COMPENDIUM OF DATA SECURITY IN CLOUD STORAGE BY APPLYING HYBRIDIZATION OF ENCRYPTION ALGORITHM

A PREPRINT

Ishu Gupta*
Cloud Computing Research Center, Department of Computer Science and Engineering
National Sun Yat-sen University Kaohsiung, Taiwan
ishugupta23@gmail.com

Deeksha Gurnani
Department of Computer Applications, National Institute of Technology, Kurukshetra, India, 136119
deekshagurnani188@gmail.com

Neha Gupta
Department of Computer Applications, National Institute of Technology, Kurukshetra, India, 136119
751nehagupta@gmail.com

Caffy Singla
Department of Computer Applications, National Institute of Technology, Kurukshetra, India, 136119
caffy.singla22@gmail.com

Prateek Thakral
Department of Computer Science & Engineering, Jaypee University of Information Technology
Solan, Himachal Pradesh, India
prateek@juit.ac.in

Ashutosh Kumar Singh
Department of Computer Applications, National Institute of Technology, Kurukshetra, India 136119
ashutosh@nitkkr.ac.in

ABSTRACT

This paper is about preserving the Cloud data whose idea is to cure everyday problems with computing. Cloud computing is fundamentally pooling the resources virtually and the resources like storage are provided to the end-users through the web. Information preservation, security, uniform quality, and interoperability are some issues related to cloud computing. However, the most essential issue is Security and how it is ensured by a cloud supplier. Security of data can be offered by means of cryptography. This paper presents an improved composite data protection mechanism to protect data on the cloud from illegitimate access.

Keywords Cloud Computing, Data Protection, Encryption, Decryption, Cryptography, RSA

1 INTRODUCTION

There is no such thing as "THE CLOUD", it's just somebody else's computer. Cloud computing is also called on-demand computing and it is a kind of web-based processing, where participating resources and data are rendered to workstations and different gadgets according to demand [1, 2]. Cloud computing is essentially intended to give the

most extreme limit from the least resources [3, 4]. The end client has the base equipment necessity yet utilizes the most extreme capacity of processing [5]. It is a technique that makes use of the Internet and Remote access servers to manage application programs and data [6, 7]. Cloud computing can provide services at a substantially reduced cost by commoditizing the IT assets and on-demand usage patterns [8]. Virtualized hardware, provisioning services rapidly, scalability, elasticity, accounting graininess, and cost assigning models make Clouds able to efficiently adapt resource issuing to the changing demands of the users on the Internet [9–11]. Recently service of cloud computing which is storage as a service (StaaS) has become popular for providing services to both private users and public users [12–14]. STaaS is a service model in Cloud in which a special organization leases the storage space to people or organizations [15–17]. The data residing on the Cloud becomes vulnerable to exploitation by the service provider or by other unauthorized persons thus this data is sensitive and needs a security [18–20]. This fragility led us to find some solution that can make users able to protect the data on the cloud [21–23]. There are various research challenges in cloud computing such as portability, exchanging data, accessing the storage, protection, expenditure, energy efficacy, etc. [24–26]. Fig. 1 presents the importance of data security and other critical issues, where data security and privacy is one of the biggest barriers to the spread of this on-demand Computing. To upgrade the protection mechanism of cloud computing it becomes essential to facilitate the users with authorization and access in a controlled manner for the security of data.

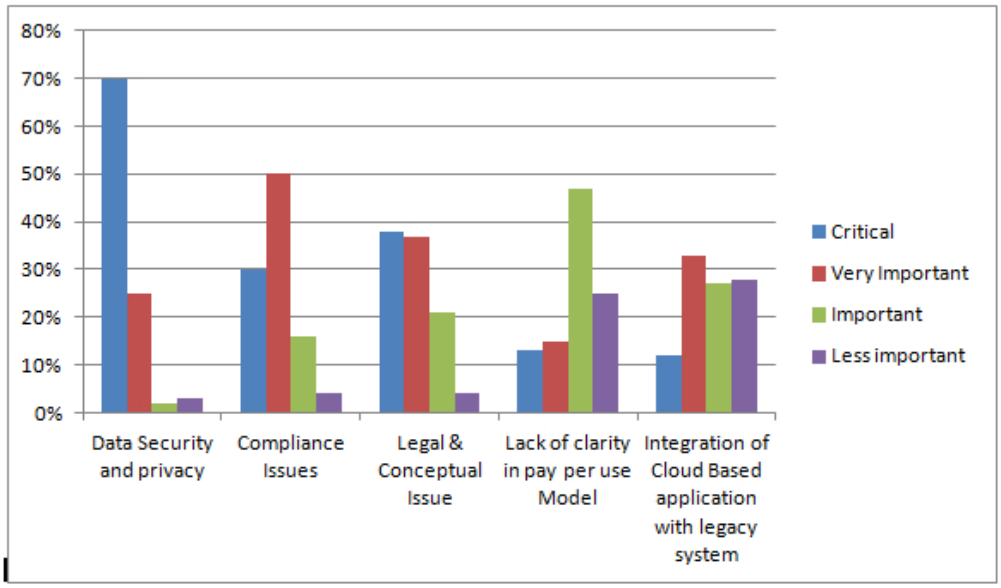

Figure 1: Data Security and Critical Issues.

