International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Hyper Elliptical Curve Cryptography (Hecc) For Cloud

G.S. Parimalam, M.Gobi

Abstract*: This system provides an insight into developing a distributed system which is secure, robust and user friendly. This thesis suggests a design and implementation of a digital envelope that combines the hashing algorithm of MD5, the symmetric key algorithm of AES and the asymmetric key algorithm of Hyper Elliptic Curve. A hybrid algorithm is designed, combining the best of both AES and ECC over GF(p) cryptography. The MD5 hash algorithm is adopted to ensure integrity of the data. Cryptography (HECC). This paper discusses securing the data in clouds through implementing the key for encryption and decryption using hyper elliptical curve cryptography. The focus is on Advanced Encryption Standard (AES), the most commonly used secret key cryptographic algorithm, and Hyper Elliptic Curve Cryptography (HECC), public key cryptographic algorithms which have gained popularity in the recent years and are replacing traditional public key cryptosystems, such as RSA and ECC. Such techniques are necessary in order to use high security cryptographic algorithms in real world applications.

Keywords:- Cloud Computing Technology, Data Computing, Elliptical Curve Cryptography, File Distribution Model, Hyper Elliptical Curve Cryptography, Reduced Service Cost, Security Model,

I. INTRODUCTION

In Today‘s technology world cloud computing plays an important role in storing and accessing files or data over the internet. Cloud computing is used to store the data and its access at a remote place and is synchronized with other web information. The term cloud is used to storing and accessing the data over the internet [1]. It is used to create, configure and customize the applications online. It can be classified into three types:

PublicCloud: A public cloud is made available in pay-as-per user basics [2]. It allows the system to be easily accessible to the general public cloud.

Private Cloud: A private Cloud’s usage is restricted to users. It allows the system and services to be accessible within an organization. It is highly secured in a privatecloud.

HybridCloud(HB): It is a combination of public+private clouds. A private cloud is a sensitive application and a public cloud is a non-sensitive application. It provides a flexible, scalable and cost-effective solution to the organization.

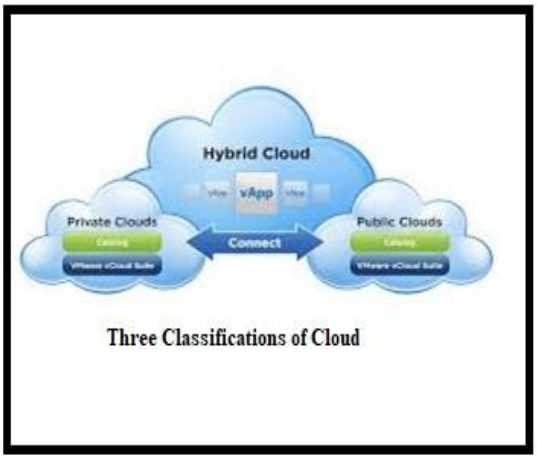

Figure: 1 Three type of Classifications of Cloud.

DiffieHellman communal furtive estimation at the same time supports fast elliptical formulas for fixed based point. It a good security level when compared to ECC. HECC algorithm is generating and verifying the message sign while accurate data [4]. To implement HECC it has three processes such as key generation for encryption and decryption. HECC has curtailed operand segment ECC and HECC overture the same surveillance elevation when compare to ECC. HECC offers power- amateurish mechanism to revamp the solitude of testimony and productivity systems.

Elliptic curve cryptography or error correction code is Associate in Nursing extension to well-known public-key cryptography. In publiccryptography, 2 keys , a publickey, generality knows, and privatekey, which only you know [5]. Encrypt, the public key has applied the information, using a predefined operation many times in discrete logarithmic problems. To decrypt, the private key is applied to, using a different predefined operation several times to get logarithmic problems. The formula depends on the fact that coding is straightforward, and decryption is hard, making decryption impractical without the key. It was the first system to allow secure information transfer without a shared key [6]. The problem is that with today's computers getting faster and faster, there will come a point where we cannot make the Logarithmic problem enough to that can attack. That is where the elliptic curve cryptography comes to encrypt and decrypt the information. Hyperelliptic Curve Cryptography which is considered to give rise to a secure cryptosystem using cloud-computing technology. Cryptography is the study of hiding the information via ciphers. The basic communication it can Alice aspiration send information, labeled unencrypted text, Bob.

