

AN RSA ALGORITHM FOR SECURING FINANCIAL DATA ON THE CLOUD

Gabriel Babatunde Iwasokun^{1*}, Oluwole Charles Akinyokun¹, Sunday Alawode¹, Taiwo Gabriel Omomule²

¹Department of Software Engineering, Federal University of Technology, Akure, Nigeria

²Department of Computer Science, Adekunle Ajasin University, Akungba-Akoko, Nigeria

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

34 infrastructure, is been considered as a strong antidote to data insecurity. It includes a group
35 of computers that are in cooperation towards providing dissimilar and heterogeneous
36 computations and tasks.

37 Cloud computing is presented as a data sharing and storage platform based on secure, cost-
38 effective, scalable and flexible IT infrastructure in [1-2]. Its main focus is on sustaining the
39 confidentiality and integrity of data by addressing the risk of theft, tampering, loss and
40 unavailability of data [1-2]. According to the authors in [3-5], cloud computing data security
41 techniques offer a numerical approach to the validation, authentication and genuineness of a
42 message (data) by pre-transfer encryption and post-delivery decryption. Cryptography-based
43 encryption techniques are often used for safe-keeping of data without delaying information
44 exchange and the existing options to this include the encryption of data prior to uploading
45 and encryption upon receipt [6-7]. Encryption can also be used to protect data at rest, in
46 transit and in use. The data encryption types include symmetric, asymmetric and password
47 hashing [8-11]. The existing encryption and decryption algorithms include Rivest, Shamir
48 and Adleman (RSA) algorithm and digital signature [10,12-13].
49

50 **2. LITERATURE REVIEW**

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

62 A system for preserving cloud data privacy and detection of skeptical cases of money
63 laundering is presented in [17]. The system aggregated and mined financial dataset towards
64 uncovering or minimization of the various risk or threats associated to financial institutions.
65 The system however, gives no consideration to artificially created datasets as well as
66 susceptible to the risk of infringing privacy. A blend of digital signature and encryption
67 algorithm was used in [18] for cloud user authentication and data defense. The encryption
68 was based on the Advanced Encryption Standard (AES) algorithm while Secure Hash
69 Algorithm (SHA) established the hodgepodge value. The ensued algorithm however lacks
70 practical results and greatly susceptible to brute force attack and key mismanagement. In
71 [19], a cloud computing data sharing security and privacy preservation technique was
72 presented. The technique used a Key Distribution Centre (KDC) and Paillier algorithms to
73 prevent data culprits from gaining access to cloud-based personal information as well as
74 distributing and maintaining attributes and secret keys to users. However, the technique is
75 prone to brute force attack due to data symmetry.

76 In [20], a framework for digital signature and advanced encryption standard for enhancing
77 data security and authentication in cloud computing is proposed. Data insecurity was
78 addressed based on data authentication and Advanced Encryption Standard (AES)-based
79 encryption. The framework however requires key management scheme since AES is a one-
80 key encryption algorithm that suffers during key exchange. The authors in [21] used AES
81 algorithm and a MAC mode operation for cloud data security. The proposed algorithm
82 mitigates data threats by enhancing key management system based on guaranteed
83 computing dynamic environments for end-users. The algorithm also uses digital signature of
84 Virtual Machine (VM) Template provided by the cloud to perform user authentication using

85 distributed approach. The algorithm however fails to secure data-at-rest and noticeable
 86 levels of overheads are observed. The author in [1] proposed a platform for the analysis and
 87 evaluation of cloud security techniques. A mixture of encryption, data loss prevention,
 88 integrity protection, authentication and authorization techniques were employed for data
 89 security. The platform however suffers consumers' confidence due to loss of confidentiality
 90 and integrity breaches. A password, RSA encryption and key derivation technique for
 91 preserving the integrity of cloud-based data is presented in [22]. RSA algorithm was used to
 92 achieve confidentiality of data, hash algorithm was used for authentication and the derivation
 93 function was used for generating encryption keys. The technique is however susceptible to
 94 brute force attack and lacks terminal security. In [23], digital signature and image
 95 steganography technique is proposed for enhancing the security of cloud based data. While
 96 the RSA algorithm formed the basis for the encryption, decryption as well as verification of
 97 data, image steganography was used to conceal the presence of the data in transit on the
 98 cloud. The technique is however prone to high computational overheads.

