International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-11, September 2019

Protecting Data on Mobile Cloud Computing

Vikram Patalbansi, G. Prasanna Laxmi

Abstract— Mobile Cloud Computing is a combination of general Cloud Computing and Mobile Computing in which we have to access resources from the remote cloud data center with the help of mobile electronics and peripherals like mobile smartphones, laptops, gadgets, etc. via Cellular Technology or Wireless Communication. Mobile devices have lots of resource constraints like storage capacity, processing speed, and battery life. Hence through simple mobile computing software and programming, we cannot manipulate on mobile devices of cloud data center information. Because of such kinds of difficulty, we have to process information or data through external mobile devices. Accessing and processing of data with the help of Trusted Third Party Agency (TPA) outside the cloud data center and mobile devices have lots of security challenges. To make cloud data secure over outside resources, lots of terminologies and theory are put forward by various researchers. In this paper, we will analyze their theory and its limitations and offer our security algorithm proposal. In this thesis article, we analyze the security framework for storing data on Cloud Server by Mobile and limitation of this process. Also, we review the theory of how data can be secure our data on cloud administrators.

Keywords: Mobile Cloud Computing, Security algorithm of cloud, Wireless security

1. INTRODUCTION

The Mobile Cloud Computing is hybrid technology in the sense of wireless communication between mobile device and cloud data storage system through cellular technology. Using Mobile Cloud Computing (MCC) all the processing and storage are happen over cloud computing area instead of mobile device due to its limitation in storage and processing power and information are stored in multiple location so that MCC is a reliable system and on-demand we can get access to any information irrespective of location and hardware configuration of user mobile electronic devices and hence sharing of information between two or more entities via wireless communication face more security challenges like phishing attacks, man-in-middle attack, denial-of-service (DoS) etc. The objective of this thesis paper is to propose a new theory of encrypting the information as well as authentication of the mobile user.

Manuscript published on 30 September 2019.
*****Correspondence Author(s)
Vikram Patalbansi, Assist. Professor , L.B.H.S.S.T's ICA Bandra Mumbai , Research Scholar Pacific University Udaipur. Email: vikrampatalbansi14@gmail.com
Dr G.Prasanna Laxmi, WOS – A Program(DST), Trainer, HMI Engineering Services. Email; prassanalaxmigandi@gmail.com

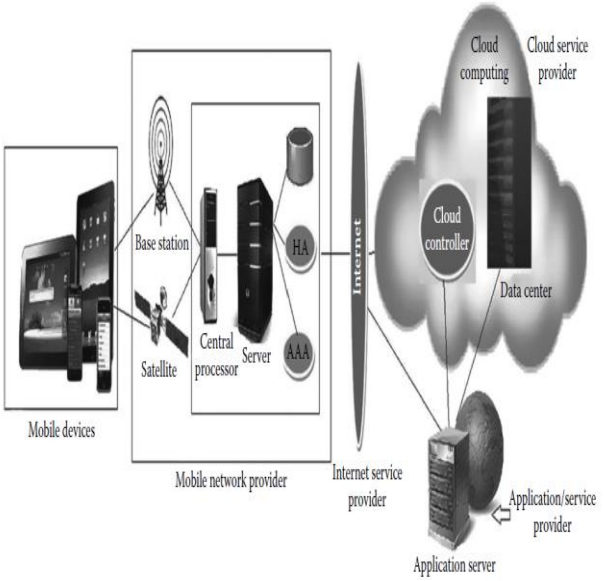

Fig. 1 Mobile Cloud Computing Architecture [4]

2. RELATED WORKS

[1]In Mobile Cloud Computing, all small portable devices are wirelessly connected with the cloud server. During wireless communication, the cloud server generates master keys for every mobile device based on their unique identity like MAC address and IMEI etc. After mutual authentication and registration, the mobile devices and cloud server communicated to each other by encrypting information with the help of cloud server, the generated master keys for specific mobile devices. The main limitation of this paper is that mobile devices having geographical area constraint and lack of central standard authenticator. If devices move from one area to another, then it has to be authenticating with a new server and may face problems of compatibility in term of hardware configuration and software. [2] In this papers authors suggested the theory of Cloud-Radio Access Network (C-RAN) to make communication between the mobile device and cloud server with the help of middle man radio base station with high radio signal bandwidth. The C-RAN network architecture has a three-layer model as L1, L2, L3. L1 is the physical layer (PHY), which mainly provides a data transmission service to the higher layers, channel coding, rate matching and Multiple Input Multiple Output (MIMO) technology, etc. L2 is the layer responsible for Media Access Control (MAC), Radio Link Control (RLC) and Packet Data Convergence Protocol (PDCR) that mainly provides data link control.

