Fuzzy Elgamal Technique for Securing Data Over Cloud

Vipin Saxena
Department of Computer Science
Babasaheb Bhimrao Ambedkar
University, Lucknow, UttarPradesh
India, 226025

Karam Veer Singh
Department of Computer Science
Babasaheb Bhimrao Ambedkar
University, Lucknow, Uttar
Pradesh, India, 226025

Banshidhar Choudhary
Department of Computer Science
Babasaheb Bhimrao Ambedkar
University, Lucknow, Uttar Pradesh
India, 226025

ABSTRACT

Cloud computing is the most popular computing approach among the scientists and engineers and lots of data are uploaded and downloaded from the cloud servers across 365x24x7 hours using high speed internet services. As the hackers are also watching transfer of the important data especially related to digital currency, hence, there is need to develop secure technique for uploading and downloading the data in secure manner. The present work is an attempt in this direction and Elgamal approach has been converted into the fuzzy based Elgamal approach for secure access of the data through cloud servers. The approach is tested by taking a case study and the results are reported in the form of tables and graphs.

Keywords

Cloud Service, Data Cube, Security Challenge, Fuzzy logic and Elgamal Technique

1. INTRODUCTION

The extensive use of cloud services provides an opportunity to the financial service providers for direct connection with the customers. Due to evolution of cloud servers, digital services can be maintainedfor the customer's relations anywhere and anytime but using internet services. The services may be storing, managing and accessing the information which is easier for the financial service providers and for the customer. One of the financial service providers is the banking sector around the globe which must have the high security levels for authenticating the services to the customers and can easily deploy and integrate different kinds of services to the customers through banking management software. The consumption of time for online services is very much in comparison of visiting the branch again and again. Using cloud services, banking sector is focusing on the customers and daily customers are increasing in the exponential manner. Cloud services by the banking sector create the secure customer centric model for digitizing the banking system which maintains the relationship between customer and bank's employee. This channel helps forstoring, backup and recovering of huge amount of data of the bank and various other services like delivering the software, transferring the data, updating and recovering of data is very easy through cloud services. The services provided by the banking sector increase the turnover of the banks by integrating cost-effective cloud solution. The banking industry needs to address the growing data with input demands of the customers. For this purpose, data centers have been created known as bank's servers but due to availability of the hackers on the internet, many attackers are attacking the servers daily which leads to form the corrupt data on the data centers, however customers are adopting the services after knowing the merits and demerits of the services like reliability, regulatory and security risk. Data centers generally go through many attacks from the hackers which corrupt and led to the loss of crucial information available on the servers of banks, but such type of attack can be eliminated by authenticating the data centers. The services ensure transaction and smooth customer experience in banks. Hosting over the internet with the help of web application provides better speed and services to the customers. Banks providethe services like payment gateway, digital wallet and online payments in which clouds ensure the secure and integrated customer experience. The above figure shows the various hand-held devices connected across the cloud servers.

