Volume 5, Issue 8, August 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Issues of Data Security on Mobile Cloud

[1]T. Chidambaram, [2]M. Durairaj

[1]Research Scholar, [2]Assistant Professor

[1, 2] School Of Computer Science, Engineering and Applications Bharathidasan University,
Trichy, Tamil Nadu, India

Abstract—Mobile Cloud Computing (MCC) is gained popularity in fast pace due to it's anytime and anywhere data access. Rapid growth of cloud computing resulted in large number of users store their data on mobile cloud. Network data security is a major problem in cloud storage media. Security is an important factor in cloud computing for ensuring clients data is placed on the secure mode in the cloud. The cloud Data must not be stolen by the third party so authentication of client becomes a mandatory task. In this paper we discuss different existing techniques used to provide security in the field of mobile cloud computing is a on the basis of various parameters. To encrypt their data before it is stored on the cloud is one of the techniques. This work is intended to provide security service such as confidentiality in the cloud services use RSA algorithm. RSA is familiar and generalized algorithm for data encryption, the advantages in terms of smaller key size and lower processing time for upload a file and download a file processing. This security mechanism uses algorithms to scratch data into unreadable text which can be only being decoding or decrypted by party who possesses the association key. In Mobile cloud computing security is the major issue. In this paper, the main working concepts of MCC and its various security algorithms which uses RSA, AES, DES and Blowflies encryption algorithms to secure the data.

Keywords — Mobile Cloud Computing (MCC), Data Security, Secret Key Encryption, RSA, AES, DSA, Encryption algorithms.

I. INTRODUCTION

Mobile Cloud Computing is a form of distributed computing technology. It is a development of distributed processing, parallel processing and grid computing. Its most basic concepts is that automatically split a huge amount of calculation program into numerous smaller subroutines through the network, and then handed over to the operation system that consists of several servers. After calculating and analyzing, it will process the results and return them to the user [1, 2]. In spite of the hype achieved by mobile cloud computing, the growth of the mobile cloud computing subscribers is still below expectations due to the risks associated with the security and privacy. To have an in deep understanding of Mobile Cloud Computing and its network security, it is necessary to get the complete grasp on mobile cloud computing. Where user is able to rent software and hardware infrastructure and computational resources as per user basic Computing concept, technology and architectures have developed and consolidated in the last decades. Cloud Computing let you access all your application and documents from anywhere in the world. It is easier for group members in different locations to collaborate. Cloud computing is not network computing. And it is a lot bigger than that. The Mobile Cloud Computing (MCC) is Internet-based data, applications and related services (computing) obtain or retrieve from a storage device as of information on accessed through Smartphone's, laptop computers, tablets and other portable devices [1, 2]. For secure communication over public network data can be protected by the method of encryption. Encryption converts that data by any encryption algorithm using the 'key' in scrambled form. Only user having access to the key can decrypt the encrypted data [4].

As MCC platform is based on cloud computing. All the security issues in cloud computing are inherited in MCC with extra limitation of resource constraint mobile devices. Because of this resource limitation, the security algorithms planned for cloud computing environment cannot be directly run on mobile device. There is a requirement of lightweight secure framework that provides security with less communication and processing overhead on mobile devices. This need is the motivation for the paper.

In this paper, the most recent articles published on mobile cloud computing technologies and security issues are briefly reviewed. The articles reviewed in this work are collected from Elsevier, IEEE and reputed journals. This paper also summarizes the cloud service delivery models, deployment model and some of the mobile computing technologies.

II. WORKING OF MOBILE CLOUD COMPUTING

The Mobile Cloud Computing (MCC) are a development of mobile computing and an extension to cloud computing. In mobile cloud computing, the previous mobile device-based intensive computing, data storage and mass information processing have been transferred to 'cloud' and thus the requirements of mobile devices in computing capability and resources have been reduced, as a result the developing, running, deploying and using mode of mobile applications have been totally changed. On the other hand, the terminals which people used to access and acquire cloud services are suitable for mobile devices like Smartphone, PDA, Tablet, and iPad but not restricted to fixed devices (such as PC), which reflects the advantages and original intention of cloud computing. Therefore, from both aspects of mobile computing and cloud computing, the mobile cloud computing is a combination of the two technologies, a development of distributed, grid and centralized algorithms, and have broad prospects for application.