99
 100 The authors in [24] presented a cloud computing data access authentication model using
 101 single encryption and multi-level virtualization for pre-transfer access and control. The model
 102 relies on authentication for inter cloud operations and therefore, it is confronted with the
 103 challenge of data insecurity, privacy and confidentiality. In [25], a proof of irretrievability
 104 (POR) protocol cloud computing data integrity and privacy model is presented. The model
 105 guaranteed data integrity verification, privacy preservation as well as provable data
 106 possession (PDP) for data files possession on un-trusted storage and Dynamic Provable
 107 Data Possession (DPDP). The model however does not address the issue of data protection
 108 against modification at the service provider's side as well as the problem of integrity
 109 checking of dynamic data operation. An enhanced attribute based encryption platform for
 110 cloud computing is presented in [26]. The platforms uses hash functions, digital signature
 111 and asymmetric encryptions scheme to establish high level security as well as access time
 112 and resource minimization. However, the platform records high computational cost as well
 113 as failure to distinguish the access control strategies embedded in the decryption key. The
 114 author in [27] presented an arbitrated digital signature model for e-authentication of digital
 115 messages. The model protects against malicious data alteration, repudiation as well as
 116 confidentiality based on all-inclusive encryption of the message and signature. However
 117 large size messages experienced time-delay and waiting state thereby increasing the
 118 transmission response time and traffic security probabilities.

119
 120 **3. PROPOSED SYSTEM**

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

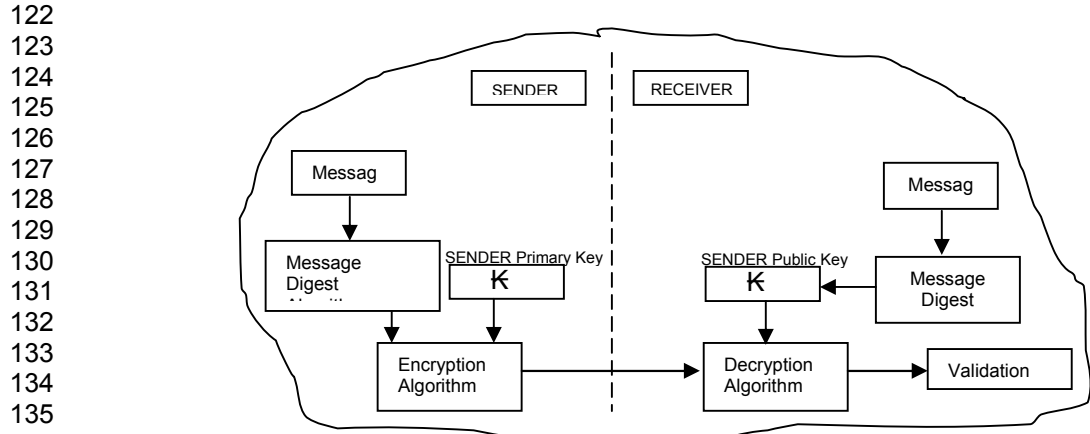


Figure 1: The Conceptualization of the proposed system

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

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

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

146 The Receiver receives the message and verifies its signature by means of a pre-determined
 147 integer, i_a and public key (n, e) . This is proceeded by the extraction of the message digest
 148 from i_a using the MD5 hash function and the computation of a post-extraction message
 149 digest i_b . The validity of the signature is premised on the equality of the two message
 150 digests. The RSA encryption algorithm that is based on the combination of Prime
 151 Factorization (PF), Euler's Totient Function (ETF), Euler's Totient Theorem (ETT) and
 152 Extended Euclidean Algorithm (EEA) is adopted for the computation of the private key
 153 required for the decryption process. PA is the fundamental theorem of arithmetic which
 154 states that any number greater than 1 can be written exactly one way as a product of prime
 155 numbers. The ETF is expressed as ∂ , and Equations 2 and 3 show its formulae for a prime
 156 number n and $n.m$ respectively:

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

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

157 The ETT, represented as φ is presented as follows:

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

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

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

163 This is followed by random selection of a prime number e ; such that $1 < e < \partial(\%)$, and e
 164 and $\partial(\%)$ are coprime. e is an exponent, which is a public key not sharing prime factor with
 165 $\partial(\%)$ and usually a prime number greater than 2.

166 A private key, v is computed as follows:

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

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

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

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

169

170 3.1 Digital Signing, Encryption, Extended Euclidean Algorithm (EEA)

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

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

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

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

176 The EEA algorithm is also known as the greatest common divisor (gcd) method and it is also
177 used to compute a private key M by using the matrix iterative scheme presented in Equation
178 9 via $\partial(\%)$.

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

180 The EEA encryption algorithm involves the following computations:
181

$$182 \quad x = \partial(\%) \setminus e \quad (10)$$

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

$$183 \quad y_2 = (x * 1) \quad (12)$$

$$184 \quad Z_1 = (\partial(\%) - y_1) \quad (13)$$

$$185 \quad Z_2 = (\partial(\%) - y_2) \quad (14)$$

$$186 \quad M(3,1) = Z_1 \quad (15)$$

$$187 \quad M(3,2) = Z_2 \quad (16)$$

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

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

$$192 \quad C = M_d^e \text{ mod } \% \quad (17)$$

193 The recipient verifies the signature by generating an integer G using the sender's public key
194 $(e, \%)$ and signature S as follows:

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

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

198 4. EXPERIMENTAL STUDY

199 The experimental study of the digital signature-based platform for securing financial
200 information on the cloud was carried out on Microsoft Windows 10 Operating System
201 environment on Pentium IV with 2.0 GHZ Duo Core Processor and 2 GB of RAM. APACHE
202 server and HTML (Sublime) with CSS, JavaScript served as the frontends while MySQL
203 database from WAMP server and PHP were the backends on Mozilla Firefox browser. The
204 financial information comprises of customer names, addresses, birth dates, contact details,

205 insurance and passport numbers, bank account details, family circumstances, transaction
 206 records and credit card details which include number, expiry date, PIN among others. The
 207 system accommodates all legal tender such as Master card, Visa card, Verve card, draft and
 208 cheque.