L3 is the Radio Resource Control (RRC) layer that mainly provides signalling and radio resource control. In this C-RAN different heterogeneous networks like Wi-Fi, Cellular Network, Wi-MAX, MANET etc. are integrated to the one standard core network via Gateway and one centralized data management system(can say .Cloud Server) manages all devices. To avoid various kinds of network threats and authentication of devices can be done by this cloud server centrally.

However, this physical system layer of C-RAN follows different privacy and security algorithm based upon the different heterogeneous network. So research should be done on one common universal and comprehensive C-RAN security framework and secure virtualization and privacy preservation mechanism.

[3] Authors explain the architecture of Mobile Cloud Computing networks as well as with their challenges and solutions. Regarding mobile devices limitations, they propose the theory of virtualization of task processing and migration of tasks from mobile devices to full-fledged processor. As MCC use the wireless network for communication, so due handover of mobile devices or network fluctuation, processing of task might hamper. Hence they proposed the solution for bandwidth degradation and faster data rate. However, they did not propose the theory of how to upgrade bandwidth and securely pass information over wireless communication. They propose the theory of task division into multiple tasks so that some parts of the task run on mobile and some parts run on a cloud server. However, they fail to show optimal strategy or algorithm on how to divide the task which one run on a cloud server and which one run on mobile.

[4] Hui Li and Tao Jing proposed the theory for mobile IoT devices that can can provide the local storage, sufficient processing power, and appropriate network functions, They provide the theory that how we can generate the lightweight cypher key with help for third party authenticator without putting extra burden on mobile device in respective of low storage and processing capacity.

[5] In Cloud computing, security can be measured based on the following points.

a) Fine-grained access control: The cloud user always attach access policy into each file, which is to be transmitted to the cloud data centre through wireless communication and mobile device.

b) Authorization: Each user who is authorized by a Trusted Third Party Authority (TPA) must be assigned with a unique key for encrypting and decrypting data at both ends of cloud computing.

c) Searching based on parameter: - If the user demands specific information from cloud data storage, then he can search the information based upon keywords.

d) Revocability: - The trusted third party authority having full right to block the content on data storage by denying particular user or attributes of keys.

3. PROPOSED MODEL FOR A DIFFERENT LEVEL OF MOBILE CLOUD COMPUTING

[8]In the Mobile Cloud Computing environment, we have breaches of security challenges at three layers as follows:

I) Security at Mobile devices for authenticating the user.

II) Security at wireless communication channels over cellular network base transceiver system (BTS) and third-party authentication server (TPS).

III) Security between cloud network infrastructure and third-party authentication server.

I)[6] In Mobile Cloud Computing, mobile devices i.e user equipment(UE) must be authenticated and registered to a cloud server to avoid the phishing attack on user communication between a mobile device and cloud server. We know that mobile devices are having IMSI (International Mobile Scriber Identity i.e. SIM card) and IMEI (International Mobile Equipment Identity, i.e. MAC or physical address of mobile devices). Both this unique identity can be a clone or duplicated with advance technologies. By hacking IMSI and IMEI code, an intruder can attack cloud storage on behalf of the original authorized user. To overcome these problems, we suggest that the cloud providers should issue the tamper-proof universal integrated circuit card (UICC) to every mobile user. UICC nothing but like a smart card on which unique integrated circuits are implements. This integrated circuit design decided by Cloud Providers only.

