Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing

Kruti H. Patel[1] Shrikant S. Patel[2]
[1]P.G. Student [2]Assistant Professor
[1,2]Department of Computer Engineering
[1,2]Alpha College of Engineering and Technology Khatraj, Kalol

Abstract— Currently cloud computing has been used by many organization, because of its benefits like total cost decrease and ease of access of data. Multi cloud storage is recently being popular through its several advantages. Though there are many benefits by using cloud computing the security breaches make some of the users to step out of using it, as they share confidential data with cloud storage providers but, they may be untrusted. We proposed to develop modified RSA algorithm, which is extensively used in the popular implementations of Public Key Infrastructures. In asymmetric key cryptography, also called Public Key cryptography, two different keys (which form a key pair) are used. One key is used for encryption & only the other corresponding key must be used for decryption. By using RSA algorithm and implementation with the digital signature (DSS). we provide data integrity over a multi cloud. Assurance of data integrity that is data remain as it is on server for long time. In our proposed research we will combine RSA with HMAC function. We provide data integrity in the secure network transaction over a multi cloud. It depends on multi cloud so, to share confidential data between clouds and to prevent them from hackers. We will also generate there digital signature by using different mechanisms. This paper will focus on some of the integrity proving techniques in detail along with their limitations.

Key words: cloud computing, digital signature, RSA, HMAC, security

I. INTRODUCTION

In IT industry cloud provides three services SaaS, Pass, Iaas. Cloud computing is a network where the user can use services providing by csp on pay per use bases. This kinds of technology helps users for handling resources effectively on-site.so the challenging factor on multicloud is strong data security and transaction mechanism over a multi cloud.

Mostly the data are stored in clouds are highly sensitive. For example, financial records and social networks. Gain the strong security over the transaction on multicloud is very much important.so, in the system provides data integrity and verified valid services to authorized users in multicloud. The process authentication is initiated for all valid transactions that is been performed.

A. Data Security

Everyone wants to use the cloud due to cost saving and new business models. But when it's come to cloud security. It's important to understand the different threats landscape that comes into play.

There are complex data security challenges in the cloud: -

1) How cloud service provides securely recycle disk space erase existing data it's about lack of standard.
2) The new party insider who does not done work for your company and who do not member pf your company but may have control and is visible to your data.
3) There are need to protect the online bank transaction, government, confidential business or regulatory data.
4) The most compliance concern is auditing and reporting.
5) Legal issues relative to such government rules as the EU data privacy directive.

B. Data Integrity Check

integrity check means there are checking the sender send whatever value to receiver will actually receive at that place or not or some modifications are done or not it will be check.in which it will be check the TPA is reliable and independent according to service level agreement(SLA).

There are three steps that manage how the integrity check on cloud:

1) User

User first chose a random parameter to develop the public and the private keys then user will sign the data using the private key to be uploaded to the cloud, then user sends the signed data to the cloud server and deletes its local copy.

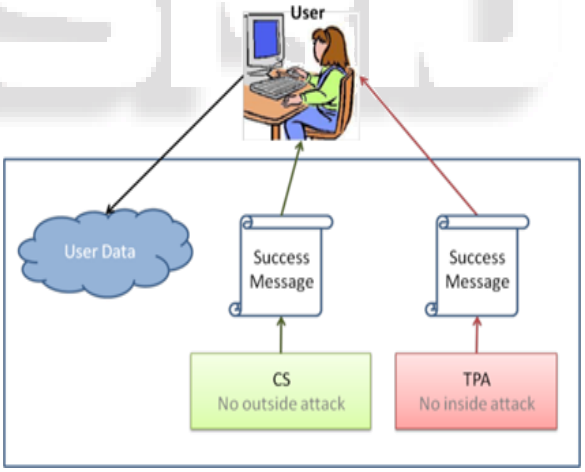

Fig. 1: No inside and outside attack

2) CS

CS (cloud server) will compute a hash value from the original data to send it to the TPA, and then takes this hash value along with the data signed in the cloud for verify using the public key. At the end, the CS will inform the user if the data in the cloud modified or not.

