Original Research Article

AN RSA ALGORITHM FOR SECURING FINACIAL DATA ON THE CLOUD

ABSTRACT

Cloud computing is a developing, very buoyant and nascent paradigm offering numerous solutions to the mirage of challenges and troubles confronting the IT world. It is an online computing solution for on-demand scaling, sharing and abstraction of unlimited resources. Since the significance of trust and confidence in cloud data or information transmission cannot be underestimated, it is obligatory that adequate mechanism be put in place to guarantee the safety of data provided on a Card-Not-Present (CNP) transaction mode. On this note, this paper presents an RSA algorithm with encryption and decryption-based solution to the problems of data confidentiality and integrity. While the encryption mechanism provides secured and safe representation of financial data (such as credit card details) on the cloud, a message digest mechanism is used to decrypt the encrypted files at the gateway as well as generate and send a digest message for the transaction instrument to the user for authentication. Decryption by unauthorized user is effectively checked because the security key is exclusive to data owner and financial data is not domiciled on the merchant network. Experimental study and online survey of the system reveal its very high ratings for guaranteeing data safety and confidentiality as well as the efficacy of the digital signature, the RSA modulus and security keys (public and private) for reliable and attack-proof transactions.

Keywords: RSA, Digital Signature, encryption, decryption, financial security

1. INTRODUCTION

Financial data is expressive of the assorted monetary transactions associated to various individuals or groups and its foundational ingredient is its constitutional history which mainly consists of details and meta-data of previous purchases and expenditures on transactions and income. The foundational ingredients also include customer names, addresses, birth dates, contact details, insurance and passport numbers, bank account details, family circumstances, transaction records, credit card details, security details among others. Unauthorized access or stolen data on national insurance numbers, payment card and banking information can be very consequential in committing identity and other related frauds with negative and colossal impact on the customer. In view of these, there are massive demands on all organizations dealing with enormous or explosive size data to ensure the safety and security of data. Some of the existing strategies for preventing insecurity in the form of unauthorized access and disclosure, alteration, destruction and loss of data include password, user account, authentication and backup. One of the far-reaching effects of the rapid and explosive growth of the Internet services is the rising spate of data insecurity. Cloud computing, which requires the utilization of computing and network infrastructure, is been considered as a strong antidote to data insecurity. It includes a group of computers that are in cooperation towards providing dissimilar and heterogeneous computations and tasks. It is a data sharing and storage platform based on secure, cost-

effective, scalable and flexible IT infrastructure. Its main focus is on sustaining the confidentiality and integrity of data by addressing the risk of theft, tampering, loss and unavailability of data [1-2]. Cloud computing data security techniques offer a numerical approach to the validation, authentication and genuineness of a message (data) by pre-transfer encryption and post-delivery decryption [3-5]. Cryptography-based encryption techniques are often used for safe-keeping of data without delaying information exchange [6]. The existing options to this include the encryption of data prior to uploading and encryption upon receipt. Encryption can also be used to protect data at rest, in transit and in use [7]. The data encryption types include symmetric, asymmetric and password hashing [8-11]. The existing encryption and decryption algorithms include Rivest, Shamir and Adleman (RSA) algorithm and digital signature [10,12-13].

2. LITERATURE REVIEW

The authors in [14] addressed the prevalent cloud security challenges via the implementation of the RSA algorithm for the encryption of data-in-transit and digital signature for message verification. The usefulness of the proposed algorithm for securing data on the cloud was buttressed, but its practical function with real cloud application and financial data could not be ascertained. In [15], digital signature and encryption algorithm were used for securing data on the cloud. The algorithm addressed the security and privacy issues of cloud computing using a multi-level approach but could not provide optimum data security during online cloud data transmission. The authors in [16] presented a system for data privacy and compliance management in cloud data transfer. Digital signature and CFX_MF algorithms were paired with a view to establishing a fool-proof data privacy and integrity. The system is however limited by its reliance on hash function which subjects it to online related attacks.