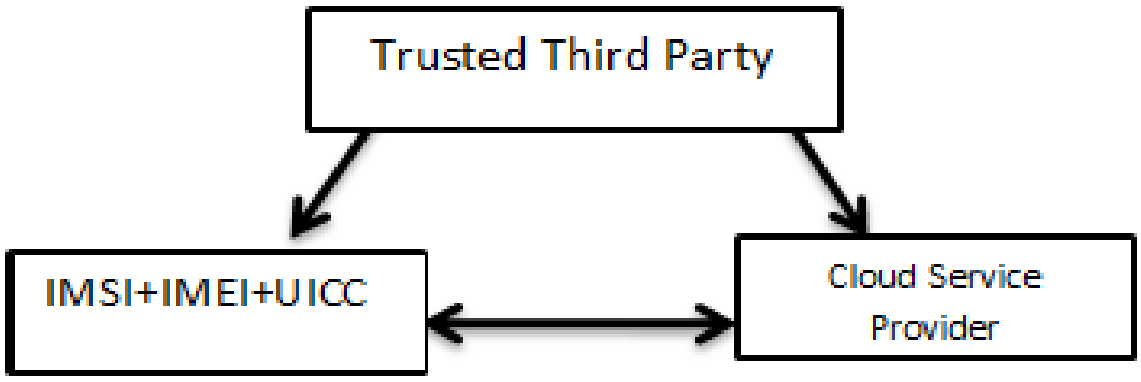

Fig. 2 Proposed Model

The above model shows the verification and authentication of the user between mobile equipment and cloud service providers. The program on mobile equipment generates the unique id with the help of hash function like

User Key (UK) = H(IMSI || IMEI || UICC

4.ALGORITHM FOR REGISTRATION OF MOBILE DEVICE TO A CLOUD SERVER & RESULTS

1) Configure and synchronize hardware communication channels of mobile device and cloud server to each other and establish a wireless connection between the mobile device and cloud data centre(Cloud-Server) and this operation mathematically represented as follows :

(i) isActivate(ME, CDC) where ME is mobile equipment and CDC is Cloud Data centre

(ii) isWirelessNetConnect(ME) … connect the mobile device with wireless network

2) Generate unique identity key as userName based on IMSI, IMEI and UICC and password. Mathematically we can represent these functionalities as follows

const UK.

Var PWD.

UK = H(IMSI||IMEI||UICC)

PWD = encrypt(PWD)

CDC send (UK || PWD) …….send to cloud data centre for registration

3) Cloud Data Center receives an encrypted file from mobile and based on its cloud server, generates a unique cloud ID for the user. Mathematically notation as follows

recive(UK || PWD)

ExpTime (expiry time for a user on cloud access)

UECertificate calculate(store(UK,PWD))

4) Generate reference key for Mobile Users and Cloud Server

$RFKey_{Mobile\_User}$ = Hash (UECertificate, ExpTime,Usage Policy,user access level)

$RFKey_{Cloud\_Server}$ = Hash(user add policy,cloud resource restriction,cloud certificate)

5) Generate Registration Key for connection between Mobile User and Cloud Server for One time only

$RegKey=Hash(Encrypt(RFKey_{Mobile\_User})\Theta Encrypt(RFKey_{Cloud\_Server}))$

Store above Registration key (RegKey) in the cloud storage area for reference by the mobile user and send this registration key to mobile user storage.

Mobile ← send(RegKey)

Moreover, registered to cloud provider via a trusted third party. Every time a mobile user sends or demands user data, with the help of registration key (RegKey) mobile equipment is validated or authenticated. With the help of this technique, we can avoid phishing attacks.

II) The Mobile Cloud Computing consists of a mobile network, trusted third party authentication(TPA) and cloud storage server or data centre.

In mobile networks, mobile devices are connected with network operator via base transceiver station (BTS), access points or satellite by establishing and controlling connection with proper functional interface. With the help of previous steps, the user equipment is authenticated and validated. However, communication between mobile devices and mobile network must be encrypted to avoid eavesdropping and man in the middle attack(MITM). The wireless signals can easily be jammed and captured without physically accessing the User Equipment(UE). To encrypt the signal, if we use the same cypher keys or stream cypher, the attackers easily guess the encrypting key or pattern of cypher text. Based on user key (UK)

UK = H(IMSI || IMEI || UICC)