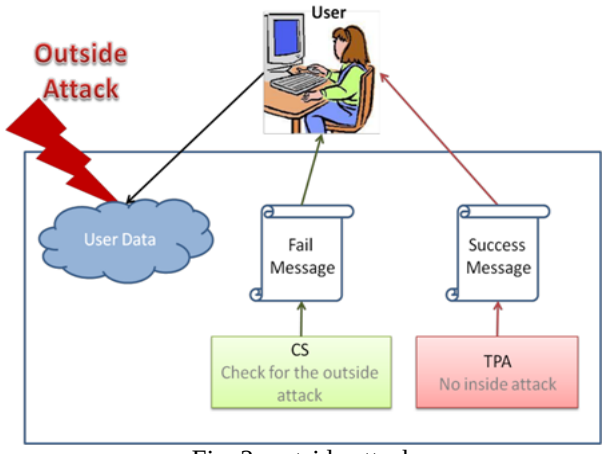

Fig. 2: outside attack

3) TPA

After the cloud server finishes its role, the TPA will be initiated to verify over the cloud server work by taking the hash value from the cloud server. TPA will take the data signed form the cloud and decrypt it with the public key. The decryption result gives the hash value that will be compared along with the hash value that the cloud server compute it in some part. After verification is finished, the TPA will inform the user if the CS was trusted or not.

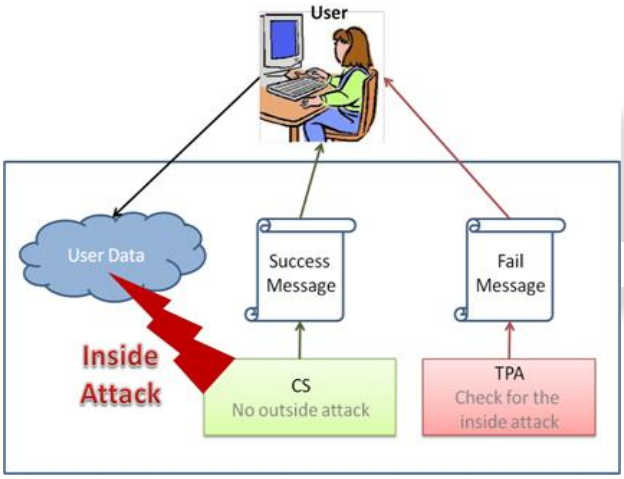

Fig. 3: Inside attack

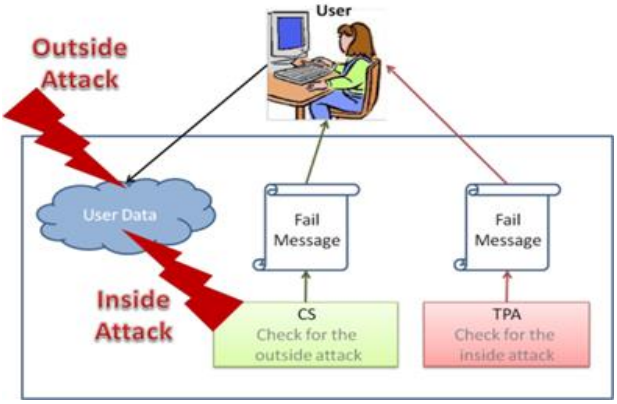

Fig. 4: Inside and Outside attack

4) Role of TPA

Third Party Auditor can be used to give security and integrity of data. Third party auditor can be a trusted third party that solves the conflicts between the cloud service provider and the client.TPA mainly used to achieve integrity concepts that helps the users to manipulate and examine the data from unauthorized people that interact with the cloud or extract from the data. Encryption and Decryption algorithms are used to provide the security to user while using third party auditor. The third party is used to resolve any kind of problems between service provider and client.

5) Various Algorithm On Cloud For Security

RSA- is an algorithm for public-key cryptography, involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. in which the message will be encrypted with the public key can only be decrypted using the private key. user data include encryption prior to storage, user authentication procedures prior to storage or retrieval, and building secure channels for data transmission.

