

# Secure Transaction of Indian Currency through Biometric Technique

Vipin Saxena

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

Pawan Kumar

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

## ABSTRACT

In the current era, every country is using the physical currency through the Automated Teller Machine (ATM), but, from the literature, it is revealed that the transaction of physical currency from the ATM is still challenging issue. Therefore, present work is an attempt for secure transaction of currency from the ATM used in the context of Indian country. In this country, ATM machine is not using the transaction of currency using biometric technique which is to be linked through the Aadhar card which is the unique identity of the Indian citizen. A concept of Unified Modeling Language (UML) is used to propose a Unified model with inclusion of biometric technique and further it is validated through the concept of Finite State Machine (FSM). Using presented model, only authorized users may use for transactions of currency.

## Keywords

Aadhar card, DNA Cryptography, FSM, UML Class Model, Fingerprint

## 1. INTRODUCTION

Identity cards for Indian residents were recommended by former Indian Prime Minister Shri Atal Bihari Vajpayee in the year 1999 and which were approved in the year 2001. The project was launched by the Indian government in the year 2009 as part of the Unique Identification Authority of India (UIDAI). In Aadhar card, there are two types of information, first is biometric information and another is demographic information. The first information has fingerprint, iris information, and photo of the resident and demographic information contains gender, date of birth, address and husband or father name. In the biometric and demographic information, some information can be changed or updated only on time such that address, phone numbers, etc.

In order to verify a user's identification, fingerprint authentication, a type of biometric authentication, digitally compares a user's fingerprint from a database of recorded fingerprints. All residents have unique fingerprint and cannot be easily guessed and alter or fake. Further an ATM is a device for transfer of electronic information that enables customers of a financial institution to perform transactions with any requirements involving a bank employee, assistant, or clerk. Indian residents use ATM's access, the accounts from anywhere at any time. By receiving a Personal Identification Number (PIN) in confidence from the bank, a client who has a bank account can access the account via ATM systems.

Deoxyribonucleic Acid (DNA) is a kind of molecule that uses biological processes to encode genetic information. Adenine (A), Thymine (T), Cytosine (C), and Guanine (G) are the four distinct basic nucleotides that make up a single strand of DNA. The lengthy sequence allows for the binding of those nucleotides. DNA serves as the building blocks for all living

things and has a remarkable capacity to reliably store and transmit information. This is made possible by DNA's modular design of four unique bases (A, C, G, and T), the sequence of which defines the genetic code, as well as the precise base pairing between complimentary bases that allows hybridization to occur into a double-stranded complex. These DNA characteristics have been used to do calculations and process data, including the encoding, and concealing of hidden messages. Let us describe some of the important references related to the present work.

In the year 2014, Kale et al. [1] implemented, the model based on biometric and Aadhar card with the help of arm controller for ATM and other banking services. Shah et al. [2] have also proposed architecture for biometric encryption with the help of Advanced Encryption Standard (AES) and changed in S-Box which depend on the key. Prasanthi et al. [3] implemented and upgraded ATM security that used palm vein technology to ensure security. Siddiqui et al. and Chatterjee et al. [4,5] proposed a combination of biometric, voice along with PIN for banking service and ATM transactions. Nelligani et al. [6] have also proposed the use of Radio Frequency Identification (RFID) as ATM debit card and biometric sensor for authenticate the card holder. If it is not card holder then use Global System for Mobile Communication(GSM) technology, send signals to near stations. Aadhar card-based ATM transactions tested/computed cyclomatic complexity and validated test cases [7]. Security improved of ATM transactions, used the weighted sum of score technique, three biometric traits, the iris, face, and fingerprint. The iris, facial, and fingerprint traits are extracted from pre-processed photos. To determine matching scores, the attributes of a query picture are contrasted with those of a catalogue image [8].

In the year 2018, Dutta et al. [9] have proposed combination of fingerprint, GSM, Global Positioning System (GPS) and PIN. The client will confirm the transaction by sending an approval message through GSM technology to ensure security while conducting transactions through swipe machines. GPS will be used to determine current locations of the customer. Sudharsan et al. [10] have proposed, executed the two actions, including money transfers and voting applications through ATM machines, by using biometric identification, such as fingerprint and face recognition, and comparing with Aadhar cards for increased security and privacy. For improved security through fingerprint, fingerprint scans in different class such as dry, wet, normal and good quality of fingerprint image [11].

