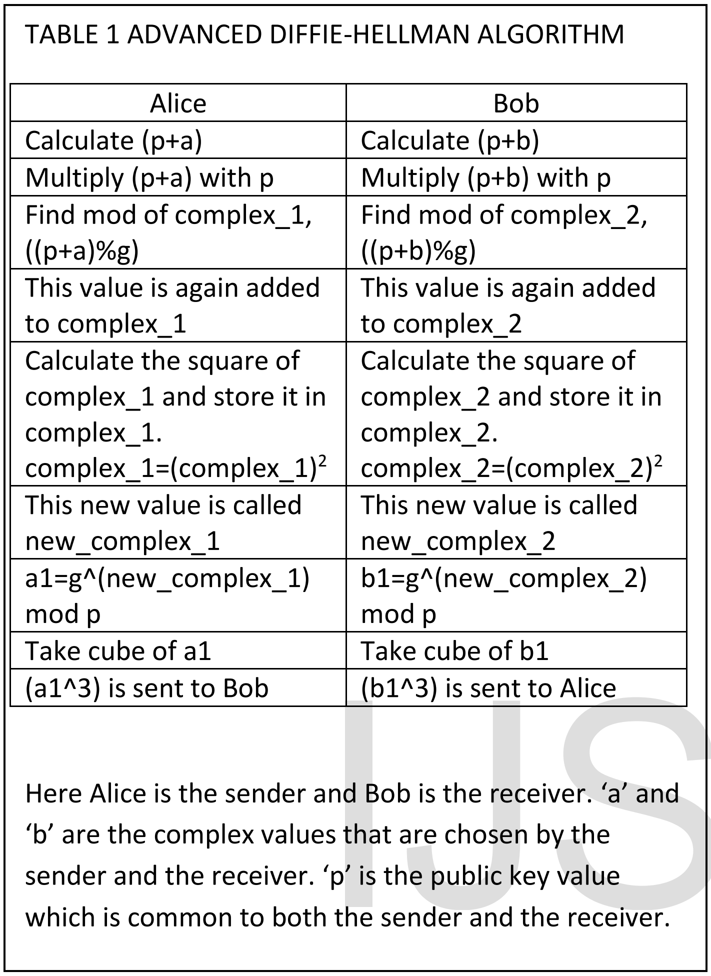


TABLE 1 ADVANCED DIFFIE-HELLMAN ALGORITHM

Alice	Bob
Calculate (p+a)	Calculate (p+b)
Multiply (p+a) with p	Multiply (p+b) with p
Find mod of complex_1, ((p+a)%g)	Find mod of complex_2, ((p+b)%g)
This value is again added to complex_1	This value is again added to complex_2
Calculate the square of complex_1 and store it in complex_1. complex_1=$(\text{complex\_1})^2$	Calculate the square of complex_2 and store it in complex_2. complex_2=$(\text{complex\_2})^2$
This new value is called new_complex_1	This new value is called new_complex_2
a1=g^(new_complex_1) mod p	b1=g^(new_complex_2) mod p
Take cube of a1	Take cube of b1
(a1^3) is sent to Bob	(b1^3) is sent to Alice

Here Alice is the sender and Bob is the receiver. 'a' and 'b' are the complex values that are chosen by the sender and the receiver. 'p' is the public key value which is common to both the sender and the receiver.

3.5 Offloading Algorithm

In this section, we propose a dynamic offloading algorithm (DOA) supported the information caching mechanism and improve task management ways with dynamic energy scheduling algorithm. In most previous offloading algorithms, changing an information item might end in cache misses. Within the information caching mechanism this trouble can be overcome by prefetching the information which will be employed in close to future.. For instance, if a client watches that the server is broadcasting an information thing which is an invalid entry2 of its neighbourhood store, it is ideal to download the information; generally, the client might need to send another solicitation to the server and the server will need to show the information again later on. To save power, clients might just wake up amid the information broadcasting period and afterward how to pre-fetch information turns into an issue. As a solution, after broadcasting the data, the server first broadcasts the id list of the data items whose data values will be broadcast next and then broadcasts the data values of the data items in the id list. Each client ought to listen to the IR in the event that it is not detached. Toward the end of the information exchange, a customer downloads the id rundown and discovers when the intrigued information will come and awakens around then to download the information. At the end of the data transfer, a client downloads the id list and finds out when the interested data will come and wakes up at that time to download the data. With this approach, power can be saved since clients stay in the snooze mode most of the time bandwidth can be saved since the server may only need to broadcast the updated data once. To gain insight on the performance of the proposed algorithm, we consider the network scenario and compare with the following methods: (1) L scheme: all mechanism measure executed locally, (2) S scheme: all mechanism are executed remotely, and (3) H scheme: all mechanism have same energy and (4)P scheme: mechanism having complete different energy.