The trust model in the UE is reasonably simple: there are two trust domains, the tamper-proof universal integrated circuit card (UICC) on which the Universal Subscriber Identity Module (USIM) resides as a trust anchor and the Mobile Equipment (ME). The ME and the USIM together form the UE. [7] According to Roger Piqueras Jover Bloomberg LP New York, NY and Vuk Marojevic Dept. Electrical and Computer Engineering Mississippi State University, Mississippi State, MS stated that universal integrated circuit card (UICC) having unique identification key provided by the cloud service provider and wireless network providers. Hence those Mobile user having User Key based upon universal integrated circuit card(UICC) can get access to cloud service through the wireless network. We have to establish a hardware security mechanism to prevent tampering in the hardware configuration of mobile devices as well as UICC card. For secure roaming of mobile device and location-based authentication, the service-based and location-based authentication, proper functionality are integrated with the service-based architecture of cloud wireless network based upon its domain. Despite the stronger cryptographic algorithms and mutual authentication, UEs and base stations exchange a substantial amount of pre-authentication messages that can be exploited to launch denial of service (DoS) and Man in the Middle attacks.

Regarding User Key (UK) which is calculated based on IMSI, IMEI and UICC, are fed up into pseudo-noise generator of UE, which is a combination of mobile hardware and transmitting antenna. Based upon User Key (UK) values as input, the pseudo-noise generator generates pseudo-noise signals to encrypt the transmitted signal by a mobile user. Also, this encrypted signals get transmitted over wireless network towards nearby Base Station of wireless network and based upon destination address of cloud data centre; it forwarded to cloud Server. With the help of User Key, which is store at the time of User Equipment authentication or validation, the cloud server generates a pseudo-code signal and decrypts the signal. While transmitting the radio wave between Base Station of wireless networks and Mobile Station(User Equipment), the two processes are applied on the radio signals of original messages generated by Mobile User such as one encrypts the plaintext and the second one protects the data from being modified by unauthorized man in the middle attackers. With the help of this algorithm, encryption procedures applied on original message radio signals with pseudo-noise signals which are generated based on User Key(UK) by hardware processor kits which are externally implemented in electronic mobile user.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Here you can use Rivest Cipher 4 (RC4) stream cypher to provide confidentially and Cyclic Redundancy Checksum polynomial 0f 32 bits length for data integrity. Consider the following steps of the algorithm for encryption [15].

1) Encryption of plain text begins with 32-bits CRC polynomial by adding at the end of plain text in the form of original signals generated by the mobile user to provide integrity to the signals.

2) The original signals with CRC code are spread over a wireless network by superimposing pseudorandom signal key sequence based on the input key as User Keys (UK). Then the pseudorandom key sequence is used to encrypt the signals by doing bitwise XOR code. The resultant encrypted signals length equals to the number of data bytes that are transmitted over a wireless network.

3) the RC4 algorithm is applied over original signals with CRC code, to avoid eavesdropping and hacking of signal in the middle of propagation of signals.

4) The payload of the wireless MAC frame for suitable on wireless signals transmitting over a wireless network is created by adding the Integrated Vector (IV) to the front of cypher text signals.

Also, consider the following algorithm steps for decryption of signals.

1) The incoming message in the form MAC frame is decrypted with the help of pseudo key signals based on registration key (RegKey) of Mobile user which is stored at cloud server at the time of registration and authentication of

the mobile user in previous stages. Then Rivest Cipher (RC4) algorithm applied to the decrypted signal to get the original signal and CRC code.

2) After checking the CRC code algorithm, the plaintext and CRC code get separated. If errors are occurred by calculating CRC code, then cloud server rejects the request and if no mistake, the cloud server creates a session with the mobile user for sharing information with the mobile user.

III) Approaches to Mitigate Security Issues in Cloud Infrastructure between and third-party authentication server.

[9]At level stage 3, the security of data over cloud server or infrastructures is crucial issues because after offloading user personal information over the data centre, the user lost his control over his stored information. The cloud computing manages the different-different user information with the help of virtualization technology, and if there are any vulnerabilities in cloud virtualization software on a cloud server or data centre, then data of one user can be accessed by another user or data may be lost by actual users.[10] Due to less encrypted measures for different users information over cloud server, there are chances for intermixing of data or information. So to face such kinds of challenges, we propose a theory for encrypting the information before sending the data towards cloud server. In this procedure, three actors are involved as Mobile User (User Equipment), Trusted Third Party and Cloud Data Centre (Cloud Server). [11]Our theory for encryption based on two security algorithm like Hash-Based Message Authentication Code and DNA Cryptography. As we know that in mobile equipment, UICC (Universal Integrated Circuit Code) microprocessor chip is implemented. By applying the Hash Function on IMSI, IMEI and UICC in combine form then we get unique key which is to be used as an encrypting key to generate block cypher message.