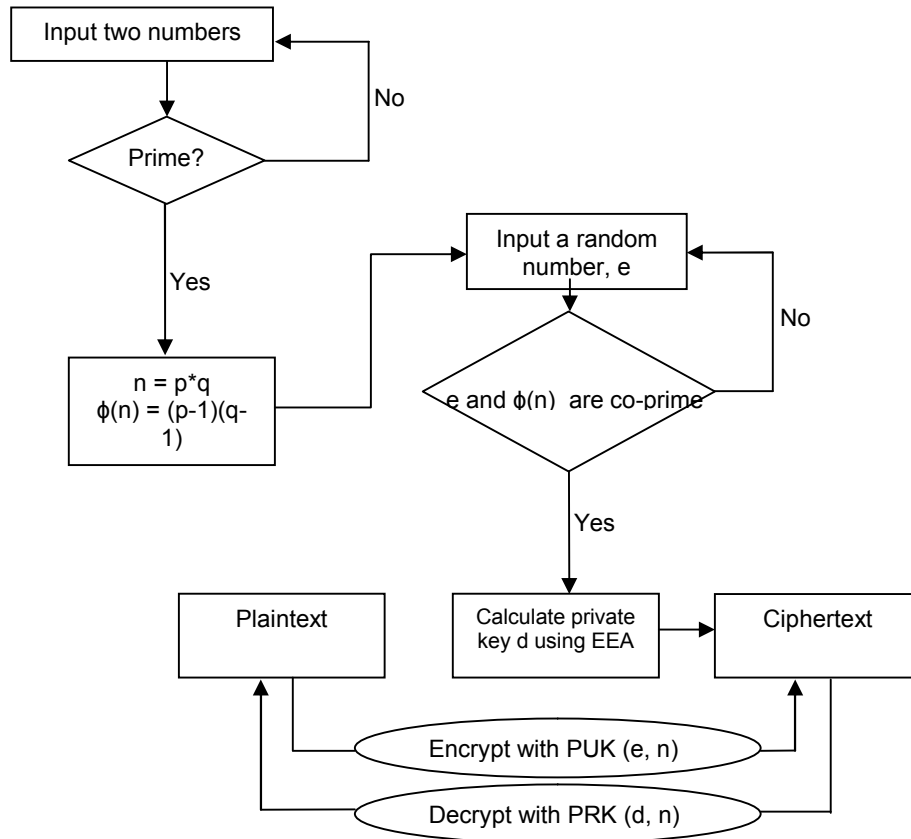


Figure 2: Flowchart of RSA Algorithm

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

257 A total of four hundred and fifty (450) pre-registered users were considered and used as
 258 samples for the online survey, assessment and rating of the system. The sample comprises
 259 of three hundred male and two hundred and fifty female comprising 150, 201 and 99 Master,
 260 Visa and Verve cards respectively. 364 of the samples were local residents (Nigerians) who
 261 were exposed to online transaction while 91 were resident outside Nigeria. The survey is
 262 based on instructional contents and reliability, speed, security, effectiveness, usability,
 263 adaptability and user-experience were the indices used. The distribution of the users' ratings
 264 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

265
 266 The result in Table 1 shows that *Security* is the index with the highest '*Excellent*' rating
 267 (81.56% of users). This figure indicates that virtually all the respondents agreed that the
 268 system offered unreserved and satisfactory security on information and data on financial
 269 transaction. This equally established the efficacy of the digital signature via its RSA modulus
 270 and security keys (public and private) for transactions. Furthermore, 62.44% and 62% of the
 271 users approved a "*Very Good*" rating of the system on *Reliability* and *Speed* respectively.
 272 These majority ratings are attributed to the stable form of the message digest, consistent
 273 digital signature operations that generated encryption and decryption results effortlessly as
 274 well as prompt network access. User rating of 66% and 64% were recorded for *Effectiveness*
 275 and *Usability* respectively. These ratings confirmed that with ease and flexibility, the system
 276 performed to users' expectations. *Adaptability* and *Experience* were rated '*Excellent*' by
 277 70.22% and 66% of users respectively. These ratings buttressed the simplicity and user-
 278 friendliness of the system.

279 The performance evaluation of the system was also carried out based on the sign-in, digest,
 280 encryption, decryption and verification times in microseconds for MasterCard, VisaCard and
 281 VerveCard. The users supplied all required information and the computation times for the
 282 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

283
 284 Table 2 reveals that the verification time for each credit card number is relatively larger than
 285 the Digest, Sign-in, Encryption and Decryption times. This is attributed to database and

286 Internet access. Strong Internet signal gives speedy verification and seamless signature
 287 validation. The higher values of the decryption times over the encryption times are attributed
 288 to the variation in the length of the obtained ciphertexts. The higher encryption times taken to
 289 generate ciphertexts compared to the Digest and Sign-in times are due to the variation in the
 290 length of the credit card numbers. MasterCard, VisaCard and VerveCard numbers have 16,
 291 13 and 19 digits respectively.
 292 The comparison of the proposed system based on desired features and functionality with
 293 some existing and relevant systems shows its comparative advantage in securing financial
 294 data on the cloud. The comparative analysis is presented Table 3.