.

2 RELATED WORK

Suruchee V.Nandgaonkar et al. [27] gave "A Comprehensive Study on Cloud Computing "which describes that cloud computing is conforming to a growing in-demand outfit in which computing assets are delivered on-demand. It defines the architecture that is all the services of the cloud. They have defined cloud computing and have described that cloud computing is becoming the next buzz in the IT industry. The structure of Cloud, Servicing Models of Cloud (IaaS, PaaS, SaaS) are explained by them. Different cloud service models are compared in their work. Different motivating factors and challenges related to cloud computing are explained by them. Zhibin Chen et al. [28] proposed a report in which they have defined cloud computing and have described all the service models. They have discussed various issues associated with cloud computing such as securing the cloud data, Privacy of user's data, Legal issues, Compliance, Freedom, etc. They have concluded the paper by describing that the Cloud environment leads us to approximately never-ending capabilities in computing, good expandability, and on-request service. Anuradha Thilakarathne et al. [29] describes "current security risks and attacks on cloud such as Virtual Machine escapes and Virtual Machine hypervisor, Cloud Zombie, DoS attacks, etc. "They have addressed the security issues associated in cloud data storage and have explored many of them such as security, privacy, reliability, legal issues, open standards, compliance, freedom, and long term viability." They have defined different security issues, the different existing security threats and attacks. They have explained Cloud Security has unavoidably turned into a significant business recognizer.

There are certain things in the cloud we need to focus on which have been explained above. In conclusion to this, security should be provided to the cloud data. There are certain encryption techniques that can be utilized to encrypt that data to protect it from malicious attacks. Techniques of encryption are further presented in modified forms."Zaid kartit et al. [30] it is proposed to apply encryption technique enhancing data security in cloud storage which is easy, secure, and provides an architecture which preserves privacy while sharing data between clouds. Encryption/Decryption algorithms are the basis of this architecture which focuses on protecting the cloud data from unauthorized access. There are two parts to these algorithms. The first is the file upload part in which, plain text is encrypted by applying the AES algorithm. The next part, which is about downloading a file, states two phases of the algorithm. The first phase comprises the decryption of the AES key by applying RSA (Rivest-Shamir-Adleman) algorithm. The second phase comprises the decryption of ciphered text by applying the AES key obtained from the server. Here, the AES key is decrypted using RSA, there are some demerits to RSA which are that are both public and private keys are directly related to 'x' which is the product of two prime no's which is easy to factorize in cases where the public key is well known to all. Uma Somani et al. [31] have described the encryption of data before sending it to the network along with electronic signature, describing RSA to be the most significant algorithm with asymmetry, associating it with electronic signature and asymmetric cryptography for increasing the protection of cloud. This is a two-tier security procedure. Viswanath et al. [32] proposes a method to enhance the protection of cloud data by making use of a combined form of (Rivest Shamir Adleman & Advanced Encryption Standard) techniques for securely uploading as well as downloading the files. Ganesan et al. [33] proposed the security which comprises a procedure with four tasks based on cryptographic techniques of Diffie Hellman and Elliptic curve algorithm to verify the legitimacy of a user within the environment of the cloud. The first task is Initiating a connection, Creating the account is the second task, Checking the legitimacy of the user is the third task and the fourth and last comprises exchanging the information. The main advantage of this technique is that its time complexity is sub-exponential due to which it is difficult to break. Prashant et al. [34] proposes Digital Signature and associating it with Advanced Encryption Standard encryption and Diffie Hellman algorithm to perform file upload as well as download over the Cloud.

3 PRELIMINARIES

3.1 Cloud Computing

It is a mechanism to enable a benefic, on-demand organized approach to a shareable domain of operating resources (for example workstations, server systems, backlogging, application programs, and management systems) that can be provided rapidly as well as released with minimal management efforts [35]. Cloud computing is generally considered as the delivery of demands [36]. It is a kind of computing in which computing resources from application programs to processing centers are asked across the Web for use and pay accordingly. [37]

(A) Features

(a) Service according to demand: The user does not require to interact with each service provider to provision facilities like time-slots of server and storage on the network.

(b) Access to Broad Cloud Network: Abilities become obtainable across the inter-network and got over basic components that encourage utilizing at different server-dependent or server-independent clients stages (for example smartphones, smart notepads, Laptops, and computer systems) [38, 39].

(c) Grouping resources: The resources figured by a supplier are grouped to provision various users utilizing multiple-inhabitant display, along with resources intangible and virtual form, powerfully relegated as well as reassigned with respect to customer's needs. Memory repositories, operating processes, and transmission capacity on the web are included in cloud resources.

(d) Quick Flexibility: Facilities provided by the cloud are flexible enough to be provided and released, correspondingly rapidly outside and inside comparative according to the need of user [40, 41].

