IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-9, Sept 2019 E-ISSN: 2347-2693

Enhancing Security of ATM Transactions via Debit Cards

Asoke Nath[1*], Sourya Saha[2], Sarthak Gupta[3], Nilarghya Das[4]

[1,2,3,4]Department of Computer Science, St. Xavier's College (Autonomous), Kolkata, India

**Corresponding Author: asokejoy1@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v7i9.152157 | Available online at: www.ijcseonline.org

Accepted: 12/Sept/2019, Published: 30/Sept/2019

***Abstract* -** Nowadays, there has been a sudden surge in thefts from ATMs. Though ATM cum debit cards provides us with a faster access to our money, there lies a big security issue with such cards. The cards are skimmed by using skimming devices and the information from these cards are often stolen when one tries to perform transactions at an ATM. This information is then misused by the people performing such thefts. This paper will shed light upon the above matter. In this paper, we will be discussing the very basics of an ATM cum debit card and an ATM. Then we will talk about the method in which such thefts take place which we can refer to as skimming. In addition to that, we will elaborate on a technique that could possibly be used to prevent such thefts from taking place. The paper will elaborate on the measures to be taken to implement such a mechanism and the scope of this mechanism.

***Keywords* –** ATM, skimming, debit card, theft, PIN, bank server, transaction, OTP.

I. INTRODUCTION

The world has seen humongous advancements in technology in the past few decades. Science is dominating almost all the fields today. A notable advancement can be seen in the field of financial and banking services. Long gone are those days when people had to stand in long queues to withdraw money from their bank accounts. Science has a solution for this too. What our forefathers could only imagine, we use that technology today. No more painful waits in the long queues in banks. Whenever we need to withdraw money from our accounts, an ATM (Automated Teller Machine) comes to the rescue.

An ATM or an Automated Teller Machine helps us in accessing our bank accounts with just clicks of few buttons and a swipe of an ATM cum Debit Card. The Debit Card has unique digits for each card holder. This card is mapped with the person's bank account. Whenever the need be, the person can swipe the card and enter a PIN (Personal Identification Number) provided by the bank to that person (the PIN is again unique for each and every card holder and shouldn't be disclosed to anyone), and access their account information and even withdraw funds, as and when required. ATMs are conveniently placed in almost every locality.

The Debit Card consists of certain important components which must be discussed before we can proceed to the problem with the existing system. The front of the Debit Card contains the following components:

- The Debit Card Number: This is a unique 16-digit number which is different from the Card holder's account number. This number is mapped with the person's account number. The first 6 digits of this number represents the Bank Identification Number and the last 10 digits represent a Unique Account Number for the Cardholder. [1]

- Issue Date and Expiration Date: The issue date is an optional component not present in all cards but the expiration date is present in all the Debit Cards. The issue date gives the date of issue of the card and the expiration date gives the date after which the card will become invalid. The dates are in the format of MM/YY (Two digits of month/Last two digits of year) [1].

- Name of Card holder: This part contains the name of the person to whom the card belongs. [1]

- Logo of the Company which the card was manufactured by: This component displays the logo of the financial service provider or company which manufactured the card. Some common companies are VISA, MasterCard, American Express, etc. [1]

- Name of the Bank: This part on the top of the card gives the name of the Bank which issued that particular Debit Card. [1]

- EMV (Euro pay Mastercard and Visa) chip or Smart Chip: This is a new feature in recent generation of Debit Cards, where all the information related to the card holder is stored in a microchip embedded on the card. [1]

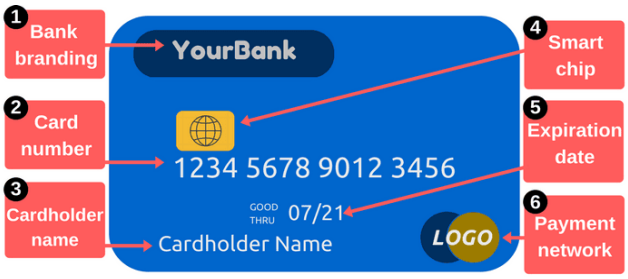


Fig. 1

The back of the Debit Card has the following parts:

- Magnetic Stripe: This is a black horizontal stripe present at the back of the Debit Card. This stripe stores information about the customer. Details such as the card number, bank account number, name of the customer, expiry date, etc. are stored in the magnetic stripe. This stripe can be read by a magnetic stripe reader. [2]

- Signature Panel: This white panel is present on the back of the card for the card holders to put their signature on. [2]

- Contact information of the related bank: This contains the bank contact information for the customer to contact on, in case any issues related to the card arise. [2]

- Hologram: Debit cards have a 3D sticker on their back. This sticker is called a hologram. Its main purpose was that it would prevent a card from being duplicated because creating holograms required very expensive machinery. Nowadays, holograms do not serve any purpose. [2]

- CVV (Card Verification Value): This number present at the back of Debit Cards is used to verify whether a person has the card with them, while making payments online or during online transactions. [2]

- Network logos: These logos tell us exactly where the card can be used. Debit cards may be used with ATMs, online transactions and transactions at PoS (Point of Sales) machines. [2]

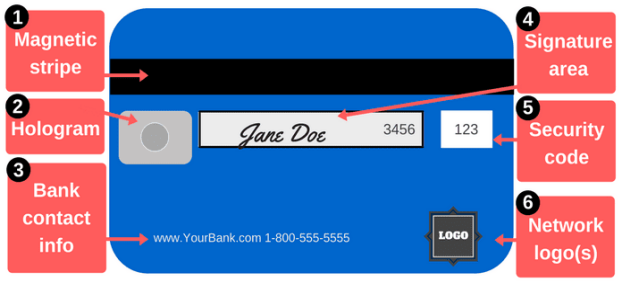


Fig. 2

All transactions with the Debit card at the ATM are done by inserting the card in the card reader slot of the ATM. A detailed working of this procedure has been provided later in this paper.

Every new technology comes with a new kind of problem. In this case, the problem can be quite serious. Imagine, walking into the ATM and performing transactions and then leaving the ATM booth. After a few days, we get to know that around a few thousands of rupees have been withdrawn from our account, which we have no knowledge about. This is what has been happening since a few years. Information from the Debit Cards are being stolen by thieves by employing deceiving means, which we will have no idea about when we perform the transactions at an ATM counter. Later this information is transferred on to dummy cards by the thieves and is used to access our accounts according to their whims and fancies.

The remaining part of the paper has been organized as follows, Section I gives an introduction to the various components of a Debit Card, Section II contains the literary survey of the paper, providing details of the use of first ATM, the components of ATM and details of what skimming is and how skimming is done, Section III describes the algorithm that we propose to use in order to tackle skimming, Section IV contains the results and discussion of the tests of our proposed algorithm and Section V concludes the paper with the future scope of our proposed algorithm.

II. LITERATURE SURVEY

The invention or arrival of the ATM cannot be credited to a single person. Around 1967, the cash dispenser which was a machine similar to the ATM was said to have been invented by John Shepherd-Barron and James Goodfellow in the United Kingdom. In more or less the same period, United States saw the introduction of similar machines found by Don Wetzel and Luther Simjian. Since then, ATMs have seen major advancements in their technology and us improved the experience of digital banking for us. [1] [3]

The main cause of concern relating to Debit Cards and their use in ATMs is the theft of information from the card. This information is maliciously used by the attacker to access the information and funds that is stored in the account of the person. This process of stealing valuable information from Debit Cards by means of deceiving technology is known as skimming. The origin of skimming cannot be traced back exactly but in around 2003, it was recorded that several people in New York who used ATMs, lost more than 200,00$ in a day. A CBS report in December of 2002 even confirmed the existence of small devices which could be used to read information from cards of customers from ATMs. These were the skimming devices. Since then, there

have been several reports of discovery of installed skimming devices at several ATMs globally. Skimming is becoming a growing problem nowadays in almost all of the countries. The people performing skimming operations on people are called Skimmers. Skimmers employ deceptive means to secretly steal information from cards that are used for transactions in an ATM. [3] [4]

Before proceeding forward with a solution that can be used to counter this problem, it is extremely important to understand how an ATM works with Debit Cards.