A system for preserving cloud data privacy and detection of skeptical cases of money laundering is presented in [17]. The system aggregated and mined financial dataset towards uncovering or minimization of the various risk or threats associated to financial institutions. The system however, gives no consideration to artificially created datasets as well as susceptible to the risk of infringing privacy. A blend of digital signature and encryption algorithm was used in [18] for cloud user authentication and data defense. The encryption was based on the Advanced Encryption Standard (AES) algorithm while Secure Hash Algorithm (SHA) established the hodgepodge value. The ensued algorithm however lacks practical results and greatly susceptible to brute force attack and key mismanagement. In [19], a cloud computing data sharing security and privacy preservation technique was presented. The technique used a Key Distribution Centre (KDC) and Paillier algorithms to prevent data culprits from gaining access to cloud-based personal information as well as distributing and maintaining attributes and secret keys to users. However, the technique is prone to brute force attack due to data symmetry.

In [20], a framework for digital signature and advanced encryption standard for enhancing data security and authentication in cloud computing is proposed. Data insecurity was addressed based on data authentication and Advanced Encryption Standard (AES)-based encryption. The framework however requires key management scheme since AES is a one-key encryption algorithm that suffers during key exchange. The authors in [21] used AES algorithm and a MAC mode operation for cloud data security. The proposed algorithm mitigates data threats by enhancing key management system based on guaranteed computing dynamic environments for end-users. The algorithm also uses digital signature of Virtual Machine (VM) Template provided by the cloud to perform user authentication using distributed approach. The algorithm however fails to secure data-at-rest and noticeable levels of overheads are observed. The author in [1] proposed a platform for the analysis and evaluation of cloud security techniques. A mixture of encryption, data loss prevention,

integrity protection, authentication and authorization techniques were employed for data security. The platform however suffers consumers' confidence due to loss of confidentiality and integrity breaches.

A password, RSA encryption and key derivation technique for preserving the integrity of cloud-based data is presented in [22]. RSA algorithm was used to achieve confidentiality of data, hash algorithm was used for authentication and the derivation function was used for generating encryption keys. The technique is however susceptible to brute force attack and lacks terminal security. In [23], digital signature and image steganography technique is proposed for enhancing the security of cloud based data. While the RSA algorithm formed the basis for the encryption, decryption as well as verification of data, image steganography was used to conceal the presence of the data in transit on the cloud. The technique is however prone to high computational overheads.

3. PROPOSED SYSTEM

The proposed system for securing financial data on the cloud is conceptualized in Figure 1.

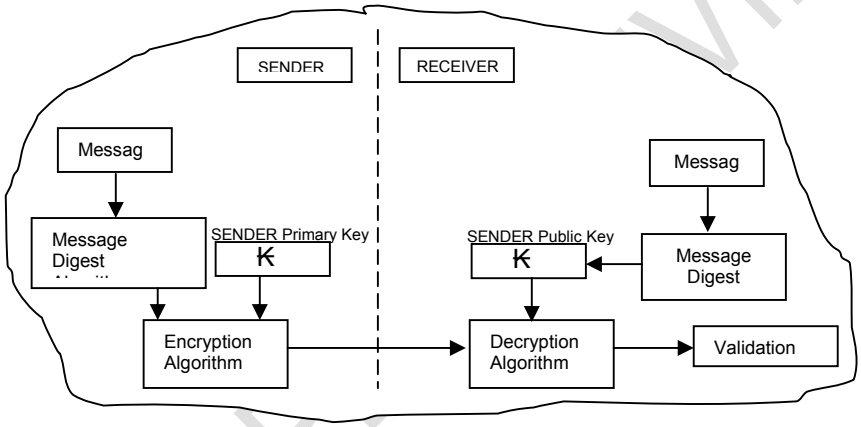

Figure 1: The Conceptualization of the proposed system

The Sender sends a message at the source node while the Message Digest (MD) algorithm is a hash function used by sender to sign the message. Specifically, MD5 hash function which involves the conversion of the message to hexadecimal form before the generation of its digital signature S using its private key d is adopted. A digital signature S is sent to the recipient, who upon receipt, computes the integer V using S and key factors e and n as follows [10].

$$V = S^e mod\ n \quad (1)$$

Upon its handing over, the RSA encryption algorithm uses the receiver's private key *d* to encrypt the message.