Manuscript published on November 30, 2019.
* Correspondence Author
G.S. Parimalam*, Research Scholar, Department of Computer Science, Chikkanna Government Arts College, Tirupur, Tamilnadu, India- 641602.
Dr. M. Gobi, Asst. Professor, Department of Computer Science, Chikkanna Government Arts College, Tirupur, Tamilnadu, India- 641602.

Alice's encryptionkey deliver her procedure by can elucidate the unencrypted text.
She energetically disseminate culminate ciphertext Bob, who may unravel the conveyance complementary explication key. routinely Alice andBob acept consequent to key, retain secret at each's . Alice unravel decoded the key. Bob solely spread key in backpedal to elucidate information. Such a way advisement termed privatekey crypto machine the surveillance mechanisam confide in upon the solitude key in 2 parts. incase Alice defines send information to Bob. Bob prepare the encryptionkey general to anyone [1,5,7]. When using this cryptography key HECC diminished key level, computationalhead less, higher security, requires and consumes less power consumption so I use HECC to encrypt and decrypt the messages [7,8]. This paper is structured in the following manner: In section II, explain briefly about cloud security key concepts related to fusion. In section III, explain cryptography and related research work architecture. In section IV, explain the proposed system algorithms result and discussion. In Section V draws our conclusions from the study results.

II. CONVENTIONAL METHOD

This overviews cloud computing securityprivacy protection, dealswith it various techniques and approaches, focal point provide cloud computing privacy protection security environment [9].
ZhiyuanYin et al., 2017 [7] deliberate privacy problems anxious cloud computing technology. The ECC algorithm is used for the ECC data security enhanced. An proposed algorithm large random sorting based encryption method. The proposed system storing huge datas but only followed limited field in discrete logarithmic problem compromises with the data fetching speed. Hence, the 80-bit H-E-C-C, and 160-bit

Above the conventional method drawbacks overcome proposed Hyper Elliptic Curve Cryptography technique uses the familiar cryptography techniques namely 1)divisor implementation 2)key implementation 3).text encryption and 4)text decryption based cloud secures..

III. SYSTEM DESIGN

The proposed hyper elliptic cryptosystem based on DL based methods, DLP is followed: C - hyperelliptic curve, Fq-finite field within C with q elements. The values D1, D2 are Jacobian, find thevalue of m ЄZ, such that D2 = mD1, prime fields considered for genus 2 & 3 in Eq. 1 & 2. Figure 2 and figure 3 resents to the both transmitter and receiver side HECC encryption and decryption.

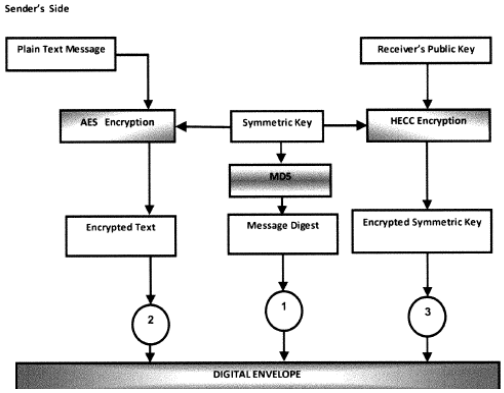

Figure 2 SenderSide and HECC Encryption

E-C-C, are provided privacy strong security public key. Li, J et al (2014), Objective of this proposed HECC algorithm huge data uploading in before file encryption[8].

