JCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-4, Issue-10 E-ISSN: 2347-2693

Enrichment of Mobile data Security over Cloud storage using New Asymmetric key algorithm

Prakash Kuppuswamy

College of Computer science & Information system, Jazan University, KSA

Available online at: www.ijcseonline.org

Received:11/Sep/2016 Revised: 22/Sep/2016 Accepted:15/Oct/2016 Published: 31/Oct/2016

Abstract**—** Using cloud storage is rapidly increasing at present in all the service and commercial zone. Safety and security concern of the data always uncertain in private, public and hybrid cloud storage system. In particular, mobile data on cloud storage facing enormous challenges and security issues. There is no limitation of mobile users, mobile data and its various services on mobile environment. Increase and deployment of mobile usage much needed to store their vast information in cloud environment, which establish to Mobile data storage on cloud environment. Cloud storage system promotes usage of cloud based services in a mobile environment. Encryption algorithm plays a vital role in securing mobile cloud system in security aspects. The core objective of this paper is to secure the mobile data on cloud environment. In this research article, we comparatively studied and analyzed various encryption algorithms used in mobile cloud base security with proposed new encryption model. Our proposed encryption/decryption method holds the higher security because the more dynamics and randomness are adaptively added into the key generation process with the help of key distribution centre (KDC).

Keywords**—** Mobile cloud computing, Cloud storage, Cloud Computing; Mobile cloud, Block cipher algorithm. Data encryption/decryption etc.,

I. INTRODUCTION

Cloud Computing is a technology that uses the internet and central remote servers to maintain data and applications. This technology allows for much more efficient computing by centralizing data storage, processing and bandwidth [1],[2]. Cloud environment providing facility to access and manipulate the information which was stored on remote servers, using any Internet-enabled platform [3],[4]. Cloud users seek the services of cloud computing, the major concern is the security of their data in the cloud storage. Securing data is always of vital importance and because of the critical nature of cloud computing and the large amounts of complex data it carries, the need is even more important. Hence forth, concerns regarding data privacy and security are proving to be a barrier to the broader uptake of cloud computing services [3],[8].

Cloud computing is extensively employed in several areas. It is clear that cloud computing is an efficient solution to furnish the smartphone's computation, memory, and energy demands [5],[6],[7]. The role of cloud computing in mobile devices creates a new domain called mobile cloud computing [7]. Mobile device is still resource constrained and some applications generally need more resources than a mobile device can pay for. To overcome this problem, a mobile device ought to get resources from an external source known as Cloud Storage. It is not always possible to save all the data and the information on the mobile device itself. So that the mobile agents can utilize the resources from the cloud, it requires the migrations of data and information between the cloud and mobile devices [9]. Mobile cloud threats and vulnerabilities are a foremost challenge in the field of research [7]. Mobile cloud computing is developed to enable mobile users to store/access a large amount of data on the cloud through wireless networks [10]. Mobile cloud computing is based on cloud computing, all the security issues are inherited in mobile cloud computing with the extra limitation of resource constraint mobile devices. Due to the resource limitation, the security algorithms proposed for the cloud computing environment may not work well directly on a mobile device [10].

Cryptography provides secured data transmission over the cloud computing. Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key cryptography, public-key (or asymmetric) cryptography, and hash functions. [12],[13] Public key encryption is implemented for random symmetric key encryption. It is basis of the protocol that enables to provide security while accomplishing an important system or network task. A protocol is an agreed-on sequence of actions that leads to desirable results. Encryption is at the heart of methods for ensuring all aspects of computer security [10]. The major advantage of asymmetric cryptography is to use two different keys, one Public (open) key and one Private (secret) key. The encrypted message by sender can be decrypted by the other at receiving end and vice versa. The earliest foundation of asymmetric algorithms known as public key cryptosystems comes from key exchange problem of symmetric algorithms. RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem [15].

The core idea of this research article is to provide effective security scheme, similar or more than other public key algorithm such as RSA, Elliptic curve and other asymmetric key structure on mobile cloud storage. Our proposed method is its rapidity and the block cipher scheme process can make the higher security and higher authentication with effective period of time. The remainder of the paper is organized as follows: In Section 2, it has been described in brief the relative researches in public key security algorithm based on mobile data and cloud environment. In Section 3 discussed about objective and necessity of our new proposed algorithm model. In Section 4 provides the structure of mobile cloud architecture. Implementation method of proposed public key security algorithm is demonstrated in Section 5. In Section 6, the experimental results and performance analysis is discussed; In Section7 identifies benefits of the proposed system and finally, Section 8 offers conclusion and future work.