Mobile cloud computing can be divided into cloud computing and mobile computing. Those mobile devices can be laptops, PDA, Smartphone's, and so on. Which connects with a hotspot or base station by 3G, WIFI, or GPRS As the computing and major data processing phases have been migrated to 'cloud', the capability requirement of mobile devices is limited, some low-cost mobile devices or even non- smartphones can also achieve mobile cloud computing by using a cross-platform mid-ware. Although the client in mobile cloud computing is changed from PCs or fixed machines to mobile devices, the main concept is still cloud computing. Mobile users send service requests to the cloud through a web browser or desktop application, then the management component of cloud allocates resources to the request to establish connection, while the monitoring and calculating functions of mobile cloud computing will be implemented to ensure the QoS until the connection is completed.

2.1 Characteristics of MCC

The key characteristics of mobile cloud computing are Reliability, Scalability, Security, Agility, Device Independence, Low Cost, and Reduced Maintenance [3].

2.2 Mobile Cloud Computing vs Cloud Computing

Both cloud computing and mobile computing have to use wireless systems to transmit data. Beyond this, these two terms are quite different. Cloud computing relates to the specific design of new technologies and services that allow data to be sent over distributed networks, through wireless connections, to a remote secure location that is usually maintained by a vendor. Cloud service providers usually serve multiple clients. They arrange access between the client's local or closed networks, and their own data storage and data backup systems. That means that the vendor can intake data that is sent to them and stores it securely, while delivering services back to a client through these carefully maintained connections.

Mobile computing relates to the emergence of new devices and interfaces. Smartphone's and tablets are mobile devices that can do more than traditional desktop and laptop computers do. Mobile computing functions include accessing the Internet through browsers, supporting multiple software applications with a core operating system, and sending and receiving different types of data. The mobile operating system, as an interface, supports users by providing intuitive icons, familiar search technologies and easy touch-screen commands. While mobile computing is largely a consumer-facing service, cloud computing is something that is used by many businesses and companies. Individuals can also benefit from cloud computing, but some of the most sophisticated and advanced cloud computing services are aimed at enterprises. For example, big businesses and even smaller operations use specific cloud computing services to make different processes like supply-chain management, inventory handling, customer relationships and even production more efficient. An emerging picture of the difference between cloud computing and mobile computing involves the emergence of smart phone and tablet operating systems and, on the cloud end, new networking services that may serve these and other devices.

III. REVIEW OF RELATED WORKS

This paper reviews the literatures on the data security schemes that focus on the reduction of the computational complexity of cryptographic algorithms and methods to secure mobile cloud computing infrastructure and data storage security. This paper also proposed an mobile cloud data storage security, encryption and decryption processing time management for mobile clients to verify the integrity of the files stored on a cloud server using an incremental message authentication code. The proposed scheme offloads most of the integrity verification code on a cloud service provider and trusted third party to minimize the processing overhead on the mobile client. The cloud service provider redirects the stored files towards the coprocessor when instructed by a mobile client. The co-processor computes incremental MAC on received files for integrity verification. The reviews of literature carried out in this work are given below.

Kuyoro S. O, *et. al.* [1] highlighted key security considerations and challenges which are currently faced in the Cloud computing security. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future.

Rajesh Piplode, *et. al* [2] highlighted that the cloud computing vulnerabilities, security threats cloud computing faces and presented the security objective that need to be achieved. On one hand, the security-sensitive applications of a Cloud computing require high degree of security on the other hand, cloud computing are inherently vulnerable to security attacks.

M. Durairaj, *et.al* [3**]** proposed a novel secure and verifiable cloud computing for mobile encryption algorithm proposed and described in the literature outlines that decryption process is reverse of the encryption. This algorithm can be used to encrypt the user data in cloud. Since the user has no control over the data once their session is logged out, the encryption key acts as the primary authentication and the number of existing techniques used to implement security in cloud. Different symmetric and asymmetric algorithms were used for devising effective security mechanism. Cloud computing is revolutionizing how information technology resources and services are used and managed, but the revolution always comes with new problem. Based on this review of literature, our work will be extended by developing combination of more than one security mechanisms as a hybrid technology for providing effective security mechanism for mobile cloud computing.