Mollah et al., 2017 [9] provides an various and different approaches based on the diffihalamaman encryption based cloud storage in data field environment in this part both encryption and decryption very essential part of recommendation conversion.
Ye, J et al., 2016 [10] improve how to manage the security issues concerned with cloud computing, it has some security threats in the finite fieldset. The HECC mechanisam designed in this paper. DiscreteLogarithmic Problem solved and following security problems associated in cloud data fetching.

Zhang, J et al., (2018) proposed various techniques combinations are f ECC, ElGamal, RSA, and HECC algorithms merged and improve best of above mentioned algorithms but in this method time taken encryption process, secure in unauthorized user access personal cloud data.

Table 1 comparison of various public-key cryptosystems

Public-Key System	Mathematical Problem	Best Known method for solving
Integer factorization e.g. RSA	Given a number n, Find its prime factors	Sub-exponential
Discrete Logarithm e.g. DH,DSA	Given a prime n, and numbers g and h, find x such that h=g^xmodn	Sub-exponential
Elliptic curve Discrete logarithm e.g. ECDH,ECDSA [JMV2001]	Given an elliptic curve and points P and Q find k such that Q=kP	Fully exponential

Considered as genus 2: y2=xs+a3x3+a2x2+alx+aO,
***Considered genus 3*:** y2 =x7+a5x5*+a4x4+a3x3+a12 x2+alx+aO.

Proposed system first two methods for keygeneration and encryption and decryption of HECC pseudo code.

Key Generation Algorithm:
Input: The public parameters are Hyperelliptic curve C,
Prime p and Divisor D
Output: The Public key PA and Private key aA
1. $a_A \in_R N$ [choose a at random in N]
2. $P_A \leftarrow [a_A]D$ [The form of PA is (u(x),v(x)) representation]
3. return PA and aA

Encryption/Decryption Algorithm:

The message 'm' that is to be sent will be encoded as a series of points represented as (u(x),v(x)). The encoded message is referred to as Em. For the encryption and decryption process is adopted ElGamal method

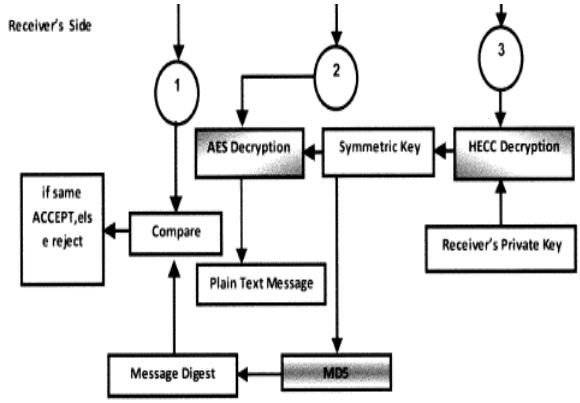

Figure 3 Receivers Side and HECC Decryption

The system was tested for the time taken for

- Divisor implementation
- Key implementation
- Text Encryption
- Text Decryption

The figure 2 values of genus 2 of HECC with a)divisor implementation, b)key implementation, and c)text encryption and 4)text decryption process better than genus 3 of HECC . HECC in Pentium(R)D intel core3 processor genus 2&3 is analyzed prime generated based on the capacity and the time duration/evaluation in the different processes. The input text contains 250bytes. Table.6 display the time (M.sec) taken for the various processes.

a) ElGamal Encryption Algorithm:

Let p be a prime and g be a generator of Zp. The private key x is an integer between 1 and p−2. Let y = gx mod p. The public key for ElGamal encryption is the triplet (p, g, y). If taking discrete logarithms is as difficult as it is widely believed, releasing y = gx mod p does not reveal x. To encrypt a plaintext M, a random integer k relatively prime to p − 1 is selected, and the following pair of values are computed:

a. $\leftarrow g^k mod\ p$
b. $\leftarrow My^k\ mod\ p$ (ElGamal Encryption)

The ciphertext C consists of the pair (a, b) computed above.

b) Elgamal decryption algorithm:

The decryption of the ciphertext C = (a, b) in the El Gamal scheme, to retrieve the plaintext M, is simple:

a. $M \leftarrow b/a^x\ mod\ p$ (ElGamal Decryption)

In the above expression, the "division" by ax be interpreted in the context of modular arithmetic, that is, M is multiplied by the inverse of ax in Zp. The correctness of the ElGamal encryption scheme is easy to verify.