In year 2019, Loya et al. [12] discussed, the Aadhar card for Indian citizen. GSM technology, fingerprint sensors, microcontroller device, and Aadhaar number are used to increase security, make it simple to complete, and take less time in transactions [13]. In the year 2020, Shrimandalkar et al. [14] implemented, smart banking system with the help of biometric, PIN and OTP. Ansar et al. [15] have proposed, enhancement of

two-tier ATM security mechanism, help of security question-based verification along with One Time Password (OTP) and Aadhar card. Gokul et al. [16] proposed, to create a security-based smart ATM that uses RFID and fingerprint authentication to provide access. The user's RFID number and fingerprint information were collected, and then recognise the card number, authorization status, and access location. The appropriate account holder receives a message indicating whether or not the authorisation is legitimate once the information has been verified, the database details that have been retrieved. The account holder is also alerted of the access's location, time, and date. Kavitha et al. [17] have proposed, fuzzy relation which was used to compare fingerprints from a family's three generations. In the year 2021, Kumar et al. [18] have proposed ATM transactions based on PIN and OTP. The ATM doors are shut, the fainting gas is released, and the area is alerted if the vibration sensor detects any suspicious behaviour.

Leonard Adleman, described how DNA molecules can be used to solve mathematical problems and also demonstrated that it is possible to use DNA molecules as a computational device[19]. Customer information is converted in a DNA sequence and store in ATM card in the form of bar code [20]. Raj et al. [ 21] have proposed symmetric cryptography algorithm with the help of DNA sequences. Pushpa [22] has proposed data hiding by DNA sequence. The data is encrypted using the principles of random values, binary coding, DNA sequences and shared DNA sequence between transmitter and recipient for the encryption and decryption processes. Roy et al. [23] have discussed different type of encryption and decryption based on DNA. Patel et al. [24] have proposed image encryption and decryption with symmetric keys with the help of 3D chaotic maps and a DNA encoding approach. This method used three symmetric keys such that prime key, American Standard Code for Information Interchange (ASCII) key and Chebyshev chaotic key which make stronger algorithm. The user's data is encrypted using both the techniques of binary coding and the creation of arbitrary keys [25].

## 2. PROPOSED WORK

In the present work, customer is registered and opened the account in a bank and then customer accesses the account in own sites. A sample block diagram is represented in the figure 1.

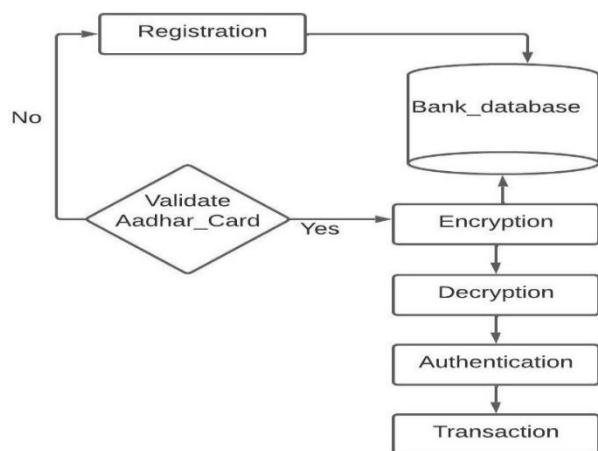


Figure 1 Block diagram of Proposed Model

In the following figure, bank employee collects the information of customer and starts registration process by the use of aadhar card information. All the credentials such that aadhar card,

mobile number, PIN, account number and customer identification number encrypted using DNA encryption algorithm and stored over bank's server. When customer accesses ATM through card, needs fingerprint and PIN for authentication. If fingerprint and PIN match respective card, then displays customer information on ATM screen that data decrypted using DNA decryption before transaction takes place.