The Receiver receives the message and verifies its signature by means of a pre-determined integer, i_a and public key (n, e). This is proceeded by the extraction of the message digest from i_a using the MD5 hash function and the computation of a post-extraction message digest i_b. The validity of the signature is premised on the equality of the two message digests. The RSA encryption algorithm that is based on the combination of Prime Factorization (PF), Euler's Totient Function (ETF), Euler's Totient Theorem (ETT) and Extended Euclidean Algorithm (EEA) is adopted for the computation of the private key required for the decryption process. PA is the fundamental theorem of arithmetic which states that any number greater than 1 can be written exactly one way as a product of prime

numbers. The ETF is expressed as ∂, and Equations 2 and 3 show its formulae for a prime number *n* and *n.m* respectively:

$$\partial(n) = np^{-1} \quad (2)$$
$$\partial(n.m) = (n^{-1})(m^{-1}) \quad (3)$$

The ETT, represented as φ is presented as follows:

$$\varphi(n.m) = (n-1)(m-1) \quad (3)$$

The RSA algorithm (flowchart shown in Figure 2) adopted for digital signature involves the five processes of Key Generation, Digital Signing, Encryption, Decryption and Signature Verification. The Key generation algorithm involves a random selection of two large positive prime numbers, *n* and *m* such that n≠*m.* The product of *n* and m*,* known as the Modulus, % is determined and $\phi(\%)$ is computed as follows:

$$\partial(\%) = (n^{-1})(m^{-1}) \quad (3)$$

This is followed by random selection of a prime number **e;** such that $1 < e < \partial(\%)$, and e and $\partial(\%)$ are coprime. e is an exponent , which is a public key not sharing prime factor with $\partial(\%)$ and usually a prime number greater than 2.

A private key, *v* is computed as follows:

$$v = \frac{1}{e \ mod \ \partial(\%)} \quad (4)$$

v is an exponent, multiplicative inverse of e with respect to $\partial(\%)$ and derived via EAA. The public key k^p and private key k^a are derived as follows:

$$k^p = (e, \%) \quad (5)$$
$$k^a = (v, \%) \quad (6)$$

3.1 Digital Signing, Encryption, Extended Euclidean Algorithm (EEA)

Given that $f = 1, 2, 3, \ldots, r$ represent set of financial data such as credit card number N_c, personal information number N_p, transaction amount N_t, a message digest M_d, is generated using MD5 algorithm while the sender sends a digital signature S for signing M_d via k^p as follows:

$$S = {M_d}^r mod \ \% \quad (7)$$

Encryption is performed at the sender side using the receiver's private key k^p as follows:

$$M_d = E^{k^p} mod \ \% \quad (8)$$

The EEA algorithm is also known as the greatest common divisor (gcd) method and it is also used to compute a private key *M* by using the matrix iterative scheme presented in Equation 9 via $\partial(\%)$.

$$M = \begin{bmatrix} \partial(\%) & \partial(\%) \\ e & 1 \end{bmatrix} \quad (9)$$