$b/a^x\ mod\ p = My^k(a^x)^{-1}\ mod\ p$
$= Mg^{xk}(g^{kx})^{-1}\ mod\ p$
$= M$

ElGamal encryption/decryption algorithm is used in the implementation of ECC and HECC.

Proposed HECC considered as genus 2 and genus 3peformance of general encrypt-decrypt process for tabulate table1 and table 2.

Table 2 genus2 prime number based results of the HECC system.

HEC Equation	C:v^2=u^5+153834295433461683634059 u^3 + 150354294776434731962993 5u^2+ 19307140258045544535800 68u + 79099282479987590526696 9 Prime: 155002234002335423222716 31 Time (Milliseconds) : 9.999
Divisor Generation	D: div (u^2 + 40442705229937248391325 40u + 93025663446912619000124 34, 87580118895861157762594 40u + 11434287076605500196003 050)
Key Generation	Time (Milliseconds) : 435
Encryption (Size of the txt file : 301 bytes)	Private key:12831136840692077787245381
Decryption	Public key:(u^2+75865172978954725179606 7u + 11796055390062364055612178, 19888780869557250460639 2u + 11976189524366495549555696)

Table 3 genus2 prime number based results of the HECC system

HEC Equation	C: v^2=u^7 + 15645165456u^5 + 156654651651u^4 + 54541516565u^3 + 5465465165464u^2 + 46544454165416516546546 54u + 465465165165464 Prime: 98335577934760928162303 17 Time (Milliseconds) : 10
Divisor Generation	D: Div(u^3 + 46409733757357037178890726u^2 + 12354239996188870576800 87u + 64525716194762067216424 3, 95111721829467726959005 2u^2 + 84672879541590199765181 92u + 94329573330661312107371 12) Time (Milliseconds) : 831
Key Generation	Private Key: 55860097895872655736210 17 Public Key : (u^3+ 80754700381501749394491 21u^2 +33243948147356425418072 24u+ 95996849402254780539153 99, 61022792109323789157806 50u^2 + 89978286368921068558239 54u + 91312564897840652226477 26) Time (Milliseconds) : 4657
Encryption (Size of the txt file : 301 bytes)	Time (Milliseconds) : 4511
Decryption	Time (Milliseconds) : 4712

Table 4 Performance Graph values

	Length of prime=35		Length of prime=55	
	Genus2	Genus3	Genus2	Genus3
Divisor Generation	690	902	871	5127
Key Generation	2343	6490	6860	10000
Encryption	3305	5918	5987	7871
Decryption	3505	6201	6398	9333

IV. RESULT AND DISCUSSION

The HECC analysis various process based to prime values timetaken process and tabled below tables 2 genus 2&3 represented values are listed. The values input text information to encryption process bytes values 301. Table5 shows the time (msec) untrained the multiple processes. The Hyper-elliptic curve cryptosystem genus 2&3 is developed virtualJava paltform and Intel core III Processor @ 954 MHertz speed with 512 MB RAM. Proposed system consist of a)divisor implementation, b)key implementation, and c)text encryption and 4)text decryption process better than genus 3 of HECC. The followings Figure 2 represents to the final analysed graphical representations of genus 2&3.