(B) Service Model for On-Demand Computing

(a) Software As A Service (SAAS): This mechanism explains that the user doesn't really have to worry about any particular software installation; it means the client can use desired software without installing it on its own system. The applications which run off the cloud are included in this layer. They are paid off on the basis of use from anywhere and anytime. These applications are available on-demand on the web [42].

(b) Storage as a service (STAAS): This service provides online remote storage independent of the client system and its platform. It felicitates cloud applications to a scale beyond their limited servers [43].

(c) Infrastructure As A Service (IAAS): Virtualized resources for computing over the internet are provided by this model. This service model delivers computer infrastructure on an outsourced site to help organizational operations. In this model, a third-party hosts its infrastructure components like hardware, software, servers, storage, etc. in place of its users. IaaS suppliers likewise have client, application programs along with maintaining systems, keeping backups, and making plans for tolerance are managed by the same [44].

(d) Platform As A Service (PaaS): This is a mechanism using which software and hardware tools needed by the user for any software development across the internet are provided by the service provider. It is a service where an integrated environment for development is provided. Example: service for java or service for c language is configured accordingly like the required software's and editor is installed and is made available to user [45].

(C) Cloud Deployment Models

(a) Private Cloud: It is a cloud environment that is hosted at both internal and external ends as well as controlled internally or by a mediator. It is available for single use and accessible exclusively by a single organization having multiple consumers that share common concerns, policies, and considerations. It may be a costlier way however it can provide a greater degree of protection, safety, and/or conforming to policies. Google's "Gov Cloud "is one of the examples of a Cloud formed by a community [46].

(b) Cloud for Public: It is a mechanism using which capabilities are obtainable by everyone; these services may be free. There is generally not much difference in the architecture of public cloud or private cloud, but security considerations can be different for them. Example: Amazon AWS, Google.

(c) Community cloud: It is an environment where the configurations can be utilized by a particular community of consumers of particular organizations having a common concern and having specific security requirements. It can be managed through multiple organizations included in that group, a mediator, or both [47].

(d) Hybrid cloud: It is the model which is the combination of two or more deployment models that are unique entities but are unified together and provide the advantages of both the models [48].

3.2 Security

The name 'Cryptography'was obtained from 'Kryptos'which is a Greek word, it stands for hidden or secret. Sometimes confidentiality of the data is a very important aspect of data transmission. Cryptography is the hiding information [49]. It is the science that is used to keep the information safe and secret. Basically, cryptography is a technique which used to transfer data safely between two parties without getting interfered with by external entities. Cryptography is based on an algorithm and key which converts information into un- understandable format [50]. The original information is called plain text. And after the conversion of information, the converted information is ciphertext [51].

When a message (data) is sent over a network or from one party to another party that message is encrypted from plain text to ciphertext and that conversion means encrypting the message. When a receiver receives ciphered data, the receiver applies decryption on the ciphered data and gets the plain text and that conversion of cipher text into plain text is called decryption [52]. The process of Encrypting and Decrypting the data is shown in Fig. 2.

Security permits the classification, respectability, and accessibility of data. The improvement of advancements and their institutionalization makes accessible an arrangement of calculations and conventions for reacting to these issues [53]. There are two categories of Cryptography, Symmetric-key encryption, is a kind of algorithm that employs the same key to apply cryptography in both the operations, encrypting and decrypting the data whereas asymmetric encryption algorithm (encryption based on public key) employs distinct keys, one key which is public, used for encrypting the data and another key which is kept private, used for decrypting the data. These two keys are linked mathematically to each other [54]. Someone is able to encrypt a message using a public key, which provides confidentiality, and then the only person possessing the private key is able to decrypt it [55]. To have cloud computing with enhanced security, it is essential to cater to objectives like verifying authenticity, authority, and accessing data in a controlled manner while working with data residing on cloud [56]. The four essential aims concerned with a security system are:

1. Authorization: This indicates that the message should be accessed by only the sender and the intended receivers. If any unauthorized person gets access to that data then confidentiality gets compromised.

2. Authentication: Using this mechanism, proof of identity is established. The origin of an electronic message or document is correctly identified and verified using this authentication process.

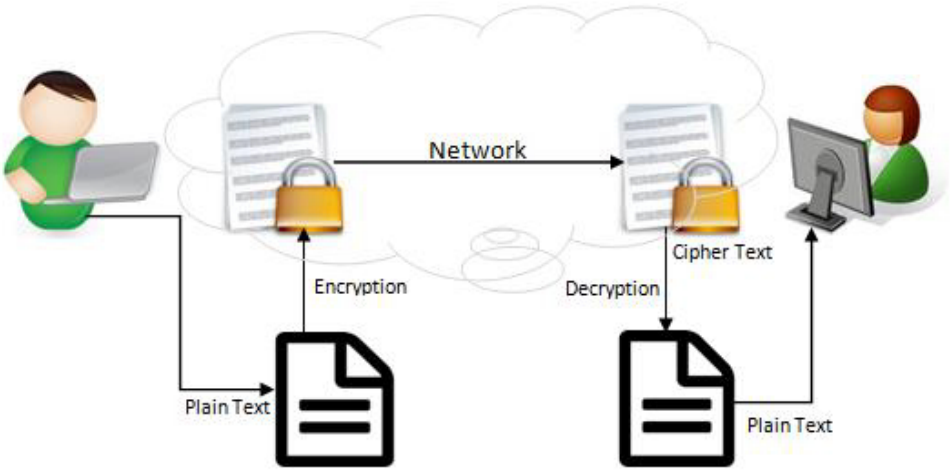

Figure 2: Encryption and Decryption Process

3. Integrity: If the contents of a message are altered after sending the data, but before reaching the intended receiver, it is known as the integrity of the message not retained. A message with lost integrity results in modification.