MD5- (Message-Digest algorithm 5), a widely used cryptographic hash function with a 128-bit hash value, processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into 512-bit blocks .whenever the message is passed the length of 512 blocks are divisible. In this sender use the public key of the receiver to encrypt the message and receiver use its private key to decrypt the message.

AES- In cryptography, the Advanced Encryption Standard (AES) is a symmetric-key encryption standard. Each of these ciphers has a 128-bit block size, and key size 128, 192 and 256 bits, respectively. AES algorithm ensures that the hash code is encrypted in a highly secure manner. Its algorithm is as follows:

1) Key Expansion
2) Initial Round
3) Add Round Key
4) Rounds
5) Sub Bytes - a non-linear substitution step where each byte is replaced with another according to a Lookup table.
6) Shift Rows - a transposition step where each row of the state is shifted cyclically a certain number of steps.
7) Mix Columns - a mixing operation which operates on the columns of the state, combining the four bytes in each column.
8) Add Round Key—each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.
9) Final Round (no Mix Columns)
10) Sub Bytes 11. Shift Rows
11) Add Round Key

6) RSA based algorithm

RSA involves a public key and private key. The public key can be known to everyone, it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key. The keys for the RSA algorithm are generated the following way:

1) Choose two different large random prime numbers p and q
   Calculate n=pq
2) n is the modulus for the public key and the private keys
3) Calculate the totient: Ø(n)=(p-1)(q-1)
4) Choose an integer e such that $1 < e < Ø(n)$, and is co prime to Ø(n) i.e.: e and Ø(n) share no factors other than 1; gcd(e, Ø(n)) = 1.
5) e is released as the public key exponent

6) Compute d to satisfy the congruence relation de=1(mod(Ø(n))) i.e.: de=1+kØ(n) for some integer k.
7) d is kept as the private key exponent

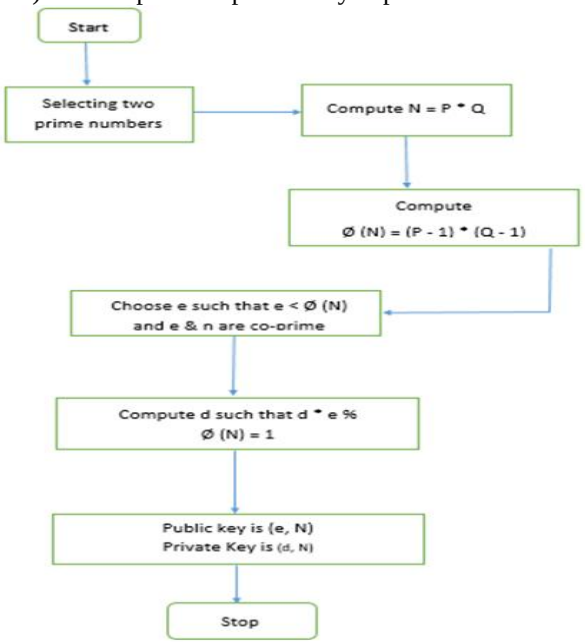

Fig. 5:

7) The HMAC function

The definition of HMAC requires a cryptographic hash function, which we denote by H, and a secret key K. We assume H to be a cryptographic hash function where data is hashed by iterating a basic compression function on blocks of data. We denote by B the byte-length of such blocks (B=64 for all the above mentioned examples of hash functions),and by L the byte-length of hash outputs (L=16 for MD5, L=20 forSHA-1). The authentication key K can be of any length up to B, the block length of the hash function. Applications that use keys longer than B bytes will first hash the key using H and then use the resultant L byte string as the actual key to HMAC. In any case the minimal recommended length for K is L bytes (as the hash output length).We define two fixed and different strings iPad and opad as follows (the 'i' and 'o' are mnemonics for inner and outer):

iPad = the byte 0x36 repeated B times
opad = the byte 0x5C repeated B times.
To compute HMAC over the data `text' we perform
H(K XOR opad, H(K XOR iPad, text))
Namely,