TABLE 5 HECC for Genus 3 over Fp (capacity of prime values 100)

HEC Equation	C:v^2=u^7+11u^6+17u^5+794319u^4 +6521255u^3+1065528u^2+3279922 u+3728927 Prime:261094452146722860343096135718189764848005451433696063113144572692654616502960219775569366441413797 3 Times periods (M.secs) Hcurve implementation: 21.0
Divisor implementation	D:div (u^3+3954414606220030303685727306238378155044425954409152934793075806939568651548874030659801079021847 2u^2+2196506606161905158625536713768975761516175931125066235611315024692924689753525065768743307508540980u+6921129574169498069440563610671136461542145109329290049337745064197872115792387261451738104538651 17,25178836248238098016139990792928145382056399257635836615137990142892500971593461567148784722780766 24u^2+3822786137012914438041678195217554692891134849718754962102695586181625386132809936106028071291919 039u+9676484617491087558710664258493065674704364556537857071285231803304389911059804878009460725183053 23) Times periods (M.secs) a) divisor implementation: 503.0
Key implementation	Privatekey: 4740790959980613145797918528506136979354167540681460471783568456218712380772542927873382734072973969 Publickey:div (u^3+2177790245879939813031918228254100634737234890841637827254160257521791715344453851323313856133053792u^2+2373789866899144936066646386579674538289821840526720189657717094049407066330898305677123950073127224u+22847536169750103314046717729700788387255279068261208049150531147669443222051872472568248064207 0 1540,751095294005252527766898102318532256226665684573945970093578805588260591291545054770154861743533376u^2+1948893547688039540512295148154392633902840861501403194367873067759220779383860656100878857450587 12u+8068717011790155127403977256062492212245131661891007893162799439942653555804550352143829540372829341) Times periods (M.secs) b) key implementation: 6235.0
Text Encryption (250 bytes)	Times periods (M.secs): 1969.0
Text Decryption	Times periods (M.secs): 2516.0

TABLE 6 HECC for genus 2&3 analysis (Lp: 75&100)

	Length of prime =75		Length of prime = 100	
	Genus 2	Genus 3	Genus 2	Genus 3
Curve Generation	26	31	15	21
Divisor Generation	424	485	454	503
Key Generation	1844	3328	3516	6235
Encryption	1094	1468	1484	1969
Decryption	1171	1813	1625	2516

The figure 4 represents HECC effective results in the prime number field number values such as 75 to 100 the total values text encryption implemented true values formation. The result values genus2 values defined 1)divisor implementation (503.0 msecs,) 2)key implementation (6235.0 msecs) , and 3).text encryption (1969.0 msecs) and 4)text decryption (2516.0 msecs) all the values produces better results in genus3. Software analysis represents to depends on the particular machanisams, on the underlying developments, to the intel core 3 processor methods performed. The particular involvements in this implementation of HECC of genus 2&3 on (GP)generalpurpose INTEL CORE 3processors in the same concept. The proposed concepts nearly authentications parameters and fair resemblance between the different of two cryptosystem belvedere. Proposed system preservation layer, the evaluation to the divisor implementation of genus2HECC & genus3HECC quites in different ranges and values of eaches genus2 and 3.