4. Availability: It is the extent up to which the data on the cloud is available to the user unceasingly from anywhere. [57]

4 PROPOSED WORK

Data encryption using Cryptography is specifically the best way for protecting the information in the cloud environment. Here we propose an algorithm for the encryption of data. The process of encryption will go through several steps of encryption. Our proposed algorithm mainly comprises two steps, the first being the substitution of letters that will follow a particular procedure and the second being the hybrid form of the RSA algorithm. "RSA is an asymmetric encryption algorithm and it was given by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1977. In this algorithm, the Public key is used for encryption and the Private key is used for decryption.". "Here, the security is based upon supposition such that it becomes tough to guess multiples of big integer values and get "private key "which is utilized to decrypt the data. However few shortcomings are associated with the Rivest-Shamir-Adleman technique such as the decrypting process is performed using q and M, so factorizing and deriving the "private key "is easy like "public key "because everyone knows it. Here M is obtained by multiplying two prime numbers and the private key is represented by q.". RSA is a Block Figure in which each message is represented as a whole number. Once the encryption of the message is done by applying the Public key, then decryption will be done using the comparing Private Key as it were. RSA is fundamentally an unbalanced form of encoding/decoding calculation. It is unbalanced in the sense, that here the public key is broadcasted to everyone such that everyone can encode data and the secret key which unscrambles the data, is kept secret and unshared by everyone. The Algorithms 1 to 3 depict the procedures for RSA key generation, encryption, and decryption respectively. The encrypted file is uploaded to the cloud. Further, the file is downloaded by the authorized user, who decrypts the file and then reads it. Fig. 3 explains the whole process of file uploads and file downloads.

(A) File Upload
The encryption is done in two phases. The first phase is about encrypting the plain text using the position of the prime no and taking the modulo of that number. Further, in the second phase, encrypted text from the first phase is taken as an input for the second phase, and a hybrid RSA algorithm is applied to generate the final encrypted text. The basic idea behind this hybrid form is to introduce a third prime no, instead of using two prime no's, we are using three prime no's to generate "public key"and "private key". The steps for key generation using a hybrid form of RSA (HRSA) are depicted in Algorithm 4. The enciphering process is explained in Algorithm 5 that uses the public key(e) generated in Algorithm 4 for encryption.

Algorithm 1 Generate_RSA_Key()

INPUT: Select two random distinct prime numbers a and b.
OUTPUT: Find Public Key (p), Private Key (q) and Modulus (x).
Begin
Procedure(x, y,p, d, M)
$M \leftarrow x * y$
$Calculate\ Euler\ \Phi()of M$
$\Phi(M) \leftarrow (x-1) * (y-1)$
Generate a public key p , such that
$GCD(p, \Phi, (M)) = 1, 1 < p < \Phi(M)$
Compute the private key q,
such that, $d \leftarrow p^{-1} mod(\Phi(M))$
End Procedure
End

Algorithm 2 Encryption_RSA()

INPUT: Select Plain text (X), Public key (p) and Modulus (M).
OUTPUT: Find Cipher text (E).
Begin
Procedure (X, p, M, E)
$E \leftarrow X^p$ mod M
End Procedure
End

Algorithm 3 Decryption_RSA()

INPUT: Select Cipher text (E), Private Key (q) and Modulus (M).
OUTPUT: Find Plain text (X).
Begin
Procedure (X, p, M, E)
$X \leftarrow E^q$ mod M
End Procedure
End

Algorithm 4 Key_Generation_HRSA ()

INPUT: Select three random prime Numbers x, y, and z.
OUTPUT: Find Public Key (p), Private Key (d) and Modulus (M).
Begin
Procedure(x, y, p, d, M)
$M \leftarrow x * y * z$
$Calculate\ Euler\ \Phi()of M$
$\Phi(M) \leftarrow (x-1) * (y-1) * (z-1)$
Generate a public key p , such that
$GCD(p, \Phi, (M)) = 1, 1 < p < \Phi(M)$
Compute the private key q,
such that, $d \leftarrow p^{-1} mod(\Phi(M))$
End Procedure
End