Shahzad, *et. al* [4] presented a complete understanding of MCC by explaining the architecture, advantages and applications. This paper is mainly focused on highlighting the issues and challenges of MCC like, data security, infrastructure security and communication channel security. The main idea behind this research is to identify these issues and challenges because they are preventing the mobile users to take on cloud services.

Soeung-Kon, *et. al* [5] discussed the different security issues that arise about how safe the mobile cloud computing environment. This paper have discussed security issues concerning mobile cloud computing. Securing mobile cloud computing user's privacy and integrity of data or applications is one of the key issues most cloud providers are given attention. Since mobile cloud computing is a combination of mobile networks and cloud computing, the security related issues are then divided into two categories: mobile network user's security; and mobile cloud security.

Shih-Hao Hung, *et. al*, [6] proposed a framework to execute mobile applications in a cloud-based virtualized execution environment controlled by mobile applications and users, with encryption and isolation to protect against eavesdropping from cloud providers. On the system level, the design is for the workload migration framework, so that the system has better flexibility to allocate workload on local processing elements or virtual processing elements on cloud servers, depending on network connectivity and core utilization. As a result, the computation resources can be better utilized.

Swarnpreet Singh, *et. al* [7] discussed opportunity for the development of mobile applications since it allows the mobile devices to maintain a very thin layer for user applications and shift the computation and processing overhead to the virtual environment. A cloud application needs a constant connection that might prove to be an Achilles heel for the cloud computing movement.

Abdullah Gani, *et. al* [8] described that the network intensive computing environment such as MCC necessitates the optimal use of networks resources in order to establish a seamless connectivity between SMDs and the cloud. Also limited battery life feature of SMDs requires minimum energy consumption in accessing the services of computational clouds. The consolidation of network terminal, cross-layer information, multi- packet casting, computing capability of network terminal and intelligent network selection algorithm appears to be an optimum solution for achieving seamless service continuity in order to facilitate seamless connectivity. Also incorporation of distributed mobility management can be an optimum solution for providing seamless connectivity.

Hoang T. Dinh, *et. al* [9] provided an overview of mobile cloud computing in which its definitions, architecture, and advantages have been presented. The applications supported by mobile cloud computing including mobile commerce, mobile learning, and mobile healthcare have been discussed which clearly show the applicability of the mobile cloud computing to a wide range of mobile services. Then, the issues and related approaches for mobile cloud computing (i.e., from communication and computing sides) have been discussed.

N Sriram , *et. al* [10] proposed a novel secure and verifiable cloud computing for mobile system using multiple servers. This method combines the secure multiparty computation protocol and the garbled circuit design with the cryptographically secure pseudorandom number generation method of Blum et al. This method preserves the privacy of the mobile client's inputs and the results of the computation, even if the evaluator colludes with all but one of the servers that participated in the creation of the garbled circuit.

M.Rajendra Prasad, *et. al* [11] presented the Mobile Cloud Computing will provide a full commercial environment for applications, providing an easy way for smaller developers to monetize their services as well as new routes to market. Crucially, Mobile Cloud Computing will eliminate the commercial and technical fragmentation that has thus far proven to be a barrier to successful collaboration between application providers and operators on a global scale.

Huajian Mao, *et. al* [12] presented the Wukong, a cloud-oriented file service for mobile devices. Wukong characterizes itself with several unique features. It provides a standard POSIX compliant interface so that existing applications can be deployed on this service directly or with few modifications. It supports multiple heterogeneous storage services, and has a capability to support new or unforeseen services. It introduces negligible overhead while providing an easy way to access cloud services in mobile devices.

Nazanin Aminzadeh, *et. al* [13] surveyed the crucial intrinsic restrictions of mobile devices and storage augmentation issues in three domains of mobile computing, cloud computing and MCC to devise a taxonomy of issues as the motivation for the emergence of effective and efficient MSA approaches in MCC. A number of approaches leverage data partitioning whereas other approaches exploit data replication, cache management, or SOA. Based on a review of the credible MSA approaches, the paper proposes taxonomy of cloud-based storage.

S. Subashini, *et. al*, [14] described that though there are extreme advantages in using a cloud-based system, there are yet many practical problems which have to be solved. Cloud computing is a disruptive technology with profound implications not only for Internet services but also for the IT sector as a whole. Still, several outstanding issues exist, particularly related to service-level agreements (SLA), security and privacy, and power efficiency. As described in the paper, currently security has lot of loose ends which scares away a lot of potential users. Until a proper security module is not in place, potential users will not be able to leverage the advantages of this technology.