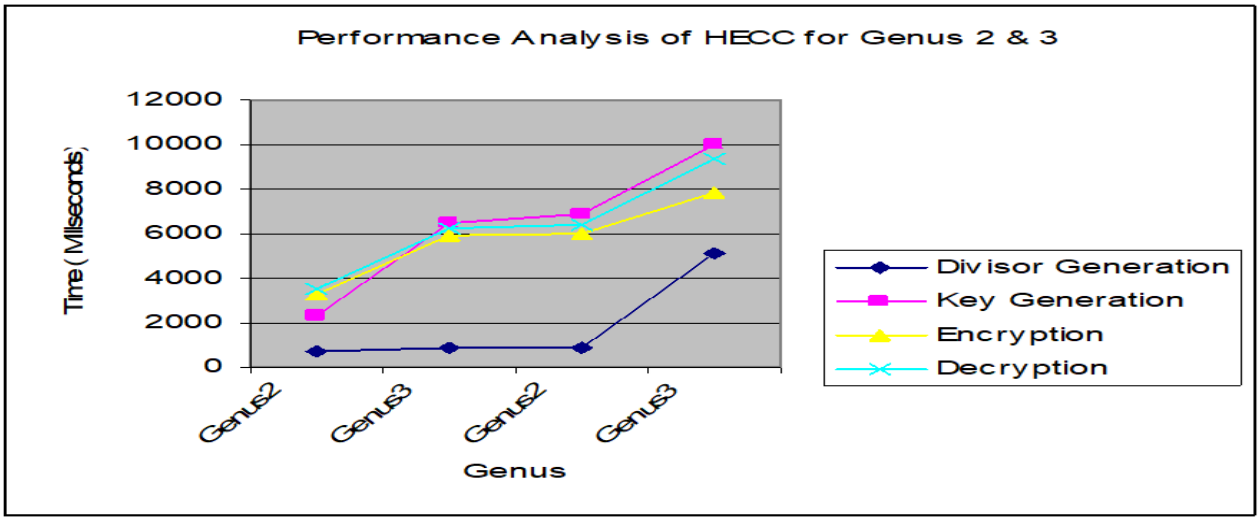

Figure 4 Performance analysis of HECC for genus 2 and 3

Various values, obtained and calculated to various focus points are graphed in graphical representation the values obtained at each points. Customizing values differentiates precalculated values in the different range of both are deviated in the certain parameters. This HECC of genus2 encryption (4740790959980613145797918528506136979354167540 6814604717835684562187123807725429278733827340729739 69) good than genus3 on every process of implementation. Proposed system genus2 based implementations are highly security based (v^2=u^7+11u^6+17u^5+794319u^4+6521255u^3+106552 8u^2+3279922u+3728927) and also perfect for exe and cloud based constrained environments applications .

Table 7 Encryption and Decryption of 128 bit AES key and MD5 using HECC and RSA

	HECC Encryption	RSA Encryption	HECC Decryption	RSA Decryption
128 bit AES key	121	110	120	140
MD5 Message digest of the Ciphertext	100	100	120	140

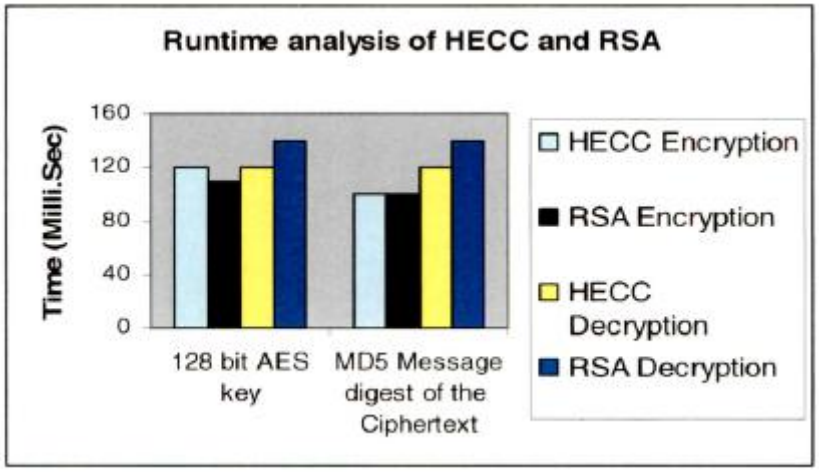

Figure 4 Encryption & Decryption of 128 bit AES key and MD5 message digest using HECC and RSA

The output is displayed in Gel editor. AES key is encrypted using the HECC encryption based on prime byte length 11 bytes. The encryption finished in 121.0 milliseconds. The decryption process took 120.0 milliseconds for the prime length of 11 bytes.