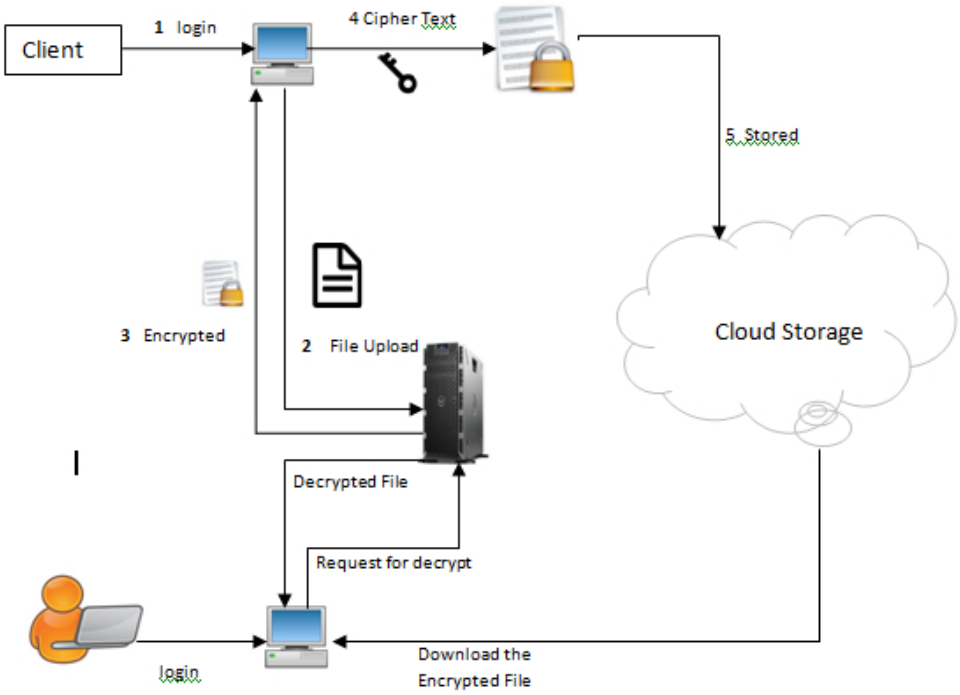

Figure 3: Procedure of File Upload and Download

Algorithm 5 Encryption_HRSA_Encryption ()

INPUT: Select Plain Text (T), Prime no(Z)
OUTPUT: Generation of Cipher Text (Z_0).
Begin
Encryption Process
Step I: INPUT(T, Z) [substitution process]
Calculate position of T
Further Z= prime no of position $T + 1$
$z_1 = Z \bmod 51$
$z_2 = Z/51$ (ignore the floating part)
Further $z_1 = z_1 + 57$
$z_3 = z_1/51$
Cipher text $Z_0 = z_1 \bmod 51$
Step II: **Encryption_HRSA()**
INPUT: Select text (Z_0), Public key (e) and Modulus (M).
OUTPUT: Calculate Cipher text (E).
Procedure (Z_0, e, M and E)
$E \leftarrow Z_0^e \bmod M$
End Procedure
End

(B) File Download
The uploaded encrypted files can be downloaded by the authorized user, then he can decrypt them and can see the file on his system. The decryption process is explained in Algorithm 6. The decryption is also done in two steps: In the first step, the ciphered data generated through the use of a public key (e) is decrypted using a private key (d), and Z_0 is generated. In phase two, Z is generated which will finally replace the position of the alphabet (original plain text).

Algorithm 6 Decryption_HRSA()

INPUT: Select Cipher Text(E), Private key (d) and Modulus(M)
OUTPUT: Plain Text (P)
Step I: Find Plain Text (Z_0)
Begin
Procedure (Z_0, e, M and E)
$Z_0 \leftarrow E^d \bmod M$
End Procedure
Step II: Z_0 (Decrypted text from 1^{st} step of Decryption)
Final Decryption
Step 1: $z_4 = ((51 * z_3) + Z_0) - 57$
Step 2: $Z = ((51 * z_2) + z_4)$
Step 3: Z is a prime no. calculate the position of prime no
from the list of Prime no starting from 2. Let the position is i.
Step 4: Replace the Z with the alphabet at position $i - 1$.
The alphabet is the final Decrypted message(T).
End

The tool hereby is providing an interface, to transfer data over the server system, from where a logical volume is shared with the client over ISCSI protocol. The features are enhanced by applying a cryptographic hash over the data before the data is transferred over to the server system. Therefore the security and integrity of data will be maintained and any kind of snooping risk over the server is also eliminated. Encryption will be provided by a C/java executable program before it gets uploaded over the drive. For all this purpose the various tools and technologies are applied at different levels of the project.

At Frontend: HTML, CSS, bootstrap, and JavaScript will be used. A user interface will be provided by HTML/CSS web pages having Cross-platform responsiveness by bootstrap and verification from javascript. At Backend: Python CGI integration with HTML, C: The Python CGI program will be integrated to execute Linux kernel command through a web interface. It will pass user input along with the Linux command to the bash shell terminal. Redhat Enterprise Linux 7.3 will be used as Operating System. PHP, My SQL Databases. Data for all the registered users will be saved in a database file using PHP, and MySQL. All the backend of RHEL OS various configurations for a repository of yum, epel, etc. are made and software like ntfscrogs, sshpass, and others are installed to provide stem less virtualization environment. General Protocols are used such as HTTP, ISCSI, and SSH. The HTTP protocol is here providing the web interface to the user for which the HTTP daemon is started on the server-side. The SSH protocol is used to log in from client to server system to make the permanent drive entry and from server to client-side to mount the drive permanently. ISCSI protocol is providing the connection for block storage.