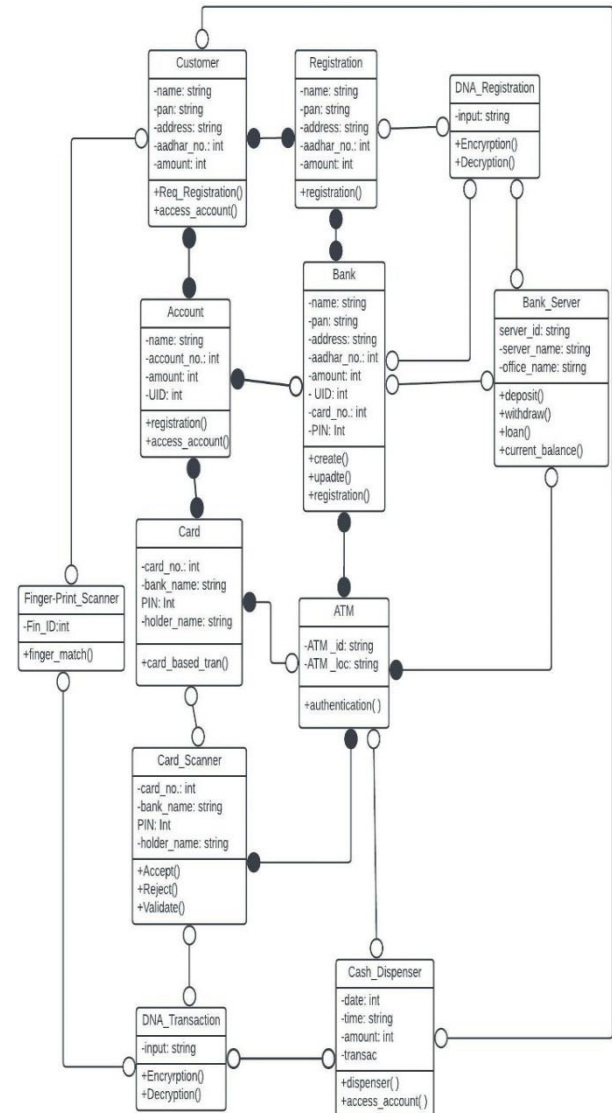


Figure 2 UML Class Diagram for Dispense of Cash after Biometric Authentication

A UML class diagram for dispense of cash after biometric authentication is proposed and represented in the figure 1. In the above diagram initially, customer got registered in the multiple banks. The customer may be one or any finite number which may be registered in single or multiple banks and after registering, the customer, bank issues the account number along-withthe ATM card which may be credit or debit card. There is a class Card\_Scanner who reads the card when it has inserted into the ATM, thereafter ATM operates the card and checks the authenticity of the card by opening the option for scanning the finger of the customer through Finger\_Print\_Scanner class and thereafter DNA cryptography is applied for checking the genuineness of customer and after

complete validation, the desired cash amount is dispensed by the Cash\_Dispatcher class which is attached to the ATM.

By the use of UML class diagram represented in the above, a finite state machine is designed in which each class is representing the state while the relationship between the classes is representing the event. On these aspects, twelve classes are denoted by the state  $q_0, q_1, q_2 \dots q_{11}$  and twenty six events are happening over the links between the classes. The description of various state is given in the following table 1.

**Table 1 List of State**

Name of State	Description
$q_0$	Customer
$q_1$	Registration
$q_2$	DNA_Registration
$q_3$	Bank
$q_4$	Account
$q_5$	Bank_Server
$q_6$	ATM
$q_7$	Card
$q_8$	Card_Scanner
$q_9$	Finger_Print_Scanner
$q_{10}$	DNA_Transaction
$q_{11}$	Cash_Dispatcher

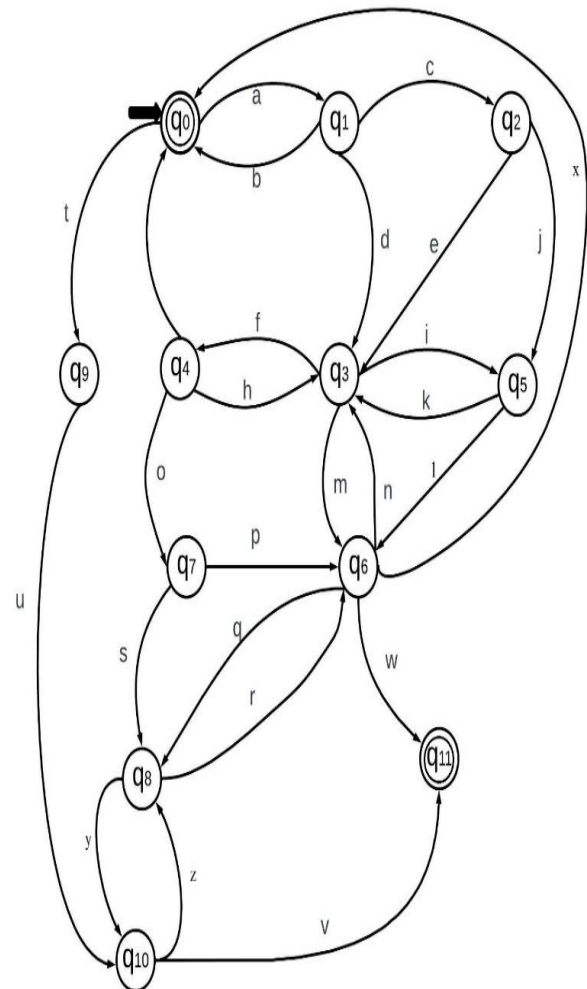
Relationship between two classes is represented by the event in the UML class diagram which is converted into the FSM. The description of each event is given below in the table 2.