1) Append zeros to the end of K to create a B byte string (e.g., if K is of length 20 bytes and B=64, then K will be appended with 44 zero bytes 0x00)
2) XOR (bitwise exclusive-OR) the B byte string computed in step (1) with iPad
3) Append the stream of data 'text' to the B byte string resulting from step (2)
4) Apply H to the stream generated in step (3)
5) XOR (bitwise exclusive-OR) the B byte string computed in step (1) with opad
6) Append the H result from step (4) to the B byte string resulting from step (5)
7) Apply H to the stream generated in step (6) and output the result

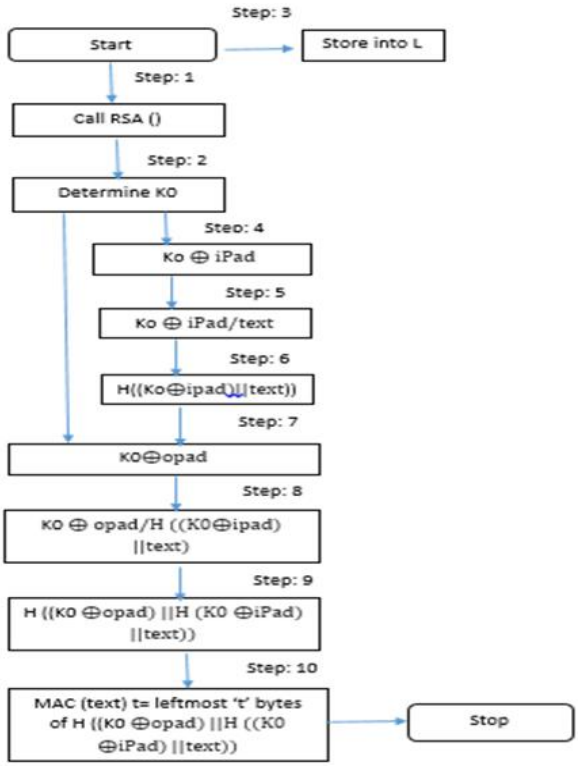

Fig. 6:

II. LITERATURE REVIEW

1) Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing.

Abstract

[1]The cloud is a next generation platform that provides dynamic resource pools, virtualization, and high availability.[2]Today, we have the ability to utilize scalable, distributed computing environments within the confines of the Internet, a practice known as cloud computing. Cloud computing is the Concept Implemented to decipher the Daily Computing Problems, likes of Hardware Software and Resource Availability unhurried by Computer users.[3] The cloud Computing provides an undemanding and Non ineffectual Solution for Daily Computing.[4] The prevalent Problem Associated with Cloud Computing is the Cloud security and the appropriate Implementation of Cloud over the Network.[5]In this Research Paper, we have tried to assess Cloud Storage Methodology and Data Security in cloud by the Implementation of digital signature with RSA algorithm.[6]

In this research paper they explain about how data will be securely storage on cloud and how it will be implemented. They implement the digital signature on it with the use of RSA algorithm. In which they are found how digital signature will be implemented by only using RSA algorithm. At very first they use the RSA algorithm for data authentication which are stored at cloud and they also implement the digital signature for verify the users data which are stored on cloud. Thus, mainly there area of research is about provide data storage security on cloud.

2) Secure Cloud Storage Model with Hidden Policy Attribute based Access Control

Abstract

[7]We propose a secure cloud storage model that prominently addresses security and storage issues in cloud. These curity is achieved by anonymous authentication of the users; where the attributes associated with individual users are hidden from cloud. [8]This helps the cloud users to remain anonymous as well authenticated, for this digital signature based authentication scheme is developed.[9] Also, a decentralized architecture is implemented for distributed key management.[10] Further, Query driven approach is developed for hiding the access policies defined by individual user for his data i.e. the access is granted to the requester only if his credentials matches with the access policy.[11] Homomorphism encryption scheme is used for encrypting the data that is stored in cloud.[12] These data are sometimes vulnerable to loss or damages. In order to address this issue, an automatic retrieval mechanism is developed where the lost data is retrieved automatically.[13]