5 CONCLUSION AND FUTURE SCOPE

Regardless of the advantages of cloud storage, there are as yet numerous real issues concerning security that should be understood. In this paper, we have explained literature related to the cloud, its models, its security issues, different encryption techniques, and its modifications to encrypt data before storing it in the cloud in such a way that the data is accessible to the legitimate person only and there would not be loss of data confidentiality. If somehow any intruder tries to access the data and somehow is able to access the data from the cloud, then he will get it in non-readable format. The algorithm proposed makes the Cryptanalysis complex as it changes the position of the plain text alphabet using the prime no and finally it applies the Hybrid RSA Algorithm with the usage of three prime no which makes it more difficult to factorize the variable 'x 'as x is directly related in key generation. In the future, perspectives, digits, and ASCII values can also be included for encryption. Encryption can also be done on portable document files.

References

[1] I. Gupta, R. Gupta, A. K. Singh, and R. Buyya, "MLPAM: A Machine Learning and Probabilistic Analysis Based Model for Preserving Security and Privacy in Cloud Environment," *IEEE Systems Journal*, vol. 15, no. 3, pp. 4248–4259, 2021.

[2] A. Acharya, H. Prasad, V. Kumar, I. Gupta, and A. K. Singh, "Host Platform Security and Mobile Agent Classification: A Systematic Study," in *Computer Networks and Inventive Communication Technologies*, vol. 58. Singapore: Springer Singapore, 2021, pp. 1001–1010, data Engineering and Communications Technologies.

[3] K. Kaur, I. Gupta, and A. K. Singh, "Data Leakage Prevention: E-Mail Protection via Gateway," *Journal of Physics: Conference Series*, vol. 933, p. 012013, jan 2018.

[4] P. Agarwal, S. Mittal, A. Tiwari, I. Gupta, A. K. Singh, and B. Sharma, "Authenticating Cryptography over Network in Data," in *2019 International Conference on Intelligent Computing and Control Systems (ICCS)*. IEEE, 2019, pp. 632–636.

[5] I. Gupta and A. K. Singh, "A Probabilistic Approach for Guilty Agent Detection using Bigraph after Distribution of Sample Data," *Procedia Computer Science*, vol. 125, pp. 662 – 668, 2018.

[6] R. Verma, V. Gautam, C. P. Yadav, I. Gupta, and A. K. Singh, "A Survey on Data Leakage Detection and Prevention," in *Proceedings of the International Conference on Innovative Computing & Communications (ICICC) 2020*. SSRN, Elsevier, May 2020, pp. 1–7.

[7] I. Gupta and A. K. Singh, "GUIM-SMD: Guilty User Identification Model using Summation Matrix-based Distribution," *IET Information Security*, vol. 14, pp. 773–782, November 2020.

[8] P. Godha, S. Jadon, A. Patle, I. Gupta, B. Sharma, and A. K. Singh, "Flooding and Forwarding Based on Efficient Routing Protocol," in *International Conference on Innovative Computing and Communications*, vol. 1166. Singapore: Springer Singapore, 2021, pp. 215–223, advances in Intelligent Systems and Computing.

[9] I. Gupta and A. K. Singh, "Dynamic Threshold based Information Leaker Identification Scheme," *Information Processing Letters*, vol. 147, pp. 69 – 73, 2019.

[10] P. Tiwari, S. Mehta, N. Sakhuja, I. Gupta, and A. K. Singh, "Hybrid Method in Identifying the Fraud Detection in the Credit Card," in *Evolutionary Computing and Mobile Sustainable Networks*, vol. 53. Singapore: Springer Singapore, 2021, pp. 27–35, data Engineering and Communications Technologies.

[11] I. Gupta, P. K. Yadav, S. Pareek, S. Shakeel, and A. K. Singh, "Auxiliary Informatics System: an Advancement towards a Smart Home Environment," 2022.

[12] I. Gupta and A. K. Singh, "SELI: Statistical Evaluation based Leaker Identification Stochastic Scheme for Secure Data Sharing," *IET Communications*, vol. 14, pp. 3607–3618, December 2020.

[13] V. Sharma, S. Jalwa, A. R. Siddiqi, I. Gupta, and A. K. Singh, "A Lightweight Effective Randomized Caesar Cipher Algorithm for Security of Data," in *Evolutionary Computing and Mobile Sustainable Networks*, vol. 53. Singapore: Springer Singapore, 2021, pp. 411–419, data Engineering and Communications Technologies.

[14] I. Gupta, V. Sharma, S. Kaur, and A. K. Singh1, "PCA-RF: An Efficient Parkinson's Disease Prediction Model based on Random Forest Classification," 2022.

[15] K. Kaur, I. Gupta, and A. K. Singh, "A Comparative Study of the Approach Provided for Preventing the Data Leakage," *International Journal of Network Security & Its Applications*, vol. 9, no. 5, pp. 21–33, 2017.