**Table 2 List of Event**

Name of Event	Description
a	Fill form for registration
b	Registration granted
c	Customer details transfer for DNA registration
d	Registration details transfer to bank
e	DNA registration details transfer to bank
f	Bank issued / updated Account number and other details
g	Account details transfer to bank
h	Request for update / modify account details
i	Customer detail's loaded/ updated on bank's server
j	DNA details loaded over bank's server
k	Bank's server is controlled by administrator of bank
l	Bank's server operated through ATM
m	Bank's updated the information through ATM
n	ATM represented as per bank's administrator
o	Account is opened through card ( credit / debit)
p	Card is inserted into ATM by customer
q	Card is scanned by card scanner

r	Card scanner responded over the ATM
s	If wrong card inserted by card scanner
t	Customer puts finger on fingerprint scanner
u	Fingerprint scanner proceed for DNA encryption
v	If matched, card dispenser act for dispense of cash
w	Cash is available over ATM
x	Customer took away cash
y	Encryption
z	Decryption

On the basis of above, FSM diagram is designed and represented below in the following figure 3.



**Figure 3 Representation of Finite State Machine**

It dispensed cash to the customer after the biometric authentication. Let us consider the two states as  $q_0$  and  $q_1$  represented for customer and registration respectively. When customer puts request for initially registration either offline/online, then after verification of aadhar card and PAN card, registration details transferred to the customer. In the similar fashion finite state machine diagram is completed.

### 3. RESULTS AND DISCUSSION

By the use of above finite state machine diagram, different important parameters are considered at the level customer or bank who is fully responsible to operate the details of account of customer. The following concept is used for generation of valid test cases:

- (1) Pan\_no. (2) Aadhar\_no. (3) Card\_no. and PIN

Let us consider the following segment diagram from the figure 3.

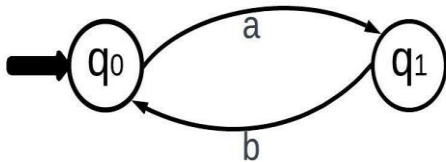


Figure 4 Segment Representation for Registration

As per above figure Customer and Registration modules interact for valid customer's registration. On this diagram, the following valid test case is generated:

#### Test case 3.1 Invalid Pan\_no.

The string ABCDE1234Zfills the entry of correct PAN. This is represented through the following figure.

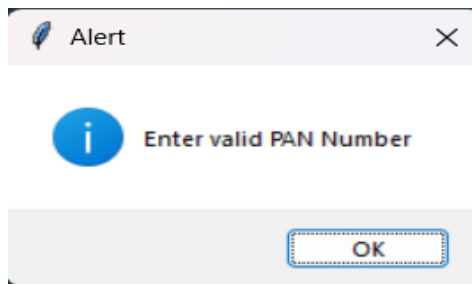


Figure 5 Alert for Invalid PAN Card Number

#### Test case 3.2 Invalid Aadhar\_no.

Similar interpretation is represented for valid aadhar card number of the customer. It will check the digit and string length equal to twelve digits of aadhar card entry field. If this format will not match then send a warning alert as shown below:

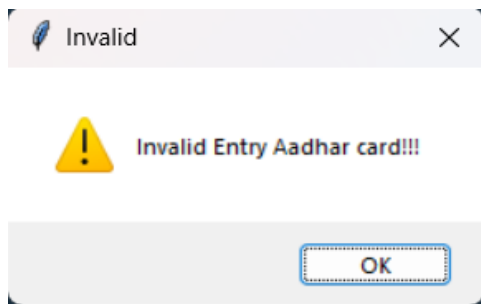


Figure 6 Alert for Invalid Aadhar Card Number

#### Test case 3.3 Invalid PIN and Card\_no.

Card\_no. and PIN codes will be verified by the system model for each consumer. If one of them, PIN or Card\_no. does not

match, an alert message will be shown on the ATM's screen. It is represented in the figure 7.