Conclusion

In this paper they will focus on data storage and security issues on cloud. They will seen some problems on bases of cloud which is types of architecture ,access control methods and the authentication techniques. They will reduces this problems over a cloud by implementing multiple KDS structure. in which they will develop a one type of structure that will reduces some problem for security and user authentication on cloud. In that structure the users don't know about their authenticated and their attributes are hidden from cloud by implementing digital signature algorithm. by using access method they will hide the users individuals files from cloud by implementing query based method. Further they enhance the storage based security issues, such as they will used homophonic encryption techniques for outsourced data. in cloud they will face also some issues related to data lost or leakage. This issue will reduced by implementing string matching algorithm it automatically match the string of data and retrieved easily.

3) Online Signature Recognition using Software as a Service (SaaS) Model on Public Cloud

[14]The signature recognition systems are widely used and measure of security and authenticity in terms of commercials well as official transactions. [15]The exciting signature recognition systems need a high configuration machine to perform multiple operations of feature vector extraction, enrollment and verification. [16]These implementations are generally standalone and implemented on a single server based architecture, in this case even a single point of failure may occur. [17]The standalone application are not scalable.[18] With the increasing number users the biometric implementation has to be scalable and capable of handling large datasets for a large population. [19] In this paper, a highly scalable, pluggable and faster cloud based online signature recognition system is proposed, which is capable of operating on enormous amounts of data, which, in turn, induces the need for sufficient storage capacity and significant processing power. [20]

Conclusion:

In this research are they will be described about how digital signature works for authentication on commercial transaction and financial transaction on cloud. they will use the Microsoft azure cloud that make the device is highly scalable, pluggable and faster online signature reorganization system. They will also use SaaS cloud model for verified the user signature and there all signature data will captured using digitizing tablet and they will be stored on blob storage in cloud. They will also provide the sufficient storage capacity and significant processing power for high amount of data. mainly they will implement one significance system that will mostly used in online banking and e-commerce, where handwritten dynamic signature can be used for authentication of transaction.

4) Research and Implementation of Four-prime RSA Digital Signature Algorithm

Abstract

[21]Big module RSA signature algorithm is very popular these years. We try to improve it and get more operation efficiency. We proposed a four-prime Chinese Remainder Theorem (CRT)-RSA digital signature algorithm in this paper. We used the Hash function SHA512 to make message digest.[22] We optimized large number modular exponentiation with Recombining in Montgomery algorithm.[23] Our experiment shows that our method got good performance. The security analysis shows higher signature efficiency on resistance of common attacks.

Keywords—RSA encryption algorithm; Four prime; Chinese remainder theorem; Montgomery algorithm; Hash function; Digital signature

Conclusion:

In this paper they will produces the higher computational efficiency of RSA algorithm by using four prime CRT-RSA signature algorithm which combines with some algorithms. Such as, modular exponentiation algorithm and the Chinese remainder theorem to optimize the process of signature. Their research will prove that the four prime signature algorithm is more useful then other known signature algorithm , and it will use for authenticated the transaction.

5) A Survey on Data Integrity Techniques in Cloud Computing

Abstract

[24]Cloud computing which is envisioned as the next generation architecture of IT Enterprise comes into focus when someone thinks about what IT always needs.[25] It is way to increase capacity or add capabilities without investing in infrastructures well as licensing cost on new software.[26] Besides of this advantage there is one major problem that needs to face while keeping sensitive data in cloud, Assurance of data integrity that is data remain as it is on server for long time. Client cannot physically access the data from the cloud server directly, without client's knowledge, Cloud Service Provider(CSP) can alter or delete data which are either unused by client from a long a time or takes large memory space. Hence, there is need of checking the data periodically for its integrity, checking data for correction is called data integrity. [27]To overcome data integrity problem, many techniques are proposed under different systems and security models.[28] This paper will focus on some of the integrity proving techniques in detail along with their limitations. [29]

Keywords :Survey, Cloud Computing, Data Integrity

Conclusion:

In this research paper they will just focus on how the data integrity works on cloud .and how the integrity of the data will be managed on for using various PDP's they will be reduced there issues on some basis. basically hey will implement the huge amount of data will be securely stored

for long time on cloud by implementing data integrity on cloud. Secure network and provide higher efficiency of data. Thus, they will choose various PDP for verify the data and POR that is based on selecting random bits on data blocks. in which they will face some issues.