II. BACKGROUND STUDY

Prakash Kuppuswamy, Dr. C. Chandrasekar (2011) proposed new algorithm, which is based on linear block cipher. It is new Asymmetric key algorithm based on linear block cipher or Hill cipher encryption codes of existing methods and design a set of simulation and emulation. They were discussed about encryption/decryption algorithm public key structure. The concept of this new algorithm is based on modular 37 (alphabets and numerals) whereas existing algorithms are based only on modular 26 (only alphabets). We are naming this linear based algorithm as New linear block cipher or Nlbc [13].

Prakash Kuppuswamy, Dr. Saeed Q Y Al-Khalidi (2014) discussed new digital signature schemes are mostly used in cryptographic protocols to provide services like entity authentication, authenticated key transport and authenticated key agreement. Proposed model architecture is related with secure Hash Function and cryptographic algorithm. There are many other algorithms which are based on the hybrid combination of prime factorization and discrete logarithms, but different weaknesses and attacks have been developed against those algorithms. In this Research paper authors presents a new variant of digital signature algorithm which is based on linear block cipher or Hill cipher initiate with Asymmetric algorithm [2].

Mohammad Shahnawaz Nasir, Prakash Kuppuswamy (2014) Author proposes new bio metric security protocol using hybrid encryption system. The hybrid encryption technique is a combination of both symmetric and asymmetric cryptographic techniques. The security of bio-metric information transfer through unreliable channel is challenging, because of external attacks. The new protocol solves make more secure and easy to encrypt and decrypt the data. Thus, in this paper, they were discussing efficient and effective mechanism for confidentiality and authentication for biometric security system by using RSA and simple symmetric key algorithm. Also it examines the possibility of using a combination of biometric attributes to overcome common problems in having a biometric scheme for authentication. It also investigates possible schemes and features to deal with variations in Biometric attribute [15].

Sujithra, Padmavathi (2015) in this research article authors discussed about mobile security. Due to increasing use of mobile devices the requirement of cloud computing in mobile devices arises, which gave birth to Mobile Cloud Computing. To ensure the correctness of users' data in the cloud, the framework mainly focuses on the data security over the Cloud Computing Paradigm by purposing new cryptographic technique named as Two Phase RSA Encryption. In this paper, we proposed a Two Phase RSA encryption algorithm for protecting the confidentiality and integrity of uploading files or data in mobile storage cloud. The selected encryption combinations A-RSA and DRSA algorithms are used for performance evaluation based on the text files used and the experimental result it was concluded that A-RSA algorithm gives better result in all aspects compared to D-RSA algorithm [8].

Mohd Rizuan Baharon, Qi Shi, David Llewellyn-Jones(2015) were discussed homomorphic mobile applications demand extensive computational power, it poses a challenge to the devices with limited computation power, memory, storage and energy. To overcome these features by cloud computing as the cloud offers virtually unlimited dynamic resources for computation, storage and service provision. Homomorphic encryption is believed to be one of the potential solutions to allowing arbitrary computation on encrypted data; its efficiency is still an obstacle for its implementation. This paper proposes a new Lightweight Homomorphic Encryption (LHE) scheme which minimizes the use of computation power at encryption and key generation. The key contribution of this work is to have a lightweight scheme with improved efficiency, while enabling homomorphism under both addition and multiplication [9].

Nitin Nagar, Ugrasen Suman(2016) The authors discussed about Mobile cloud computing based services in a mobile environment. Mobile devices are unable to utilize resources, communication delay, and unexpected mobile vulnerabilities or attacks. These challenges have great effect in the improvement of service qualities of mobile cloud. In this paper, the survey of different vulnerability and attacks on mobile cloud computing identified and also design a secure mobile cloud storage environment through encryption algorithm. Author's proposed mechanism use to prevent mobile cloud environment from attack. In this article many more algorithms to be evaluated and their results can be analyzed with one another to produce the best implemented security algorithm in mobile cloud environment for the future use [6].

III. RESEARCH OBJECTIVES

Mobile cloud storage can be connected to by a mobile computing device over a mobile network. The client and server have wireless connections. Mobile data storage is a structured way to organize information. This could be a list of items such as customer id, customer name, phone number and device information. One of the key characteristics of the mobile data storage systems is their ability to deal with disconnection. Confidentiality, Integrity, Authentication, Authorization and Nonrepudiation are the fundamental requirements for storage security.