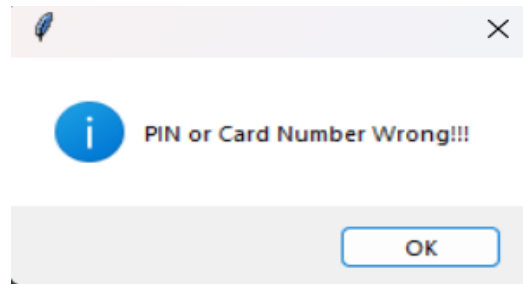


Figure 7 Customer Enters invalid PIN or Card

### 4. CONCLUSIONS

From the above work, it is concluded that UML is a very powerful modeling language to design the blueprint of the software products which can be implemented vary easily by the use of any object-oriented programming language. A secure transaction of currency from ATM machine is validated through the biometric authentication; therefore, at the time of registration, data will be encrypted by DNA cryptography. When customer wants to transact the currency from ATM then all information of the customer will be decrypted by DNA cryptography and it will be displayed on ATM screen for the authentication of the user. Using the above technique, only authorized customers having cards shall operate the ATM machine as biometric information which has already been included for the authentication purpose. Using the above work, only authorized users can access the ATM machine for transaction purpose. If anyone is carrying the ATM of father along with PIN information then only father can transacts the currency while daughter/son cannot.

### 5. REFERENCES

- [1] Kale, A. S., and Nanda, S. K. (2014), A Review Paper on Design of Highly Secured Automatic Teller Machine System by using Aadhaar card and Fingerprint, *International Journal of Advance Research in Computer Science and Management Studies Research Paper*, Vol. 2, pp. 320-322.
- [2] Shah, D. K., Bharadi, V., Kaul, V., Amrutia, S. and Ambardekar, A. (2015), Implementing Enhanced AES for Cloud based Biometric SaaS on Raspberry Pi as a Remote Authentication Node, *Proceedings of International Conference and workshop on Communication, Computing and Virtualization, Series icwccv*, Vol. 2, pp. 17-22.
- [3] Prasanthi, B. V., Hussain, S. M., Kanakam, P. and Chakravarthy, A. S. (2015), Palm Vein Biometric Technology: An Approach to Upgrade Security in ATM Transactions, *International Journal of Computer Applications*, Vol. 112, pp. 1-5, doi: 10.5120/19691-1440.
- [4] Siddiqui, A. T. (2015), Biometric Authentications to Control ATM Theft, *Asian Journal of Technology & Management Research*, Vol. 5, no. 1.
- [5] Chatterjee, P. and Nath, A. (2015), Biometric Authentication for UID-based Smart and Ubiquitous Services in India, *Fifth International Conference on Communication Systems and Network Technologies*, pp.662-667, doi: 10.1109/CSNT.2015.195.