V. CONCLUSION

Cloud data storage increased by the past few years many industries and institutions are pass their information for flexible and cost savings. This paper discussed about Hyper Elliptical Curve Cryptography (HECC). When compare to ECC using Discrete Logarithmic Problem using Genes 2 and Genes 3 describes the algorithm for Key implementation (6235.0 msecs) process for text Encryption (1969.0 msecs) and text Decryption (2516.0 msecs). To provide the Performance Analysis using HECC for Curve Generation, Divisor Generation, Key Generation. Using HECC Genus 3 over Fb to calculate the Prime length using the HECC equation (v^2=u^7+11u^6+17u^5+794319u^4+6521255u^3+1065528u^2+3279922u+3728927) it takes millisecond curve generation to encrypt and decrypt the data. When Compare to ECC HECC is high secured and their key size is shorter than ECC .so, HECC is a more secure algorithm in cloud computing Technology. Finally, NIST recommended 80-bits key in size for hyper-elliptic curve, and 1024-bits and 160-bits for RSA and ECC respectively. Therefore, one can use HECC asymmetric key technique as an alternative to RSA in the digital envelope.

REFERENCES

1. Atta ur Rehman Khan, Mazliza Othman ,Feng Xia ,Abdul Nasir Khan, “Context-Aware Mobile Cloud Computing and Its Challenges”, In Proceedings of IEEE International conference on Cloud Computing, vol. 2(3),pp. 42-49,2015
2. Laiphrakpam Dolendro Singh and KhumanthemManglem Singh. “Image Encryption using Elliptic Curve Cryptography”, Procedia Computer Science, vol 54,pp. 472-481,2015
3. Christina Thomas ,Gnana Sheela K , Saranya P Krishnan. “An Efficient Elliptic Curve Scalar Multiplication using Karatsuba Multiplier” ,International Journal of Engineering Research and General Science, vol. 3, pp. 1074-1086,2015
4. Medhat Tawfeek, Ashraf El-Sisi, ArabiKeshk and FawzyTorkey. “Cloud Task Scheduling Based on Ant Colony Optimization”, The International Arab Journal of Information Technology, vol. 12(2), March 2015
5. Mehdi Bahrami. “Cloud Computing for Emerging Mobile Cloud Apps” In proceedings of IEEE international conference, pp. 4-5,2015
6. C. Aguero, N. Koenig, I. Chen, H. Boyer, S. Peters, J. Hsu, B. Gerkey, S. Paepcke, J. Rivero, J. Manzo, E. Krotkov, and G. Pratt. “Inside the Virtual Robotics Challenge: Simulating Real-time Robotic Disaster Response”, In Proceedings of IEEE International conference on Automation Science and Engineering ,vol. 12(2), 2015.
7. Zhiyuan Yin; Yu, F.R.; Shengrong Bu; Zhu Han. “Joint Cloud and Wireless Networks Operations in Mobile Cloud Computing Environments With Telecom Operator Cloud” In Proceedings of IEEE International conference on Wireless Communications,vol.14(7), pp.4020-4033,2015
8. Li, J., Li, J., Chen, X., Liu, Z., & Jia, C. (2014). Privacy-preserving data utilization in hybrid clouds. Future Generation Computer Systems, 30, 98-106.
9. Mollah, M. B., Azad, M. A. K., & Vasilakos, A. (2017). Security and privacy challenges in mobile cloud computing: Survey and way ahead. Journal of Network and Computer Applications, 84, 38-54.
10. Ye, J., Xu, Z., & Ding, Y. (2016). Secure outsourcing of modular exponentiations in cloud and cluster computing. Cluster Computing, 19(2), 811-820.
11. Zhang, J., Chen, B., Zhao, Y., Cheng, X., & Hu, F. (2018). Data security and privacy-preserving in edge computing paradigm: Survey and open issues. IEEE Access, 6, 18209-18237.
12. Liu, X., Xia, Y., Xiang, Y., Hassan, M. M., & Alelaiwi, A. (2015, November). A secure and efficient data sharing framework with delegated capabilities in hybrid cloud. In 2015 International Symposium on Security and Privacy in Social Networks and Big Data (SocialSec) (pp. 7-14). IEEE.