Zaheer Ahmad, *et. al*, [15] emphasized that the security may be added in the form of additional authentication processes and management, which should not interfere with existing (U)SIM authentication, however, there is opportunity to expand the use of the (U)SIM to create an attack resistant foundation for the added security. Virtualization has received a lot of attention on Smart phones and there are several hypervisor products, however, the security foundations will be paramount as the powerful capabilities of hypervisors have much in common with types of published malware.

IV. METHODOLOGIES AND TOOLS

In this section, experimental result for the application of Encryption algorithm AES, DES, RSA, and Blowfish which are widely used Public-Key algorithm discussed. In the encryption algorithms such as - AES, DES, RSA and Blowfish are used to ensure the security of data, file upload and download time management in cloud. For the perspective of different users, these algorithms are proposed. DES is developed in early 1970s; Blowfish is developed by Bruce Schneier, in 1993. AES is developed by NIST in 2001. All of these algorithms are symmetric key, in which a single key is used for encryption/decryption purposes. RSA is asymmetric key algorithm, created by Ron Rivets, Adi Shamir and Lenard Adleman in 1978. This algorithm is used for public key cryptography. In this, two public/private keys are used for encryption/decryption. There are always options to the users to choose any algorithm according to him/her need and accordingly encrypt/decrypt the data on cloud.

4.1 Security Algorithms

The security algorithm discussed in this paper is listed below:

(a) RSA Algorithm
(b) DES Algorithm
(c) AES Algorithms
(d) Blowfish Algorithm

4.2 RSA Algorithm

The RSA algorithm is given below:

Select two prime numbers.
Calculate n = p*q.
Calculate f (n) = (p-1) (q-1)
Select e such that e is relatively prime to f (n) and less than f (n).
Determine d such that de congruent modulo 1 (mod f (n)) and d<f (n).
Public key = {e, n}, Private Key = {d, n}
Cipher text c = message e mod n
Plain text p = cipher text d mod n

4.3 DES Algorithm

Triple DES uses a "key bundle" which comprises three DES keys, K1, K2 and K3, each of 56 bits (excluding parity bits).

The encryption algorithm is: Cipher text = EK3 (DK2 (EK1 (plaintext)))

i.e., DES encrypts with K1, DES decrypt with K2, then DES encrypt with K3.

Decryption is the reverse: Plain text = DK1 (EK 2(DK3 (cipher text)))

i.e., decrypt with K3, encrypt with K2, and then decrypt with K1.

Each triple encryption encrypts one block of 64 bits of data.

4.4 AES Algorithm

This algorithm proposed for securing of files through file encryption. The file present on the device will be encrypted using password based AES algorithm. The user can also download any of the uploaded encrypted files and read it on the system. The advantages of AES are many. AES is not susceptible to any attack but Brute Force attack. However, Brute Force attack is not an easy job even for a super computer. This is because the encryption key size used by AES algorithm is of the order 128, 192 or 256 bits which results in billions of permutations and combinations. AES is also much faster than the traditional algorithms like RSA. Thus, it makes a fine choice for protection of data on the cloud. The steps involved in AES algorithm are as given below:

1. Key Expansion—round keys are derived from the cipher key using Irondale’s key schedule
2. Initial Round
    1. Add Round Key—each byte of the state is combined with the round key using bitwise x or
3. Rounds
    1. Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
    2. Shift Rows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
    3. Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
    4. Add Round Key
4. Final Round (no Mix Columns)
    1. Sub Bytes
    2. Shift Rows
    3. Add Round Key

4.5 Blowfish Algorithm

Blowfish has a 64-bitblock size and a variable key length from 1 bit up to 448 bits. It is a 16-round Feistel cipher and uses large key-dependent S-boxes. In structure, it resembles CAST-128, which uses fixed S-boxes. Each line represents 32 bits. The algorithm keeps two sub key arrays: the 18-entry P-array and four 256-entry S-boxes. The S-boxes accept 8-bit input and produce 32-bit output. One entry of the P-array is used every round, and after the final round, each half of the data block is XOR end with one of the two remaining unused P-entry.