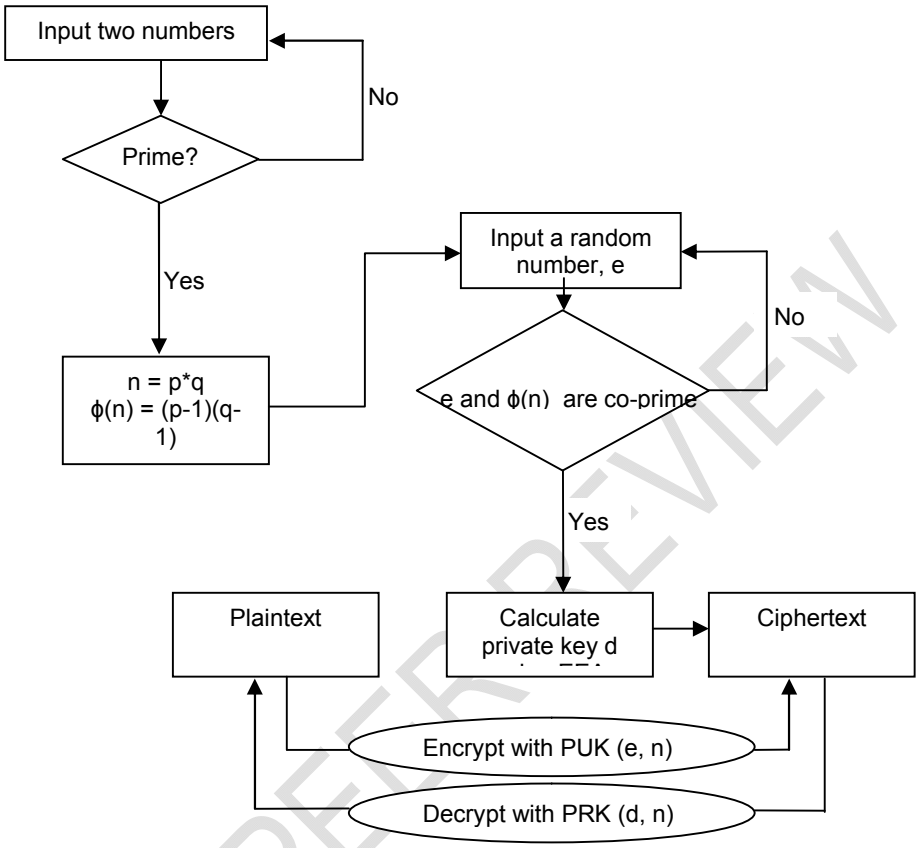

Figure 2: Flowchart of RSA Algorithm

The EEA encryption algorithm involves the following computations:

$$x = \partial(\%) \backslash e \quad (10)$$

$$y_1 = (x * e) \quad (11)$$

$$y_2 = (x * 1) \quad (12)$$

$$Z_1 = (\partial(\%) - y_1) \quad (13)$$

$$Z_2 = (\partial(\%) - y_2) \quad (14)$$

$$M(3,1) = Z_1 \quad (15)$$

$$M(3,2) = Z_2 \quad (16)$$

If $M(3,1) \neq 1$, *M(1,1)* and M(1,2) are cancelled out while negative value from Equation 13 leads to addition of $\partial(\%)$ computed in Equation 3 to make it positive.

For decryption, the Recipient converts the ciphertext, C, to plaintext M_d using the sender's public key $(e, \%)$ as follows:

$$C = {M_d}^e \bmod \% \quad (17)$$

The recipient verifies the signature by generating an integer G using the sender's public key $(e, \%)$ and signature S as follows:

$$G = E^e mod \% \quad (8)$$

A message digest M1, is extracted from the integer G using MD5 algorithm. The computation of message digest M2 from the signature S then follows. The signature is valid if M1= M2.

4. EXPERIMENTAL STUDY

The experimental study of the digital signature-based platform for securing financial information on the cloud was carried out on Microsoft Windows 10 Operating System environment on Pentium IV with 2.0 GHZ Duo Core Processor and 2 GB of RAM. APACHE server and HTML (Sublime) with CSS, JavaScript served as the frontends while MySQL database from WAMP server and PHP were the backends on Mozilla Firefox browser. The financial information comprises of customer names, addresses, birth dates, contact details, insurance and passport numbers, bank account details, family circumstances, transaction records and credit card details which include number, expiry date, PIN among others. The system accommodates all legal tender such as Master card, Visa card, Verve card, draft and cheque.

The message digest operation on the financial information is based on the implementation of the MD5 hash algorithm. The operation records the commencement and completion times as well as the digest time which connotes the time taken to create a message digest. The message digest operation is proceeded with the digital signature operation which generates the private key with its *sign-in info* and *digest data* attributes. While the *sign-in info* attributes include the nature of digest, credit card number, digest time among others, the *sign-in info* attributes include the operation's start, completion and signing times in microseconds (μs). The RSA public key encryption on the financial information produced digital signing as well as ciphertext of the financial instrument which is decrypted using the RSA private key. The validity of the obtained digital signature is investigated via an integer value created from the message digest and the public key generated from digital signature. A digital signature verification status of 0 means the signature is invalid while 1 implies valid signature. Similarly, the message digest operation is only valid if integer values M1 and M2 are obtained such that $M1 = M2$. This condition requires obtaining new private and public keys for every signing-verification and encryption-decryption operations. A new modulus is also required for every encryption-decryption operation.

A total of four hundred and fifty (450) pre-registered users participated in the online survey conducted for the assessment and rating of the system. The survey is based on instructional contents and reliability, speed, security, effectiveness, usability, adaptability and user-experience were the indices used. The distribution of the users' ratings based on these indices is presented in Table 1.