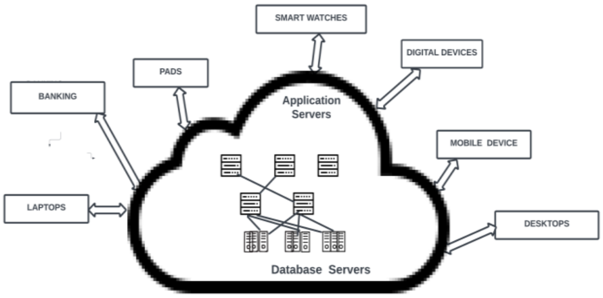


Figure 1. Accessing of Cloud Servers by Banking Sector

Due to the rapidly growing internet services, every person around the globe needs to avail round the clock various services covers under e-commerce or m-commerce. The three types of services are business under E-commerce Business to Business (B2B),Business to Customer (B2C) and Customer to Customer (C2C) and for all thekinds of the services, there is a need of secure payment system for secure transaction over the internet. A Secure Electronic Transaction (SET) is a system, which ensures the security of the financial transaction of funds. Banks play an essential role in all these transactions, every person who needs to avail the services on the internet should have an account in the bank and bank will provide the debit/credit card to the customers and the customers avail the benefits of E-commerce and M-commerceusing thecards. Since the database of the banking sector is very huge, therefore, as Online Analytical Processing (OLAP) cube technology is used for faster accessing of the database by the customers and the data of the customers is transmitted on the internet for the completion of a transaction. Therefore, SET is very necessary for a secured electronic transaction. For said purpose, there are lots of cryptographic techniques which are reported in the literature for example RSA, Elliptic Cryptography, Conventional Cryptography, Elgamal and many more. Everyone uses computers all around the globe and whatever the qualification and age of the individuals for commercial purposes as well as for individual purposes. As technology develops, crime also increases in all fields. To avoid the crime, there is an alternate way of solving above type of cyber-crime issue, which is known as cryptography technology. This powerful technology can take control of both node and medium and does not allow hackers or theft to steal information without the security key. This technology plays an important role in the encryption and decryption of the communicated data for both sender and the receiver. The various cryptography algorithms are existing for the encryption and decryption of data during communication in the last two decades. After applying these techniques for providing high security in data communication, there are lots of cyber-crime that have been arising from the development of advanced technology and the same is focusing to use the malfunctions.

In the present work, a set of rules has been introduced for the processing of the encryption and decryption as a part of proposing a new cryptography algorithm that is incorporated with a fuzzy set. Fuzzy logic is a powerful tool for modeling and controlling the uncertain inputs in the Elgamal cryptosystem that follows public key cryptography and utilizes asymmetric key encryption for extended communication across the two members. The cloud also allowed its users to access the data from anywhere at any time, it utilizes the web as well as the centralized server located remotely to back up the information of its users. There are various kinds of services provided by cloud services like for cloud computing, which are SaaS (Software as Service),PaaS (Platform as Service), IaaS (Infrastructure as Service). Fuzzy based encryption of data to be stored over the cloud is represented by the figure 2.

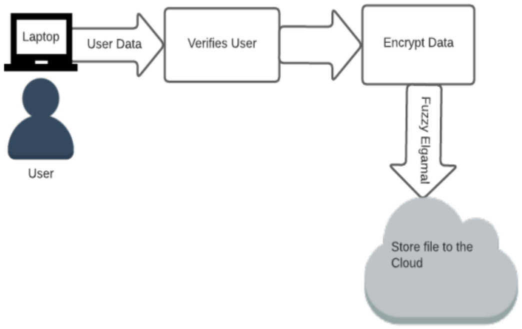


Figure 2. Representation of Fuzzy Based Encryption of Data

2. RELATED WORK

Before implementing the above concepts, exhaustive review of literature is done and very little amount of research work is available on the fuzzy based encryption and decryption of database, therefore it is necessary to explain some of the important research papers related to the proposed work

In the year 1981, Davida et al. [1]have proposed a new cryptosystem that has a sub-key field property, which is an important property for encryption and decryption of the database, and it was based on the Chinese Remainder Theorem. He and Wang [2] studied the cryptographic point of view for the modern relational database management system security problem, which gives a secure environment for storing and processing business data. Oracle[3]provided high security in the form of storing encrypted data; solved the query in the form of decrypted message that prevents unauthorized data access and leaking of data.Hacig¨um¨us et al.[4] explored a new model of third-party service provider host “database as a service” to its user or organization. The author’s provide the challenges for the database community, and for database as service development. Brown[5]has given information related to database encryption mechanism, for all kinds of data stored in a database in the form of text, audio and video. Chang et al.[6]proposed three algorithms for parallel modular arithmetic, parallel subs tractor and a parallel comparator for molecular operation based on DNA, for a product of two large prime numbers, which is used in a biological operation, using molecular operation. Kumar and Arya [7]have proposed the principle of computation of energy consumption efficiency of various security algorithms with energy constrain and proposed user performance of resource management through a control algorithm. OMG [8] designed a user interface with the use of Unified Modeling Language and discussed its strength and weakness. MeikangQiu et al. [9]proposed a principle of energy consumption of different security algorithms for power grid Wide Area Monitoring System (WAMS) with some energy constrain. SingalandRaina [10]analyzed the comparatively two security algorithms AES and RC4 with different parameters like process time, memory utilization, throughput, key size variation, encryption and decryption.