III. METHODOLOGY

A. Old Approach

Step 1:apply key generation algorithm.
Step 2:create digital signing.
Step 3:apply encryption method on that particular dataset by sender.
Step 4:apply decryption method on that data by receiver.
Step 5:match the signature verified or not.

B. New Approach

Step 1: Apply modified RSA algorithm on sender data
Step 2: Generate public key by sender and encryption is perform at sender side
Step 3: Generate private key by receiver and decryption is perform at receiver side
Step 4: Send this data into HMAC function
Step 5: HMAC create a secret hash key and apply it both the side
Step 6: This two secret hash keys are maintained by the TPA
Step 7: If the hash key is match at sender side or else receiver side
Step 8: Then authentication function are matched
Step 9: If not match the secret key any one side repeat step 2
Step 10: If Match then repeat step below step
Step 11: Apply digital signature both the side
Step 12: If match digital sign then the user send the data to the receiver
Step 13: If do not match digital sign of any one side then repeat step 4

IV. CONCLUSION

In early years there are various technologies are updated by RSA algorithm. And very high level security achieved by using RSA and digital signature algorithm. But there are some limitation that can not provide highly sufficient and secure transaction of huge amount of data over a cloud. Our system provides higher efficiency and construct high security on all types of cloud.in our system we proposed to develop the RSA higher efficience algorithm and TPA for authentication our data over perform transaction on cloud and apply the digital signature on that TPA through verify the sender and also apply on that HMAC function for hashing the key value on cloud. thus, experimental results showed that the proposed RSA and digital signing algorithm is more efficient than other signature algorithm used on cloud.

V. FUTURE WORK

In future work there is a capacity for verifying over the other services that the cloud performs. It would be preferable to check over the ability to edit or delete the data in the cloud. In addition, TPA would be enhanced if there is a serious proof for its credibility. The verification process could be done by further techniques rather than the digital signature to improve the efficiency and security. We can improve the implementation by enabling the user to enter different kinds of data to be verified.

REFERENCES

[1] Uma Somani,Kanika Lakhani and Manish Mundra , 'Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing" ,978-1-4244-7674-9/10/$26.00 ©2010 IEEE
[2] http://en.wikipedia.org/wiki/Cloud_computing
[3] http://www.cloudcomputing china.cn/Article/luilan/200909/306.html
[4] http://searchcloudcomputing.techtarget.com/s Definition/0, sid201_gci1287881,00.html
[5] http://www.boingboing.net/2009/09/02/cloudcomputing -skep.html
[6] (U.S.) Nicholas. Carr, fresh Yan Yu, "IT is no longer important: the Internet great change of the high round - cloud computing," The Big Switch: Rewining the world from Edison to Google, CITIC ublishing House, October 2008 1-1
[7] M. Sowmiya, PG Student and M. Adimoolam, Assistant Professor ,"Secure Cloud Storage Model with Hidden Policy Attribute based Access Control" ,978-1- 4799-4989-2/14/$31.00 © 2014 IEEE
[8] S. Ruj, M. Stojmenovic and A. Nayak, "Decentralized Access Control with Anonymous Authentication of Data Stored in Cloud", IEEE/ACMInternational Symposium on Cluster, Cloud and Grid Computing, pp. 556–563, 2013
[9] S. Jahid, P. Mittal and N. Borisov, "EASiER: Encryption-based access control in social networks with efficient Re-vocation," in ACM ASIACCS.
[10] Kan Yang, XiaohuaJia and Kui Ren, 'DAC-MACS: Effective DataAccess Control for Multi-Authority Cloud Storage Systems', IACR Cryptology e-Print Archive, pp 419, 2012.
[11] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to role-basedaccess control," IEEE Computer, vol. 43, no. 6, pp. 79–81, 2010.
[12] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, "Toward Secure andDependable Storage Services in Cloud Computing", IEEE T. Services Computing, vol. 5, no. 2, pp. 220–232, 2012.
[13] J. Hur and Kun Noh, "Attribute-Based Access Control with EfficientRevocation in Data outsourcing Systems", IEEE Trans. Parallel Distrib.Syst.,vol. 22, no. 7, pp. 1214–1221, 2011.
[14] Dr. Vinayak Ashok Bharadi and Mr. Godson Michael D'silva, "Online SignatureRecognition using Software as a Service (SaaS) Model on Public Cloud" ,978-1-4799-6892-3/15 $31.00 © 2015 IEEEDOI 10.1109/ICCUBEA.2015.208
[15] H B Kekre, V A Bharadi , "Dynamic signature preprocessing by modifieddigital difference analyzer algorithm" , Springer India, Thinkquest, pp 67-73, 2011.
[16] H B Kekre, V A Bharadi, T K Sarode , "Dynamic Signature Recognitionusing Time based Vector Quantization by Kekre's Median Codebook Generation Algorithm", springer India,Thinkquest,10.1007/978-81-8489- 9894_46,2011.