Table 1: Statistical summary of users' responses in the online survey

Indices	Excellent	Very Good	Good	Average	Poor
Reliability	104	281	65	0	0
Speed	123	279	48	1	0
Security	367	79	4	0	0
Effectiveness	301	110	35	4	0
Usability	288	96	64	2	0
Adaptability	316	81	52	1	0
Experience	297	120	31	2	0

The result in Table 1 shows that *Security* is the index with the highest '*Excellent'* rating (81.56% of users). This figure indicates that virtually all the respondents agreed that the system offered unreserved and satisfactory security on information and data on financial

transaction. This equally established the efficacy of the digital signature via its RSA modulus and security keys (public and private) for transactions. Furthermore, 62.44% and 62% of the users approved a "*Very Good*" rating of the system on *Reliability* and *Speed* respectively. These majority ratings are attributed to the stable form of the message digest, consistent digital signature operations that generated encryption and decryption results effortlessly as well as prompt network access. User rating of 66% and 64% were recorded for *Effectiveness* and *Usability* respectively. These ratings confirmed that with ease and flexibility, the system performed to users' expectations. *Adaptability* and *Experience* were rated '*Excellent'* by 70.22% and 66% of users respectively. These ratings buttressed the simplicity and user-friendliness of the system.

The performance evaluation of the system was also carried out based on the sign-in, digest, encryption, decryption and verification times in microseconds for MasterCard, VisaCard and VerveCard. The users supplied all required information and the computation times for the metrics are presented in Table 2.

Table 2: Computation times for various metrics

Metric	MasterCard	VisaCard	VerveCard
Time/Frequency	171.93/368	23.45/57	10.11/25
	167.33/368	22.98/57	9.71/25
	166.79/368	21.82/57	9.33/25
	177.83/368	27.16/57	10.75/25
Digest Time	0.46	0.41	0.40
Sign-in Time	0.45	0.40	0.38
Encryption Time	0.45	0.38	0.37
Decryption Time	0.47	0.46	0.44
Verification Time	0.48	0.47	0.46

Table 2 reveals that the verification time for each credit card number is relatively larger than the Digest, Sign-in, Encryption and Decryption times. This is attributed to database and Internet access. Strong Internet signal gives speedy verification and seamless signature validation. The higher values of the decryption times over the encryption times are attributed to the variation in the length of the obtained ciphertexts. The higher encryption times taken to generate ciphertexts compared to the Digest and Sign-in times are due to the variation in the length of the credit card numbers. MasterCard, VisaCard and VerveCard numbers have 16, 13 and 19 digits respectively.

The comparison of the proposed system based on desired features and functionality with some existing and relevant systems shows its comparative advantage in securing financial data on the cloud. The comparative analysis is presented Table 4.

Table 3: Comparative Analysis with some existing works

Research	Security Level	Efficiency	Crypto-System Algorithm	Key size (for data)	Cloud Environment	Adaptability
Jingxin and Xinpei, 2012	Average	Average	Certificate Authority (CA) and Public Key Infrastructure (PKI)	Not used	Used	Low
Mohammed & Anazida, 2014	High	Average	MD5, AES, and RSA-based PHE	Average (128 bits)	Used	Average
Kumar *et al.,* 2014	Average	Low	Attribute Based Encryption(ABE)	Not used	Not Used	Low

Ranjith *et al.,* 2015	High	Average	RSA	Average (1024 bits)	Not Used	Average
Current Research	High	High	RSA, Digital Signature and MD5	Strong (2048 bits)	Not Used	High

5. CONCLUSION

Cloud computing has been an evolving, very hopeful and budding technology due to its array of solutions to IT related challenges and problems. It is an Internet-based computing solution with series of on-demand self-services, shared resources, utilities, abstraction of unlimited resources and support for on-demand scaling. Since analysis remains very germane task in decision making, the significance of trust and confidence in cloud data or information transmission cannot be underestimated. Hence it is required that adequate mechanism be put in place to guarantee the safety of sensitive credit card and other financial data provided in a Card-Not-Present (CNP) transaction. On this note, this paper presented an RSA algorithm with encryption and decryption-based solution to the mirage of problems confronting cloud computing data confidentiality and integrity. While the encryption mechanism provides secured and safe representation of financial data (such as credit card details) on the cloud, the message digest mechanism decrypt the encrypted files at the gateway and generate and send a digest message for the transaction instrument to the user for authentication. Decryption by unauthorized user is effectively checked because the RSA security key is exclusive to data owner and financial data is not domiciled on the merchant network. The online survey of the system reveals its very high ratings for guaranteeing data safety and confidentiality as well as the efficacy of the digital signature, the RSA modulus and security keys (public and private) for reliable and attack-proof transactions.