Further, Cuzzocrea and Russo [11]described the OLAP technology alongwith the concepts of data warehousing and Mining.Kumar et al. [12] designed a framework for OLAP data cube for analysis of Vehicle Insurance Policy (VIP) system for identification of entity liked by the customers. Bhati et al. [13] proposed a “Byte–Rotation Encryption Algorithm” (BREA) alongwith the “Parallel Encryption Model” which are better than other security algorithms in terms of security and speed. Madanayake et al.[14]proposed advanced security and processing level-based algorithm through fuzzy logic used for various keys for encryption and decryption. Maram et al. [15]have proposedencryption and decryption algorithms for 2-D matrix architecture that can reduce the path delay and path shared keys like intermediate key and session key. Khan et al. [16] designed an encryption mechanism based on RSA algorithm base on geographic location with latitude as the source and longitude as the destination. Bhagat et al. [17] proposed a new encryption algorithm, which is simple and fast for more applications and the algorithm provides maximum security and saves time, cost and known as Reverse Encryption Algorithm (REA). BhosleandPandey [18]proposed a technique for routing protocol AODV of Mobile ad-hoc networks with the use of a Symmetric Encryption algorithm (AES). Singh andSingh [19]proposed an algorithm for image encryption and decryption using a secret key block cipher called 64-bits Blowfish algorithm realized in MATLAB. Chaudhari and Saxena [20] proposed symmetric encryption and lossless compression using Huffman Coding, which is fast and secure.

In the year 2013, Jamgekarand Joshi [21] presented a modified RSA algorithm for secure file transmission, which eliminates some loopholes of RSA with comparison. Rad et al. [22] proposed the image encryption of largerbased framework. Pal [23] has discussed DNA sequencing for data security and cryptography. Kaur and Singh [24] proposed a framework for encryption of the cloud and security in a cloud environment. Sharma et al. [25] shared architectures for both encryption and decryption. Dehkordi [26] also proposed a data perturbation-based approach to provide privacy preserving in association rulemining on a data cube in a data warehouse and used different hiding styles in various multi-objective fitness functions. Blanco et al. [27-28]showed the benefits of the architecture of data warehouse to develop secure OLAP applications and also proposed for developing secure OLAP applications and defined a logical metamodel for OLAP applications and further it defines the implementation of transformation from conceptual to logical model and from logical model to secure implementation in a Specific OLAP tool. Ravi and Chidambaram [29] provided survey on the various research papers and finding the concepts, algorithm limitation and enhancement regarding each in near future and provided the comparative statement formats for each paper. Gupta and Shanndilya [30]outlined the security tools available for data warehouses, the security challenges to data warehouse administration can be solved using security algorithms, and encryption.Prathana and Gangadhar[31] focused on an effective multidimensional process for User Behavior Anomaly Detection (UBAD) which is developed to detect anomaly using UBAD multidimensional statistical test. Ranasinghe and Athukorala [32] proposed a generalization of the original Elgamalsystem, which also depends on the logarithm problem and method is like that of the basic Elgamalalgorithm; it preserves the immunity against the Chosen Plaintext Attack (CPA).

Recently, Saif et al. [33] proposed a mathematical model in which two functions are defined one for public key and another for mathematical decryption. Shen et al. [34] focused on the present types of asymmetric cryptography, including RSA, Elgamal and Elliptical curve cryptography (ECC) algorithms. Umapathy and Khare [35] presented a Privacy Preserved Hadoop Environment (PPHE), which detects sensitive attributes using data mining techniques and finally evaluates the system.Performance in terms of accuracy recall and F-measure. Buffalo [36] described the modulo operation and we recollect the main approach to computing the modulus. Madhu and Prajeesha [37] proposed a new approach to prevent the FDI attacks on NIC thereby smart meters using the asymmetric key cryptography algorithm, Elgamal and hashing algorithm SHA 512. Maxrizal and Irawadi [38] proposed improvements for the Elgamal cryptosystem by using non-commutative algebra. Charles et al. [39] studied the enhanced Elgamal Encryption-decryption of heart disease feature is transformed using ResNet-50 Classifier.