Table 3: Comparative Analysis with some existing works

Research	Security Level	Efficiency	Crypto-System Algorithm	Key size (for data)	Cloud Environment	Adaptability
Wang and Jia, 2012 [24]	Average	Average	Certificate Authority (CA) and Public Key Infrastructure (PKI)	Not used	Used	Low
Al-Jaberi & Zainal, 2014 [25]	High	Average	MD5, AES, and RSA-based PHE	Average (128 bits)	Used	Average
Kumar <i>et al.</i> , 2014 [26]	Average	Low	Attribute Based Encryption (ABE)	Not used	Not Used	Low
Ranjith <i>et al.</i> , 2015 [27]	High	Average	RSA	Average (1024 bits)	Not Used	Average
Current Research	High	High	RSA, Digital Signature and MD5	Strong (2048 bits)	Not Used	High

295 It is important to state that the system is network based and like any other online system, it
 296 requires efficient, strong and stable Internet connection for optimal performance as result
 297 degradations were experienced with poor Internet connectivity. The application also depends
 298 on the gateway operators' service for successful execution of the message digest as well as
 299 the encryption and the decryption operations. Service disruption on the part of the gateway
 300 operator results in incomplete processing or encryption and/or decryption failure.

301 5. CONCLUSION

302
 303 Cloud computing has been an evolving, very hopeful and budding technology due to its array
 304 of solutions to IT related challenges and problems. It is an Internet-based computing solution
 305 with series of on-demand self-services, shared resources, utilities, abstraction of unlimited
 306 resources and support for on-demand scaling. Since analysis remains very germane task in
 307 decision making, the significance of trust and confidence in cloud data or information
 308 transmission cannot be underestimated. Hence it is required that adequate mechanism be
 309 put in place to guarantee the safety of sensitive credit card and other financial data provided
 310 in a Card-Not-Present (CNP) transaction. **Financial related crime dangers are numerous,**
 311 **complex, and ever changing. Any financial crime that can be perpetrated on the traditional**
 312 **in-house and cloud based servers even on a much larger scale because of the magnitude of**
 313 **the stored data.** On this note, this paper presented an RSA algorithm with encryption and
 314 decryption-based solution to financial crimes and the mirage of problems confronting cloud
 315 computing data confidentiality and integrity. While the encryption mechanism provides
 316 secured and safe representation of financial data (such as credit card details) on the cloud,

317 the message digest mechanism decrypt the encrypted files at the gateway and generate and
318 send a digest message for the transaction instrument to the user for authentication.
319 Decryption by unauthorized user is effectively checked because the RSA security key is
320 exclusive to data owner and financial data is not domiciled on the merchant network. The
321 online survey of the system reveals its very high ratings for guaranteeing data safety and
322 confidentiality as well as the efficacy of the digital signature, the RSA modulus and security
323 keys (public and private) for reliable and attack-proof transactions. **The obtained results had**
324 **established that the proposed model will provide a suitable way of securing sensitive**
325 **financial information such as credit card details using multi-level security strategy for the**
326 **cloud. It is also established that the digital signature and encryption algorithm based**
327 **approach will provide feasible solutions to security related challenges confronting merchant**
328 **site owners, e-commerce providers, financial institutions, online payment solutions and cloud**
329 **service providers. The major challenges confronting cloud computing include security issues,**
330 **cost management and containment, lack of resources/expertise and governance and control.**
331 **Cloud computing insecurity are being confronted through several intelligent applications**
332 **while the existing ways of keeping cloud computing cost in check include engagement of**
333 **proven financial analytics and presentation and control policies mechanization. The problem**
334 **of lack of resources and expertise can be ameliorated via further training of information**
335 **technology and development personnel as well as the engagement of the state of the art**
336 **tools. In the present day, information technology seems not in full control of the provisioning,**
337 **de-provisioning and operations of infrastructure which has raised the overheads for**
338 **governance, risks and data quality management. The solutions to this include adoption of**
339 **the cloud into the traditional information technology framework and control processes as a**
340 **way of gradually providing governance support and superlative practices.**