Algorithm Steps are as follows:

1) As we know user equipment having processing constraint, hence most of the processing is to do outside mobile equipment.

2) According to Hash-Based Message Authentication Code, the input message should be in uniform b-bits size for each block. Hence make it slice or fragments of all messages into numbers of blocks having each block same b-bits.

3) Then arranges all message block in a continuous order and padding-left block is inputted into hash function along with User Key UK

[UK = H(UICC || IMSI || IMEI)] to generates temporary message MD'.

4) MD' again is appended to an output signature and on the whole message, a hash function is applied again, the result is our final message digest MD.

Here is a simple structure of HMAC:

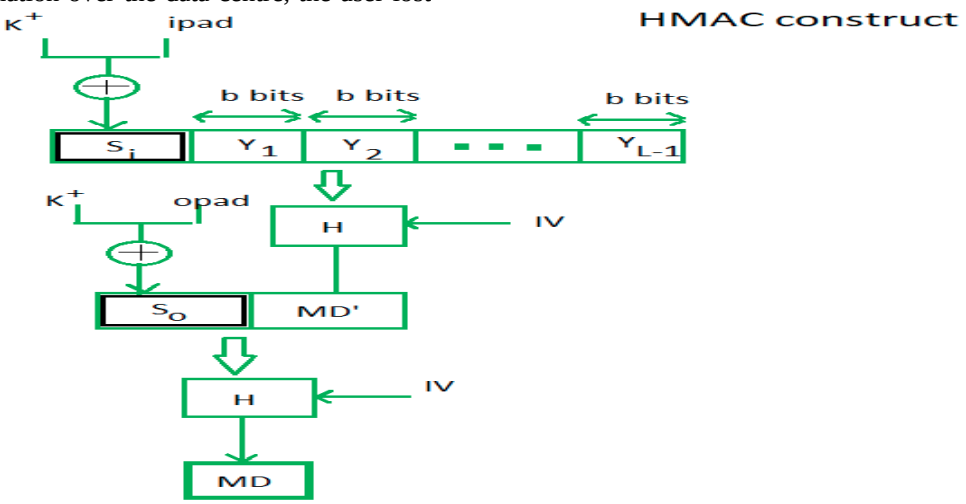

Fig. 3 Hashing Steps

Here, H stands for Hashing function is the original message.

Si and So are input and output signatures respectively,

Yi is the ith block in original message M, where i ranges from (1, L)

L = the count of blocks in M

K is the secret key used for hashing which is equivalent to User Key (UK)

IV is an initial vector (some constant)

The generation of input signature and output signature Si and So respectively.

[13] To a normal hash function, HMAC adds a compression instance to the processing. This structural implementation holds efficiency for shorter MAC values.

5) Then these message bits MD are sending to the Trusted Third Party (TPA) over wireless communication. This message is in an encrypted format so that signal snipping or man in the middle attacks are so difficult because of unique encrypting keys based on UICC.

6) On Trusted Third Party (TTP), we can apply the DNA cryptography on receiving bits coming from Mobile User Equipment through wireless communication channels. With the help of modem, wireless signals converted into binary or digital bits. In this case, every block must contain a uniform number of bits. Assume each block are having b-bits.

7) Mr Leonard Max Adleman had shown how by combing cryptology and modern biotechnology user can design and implement more complex Crypto algorithms. Cryptography can be defined as hiding data in terms of DNA Sequence.

8) DNA computing offers more speed, minimal storage and power requirements.

9) DNA stores memory at a density of about 1 bit/nm3 where conventional storage media requires 1012 nm3/bit. No power is required for DNA computing, while the computation is taking place. One gram of DNA contains 1021 DNA bases, which are equivalent to 108 TB of data.

10) To encode data in a DNA strand which is mainly made, up of 4 nitrogenous bases namely:

1. Adenine (A)
2. Thymine (T)
3. Cytosine (C)
4. Guanine (G)

The easiest way to encode is to represent these four units as four figures:

A(0) –00
T(1) –01
C(2)–10
G(3)–11

By these encoding rules, there are 4!=24 possible encoding methods. Based on some principles as A and G make pairs while T and C make pairs.