3. PROPOSED WORK

In the recent years, it is seen that financial organization depends over the cloud services, however, it is open to common attackersand hackers who may performed the attacks over the cloud services via internet. For securing the cloud services, there is need to develop the strong security algorithm for the services rendered over the internet. In the present work, a framework is proposed in which the user initially encrypts the data and writes with the proper integer selection that is put forth by the fuzzy rule system that operates on Madman's method. The framework is represented in the following figure 3 which represents systematic steps to secure the data stored over the cloud.

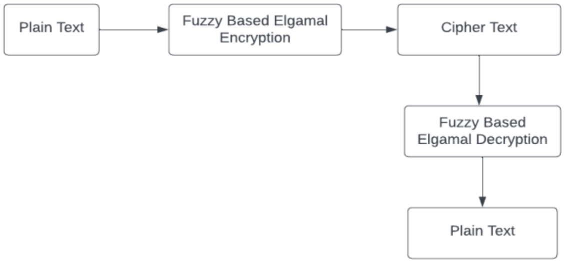

Plain Text
Fuzzy Based Elgamal Encryption
Cipher Text
Fuzzy Based Elgamal Decryption
Plain Text

Figure 3. Proposed Framework

For the proposed model, the Elgamal Cryptosystem with the Fuzzy rule is considered. The cryptosystem depends on the complexity of identification, discrete logarithm in a cyclic. The following algorithm is used for fuzzy based encryption and decryption through Elgamal technique:

```
fuzzy_elgamal()
{
key_generation()
{
select any large prime number;
select any integer as secret key(k), to be primitive root of mod P(m);
compute $A_1$=$m^k$ mod P;
get public key= ($A_1$, m, P);
convert private key into fuzzy set and obtain fuzzy key;
}
encryption()
{
choose unique random number key $k_1$ between 1 to (P-1);
using public key and key, compute cipher text (c1, c2);
}
decryption()
{
defuzzyfing first the fuzzy key into a private key;
decryption proceeds as cipher text and will get plain text.
}
}
```

In the above algorithm, the integer selection from the cyclic group is done using the Mamdani fuzzy rule system that depends on the simple structure of Min-Max operations and by applying the triangular and the trapezoidal functions to calculate the optimal value and estimate the optimal values as integers to enhance the security for the cloud data. The triangular and the trapezoidal functions are given below by equations (1) and (2), respectively:

$$0 \quad x \leq a$$

$$\mu\text{A}(\text{x}) = \frac{x-a}{m-a} a \leq x \leq m$$

$$\frac{b-x}{b-m} m < x < b$$

$$0 \qquad x \geq b$$

(1)

$$0 \quad x < aorx > d$$

$$\mu A(x) = \begin{array}{ll} \dfrac{x-a}{b\ -a} & a \le x \le b \\ \dfrac{d-x}{d-c} & c \le x \\ 1 & b \le x \le c \end{array}$$

(2)

4. RESULTS AND DISCUSSION

To describe the above concept, let us consideredthe plain text as**BANSHI** in which alphabets are represented as A=00, B=01, C= 02, …………, Z=25 and on the basis of this value the plain text becomes as **0100 1318 0708**. The sender **S** desires to send a message BANSHI to the receiver **R** by using the following steps:

Step 1:Public and private keysare calculated by R

- Take the prime modulus as P =2539;
- Take the Primitive root as a=2;
- Take the Private Key k=51;
- Therefore, the public key is b =a^kModP= 2^51 Mod 2539 =403.

Step 2: Elgamalkeyis generatedby S

- Now S chooses the following sequence of Exponents to use for constructing the key 15 23 11;
- Now S uses A_K=15 to calculate the Eelgamal key;
- Now compute the PowerMod of b, $A_{k,}$P using the function PowerMod [b, $A_{k,}$P];
- PowerMod [b, A_K, P] =PowerMod[403, 15, 2539] = 1794.