[17] H B Kekre and V ABharadi, "Gabor Filter Based Feature Vector forDynamic Signature recognition", International Journal of ComputerApplications (0975 – 8887), vol 2 No: 03, May 2010.
[18] Peter Mell,T, Grance, "The NIST Definition of Cloud Computing", Recommendations of the National Institute of Standards and Technology, Special Publication 800-145, September 2011
[19] H B Kekre, V A Bharadiet. al., "Online Signature Recognition UsingKekre's Vector Quantization Algorithms KMC & KFCG", ACMInternational Conference & Workshop on Emerging Trends in Technology2011, Pages 415-421, ISBN: 978-1-4503-0449-8, DOI10.1145/1980022.1980110,ICWET 2011, TCET,Mumbai,India.
[20] V ABharadi,V ISingh, "Hybrid Wavelet based Feature Vector Generation from Multidimensional Data set for On-line Handwritten Signature Recognition", IEEE International Conference - Confluence 2014, Sept 25th , 26th 2014, Amity University, UP, India, ISBN (XPLORE): 978-1-4799-42367, DOI:10.1109/CONFLUENCE.2014.6949038,Page(s):561-568,Sept2014
[21] Zhenjiu Xiao and Yongbin Wang, Zhengtao Jiang, "Research and Implementation of Four-prime RSADigital Signature Algorithm" , 978-1-4799-8679-8/15/$31.00 copyright 2015 IEEE ICIS 2015, June 28-July 1 2015, Las Vegas, USA
[22] D. Boneh, G. Durfee. "Cryptanalysis of RSA with private key d lessthan N0.292," IEEE Information Theory Society, vol.46, pp. 1339-1349,2000.
[23] K. Y. He. "Algorithm implementation research of the improved RSA," Chengdu: University of Electronic Science and Technology, 2010.
[24] Hewitt, C. (2008) "ORGs for scalable, robust, privacy friendly client Cloud Computing Environment in IEEE Proceedings Volume 12 Issue 5, September 2008.
[25] Chandran S. and Angepat M., "Cloud Computing: Analyzing the risks involved in cloud computing envionments," in Proceedings of Natural sciences and Engineering, Sweden, 2010.
[26] Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr. AtanuRakshit, "Cloud SecuritysIssues", in Proceedings IEEE International Conference on Services Computing, September 2009.
[27] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik,"Scalable and Efficient Provable Data Possession," In Proceedings of Secure Comm '2008.
[28] M. A. Shah, M. Baker, J. C. Mogul, and R.Swaminathan, "Auditing to keep online storage serviceshonest," in Proceedings of the 11th USENIX work shop on Hot topics in operating systems, 2007.
[29] Berkeley, CA, USA, 2007, pp. 1–6. C. Erway, A.K¨up¸c¨u, C. Papamanthou, and R. Tamassia. Dynamic provable data possession in Proceedings of the 16thACM conference on Computer and Communication security, CCS '09, New York, NY, USA, 2009.