Of those 24 methods, only 8 match the DNA pairing rule but the best encoding scheme is 0123/CTAG.

11) Then with the help of Trusted Third Party generates OTP to the mobile user equipment and mobile user re-enter same OTP to send to again Trusted Third Party.

12) The encrypted message MD and the OTP key are converted to ASCII bits.

13)Zero Padding is added to the message and the key to make the size of their binary codes even.

14)The message and the key are XORed together.

15)The XOR output is represented in the DNA bases format, and it is our enciphered text.

16) Enciphered text is sent to a cloud storage server for storing into an encrypted format. This data can be decrypted with help if User Key (UK) and OTP randomly generated by a Trusted Third Party(TTP) to the mobile user. Hence data or information are more secured from hacking as well as cloud administrators.

[14] If any mobile user wants to access their data from the cloud server, then it sends the request to TTP and TTP send the request to the cloud server. After authentication and validation of user with the help of User Key (UK = H(UICC||IMSI||IMEI), the logical connection are established between the mobile user and cloud server via Trusted Third Party (TTP).

1. After authentication of the user, information is retrieved from cloud storage in the form of a DNA base format (enciphered text).
2. This DNA based format is converted into the binary format by TTP.
3. Trusted Third party generated OTP to the mobile user, and after entering OTP by the mobile user, then DNA base format equivalent binary bits and OTP are XORed, and we will get MD in the form of ASCII bits.
4. Then this MD send to the mobile user and over there again XORed User Key (UK) and MD bits. Finally, the mobile user gets the original message.

5. CONCLUSION

Cloud computing emerges as highly popular technology today. If this technology combines with Wireless Technology and with the help of handheld electronic devices, we can access any information by one click away from over mobile device. Then these combine functionalities become Mobile Cloud Computing. In MCC, there are lots of security threats in a mobile device, wireless connection and transmission of signals and cloud infrastructure storage area have been explaining correctly. The solution is given on issues were related to ensuring privacy, authentication, security, trust, and so on, to data and applications that are offloaded to the cloud from mobile devices. Also, we discussed how mobile uses are uniquely authenticated with the cloud server and how trusted the third party perform proper encryption and decryption to avoid various security threats at various levels of Mobile Cloud Computing. By encrypting data before offloading over cloud storage or Server can avoid problems of security at the cloud server.

REFERENCES:

1. Ruben Rios, Rodrigo Roman, Jose A. Onieva and Javier Lopez Network, Information, and Computer Security (NICS) Lab Universidad de M'alaga Campus de Teatinos s/n, 29071. M'alaga, Spain “From Smog to Fog: A Security Perspective” 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC) 978-1-5386-2859-1/17/$31.00 ©2017 IEEE.
2. FengYu Tian, Peng Zhang, and Zheng Yan, Senior Member, IEEE “A Survey on C-RAN Security” IEEE ACCESS, MANUSCRIPT ID Published by the IEEE Computer Society, Citation information: DOI 10.1109/ACCESS.2017.2717852, IEEE Access.