[16] A. Kesharwani, A. Nag, A. Tiwari, I. Gupta, B. Sharma, and A. K. Singh, "Real-Time Human Locator and Advance Home Security Appliances," in *Evolutionary Computing and Mobile Sustainable Networks*, vol. 53. Singapore: Springer Singapore, 2021, pp. 37–49, data Engineering and Communications Technologies.

[17] K. N. Kaur, Divya, I. Gupta, and A. K. Singh, "Digital Image Watermarking Using (2, 2) Visual Cryptography with DWT-SVD Based Watermarking," in *Computational Intelligence in Data Mining*, vol. 711. Singapore: Springer Singapore, 2019, pp. 77–86, advances in Intelligent Systems and Computing.

[18] A. K. Singh and I. Gupta, "Online Information Leaker Identification Scheme for Secure Data Sharing," *Multimedia Tools and Applications*, vol. 79, no. 41, pp. 31 165–31 182, November 2020.

[19] S. Jalwa, V. Sharma, A. R. Siddiqi, I. Gupta, and A. K. Singh, "Comprehensive and Comparative Analysis of Different Files Using CP-ABE," in *Advances in Communication and Computational Technology*, vol. 668. Singapore: Springer Singapore, 2021, pp. 189–198, electrical Engineering.

[20] I. Gupta, H. Mittal, D. Rikhari, and A. K. Singh, "MLRM: A Multiple Linear Regression based Model for Average Temperature Prediction of A Day," 2022.

[21] I. Gupta, A. K. Singh, C.-N. Lee, and R. Buyya, "Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions," *IEEE Access*, vol. 10, pp. 71 247–71 277, 2022.

[22] P. Godha, S. Jadon, A. Patle, I. Gupta, B. Sharma, and A. Kumar Singh, "Architecture, an Efficient Routing, Applications, and Challenges in Delay Tolerant Network," in *2019 International Conference on Intelligent Computing and Control Systems (ICCS)*. IEEE, 2019, pp. 824–829.

[23] I. Gupta and K. Gupta, "Evaluation of Intrusion Detection Schemes in Wireless Sensor Network," *IOSR Journal of Computer Engineering*, vol. 18, no. 2, pp. 60–63, Mar-Apr. 2016.

[24] K. Kaur, I. Gupta, and A. K. Singh, "A Comparative Evaluation of Data Leakage/Loss Prevention Systems (DLPS)," in *Proc. 4th International Conference Computer Science & Information Technology*, 2017, pp. 87–95.

[25] I. Gupta and A. K. Singh, "A Probability based Model for Data Leakage Detection using Bigraph," in *Proceedings of 7th International Conference on Communication and Network Security (ICCNS)*, ser. ICCNS 2017. New York, NY, USA: Association for Computing Machinery (ACM), 2017, p. 1–5.

[26] I. Gupta, T. K. Madan, S. Singh, and A. K. Singh, "HISA-SMFM: Historical and Sentiment Analysis Based Stock Market Forecasting Model," 2022.

[27] Nandgaonkar, S. V., & Raut, A. B. (2014). "A comprehensive study on cloud computing. International Journal of Computer Science and Mobile Computing ", 3(4), 733-738.

[28] Yang, J., & Chen, Z. (2010, December). "Cloud computing research and security issues. In Computational intelligence and software engineering "(CiSE), 2010 international conference on (pp. 1-3). IEEE.

[29] Thilakarathne, A., & Wijayanayake, J. I. (2014). "Security Challenges Of Cloud Computing. International Journal of Scientific & Technology Research ", 3(11), 200-203.

[30] Kartit, Z., & El Marraki, M. (2015). "Applying Encryption Algorithm to Enhance Data Security in Cloud Storage ". Engineering Letters, 23(4).

[31] Somani, U., Lakhani, K., & Mundra, M. (2010, October)."Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing ". In Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on (pp. 211-216). IEEE.

[32] Mahalle, V. S., & Shahade, A. K. (2014, October)."Enhancing the data security in cloud by implementing hybrid (RSA & AES) Encryption Algorithm". In Power, Automation and Communication (INPAC), 2014 International Conference on (pp. 146-149). IEEE.

[33] Tirthani, N., & Ganesan, R. (2014). "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography ". IACR Cryptology ePrint Archive, 2014, 49.

[34] Rewagad, P., & Pawar, Y. (2013, April). "Use of digital signature with diffie hellman key exchange and AES encryption algorithm to enhance data security in cloud computing ". In Communication Systems and Network Technologies (CSNT), 2013 International Conference on (pp. 437-439).IEEE.

[35] D. Saxena, I. Gupta, J. Kumar, A. K. Singh, and X. Wen, "A Secure and Multiobjective Virtual Machine Placement Framework for Cloud Data Center," *IEEE Systems Journal*, pp. 1–12, 2021.

[36] A. Nag, A. Kesharwani, B. Sharma, I. Gupta, A. Tiwari, and A. K. Singh, "Potential and Extention of Internet of Things," in *Second International Conference on Computer Networks and Communication Technologies (ICCNCT)*, vol. 44. Cham: Springer International Publishing, 2020, pp. 542–551.