Most common issues of Mobile cloud storage are data theft risk, privacy of data, violation of privacy rights, loss of physical security, handling of encryption and decryption keys and security etc., In addition to the data security threats on mobile cloud side, there are some attacks, which are probable at end user smartphone such as, device data theft, virus and malware attacks via wireless communication channel. In cloud infrastructure, a variety of attacks are identified along with the mobile cloud, which include attacks such as, attacks on virtual machines, vulnerabilities at platform levels, phishing, attack on authorization and authentication level, attacks from local users, and hybrid cloud security management. Some other major challenges and issues have such as partitioning, execution delay, and communication delay are common issues.

RSA cryptosystem can certainly eliminate several drawbacks associated with symmetric approaches. However, this cryptosystem still has some problems regarding complexity of algorithm as it works very slowly due to the fact that it is mathematically intensive and requires extra management for public keys. The new proposed linear block cipher algorithm as it works efficiently and more secure than other algorithm. In this proposed module we encode biometric code by making public key, and use that key to send a message. Our proposed algorithm based on linear block cipher, we can use different set of variables structure such as 2 block, 3 block, 4 block and so on. So, new algorithms or techniques must be designed for securing Mobile Cloud Data storage keeping in mind the restrictions of mobile devices such as limited memory capacity, less computation capability and battery power consumption. Security approaches based on encryption play a vital role in securing mobile cloud data storage Encryption plays a major role in protecting such sensitive data. Mobile users using wireless communication channel that carry their sensitive and financial data outside the physical boundaries for transaction. Due to this there is a possibility of data can be theft, modify and lost. Therefore security is a major concern for such type of malware functions. In order to ensure the security of the mobile cloud data storage need, proper authentication mechanism, suitable access control scheme and strong encryption technique must be implemented to protect the data privacy. In the following figure1 refers mobile cloud data storage working on various operating system and mentioned significance of cloud based security management and mobile device based user data management.

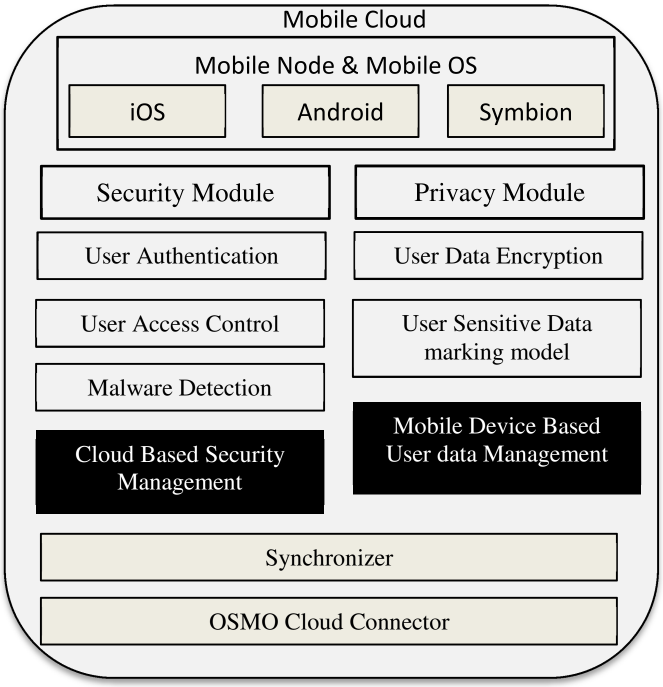

Figure 1. Mobile cloud environment

IV. PROPOSED ARCHITECTURE

In the mobile cloud storage, the encrypted data is stored in mobile memory device which is then later used for accessing by decrypting the data. These encryption/decryption usually processes and computes in the memory of mobile storage device which is still prone to unauthorized access. Mobile Cloud storage architecture is designed by linear block cipher cryptographic algorithms with Mobile storage device environment. The cryptographic algorithms to be used are selected based on comparative study from previous researches. So the symmetric, asymmetric and digital signature algorithms AES, DES, RSA, ECC, and MD5 are selected and used for cryptographic application in the public, private and hybrid clouds depends on the user requirement. Proposed architecture designed with unused linear block cipher symmetric key algorithm, we modified linear block cipher algorithm usable format as a asymmetric or public key algorithm.