Step 3: Calculate Elgamal Key for First Block of Message

- The first block of message is 0100;
- PowerMod [a, A_K, P] = PowerMod [2, 15, 2539] =2300;
- 2300 is the first Elgamal key;

Step 4: Calculate Masking Key of First Block of Message

- PowerMod [b, A_K, P] = PowerMod [403, 15, 2539] is the first masking key.

Step 5: Cipher Text of First Block

- Mod [First Block Message * PowerMod [b, A_K, P], P]; =Mod [0100 * PowerMod [403, 15, 2539], 2539] =1670;
- The first block of cipher text is (2300, 1670).

Step 6: Calculate Elgamal Key of Second Block ofMessage

- Now second block of message is 1318;
- PowerMod [a, A_k, P] = PowerMod [2, 23, 2539] =2291;
- So 2291 is the second Elgamal key.

Step7: Calculate Masking Key of Second Blok of Message

- PowerMod [b,A_K,P];
- PowerMod [403, 23, 2539] is the second masking Key.

Step 8: Calculate Cipher Text of Second Block of Message

- Mod [second block message *PowerMod [b, A_K, P], P];

= Mod [1318 * PowerMod [403, 23, 2539], 2539] =1991;

- The second block cipher text is (2291, 1991).

Step 9: CalculateElgamal Key of Third Block of Message

- PowerMod [a, $A_{K,}$ P];
- PowerMod [2, 11, 2539] =2048;
  and 2048 is the third Elgamal key.

Step 10: Calculate Masking Key of Third Block of Message

- PowerMod [a, AK, P];
- PowerMod [403, 11, 2539] is the third masking key.

Step 11: Calculate Cipher Text of Third Block of Message

- Mod [Third block of message * PowerMod[b, A_K, P], P];
- Mod [0708 * PowerMod[403, 11, 2539], 2539] = 198;
- The third block of Cipher text is (2048, 198).

So the all block cipher text message is (2300, 1670) (2291, 1991) (2048, 198)

Decryption of Cipher Text of Message

Now for decryption, we use the notation (Y, Z) for the cipher text, for each block and we first compute the inverse of the Elgamal key Y Mod 2539, then Z* (Y^ (-1) ^n which should be the plain text.

Step1: Calculate Inverse of First Elgamal Key

- ExtendedGCD [first Elgamal key, P] = ExtendedGCD [2300, 2539] = {1, {818, -741}};
- The inverse of Y is 818.

Step 2: Convert First Block Cipher Text to Plain Text

- Mod [1670 *PowerMod[Y^{-1}, k, P], P];
- Mod [1670 *PowerMod[818, 51, 2539], 2539] = 100;
- 100 will be written as 0100;
- The first plain text block is 0100.

Step 3: Calculate Inverse of Second Elgamal Key

- ExtendedGCD [second Elgamal key, P];
- ExtendedGCD [2291, 2539] = {1, {-215, 194}};
- Mod [-215, 2539] = 2324;
- The inverse of Y is 2324.

Step 4: Convert Second Block Cipher Text to Plain Text

- Mod [1991, *powerMod [Y^{-1}, K, P], P] ;
- Mod [1991, *powerMod [2324, 51, 2539], 2539]= 1318;

- The second plain text block is 1318.

Step 5: Calculate Inverse of Third Elgamal Key

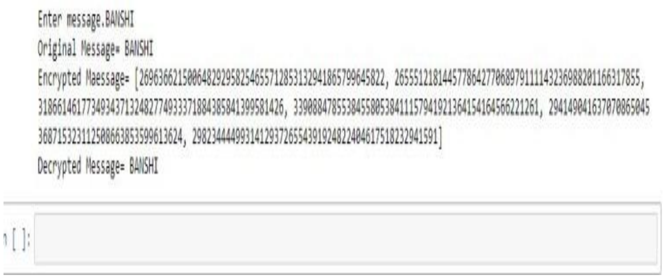
- ExtendedGCD [third Elgamalkey, P]
- ExtendedGCD [2048, 2539] = {1, {393, -317}}
- The inverse of Y is 393

Step 6: Convert Third Block Cipher Text to Plain Text

- Mod [198 * powerMod [Y^{-1}, k, P], P]
- Mod [198 * powerMod [393, 51, 2539], 2539] = Mod [198 * 2004, 2539] = 708;
- The third plaintext block is 0708

So decrypted message is 0100 1318 0708and is equivalent to BANSHI.