[37] I. Gupta and A. K. Singh, "An Integrated Approach for Data Leaker Detection in Cloud Environment," *Journal of Information Science and Engineering*, vol. 36, pp. 993–1005, Sep. 2020.

[38] U. Arora, S. Verma, I. Gupta, and A. K. Singh, "Implementing Privacy using Modified Tree and Map Technique," in *2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall)*. IEEE, 2017, pp. 1–5.

[39] I. Gupta and A. K. Singh, "A Confidentiality Preserving Data Leaker Detection Model for Secure Sharing of Cloud Data using Integrated Techniques," in *2019 7th International Conference on Smart Computing Communications (ICSCC)*. Curtin University, Sarawak Malaysia: IEEE, 2019, pp. 1–5.

[40] I. Gupta, N. Singh, and A. Singh, "Layer-based Privacy and Security Architecture for Cloud Data Sharing," *Journal of Communications Software and Systems (JCOMSS)*, vol. 15, no. 2, 2019.

[41] G. Batra, H. Singh, I. Gupta, and A. K. Singh, "Best Fit Sharing and Power Aware (BFSPA) Algorithm for VM Placement in Cloud Environment," in *2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall)*. IEEE, 2017, pp. 1–4.

[42] D. Saxena, I. Gupta, A. K. Singh, and C.-N. Lee, "A Fault Tolerant Elastic Resource Management Framework Towards High Availability of Cloud Services," *IEEE Transactions on Network and Service Management*, pp. 1–1, 2022.

[43] I. Gupta, A. Tiwari, P. Agarwal, S. Mittal, and A. K. Singh, "Dodging Security Attacks and Data Leakage Prevention for Cloud and IoT Environments," in *Intelligent Analytics for Industry 4.0 Applications*. FL, USA: CRC Press-Taylor & Francis Group, 2022.

[44] N. Singh, I. Gupta, and A. K. Singh, "Senso_scale: A Framework to Preserve Privacy over Cloud Using Sensitivity Range," in *Advances in Cyber Security and Intelligent Analytics*. FL, USA: CRC Press-Taylor & Francis Group, 2022.

[45] I. Gupta and A. K. Singh, "A Framework for Malicious Agent Detection in Cloud Computing Environment," *International Journal of Advanced Science and Technology (IJAST)*, vol. 135, pp. 49–62, Feb 2020.

[46] K. Gupta and I. Gupta, "A Comprehensive Study on Architecture, Security issues and Challenges in Cloud Computing," *International Journal of Scientific & Engineering Research*, vol. 7, no. 12, pp. 128–131, Dec. 2016.

[47] R. Gupta, I. Gupta, D. Saxena, and A. K. Singh, "A Differential Approach and Deep Neural Network based Data Privacy-Preserving Model in Cloud Environment," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–14, 2022.

[48] I. Gupta and K. Gupta, "Review on Intrusion Detection System Architectures in WSN," *International Journal of Scientific & Engineering Research*, vol. 7, no. 12, pp. 111–115, Dec. 2016.

[49] I. Gupta, "A Comparative Study of the Approach Provided for Preventing the Data Leakage," *Other Topics Engineering Research eJournal*, vol. 9, no. 5, September 2017.

[50] K. Kaur, I. Gupta, and A. K. Singh, "E-Mail Protection System to Prevent Data Leakage," *Vigyan Prakash*, vol. 16, pp. 30–36, 2018.

[51] A. K. Singh, I. Gupta, R. Verma, V. Gautam, and C. P. Yadav, "A Survey on Data Leakage Detection and Prevention," in *Proc. Int. Conf. Innov. Comput. Commun.*, 2020.

[52] I. Gupta and A. K. Singh, "A Hybrid Technique for the Detection of Data Leakage in Cloud computing Environment," in *Ist International Conference on Science in Hindi*, August 2017, vigyan Prakash.

[53] A. Acharya, H. Prasad, V. Kumar, I. Gupta, and A. K. Singh, "MACI: Malicious API Call Identifier Model to Secure the Host Platform," in *Proceedings of the Seventh International Conference on Mathematics and Computing*. Singapore: Springer Singapore, 2022, pp. 309–320.

[54] Khushbu, P. Nishad, V. Kashyap, and I. Gupta, "A Classification and Distribution Model for Data Leakage Prevention and Detection," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 3, no. 2, pp. 348–354, Feb. 2021.

[55] I. Gupta, S. Mittal, A. Tiwari, P. Agarwal, and A. K. Singh, "TIDF-DLPM: Term and Inverse Document Frequency based Data Leakage Prevention Model," 2022.

[56] Khushbu, P. Nishad, V. Kashyap, I. Gupta, and A. K. Singh, "An Organized Study on Data Divulge Elimination and Discernment," in *Computer Networks and Inventive Communication Technologies*. Singapore: Springer Singapore, 2021, pp. 569–578.

[57] I. Gupta and A. K. Singh, "A Holistic View on Data Protection for Sharing, Communicating, and Computing Environments: Taxonomy and Future Directions," 2022.