Our proposed architecture provides high security which can be suitable for all type of cloud storage model. In the following figure.2 mobile users has facility to encrypt/decrypt the data with the help of Key Distribution Centre. The KDC connected with mobile cloud data storage. The mobile cloud data storage and KDC is part of the mobile cloud storage. This architecture model is suitable for private, public and hybrid cloud data storage system. The key generation responsibility carried out by Key Distribution Centre. The generated key is distributed to the concern user through secure channel to encrypt and decrypt the mobile data.

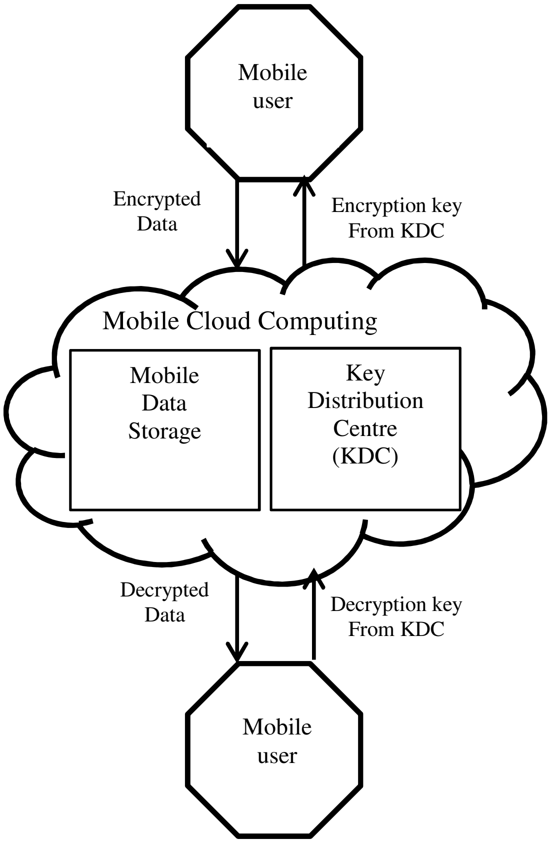

Figure 2. Mobile cloud storage architecture

V. IMPLEMENTATION SCHEME

We are implementing our proposed new public key algorithm on mobile cloud storage environment in 3 phases, first is key generation second encryption and finally decryption model. We still want to use public key cryptography for critical information exchange and symmetric cryptography, which is more efficient, for the protection of the data both on the mobile phone and during upload/download. Also, we would like to optimize efficiency of the cryptographic operations on the device, and minimize the communication overhead. The key decides the strength of the cryptosystem. The strength of proposed linear block cipher key typically refers to the n * n square matrix.

A. SSK key generation method

Select (n * n) inverse matrix on modulo 37 call as ‘k’.

Inverse of the matrix assume as private key k1. On condition of (k *k^{-1})mod37=1

Choose any integer number assume as a public key “e” . On condition of (e * d)mod =1

Now announce 37, d, e as public key k^{-1} is private key

B. Encryption method

Encryption phase allows users to encrypt their files and create the encrypted value of these files, before storing them on Mobile cloud storage. The steps include for the encryptions are:

Step 1: To encrypt a text message at first the arrange the message according to the square matrix size.

Step 2: Multiply message with selected square matrix (key) and e value.

Step 3: Use modulation 37 with derived message. The remainder value is encrypted message.

Step 4: Then the message can be stored in cloud data storage.

C. Decryption method

Decryption phase allows users to decrypt the required data from Mobile cloud data storage after decrypting and verifying the integrity of these files. Steps require for decryption are as follows:

Step 1: Receiving encrypted message and Private key k^{-1} from KDC and d from public key

Step 2: Arrange encrypted message as r blocks.

Step 3: Calculate with cipher text using Private key k and d.

Step 4: Now we use modulation with calculated value the remainder value is expected message.

The encryption message and decryption message between the sender and receiver coordination determined by the mobile data cloud storage provider. There is no secure communication channel convenient and safety for the sender to notify the receiver secret key. So, we are choosing key distribution centre as trusted third party. Key distribution centre is responsible of message transaction between the two mobile users to store the data on the cloud storage.