3. Han Qi, Abdullah Gani, Faculty of Computer Science and Information Technology University of Malaya Kuala Lumpur, Malaysia "Research on Mobile Cloud Computing: Review, Trend and Perspectives ".
4. Hui Li and Tao Jing from School of Computer and Information Technology, Beijing Jiaotong University, China "A Lightweight Fine-Grained Searchable Encryption Scheme in Fog-Based Healthcare IoT Networks" published in Hindawi Wireless Communications and Mobile Computing Volume 2019, Article ID 1019767, 15 pages https://doi.org/10.1155/2019/1019767.
5. Hui Li and Tao Jing School of Computer and Information Technology, Beijing Jiaotong University, China "A Lightweight Fine-Grained Searchable Encryption Scheme in Fog-Based Healthcare IoT Networks" published in Wireless Communications and Mobile Computing Volume 2019, Article ID 1019767, 15 pages.
6. New Authentication Scheme to Secure against the Phishing Attack in the Mobile Cloud Computing Munivel E and Kannammal A. Department of Electronics and Communication Engineering, PSG College of Technology, Coimbatore, India published in Hindawi Security and Communication Networks Volume 2019, Article ID 5141395, 11 pages. https://doi.org/10.1155/2019/5141395 https://www.garykessler.net/library/crypto.html
7. Security and Protocol Exploit Analysis of the 5G Specifications Roger Piqueras Jover Bloomberg LP New York, NY rpiquerasjov@bloomberg.net Vuk Marojevic Dept. Electrical and Computer Engineering Mississippi State University, Mississippi State, MS. vuk.marojevic@msstate.edu
8. Efficient Attribute-Based Encryption with Privacy-Preserving Key Generation and Its Application in Industrial Cloud Yujiao Song,1 HaoWang ,1,2 XiaochaoWei,1 and LeiWu 1,3. School of Information Science and Engineering, Shandong Normal University, China. School of Computing and Information Technology, University of Wollongong, Australia. Shandong Provincial Key Laboratory of Software Engineering, China. Hindawi Security and Communication Networks Volume 2019, Article ID 3249726, 9 pages. https://doi.org/10.1155/2019/3249726
9. Authorized Client-Side Deduplication Using CP-ABE in Cloud Storage. Taek-Young Youn, 1 Nam-Su Jho, 1 Kyung Hyune Rhee, 2 and Sang Uk Shin 2. Electronics and Telecommunications Research Institute (ETRI), Daejeon 34129, Republic of Korea. Department of IT Convergence and Application Eng., Pukyong National University, Busan 48513, Republic of Korea Hindawi Wireless Communications and Mobile Computing Volume 2019, Article ID 7840917, 11 pages. https://doi.org/10.1155/2019/7840917
10. Secure Device-to-Device Authentication in Mobile Multi-hop Networks Hyunsoo Kwon1, Changhee Hahn1, Daeyoung Kim1, Kyungtae Kang2, and Junbeom Hur School of Computer Science and Engineering, Chung-Ang University, Seoul, Republic of Korea. {khs910504,Mckinsey,rlaeod,jbhur}@cau.ac.kr Department of Computer Science and Engineering, Hanyang University, Ansan, Republic of Korea. .ktkang@hanyang.ac.kr
11. Z. Cai et al. (Eds.): WASA 2014, LNCS 8491, pp. 267–278, 2014. c_Springer International Publishing Switzerland 2014. Secure and Efficient Searchable Public Key Encryption for Resource-Constrained Environment Based on Pairings under Prime Order Group. Yu Zhang, 1 Yin Li, 1 and YifanWang2 School of Computer and Information Technology, Xinyang Normal University, Xinyang 464000, China Wayne State University, 42 WWarren Ave, Detroit, MI 48202, USA. Hindawi Security and Communication Networks Volume 2019, Article ID 5280806, 14 pages. https://doi.org/10.1155/2019/5280806
12. Authorized Client-Side Deduplication Using CP-ABE in Cloud Storage Taek-Young Youn, 1 Nam-Su Jho, 1 Kyung Hyune Rhee, 2 and Sang Uk Shin 2 Electronics and Telecommunications Research Institute (ETRI), Daejeon 34129, Republic of Korea Department of IT Convergence and Application Eng., Pukyong National University, Busan 48513, Republic of Korea. Hindawi Wireless Communications and Mobile Computing Volume 2019, Article ID 7840917, 11 pages. https://doi.org/10.1155/2019/7840917
13. A Collaborative Key Management Protocol in Ciphertext Policy Attribute-Based Encryption for Cloud Data Sharing. Guofeng Lin, Hanshu Hong, and Zhixin Sun Citation information: DOI 10.1109/ACCESS.2017.2707126, IEEE Access.
14. Security for 5G Mobile Wireless Networks DONGFENG FANG1, YI QIAN 1, (Senior Member, IEEE), AND ROSE QING YANG HU2, (Senior Member, IEEE). Department of Electrical and Computer Engineering, University of Nebraska_Lincoln, Omaha, NE 68182, USA Department of Electrical and Computer Engineering, Utah State University, Logan, UT 84321, USA. Corresponding author: Yi Qian (yqian2@unl.edu) IEEE Access Digital Object Identifier 10.1109/ACCESS.2017.2779146.