341 REFERENCES

- 342 [1] Jakimoski K. (2016), "Security Techniques for Data Protection in Cloud Computing",
343 International Journal of Grid and Distributed Computing, Vol. 9, No. 1, pp.49-56
344 Available: <http://dx.doi.org/10.14257/ijgdc.2016.9.1.05>, Accessed 23/02/2018
- 345 [2] Mell P. and Grance T. (2009) 'The NIST Definition of Cloud', Reports on Computer
346 Systems Technology, National Institute of Standard and Technology, Available:
347 <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>,
348 Accessed 14/09/2016
- 349 [3] Ranjith P., Chandran P. and Kaleeswaran S. (2015), "On covert channels between
350 virtual machines", Springer *Journal in Computer Virology Springer*, Vol. 8, pp 85–97.
- 351 [4] Mijanur R., Tushar K. S. and. Al-Amin B. (2012), "Implementation of RSA Algorithm for
352 Speech Data Encryption and Decryption", International Journal of Computer Science
353 and Network Security, Vol.12, No.3
- 354 [5] Turner D. (2016), "Major Standards and Compliance of Digital Signatures - A World-Wide
355 Consideration", [https://www.cryptomathic.com/news-events/blog/major-standards-and-](https://www.cryptomathic.com/news-events/blog/major-standards-and-compliance-of-digital-signatures-a-world-wide-consideration)
356 [compliance-of-digital-signatures-a-world-wide-consideration](https://www.cryptomathic.com/news-events/blog/major-standards-and-compliance-of-digital-signatures-a-world-wide-consideration), Accessed 07/01/2016.
- 357 [6] Kunze M., Lizhe W., Jie T., Gregor V. L. (2008), "Cloud Computing: A Perspective
358 Study, Rochester Institute of Technology RIT Scholar Works.
- 359 [7] Jeff H. (2012), "Smart Grids: Digital Certificates and Encryption Play Key Role in
360 Security", WYSE Technology
- 361 [8] Jerry G. (2015), "Cloud Testing- Issues, Challenges, Needs and Practice, International
362 Journal of Software Engineering, Vol. 1, No. 1
- 363 [9] Stallings W. (2006), "Cryptography and Network security: Principles and Practices,
364 Pearson Education
- 365 [10] Tirthani N. and Ganesan R. (2014), "Data Security in Cloud Architecture Based on
366 Diffie Hellman and Elliptical Curve Cryptography", IACR Cryptology ePrint Archive, Vol.
367 49, Issue 5
- 368 [11] Stevens M. M. J. (2007), "On Collisions for MD5", Master Thesis, Department of
369 Mathematics and Computing Science, Eindhoven University of Technology, Available:

- 370 [https://www.win.tue.nl/hashclash/On%20Collisions%20for%20MD5%20-%20M.M.J.%](https://www.win.tue.nl/hashclash/On%20Collisions%20for%20MD5%20-%20M.M.J.%20Stevens.pdf)
371 [20Stevens.pdf](https://www.win.tue.nl/hashclash/On%20Collisions%20for%20MD5%20-%20M.M.J.%20Stevens.pdf), Accessed 15/02/2019.
- 372 [12] Neha J. and Gurpreet K. (2012), "Implementing DES Algorithm in Cloud for Data
373 Security" VSRD International Journal of Computer Science and Information
374 Technology, Vol. 2, Issue 4, pp. 316-321.
- 375 [13] Ing M. and Christof P. (2010), "Optimization and analysis of explicit formulae for hyper-
376 elliptic curve cryptosystems", IEEE Transactions on Computers, 54(7):861–872, 2010.
- 377 [14] Somani U., Lakhani K. and Mundra M. (2010), "Implementing digital signature with RSA
378 encryption algorithm to enhance the data Security of Cloud in Cloud Computing.", *1st*
379 *International conference on parallel distributed and grid Computing (PDGC)*. IEEE
380 Computer Society Washington, DC, USA; pp 211–216.
- 381 [15] Rewagad P. and Pawar Y. (2014), "Use of Digital Signature with Diffie Hellman Key
382 Exchange and AES Cryptography Rule to Boost information Security in Cloud
383 Computing", International Journal of Scientific and Research Publications, Vol. 5, Issue
384 6.
- 385 [16] Rajak S., and Ashok V. (2012), "Secure Data Storage in the Cloud using Digital
386 Signature Mechanism", International Journal of Advanced Research in Computer
387 Engineering and Technology Vol. 1, Issue 4
- 388 [17] Nhienan L. and M-Tahar K. (2014), "Toward a New Cloud-Based Approach to Preserve
389 the Privacy for Detecting Suspicious Cases of Money Laundering in an Investment
390 Bank, Available: [https://www.insight-centre.org/sites/default/files/publications/iccs-](https://www.insight-centre.org/sites/default/files/publications/iccs-2014.pdf)
391 [2014.pdf](https://www.insight-centre.org/sites/default/files/publications/iccs-2014.pdf), Accessed 23/08/2018.
- 392 [18] Sivasakthi T. and Prabakaran N. (2014), "Applying Digital Signature with Encryption
393 Algorithm of User Authentication for Data Security in Cloud Computing"; International
394 Journal of Innovative Research in Computer and Communication Engineering, Vol. 2,
395 Issue 2.
- 396 [19] Kadam P. and Thoutam N. C. (2015), "Data Sharing Security and Privacy Preservation
397 in Cloud Computing", International Conference on Green Computing and Internet of
398 Things (ICGCloT), 8-10 October 2015. Noida, India
- 399 [20] Nair S., Nupur G. and Meenakshi C. (2015), "Using Kerberos with Digital Signature and
400 AES Encryption to Provide Data Security in Cloud Computing", International Journal of
401 Computer Applications (0975 – 8887) Vol. 95– No.18.
- 402 [21] Pauliesther M. and Visumath J. (2015), "Towards secure cloud computing using digital
403 signature", Journal of Theoretical and Applied Information Technology, Vol. 79. No. 2
- 404 [22] Mathews C. (2016), "Cloud Data Integrity using Password Based Digital Signature",
405 International Journal of Computer Science and Information Technologies, Vol. 7, Issue
406 pp 101-103.
- 407 [23] Abdulkarim A. I., Boukari S. (2017), "An Enhanced Cloud Based Security System Using
408 RSA as Digital Signature and Image Steganography", International Journal of Scientific
409 and Engineering Research Vol. 8, Issue 7
- 410 [24] Wang J. K. and Jia X., (2012), "Data Security and Authentication in Hybrid Cloud
411 Computing Model", IEEE Global High Tech Congress on Electronics, pp 117-120.
- 412 [25] Al-Jaberi M. F., and Zainal A. (2014), "Data Integrity and Privacy Model in Cloud
413 Computing", *International Symposium on Biometrics and Security Technologies*, pp
414 280-284
- 415 [26] Kumar S., Rajya Lakshmi G. V. and Balamurugan, B. (2014), "Enhanced Attribute
416 Based Encryption for Cloud Computing", International Conference on Information and
417 Communication Technologies, pp 689 – 696
- 418 [27] Ranjith G., Prathusha B. and Sagarika P. (2015), "Arbitrated Digital Signature For E-
419 Authentication Technique Of a Digital Message", International Journal of Advances in
420 Engineering and Technology, Vol. 8, Issue 5, pp. 753-759