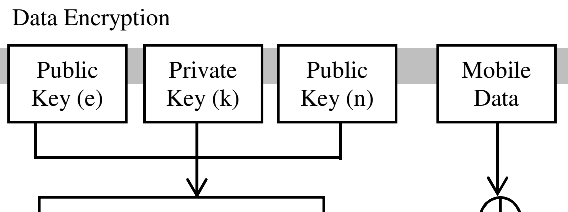

Figure 3. Encryption/Decryption process

VI. PERFORMANCE ANALYSIS

The performance of implementation of the new algorithm examined, primarily on Intel Pentium Dual CPU Core i7 Ghz, 4.00 GB RAM 64 Bit Operating system offer a reasonable number of processors which allows for good scalability testing. The proposed mobile cloud data storage performance calculated according to key generation, encryption and decryption time duration using same data consist of 100 charters. Here we have analysis with existing public key algorithm to find out our New algorithm key generation, encryption/decryption performance.

Algorithm	Key generation/encryption /Decryption Execution time
RSA	30 Sec.
Chaum's	28 Sec.
Diffie-Hellman	32 Sec
New Nlbc algorithm	25 Sec.
No. of characters 100	

Table 1. Performance analysis of various algorithms

Encryption technique is very authoritative and straight forward. In this algorithm we can make any number of square matrix and blocks. The algorithm based on the 'r x r' square matrix. Therefore we can select square matrix with any variables. If comparing to other algorithm, The RSA algorithm calculates each and every text variable for encryption. The chum's algorithm produces two different cipher texts for single encryption. The diffie hellman method needs two user to compute a common secret key exchange value. The New algorithm decryption is complex without the private key. All the plain text is decryption using inverse matrix as a key, Therefore it is providing secure from the unauthorized entities and susceptible. Moreover we are sending secret key through secured channel through key distribution centre or valid entity.

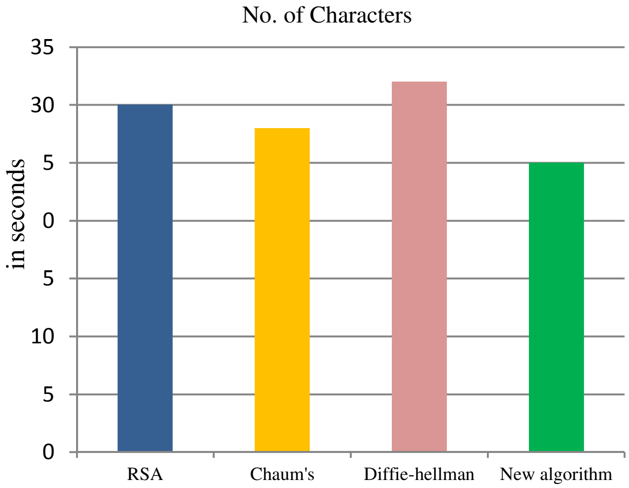

Figure 4. Execution time of various algorithms

VII. RESEARCH BENEFITS

- Our new proposed algorithm provides transparent encryption to mobile cloud data storage security mechanism and also it can be used to other cloud services.
- Proposed algorithm enables to provide key generation facility which can facilitate by the mobile cloud storage provider.
- It provides the benefits of cloud computing while securing mobile data.
- It is strong and identical encryption algorithm that provides more secure and fast.
- The benefit of our new algorithm engage only authorized mobile users.
- It engages all type of cloud storage such as public, private and hybrid.
- Mobile cloud data storage facilitates access to encrypted data from anywhere and any place.

VIII. CONCLUSION AND FUTURE WORK

Our New algorithm using asymmetric key based on the block cipher. The linear block cipher openness to cryptanalysis has rendered it unusable format in practices for the public key encryption/decryption system. It still serves an important academic role in both cryptology and linear mathematics. The reason for selecting linear block cipher for our new algorithm, the linear algebra will not produce same kind results for the repeated text variable. Also, we can construct 2 to 6 characters data block message in single cycle data encryption. Satisfying security requirements is one of the most important goals for mobile cloud system security designers. The proposed method is increase the performance of mobile cloud system security rabidly. Also it will ensure the confidentiality, integrity and message authenticity. The AES algorithm provides confidentiality, the chaums's hash function provides the integrity and the modification of Diffie-Hellman will ensure the authentication. We made experiment with data sample using different size of message and constraint. The experimental result shows that our mobile cloud data storage methodology is improved the performance of interacting, while providing high quality of security service for desired mobile cloud data transactions. Several points can be concluded from the experimental result. It has been concluded that the proposed mobile cloud data storage method works on least computation time and others methodology has taken maximum time for similar message. It can notice that as more safeguards added for any data transaction method, then more secure system is resulted. The result of the performance table 1 shows percent of efficiency of security methods of proposed mobile cloud data storage model.