The above steps have been programmed through the Python programming language and the result is represented in the following figure 4.



```
Enter message.BANSHI
Original Message= BANSHI
Encrypted Maessage= [269636621500648292958254655712853132941865799645822, 265551218144577864277068979111143236988201166317855,
318661461773493437132482774933371884385841399581426, 339088478553845580538411157941921364154164566221261, 29414904163707086505045
368715323112508663853599613624, 298234444993141293726554391924822404617518232941591]
Decrypted Message= BANSHI
```

Figure 4. Encryption and Decryption through Fuzzy based Elgamal Algorithm

5. CONCLUSIONS

For the above work, it is concluded that there is always need of the security algorithm for protectionof cloud data available in form of files and folders over the cloud servers. In the above, fuzzy technique is used to convert the normal Elgamal algorithm into fuzzy Elgamal algorithm by encrypting and decrypting the information into the blocks and integer selection is performed through Mamdani fuzzy rule system. The proposed work shall protect the hackers to access the important information from the cloud servers and fuzzy technique based algorithm shall minimize the security risks for accessing the cloud data through high speed internet services.

6. REFERENCES

[1] Davida, G., Wells, D. L., and Kam, J. B.,A Database Encryption System with Sub-Keys, ACM Transactions on Database Systems;1981; 6(2): 312–328.

[2] He, J. and Wang, M., Cryptography and Relational Database Management System, IDEAS;2001; 273–284.

[3] Oracle, Oracle9i Database Security for e-Business, An Oracle White Paper, June 2001.

[4] Hacig¨um¨us, H., Iyer, B., andMehrotraS.,Providing Database as a Service, Proceedings of ICDE; 2002; 29– 38.

[5] Brown, H., Considerations in Implementing aDatabase Management System Encryption Security Solution, Research Report Presented to The Department of Computer Science at the University of Cape Town, 2003.

[6] Chang,Weng-Long,MinyiGuo and Ho, M.S.,Fast Parallel Molecular Algorithms for DNA-based, International Journal of Computer Applications (0975 – 8887); October 2013, 79(14).

[7] Kumar, N. and Arya, Y. D. S., Rate Controlled Adaptive Resource Coordination Framework for Wireless Aware Multimedia Applications, International Journal of Computer Science and Network Security; 2010; 10(12): 99-105.

[8] OMG, UnifiedModeling Language Specification, 2010, http://www.omg.org.

[9] MeikangQiu, Chen WenzhongGao Min, NiuJian-Wei and Zhang Lei,Energy Efficient Security Algorithm for Power Grid Wide Area Monitoring System,SmartGrid, IEEE Transactions; 2011; 2(4), 715 – 723.

[10] Singhal,Nidhi and RainaJ.P.S.,Comparative Analysis of AES and RC4 Algorithms for Better Utilization, International Journal of Computer Trends and Technology-July to Aug Issue 2011.

[11] Cuzzocrea, A., and Russo, V., Privacy Preserving OLAP and OLAP Security. In Encyclopedia of Data Warehousing and Mining, Second Edition. 2011. https://doi.org/10.4018/978-1-60566-010-3.ch241

[12] Kumar,Narander,Verma,VishalandSaxenaVipin, Data Cube Representation for Vehicle Insurance Policy System, International Journal of Computer and Application;2012; 58(1): 1-4.

[13] Bhati,Sunita, Bhati, Anita and Sharma, S. K., A New Approach towards Encryption Schemes: Byte–Rotation Encryption Algorithm, Proceedings of the World Congress on Engineering and Computer Science;2012; 2:1-4.