Table 1: Specifications of existing encryption standards used parameters used security.

Algorithm name	Key size	Encoding	Padding	Initial vector size
DES ede/ Triple DES	192 bits	CBC	PKCS5 Padding	64 bits
AES	128 bits	CBC	PKCS5 Padding	128 bits
Blowfish	64 bits	CBC	PKCS5 Padding	64 bits

V. PERFORMANCE EVALUATION

This thesis used NS2 Simulation principles and strategies adopting the separated object model and using two languages C++ and tclNS2 fulfill the achievement of simulation for specific protocols and the configuration data and establishment of network simulation environment respectively. Wamp server is used as the cloud server. Security algorithms applied on network simulator to provide cloud data security. It can be applied on mobile cloud computing for data transmission security is discussed. The RSA algorithm is the most commonly used encryption. Till now it is the only algorithm used for private and public key generation and encryption. RSA perform fast encryption. DSA algorithm is proposed for efficient of entropy, secrecy, and uniqueness of the random signature value *k* is critical [10]. It is so critical that violating any one of those three requirements can reveal the entire private key to an attacker. Using the same value twice (even while keeping *k* secret), using a predictable value, or leaking even a few bits of *k* in each of several signatures, is enough to break DSA. It is one of the most common public algorithms provided by Bruce Schneier. Blowfish is a variable length key, 64-bit block cipher. No attack is known to be successful against this. Various experiments and research analysis proved the superiority of Blowfish algorithm over other algorithms in terms of the processing time. The Both AES and DES are block ciphers. It has variable key length of 128, 192, or 256 bits; default 256. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications.

5.1 Mobile Cloud Data Storage - File Upload

In this section performance of file upload data in cloud data storage we my used ns2 simulation network and data security encrypt and decrypt the (MCC) network data, the file data transfer between cloud data storage within the scenario by using algorithms for security and processing time management. In the simulation apply the AES, DES, RSA AND Blowfish algorithm to package information that transfers between the cloud storage.
The steps for the file upload an algorithm to simulation process are explained here.

Files upload Key Generation Algorithm

1) Randomly and secretly choose two large primes: p, q and compute $n = p. q$
2) Compute ϕ (n) = (p – 1) (q – 1).
3) Select Random Integer: e such as $1< e< n$ and gcd (e, ϕ) = 1.
4) Compute d such as $e. d \equiv 1 \mod \phi (n)$ and $1 < d < \phi (n)$.
5) Public Key: (e, n)
6) Private Key: (d, n).
7) This key sends to user's email id.
8) Upload the file on to the cloud
9) ask the user if he wishes to delete the file once it is uploaded
10) Delete the file if the user selects the option for deletion
11) Disconnect connection with the cloud.

In both systems the key generation times were not the same every time, even though the key length is the same and it can sometime a take very long time to generate the keys. Figure 1 show that for smaller key sizes the key generation time is almost equal in both cases, but as the key size grows RSA, AES, DSA and Blowfish algorithms to compare the all algorithm takes more amount of time to generate the keys and this time increases exponentially by the key size. And comparison of the key generation in processing times for algorithms.

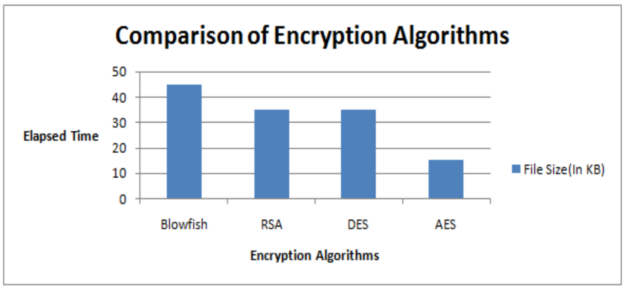


Figure 1.Key dispersal for a 128 bit key with n=10. vs Time for uploading

Upload the file on to the cloud

5.2 Mobile Cloud Data - File Download

In this section file download in decryption process in cloud security file we can implement the algorithm to apply the simulation to perform the decryption process. The steps for file download process are explained here:

Step 1 is same as step 1 of file upload. The identity of the user is authenticated in this step.

In the second step, the array of files that the user has uploaded on the cloud so far is displayed. The user is asked to select one of the files from the list.