REFERENCES

[1] Prakash Kuppuswamy, and Saeed Q Y Al-Khalidi, "Analysis of security threats and prevention in cloud storage: Review report", International Journal of Advanced Research in Engineering and Applied Sciences ISSN: 2278-6252, Vol. 3, January 2014.

[2] Prakash Kuppuswamy, and Saeed Q. Y. Al-Khalidi, "Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm", MIS Review Vol. 19, No. 2, March 2014, pp. 1-13.

[3] Prakash Kuppuswamy, "Security implementation on Cloud Storage using New Public key algorithm based on Block cipher", International Journal of Management, IT and Engineering, Volume 4, Issue 5 ISSN: 2249-0558, May 2014.

[4] P. Sharma and S. S. Gautam, "Exploration of efficient symmetric algorithms," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2016, pp. 663-666

[5] R. Ferzli, and I. Khalife, "Mobile cloud computing educational tool for image/video processing algorithms", In IEEE Digital Signal Processing Workshop and IEEE Signal Processing Education Workshop, 2015, pp. 529-533.

[6] Md Asif Mushtaque, "Comparative Analysis on Different parameters of Encryption Algorithms for Information Security", International Journal of Computer Sciences and Engineering, Volume-02, Issue-04, Page No (76-82), Apr - 2014

[7] Dhanalakshmi, S., S. Suganya, and K. Kokilavani. "Mobile learning using cloud computing." International Journal of Computer and Engineering 2.11 (2014): 102-108.

[8] Parsi kalpana, and Sudha singaraju, "Data Security in Cloud Computing using RSA Algorithm", International Journal of Research in Computer and Communication technology, ISSN 2278-5841, Vol. 1, Issue 4, September 2012.

[9] M. Sujithra, and G. Padmavathi, "Ensuring Security on mobile device data with two phase RSA algorithm over cloud storage", Journal of Theoretical and Applied Information Technology, Vol.80. No.2 ISSN: 1992-8645, October 2015.

[10] Mohd Rizuan Baharon, Qi Shi, David L, and Lewellyn-Jones, "A New Lightweight Homomorphic Encryption Scheme for Mobile Cloud Computing", 978-1-5090-0154-5/15, IEEE International Conference on 2015.

[11] John Rhoton, "Cloud Computing Explained: Implementation Handbook for Enterprises", 2013.

[12] P. Menezes, Van Oorschot, and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.

[13] Prakash kuppuswamy, and C.Chandrasekar, "Enrichment of security through cryptographic public key algorithm based on block cipher", Indian Journal of Computer Science and Engineering (IJCSE), ISSN : 0976-5166 Vol. 2 No. 3 Jun-Jul 2011.

[14] Prakash Kuppuswamy, C. Chandrasekar, "Optimisation of Public key Algorithm in Block Cipher using Negative Variables", International Journal of Computer Science Research and Application, Vol. 01, Issue. 01, 2010, pp. 11-23.

[15] Pradeep Sharma, and S. S. Gautam. "Classification of Efficient Symmetric Key Cryptography Algorithms." International Journal of Computer Science and Information Security 14.2 (2016): 105.

[16] E. Ahmed Youssef, "A Framework for secure Healthcare systems based on Big data analytics in mobile cloud computing environments", International Journal of Ambient Systems and Applications (IJASA) Vol.2, No.2, June 2014.

[17] K. Priyanka and Nagarathna Kulennavar, "A Survey On Big Data Analytics In Health Care", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, PP.5865-5868.

[18] Javier Andreu-Perez, C.Y. Carmen Poon, D. Robert Merrifield, T.C. Stephen Wong, and Guang-Zhong Yang, "Big Data for Health", IEEE Journal of biomedical and health informatics, Vol.19 No.4, July 2015.

Author Profile

Prakash Kuppuswamy, Lecturer, Computer Engineering & Networks Department in Jazan University, KSA. He is research Scholar-Doctorate Degree yet to be awarded by University. He has published 25 International Research journals/Technical papers and Participated in many international Conferences in Maldives, Libya and Ethiopia. His research area includes Cryptography, Bio-informatics and E-commerce security, Cloud Security etc.