[14] Madanayake,Ravindu,Peiris,Nikila andRanaweera,Gayan, Advanced Encryption Algorithm using Fuzzy Logic, International Conference on Information and Computer Networks, IACSIT Press Singapore;2012; 27: 32-36.

[15] Maram,Balajee, Rao, K. Lakshmanaand Kumar, Y.Ramesh, Encryption and Decryption Algorithm using 2-D Matrices, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X;2013; 3(4):352-356.

[16] Khan, Ayesha, Bhanarkar,Parul and Patil,Pragati, RSA Encryption Technique based on Geo Location, International Journal of Advanced Research in Computer Science and Software Engineering; ISSN: 2277 128X;2013; 3(4):352-356.

[17] Bhagat,Priti, V., Satpute,Kaustubh, S. andPalekar,Vikas, R., ReverseEncryption Algorithm: A Technique for Encryption andDecryption, International Journal of Latest Trends in Engineering and Technology;2013;2(1): 99-95.

[18] Bhosle,Amol and Pandey,Yogadhar, ApplyingSecurity to Data using Symmetric Encryption in MANET, International Journal of Emerging Technology and Advanced Engineering;2013; 3(1): 426-430.

[19] Singh, Pia and Singh,Karamjeet, Image Encryption and Decryption usingBlowfish Algorithm in MATLAB, International Journal of Scientific & Engineering Research;2013; 4(7): 150-154.

[20] Chaudhari,MohiniandSaxena,Kanak, Fast and Secure Data Transmission using Symmetric Encryption and Loss-less Compression, International Journal of Computer Science and Mobile Computing;2013; 2(2): 58 – 63.

[21] Jamgekar,Rajan, S. andJoshi,Geeta, Shantanu, File Encryption and Decryption using Secure RSA, International Journal of Emerging Science and Engineering (IJESE);2013; 1(4): 11-14.

[22] Rad Reza,Moradi, Attar,Abdolrahman and Ebrahimi,Atani Reza, A Comprehensive Layer based Encryption Method for Visual Data, International Journal of Signal Processing, Image Processing and Pattern Recognition; February 2013; 6(1): 37-48.

[23] Pal,Mukul, Chandra, Data Security and Cryptography based on DNA Sequencing, International Journal of Computer Applications; July/August 2013;10(3):1-9.

[24] Kaur,Manpreet and Singh,Rajbir, Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing, International Journal of Computer Applications (0975 – 8887);May 2013;70(18): 1-6.

[25] Sharma,RichaKumari, Biradar, S.R. and Singh, B.P., Shared Architecture forEncryption/Decryption of AES, International Journal of Computer Applications; May 2013;69(18): 1-6.

[26] Dehkordi, M. N., ANovel Association Rule Hiding Approach in OLAP Data Cubes, Indian Journal of Science and Technology;2013; 6(2): 1–13. https://doi.org/10.17485/ijst/2013/v6i2.17

[27] Blanco, C. and de Guzmán, I. G. R., Fernández-Medina, E., and Trujillo, J,Showing the Benefits of Applying a Model Driven Architecture for Developing Secure OLAP Applications,Journal of Universal Computer Science;2014; 20(2). https://doi.org/10.3217/jucs-020-02-0079

[28] Blanco, C., G., Fernández-Medina, E., and Trujillo, J., An MDA Approach for Developing Secure OLAP Applications:Metamodels and Transformations, Computer Science and Information Systems; 2015; 12(2):541–565. https://doi.org/10.2298/CSIS140617007B

[29] Ravi, C. N., andNalini, Chidambaram, C, Comparative Study on OLAP Security and Integrity in Data Warehousing, International Journal of Pharmacy and Technology; 2016;8(4).

[30] Gupta, A., and Shandilya, K,SecurityTools for Data Warehousein Data Storage, Journal of Systems, Management and Security Issues, 2017

[31] Prarthana, T. S., and Gangadhar, N. D., UserBehaviourAnomaly Detection in Multidimensional Data, Proceedings - 2017 IEEE International Conference on Cloud Computing in Emerging Markets, CCEM 2017; 2018-January.https://doi.org/10.1109/CCEM.2017.19.