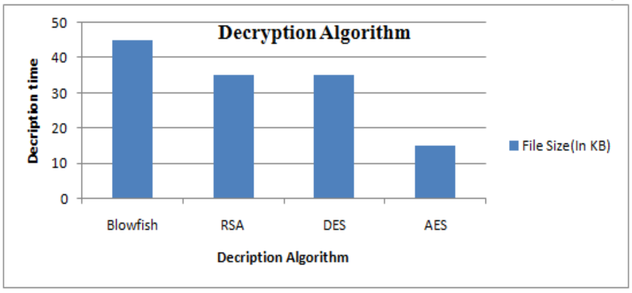
Once the user does not wish to download any more files from the cloud, log out of the user account and disconnect the established connection with the cloud. This is the last step of the download process.

```
1. Accept user name and password from the user
    a) If user is authenticated, establish connection with the cloud
    b) Else, show authentication error
2. Ask user to select file to be downloaded
3. Ask the user to enter a password for the decryption process
4. Check the validity of this password
INPUT: Public key (n, e), private key d, cipher text c.
OUTPUT: Plaintext m.
1. Compute m = cd mod n.
2. Return (m).
    a) If the password entered is valid, generate a key
    b) Else show an error message and reject password
5. Apply the decryption algorithm
6. Download the file from the cloud
7. Ask user if he wants to delete the uploaded encrypted file
    a) Delete the encrypted file from the cloud if user selects the delete option
8. Disconnect connection with the cloud.
```

5.3 Key Recovery Time from Shares

The Encryption time process in apply the simulation had to compare the encryption/decryption times between the AES, DES, RSA and Blowfish algorithms with different key sizes. Looking at the results, for smaller key sizes to provide much faster encryption/decryption as compared to the higher key sizes the encryption/decryption times grow exponentially with the given key size.

Key recovery from shares for a 128 bit key with n=10. Size vs Time for downloading.



Download the file from the cloud and Comparison of Decryption times.

Figure 2 shows the decryption times. Time taken by two algorithms for encryption shows that; AES, Blowfish is much faster than RSA, DES. Based on the input key size AES, Blowfish encryption time varies linearly whereas in case of RSA, DES it increases exponentially due to the large amount of computation involved and it remains the exponential increase in decryption time too, as shown in the Figure 2. Even though the decryption time is lesser than the encryption time in both algorithms, the decryption time varies exponentially with key size for RSA, DES and it remains linear for AES and Blowfish as the case with encryption.

5.4 File Download Time in Cloud Data

It includes time to collect the shares, generate the secondary key and merge the master key and the secondary key and time to decrypt the input file. It is the time between the two points when the user makes a request to download a file and user actually receives the time to taken for file downloading for different file sizes.

VI. RESULT AND DISCUSSION

In this paper presents a performance of simulations used a number algorithms are AES, DES, and Blowfish, RSA. Several points can be concluded from the results are displayed either in Security is a major requirement mobile cloud computing while we talk about data storage. There are number of existing techniques used to implement security in cloud. In this paper, we discussed number of symmetric and asymmetric algorithms. Our future will be considering some problems related to existing security algorithms and implement a better version of DES, AES, RSA, Blowfish. Based on this review of literature, our work will be extended by developing combination of more than one security mechanisms and technology for providing effective security mechanism for mobile cloud computing.

6.1 Comparison of Exiting and Proposed Security Algorithms.

In this section, we compared the existing algorithms on the basis of different parameters. In this work, we applied RSA, DES, AES and Blowfish algorithms using simulation. The results are encouraging and depicted in Table1, which includes Block Size, Key Length, Security, and Speed.

Table 2 Comparison for implement the algorithms and different parameters used in high security.

Characteristics	DES	Blowfish	RSA	AES
Developed	1977	1993	1994	2000
Block Size/ Key Length	56	32-448	MAX2040,112,168	128,192 or 256
Security	Proven Inadequate	Considered Secure	Considered Secure	Considered Secure
Speed	Very slow	Fast	Slow	Very fast

This paper presents the results obtained from the application of different symmetric encryption algorithms for the analysis of their performances. The selected algorithms are AES, DES, RSA and Blowfish, and we concluded from the results as briefed in the conclusion.