4. CONCLUSION

This paper proposes a strong user authentication framework for cloud computing with Advanced Diffie-Hellman algorithm, AES ,3DES and Digital Signature. In the proposed work a offloading algorithm, we incorporate the data caching mechanism and improve task management strategies with dynamic energy scheduling algorithm which shows that the high efficiency of our algorithm allows the mobile device to calculate the optimal offloading decision at the local end with much lower time complexity and energy consumption. It rejects the unused or unwanted task from the mobile environment for reducing the traffic overload occurring between the mobile devices and cloud servers. It provides secure and trust-aware access control and defends against the internal attacks like collusion attacks, bad mouthing attacks and information disclosure attacks the MCC. The proposed method can obtain energy optimization and removes the waste energy form the mobile devices, it reduces the latency delay and traffic overload in the Mobile cloud computing.

REFERENCES

[1] B.Karthikeyan, Dr.T.Sasikala and K.Nithya, "SECURE AND ENERGY EFFICIENT MODEL WITH MODIFIED OFFLOADING ALGORITHM IN MOBILE CLOUD COMPUTING," Asian Journal of Research in Social Sciences and Humanities Volume 6, Special Issue, Sept 2016 (BASE PAPER)

[2] Ragini, Parul Mehrotra, S.Venkatesan, "AN EFFICIENT MODEL FOR PRIVACY AND SECURITY IN MOBILE CLOUD COMPUTING," International Conference on Recent Trends in Information Technology, 2014.

[3] Mazhar Ali, Samee U. Khan, Athanasios V. Vasilakos," SECURITY IN CLOUD COMPUTING: OPPURTUNITIES AND CHALLENGES" http://dx.doi.org/10.1016/j.ins.2015.01.025.

[4] Saurabh Dey, Srinivas Sampalli, Qiang Ye, "A LIGHT-WEIGHT AUTHENTICATION SCHEME BASED ON MESSAGE DIGEST AND LOCATION FOR MOBILE CLOUD COMPUTING," IEEE 2014.

[5] Xu Yang, Xinyi Huang, Joseph K. Liu. http://dx.doi.org/10.1016/j.future.2015.09.028.

[6] Hui Suo, Zhuohua Liu, Jiafu Wan, Keliang Zhou, "SECURITY AND PRIVACY IN MOBILE CLOUD COMPUTING," IEEE 2015.

[7] D. AB. Fernandes, L. FB Soares, J. V. Gomes, M. M. Freire, and P. RM Inácio, "SECURITY ISSUES IN CLOUD

ENVIRONMENTS: A SURVEY," International Journal of Information Security, Volume 13, No. 2, 2014, pp. 113-170.

[8] N. Khan, M. L. M. Kiah, M. Ali, S. A. Madani, and S. Shamshirband, "BLOCK-BASED SHARING SCHEME FOR SECURE DATA STORAGE SERVICES IN MOBILE CLOUD ENVIRONMENT," The Journal of Supercomputing, Vol. 70, No. 2,2014, pp. 946-976.

[9] Zhang, B. Luo, W. Shi, and A. M. Almoharib, "CLOUDSAFE: STORING YOUR DIGITAL ASSET INCLOUD-BASED SAFE," Wayne State University,Detroit, USA, Tech. Rep., 2013.

[10] Uma Somani, Kanika Lakhani, Manish Mundra "IMPLEMENTING DIGITAL SIGNATURES WITH RSA ENCRYPTION ALGORITHM TO ENHANCE THE DATA SECURITY OF CLOUD IN CLOUD COMPUTING" 2010 IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[11] D. Cavdar and F. Alagoz, (Eds.), "A SURVEY OF RESEARCH ON GREENING DATA CENTERS", Proceedings of the IEEE Global Communications Conference (GLOBECOM), (**2012**) December 3-7; Anaheim, CA.

[12] Ankita Atrey, Nikita Jain and Iyengar N.Ch.S.N, "A STUDY ON GREEN CLOUD COMPUTING," International Journal of Grid and Distributed Computing, Vol.6. No.6(2013).

[13] Monalisa Jha and Shraddha Patil, "ADVANCEMENT IN DIFFIE-HELLMAN ALGORITHM," International Journal of Engineering research and Applications, Volume 5, Issue 7, (Part-4) July 2015.

[14] Mrs. Mamatha and Mr. Pradeep Kanchan, "USE OF DIGITAL SIGNATURE WITH DIFFIE HELLMAN KEY EXCHANGE AND HYBRID CRYPTOGRAPHIC ALGORITHM TO ENHANCE DATA SECURITY IN CLOUD COMPUTING," International Journal of Scientific and Research Publications, Volume 5, Issue 6, June 2015.

[15] Preeti and Bandana Sharma, "REVIEW PAPER ON SECURITY IN DIFFIE-HELLMAN ALGORITHM," Volume 4, Issue 3, March 2014.