[32] Ranasinghe, R., and Athukorala, P, AGeneralization of the ElGamalPublic-key Cryptosystem,Journal of Discrete Mathematical Sciences and Cryptography;2021.https://doi.org/10.1080/09720529.2020.1857902.

[33] Saif, H. A., Gharib, G. M. I., and AL-Mousa, M. R, AMathematicalProposed Model for Public Key Encryption Algorithm in Cybersecurity, Advances in Mathematics: Scientific Journal;2021;10(9). 2021.https://doi.org/10.37418/amsj.10.9.1.

[34] Shen. Y., Sun. Z. and Zhou. T, Survey on Asymmetric Cryptography Algorithms, International Conference on Electronic Information Engineering and Computer Science; EIECS 2021. 2021. https://doi.org/10.1109/EIECS53707.2021.9588106.

[35] Umapathy, K., andKhare,N., PPHE-Automatic Detection of Sensitive Attributes in a Privacy Preserved Hadoop Environment using Data Mining Techniques. International Journal of Computer Aided Engineering and Technology;2021; 14(3). https://doi.org/10.1504/IJCAET.2021.114488.

[36] Bufalo, M., Bufalo, D., and Orlando, G., ANote on the Computation of the Modular Inverse for Cryptography. Axioms; 2021; 10(2). https://doi.org/10.3390/axioms10020116.

[37] Madhu, A., and Prajeesha,P., Prevention of FDI Attacks in Smart Meter by providing Multi-Layer Authentication using El-Gamal and SHA, Proceedings-5th International Conference on Computing Methodologies and Communication, ICCMC 2021. https://doi.org/10.1109/ICCMC51019.2021.9418464.

[38] Maxrizal and Irawadi S., Nonsingular Matrix as Private Key on ElGamalCryptosystem, Journal of Physics: Conference Series; 2021; 1821(1).https://doi.org/10.1088/1742-6596/1821/1/ 012018.

[39] Charles, V. B., Surendran, D., and Suresh,Kumar A, HeartDisease Data based Privacy Preservation using Enhanced ElGamal and ResNetClassified, Biomedical Signal Processing and Control, 7; 2022. https://doi.org/10.1016/j.bspc.2021.103185.

7. AUTHORS' PROFILES

Prof. Vipin Saxena received his Ph.D. degree from Indian Institute of Technology, Roorkee, Uttarakhand, India. Presently, he is working as Professor in Department of Computer Science, Babasaheb Bhimrao Ambedkar University, Lucknow, India. He has published more than 190 research articles in the International and National Journals and Conferences, authored 05 books in the field of Computer Science and Scientific Computing, attended 55 International and National Conferences and received three National Awards for meritorious research work in the field of Computer Science and other details are available on www.profvipinsaxena.com. His research interests are Scientific Computing, Computer Networking and Software Engineering.

Karm Veer Singh received his Ph.D. degree from Indian Institute of Technology (BHU), Varanasi, India. He is working as Assistant Professor in Department of Computer Science, Babasaheb Bhimrao Ambedkar University, Lucknow, India. His research interests include Multimedia Information Retrieval, Pattern Recognition, Mathematical Modeling, Data Science, Medical Imaging, Quantum Neural Networks, Reliability, Cyber Security and Artificial Intelligence.

Banshidhar Choudhary received Post Graduate Degree in Computer Applications (M.C.A.) from Indira Gandhi National Open University, New Delhi in 2002 and M.Phil. Degree from Madurai Kamraj University in 2007 and currently a research scholar in the Department of Computer Science, Babasaheb Bhimrao Ambedkar University. He has 15 years of teaching experience in Computer Science field in the various Indian Universities and 03 years in the Al-Jabal Al-Garbi University, Libya. Currently, he is solving the research problems related to security of cloud data and data mining in the Department of Computer Science, Babasaheb Bhimrao Ambedkar University, Lucknow, Uttar Pradesh, India under fellowship program of University Grant Commission (UGC), New Delhi.