- [6] Nelligani, B. M., Reddy, N. U. and Awasti, N. (2016), Smart ATM Security System using FPR, GSM, GPS, *International Conference on Inventive Computation Technologies (ICICT)*, Vol. 3, pp. 1-5, doi: 10.1109/INVENTIVE.2016.7830093.
- [7] Rhmann, W. and Saxena, V. (2016), Test Case Generation from UML Sequence Diagram for Aadhaar Card Number based ATM System, *International Journal of Applied Information Systems*, Vol. 11, no. 4, pp. 1221-1229, Test Case Generation from UML Sequence Diagram for Aadhaar Card Number based ATM System (ijais.org).
- [8] Balaji, S., Reddy, M. J., Khan, H. and Mounika, K. (2017), Development of Fusion Biometric System for ATM Machines, *International Journal of Mechanical Engineering and Technology*, Vol. 8, no. 7, pp. 649-655.
- [9] Dutta, M., Psyche, K. K., Khatun, T., Islam, M. A. and Islam, M. A. (2018), ATM Card Security using Bio-metric and Message Authentication Technology, *IEEE International Conference on Computer and Communication Engineering Technology (CCET)*, pp. 280-285, doi: 10.1109/CCET.2018.8542227.
- [10] Sudharsan, K., Kumar, V. A., Venkatesan, R., Sathyapreiya, V. and Saranya, G. (2019), Two Three Step Authentication in ATM Machine to Transfer Money and for Voting Application, *Procedia Computer Science*, Vol. 165, pp. 300-306, doi.org/10.1016/j.procs.2020.01.046.
- [11] Sharma, R. P. and Dey, S. (2019), Two-Stage Quality Adaptive Fingerprint Image Enhancement using Fuzzy C-means Clustering Based Fingerprint Quality Analysis, *Image and Vision Computing*, Vol. 83, pp. 1-16, doi.org/10.1016/j.imavis.2019.02.006.
- [12] Loya, B. S. and Thithe, M. K. (2019), Aadhaar Card: Benefits and Challenges in India. *Think India Journal*, Vol. 22(33), pp. 407-411.
- [13] Balamurugan, C. R., Kumar, K. R. and Thirumalai, A. (2019), Secured Smart ATM Transaction. *International Journal of Reconfigurable and Embedded Systems*, Vol. 8, no.1, pp. 61-67, doi: 10.11591/ijres.v8.i1.pp61-74.
- [14] Shrimandalkar, S. K., Imran, M. and Sagar, S. I. Design and Implementation of Smart Banking System. *Institute of Scholars*, 2020.
- [15] Ansar, S. A., Kumar, S., Khan, M. W., Yadav, A. and Khan, R. A. (2020), Enhancement of two-tier ATM Security Mechanism: Towards Providing a Real-time Solution for Network Issues, *International Journal of Advanced Computer Science and Applications*, Vol. 11, no.7, doi:10.14569/IJACSA.2020.0110717.
- [16] Gokul, S., Kukan, S., Meenakshi, K., Priyan, S. V., Gini, J. R. and Harikumar, M. E. (2020), Biometric Based Smart Atm using RFID. *Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pp. 406-411, doi: 10.1109/ICSSIT48917.2020.9214287.
- [17] Kavitha, S. and Vidhya, D. (2020), Fingerprint Matching based on Fuzzy Attribution. *Conference Proceedings*, Vol. 2277, No. 1, pp. 090016. <https://doi.org/10.1063/5.0025190>.
- [18] Kumar, M. N., Raghul, S., Prasad, K. N. and Kumar, P. N. (2021), Biometrically Secured ATM Vigilance System, *7th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Vol. 1, pp. 919-922. doi: 10.1109/ICACCS51430.2021.9441975.
- [19] Adleman, L. M. (1994), Molecular Computation of Solutions to Combinatorial Problems, *Science*, Vol. 266, no. 5187, pp. 1021-1024, doi: 10.1126/science.7973651.
- [20] Prasanthi, B. V., Jyothi, U. P., Sridevi, B. and Krishna, T. V. (2014), Security Enhancement of ATM System with Fingerprint and DNA Data, *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 4, no. 12, pp. 477-479.
- [21] Raj, B. B., Vijay, J. F. and Mahalakshmi, T. (2016). Secure Data Transfer through DNA Cryptography using Symmetric Algorithm, *International Journal of Computer Applications*, vol. 133, no. 2, pp. 19-23.
- [22] Pushpa, B. R. (2017), A New Technique for Data Encryption using DNA Sequence, *International Conference on Intelligent Computing and Control*, pp. 1-4, doi: 10.1109/I2C2.2017.8321834.
- [23] Roy, M., Chakraborty, S., Mali, K., Swarnakar, R., Ghosh, K., Banerjee, A. and Chatterjee, S. (2019), Data Security Techniques based on DNA Encryption, *Proceedings of International Ethical Hacking Conference 2019, Kolkata, India*, vol. 1065, pp. 239-249, [https://doi.org/10.1007/978-981-15-0361-0\\_19](https://doi.org/10.1007/978-981-15-0361-0_19).
- [24] Patel, S., Bharath, K. P. and Kumar, R. (2020), Symmetric Keys Image Encryption and Decryption using 3D Chaotic Maps with DNA Encoding Technique, *Multimedia Tools and Applications*, Vol. 79, no. 43, pp. 31739-31757, <https://doi.org/10.1007/s11042-020-09551-9>.
- [25] Kumar, B. M., Sri, B. R. S., Katamaraju, G. M. S. A., Rani, P., Harinadh, N. and Saibabu, C. (2020, March). File encryption and decryption using DNA technology. In *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, pp. 382-385, Doi: 10.1109/ICIMIA48430.2020.9074970.

## 6. AUTHOR'S 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](http://www.profvipinsaxena.com). His research interests are Scientific Computing, Computer Networking and Software Engineering.

**Pawan Kumar** received Post Graduate Degree in Computer Application (M.C.A.) and Master of Technology (M.Tech) from Babasaheb Bhimrao Ambedkar University, Lucknow, India in respectively 2016 and 2018. Currently research scholar in the Department of Computer Science, Babasaheb Bhimrao Ambedkar University. He is solving the research problems related to security of cloud data and data security in the Department of Computer Science, Babasaheb Bhimrao Ambedkar University, Lucknow, Uttar Pradesh, India under fellowship program of University Grant Commission (UGC), New Delhi.