REFERENCES

[1] Jakimoski Kire., “Security Techniques for Data Protection in Cloud Computing”. International Journal of Grid and Distributed Computing Vol. 9, No. 1 (2016), pp.49-56 http://dx.doi.org/10.14257/ijgdc.2016.9.1.05.

[2] Mell P, (2009) 'The NIST Definition of Cloud', Reports on Computer Systems Technology, sept., p. 7

[3] Ranjith P, Chandran P, Kaleeswaran S: On covert channels between virtual machines. *Journal in Computer Virology Springer* 2015, 8: 85–97. 10.1007/s11416-012-0168-x

[4] Mijanur Rahman. Md, Tushar Kanti Saha, Md. Al-Amin Bhuiyan , “Implementation of RSA Algorithm for Speech Data Encryption and Decryption”, Manuscript received March 5, 2012 Manuscript revised March 20, 2012

[5] Turner, Dawn. "Major Standards and Compliance of Digital Signatures - A World-Wide Consideration". Cryptomathic. Retrieved 7 January 2016.

[6] Kunze Marcel, Lizhe Wang, Jie Tao, Gregor von Laszewski; 2008 “Cloud Computing: A Perspective Study, Rochester Institute of Technology RIT Scholar Works.

[7] Jeff Hudson; “Smart Grids: Digital Certificates and Encryption Play Key Role in Security”, October 18, 2012, WYSE Technology

[8] Jerry Gao Cloud Testing- Issues, Challenges, Needs and Practice, Software engineering: an international Journal (SeiJ), Vol. 1, no. 1, SePteMBer 2015

[9] Stallings, W. (2006). Cryptography and network security: principles and practices. Pearson Education India [10] Tirthani, N., & Ganesan, R. (2014). Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography. IACR Cryptology ePrint Archive, 2014, 49. 5

[11] Stevens M.M.J. (June 2007). "On Collisions for MD5" (PDF). [...] we are able to find collisions for MD5 in about $2^{24.1}$ compressions for recommended IHV's which takes approx. 6 seconds on a 2.6GHz Pentium 4".
[12] Neha Jain and Gurpreet Kaur, Implementing DES lgorithm in Cloud for Data Security" VSRD International Journal of CS & IT Vol. 2 Issue 4, 2012, pp. 316-321.
[13] Ing and Christof Paar: Optimization and analysis of explicit formulae for hyperelliptic curve cryptosystems. IEEE Transactions on Computers, 54(7):861–872, 2010.
[14] Somani U, Lakhani K, Mundra M: Implementing digital signature with RSA encryption algorithm to enhance the data Security of Cloud in Cloud Computing. In *1st International conference on parallel distributed and grid Computing (PDGC)*. IEEE Computer Society Washington, DC, USA; 2010:211–216.
[15] Rewagad Prashant and Pawar Yogita, Dept of computing & Engineering, student, Dept of Computing & Engineering. "Use of Digital signature with differ hellman key Exchange and AES cryptography rule to boost information Security in Cloud Computing".
[16] Rajak Shobha, Ashok Verma, "Secure Data Storage in the Cloud using Digital Signature Mechanism", International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 4, June 2012
[17] NhienAn LeKhac, and M-Tahar Kechad."Toward a new cloud-based approach to preserve the privacy for detecting suspicious cases of money laundering in an investment bank, 2014.
[18] Sivasakthi T. and Dr. Prabakaran N.; "Applying Digital Signature with Encryption Algorithm of User Authentication for Data Security in Cloud Computing"; International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 2, February 2014.
[19] Kadam Prasad and Prof. N. C. Thoutam, "Data Sharing Security and Privacy Preservation in Cloud Computing", InternationalConference on Green Computing and Internet of Things (ICGCIoT), 2015.
[20] Nair Sreeja, Nupur Gautam and Meenakshi Choudhary. "Using Kerberos with Digital Signature and AES Encryption to Provide Data Security in Cloud Computing", International Journal of Computer Applications (0975 – 8887) Volume 95– No.18, June 2015.
[21] Pauliesther Merlin and J. Visumathi, 2015, "Towards secure cloud computing using digital signature", Research Gate
[22] Mathews Ceena. "Cloud Data Integrity using Password Based Digital Signature", Ceena Mathews / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (1), 2016, 101-103.
[23] Abdulkarim Adamu Ismail, Boukari Souley; "An Enhanced Cloud Based Security System Using RSA as Digital Signature and Image Steganography", IJSER © 2017 http://www.ijser.org
.