VII. CONCLUSION

In this paper, different security algorithm applied (MCC) data security in the Mobile Cloud Computing and effectiveness of this mechanism was discussed. Security and Privacy of data stored in Cloud Computing is an area which has full of challenges and of paramount Importance. The number of techniques were applied to provide secured communication between the user and the mobile cloud computing. Encryption has the speed and computational efficiency to handle encryption of large volumes of data in cloud storage. The encryption algorithm can be applied by the user to ensure that the data is stored only on secured storage. Based on the review of literatures carried out in this work, this paper proposes a technique for effective application of mechanisms as AES, DES, RSA and Blowfish.

REFERENCE

[1] S. O. Kuyoro, F. Ibikunle and O. Awodele, "Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), vol. 3, Issue 5, (2011).

[2] Rajesh Piplode, Umesh Kumar Singh " An Overview and Study of Security Issues & Challenges in Cloud Computing ", International Journal of Advanced Research in Computer Science and Software Engineering , Vol 2, Issue 9, September 2012 ISSN: 2277 128X.

[3] M.Durairaj, T.Chithambaram, “Networks Security on Mobile Computing – A Survey”. International Journal of Computer Science & Engineering Technology (IJCSET). ISSN : 2229-3345 Vol. 6 No. 04 Apr 2015.

[4] Abid Shahzad and Mureed Hussain, "Security Issues and Challenges of Mobile Cloud Computing ", International Journal of Grid and Distributed Computing Vol.6, No.6 (2013),

[5] Soeung-Kon, J. -H. Lee and S. W. Kim, "Mobile Cloud Computing Security Considerations", Journal of Security Engineering, no. 9, (2012) April.

[6] Shih-Hao Hung, Chi-Sheng Shih, Jeng-Peng Shieh, Chen-Pang Lee, Yi-Hsiang Huang, " Executing mobile applications on the cloud: Framework and issues ", Computers and Mathematics with Applications 63 (2012) 573–587. Elsevier Ltd.

[7] Swarnpreet Singh, Ritu Bagga, Devinder Singh, Tarun Jangwal "Architecture Of Mobile Application, Security Issues And Services Involved In Mobile Cloud Computing Environment ", International Journal O Computer Science And Electronics Research.Vol.Issues.Agu(2012).

[8] Abdul Nasir Khan, M.L. Mat Kiah, Samee U. Khan, Sajjad A. Madani " A review on interworking and mobility techniques for seamless connectivity in mobile cloud computing: Journal of Network and Computer Applications 43 (2014)84–102 (2014) Elsevier Ltd.

[9] Hoang T. Dinh, Chonho Lee, Dusit Niyato, and Ping Wang, " A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches", Department of Computer Science and Computer Engineering, La Trobe University, Australia 31 Accepted 30 May 2012,Available online 6 June 2012.

[10] Sriram N. Premnatha, Zygmunt J. Haas, " A Practical, Secure, and Verifiable Cloud Computing for Mobile Systems", The 11th International Conference on Mobile Systems and Pervasive Computing (MobiSPC-2014).

[11] M.Rajendra Prasad, Jayadev Gyani, P.R.K.Murti, " Mobile Cloud Computing: Implications and Challenges ", Journal of Information Engineering and Applications ISSN 2224-5782 (print) ISSN 2225-0506 (online) Vol 2, No.7, (2012).

[12] Huajian Mao, Nong Xiao, Weisong Shi, Yutong Lu, "A cloud-oriented file service for mobile Internet devices ", J. Parallel Distrib. Compute. 72 (2012) 171–184 31 October 2011, Available online 11 November (2011) Elsevier Ltd.

[13] Nazanin Aminzadeh, Zohreh Sanaei, Siti Hafizah Ab Hamid, " Mobile storage augmentation in mobile cloud computing: Taxonomy, approaches, and open issues ", Simulation Modeling Practice and Theory (2014) Elsevier Ltd.

[14] S. Subashini, V.Kavitha, "A survey on security issues in service delivery models of cloud computing ", Journal of Network and Computer Applications 34 (2011) 1–11, Elsevier Ltd.

[15] Zaheer Ahmad, Keith E. Mayes, Song Dong, Kostas Markantonakis, " Considerations for mobile authentication in the Cloud information security technical report 1 6 (2011) 123to1 3 0 Elsevier Ltd.