An ATM has two input channels and four output channels. It is actually a data station which is connected to a host system. The host system is similar to an Internet Service Provider. The host provides the ATM with a database of all the bank accounts that are available to all the account holders around the world. The ATM can derive the account information of any person from anywhere with the help of this host system. The two input channels of an ATM are a card reader and a keypad. [5]

The Card Reader reads the account information that is stored on the back of the Debit Card in a black strip which is a magnetic strip. This information is then sent to the host for verification and for fetching the details of the linked account. [5]

The Keypad in an ATM is square in shape and is metallic. It consists of certain numeric keys and function keys which is used to enter the PIN by a cardholder or to direct the ATM do carry out certain operations.

The output channels of an ATM are:
• A speaker – The voice from the speaker guides the person on the steps to be taken next to carry
out a transaction. [5]
• A screen – This is the most important part of an ATM which displays the account information and the options that could be considered by the user as their next probable choice. The screen also displays the balance, cash amount to be withdrawn and the transactions being performed. [5]
• A cash dispenser – This slot in the ATM dispenses the exact amount of cash that a person withdraws from their account. [5]
• Receipt Printer – This device prints receipts containing details of the transaction just performed, the available balance, the amount of cash withdrawn and other account information. [5]

When a person wants to withdraw money from an ATM, he/she inserts the card in the card reader slot. As soon as this is done, the card reader reads the information that is present in the magnetic strip on the back of the card and sends this information to the host. The host verifies whether the information is valid and then fetches the corresponding details of the cardholder's account from a database of all bank accounts that it is able to access. The user is then asked to enter the assigned PIN to continue the transaction. The person uses the keypad to enter the PIN. After entering the pin, the person presses on a button at the side of the screen to confirm that he/she has entered the PIN. The ATM sends the PIN to the host and checks whether the user has entered the correct PIN. If the entered PIN is wrong, the screen displays that the PIN is incorrect, else the screen provides the user with options as to what he/she wants to do. These include Balance Inquiry, Cash Withdrawal, and many more. One who wants to withdraw cash presses on the button next to cash withdrawal written on the screen. The ATM asks the user to enter the amount. The user enters the amount via the keypad and then presses on a button to confirm that he/she has entered the amount to be withdrawn. After this, the ATM checks whether the user has more balance in his account than the amount he/she wants to withdraw. If no, the screen displays the appropriate message, else the ATM checks whether the entered amount of money is available in the machine itself. If no, again the screen displays the appropriate error message. If the cash is available, the ATM performs the transaction, deducts the withdrawn amount from the available balance of the user and sends this information back to the host. Along with this, it dispenses the cash from the cash dispenser. The ATM also prints a receipt of the transaction if the person asks for it by choosing to do so in the screen. [6]

Now let us understand how banking software works in coordination with an ATM. Whenever a person performs a transaction at an ATM, the ATM communicates with a host server. This host server in turn communicates with the banking software in the bank server. The bank server holds all the required information about the cardholder's account with the bank. The host server checks for verification of information provided by the cardholder by requesting data from the bank server. The process occurs in the blink of an eye. When a cardholder wants to withdraw money from his/ her account, the ATM checks with the bank server if the person has available balance in his account to allow the withdrawal to take place. If funds are available, the ATM dispenses the stated funds and deducts the same amount from the available balance. It then sends this information to the host, which in turn sends the same to the bank server to update the data of the cardholder in its database. On getting withdrawal information, the bank software on the bank server end sends a message to the cardholder's registered mobile number stating that a cash withdrawal of a certain amount has taken place.

A skimmer is able to steal the card information from a cardholder in many ways. One of the common methods of skimming is where the skimmer uses a false card reader just above the original card reader which reads all the card information stored in the magnetic strip. Along with this, a

pinhole camera captures the PIN when the person enters it. The information from the card reader is later downloaded onto another computer by the skimmer and transferred onto fake cards, to be used to access the victim's account. [7]

There is one more method of skimming, which applies the false card reader with a false keypad to capture the PIN entered by the cardholder. [7]

Having talked about how the old system works, we will now shift our emphasis towards the new system. The new system will be designed in such a manner that it eliminates the problem of theft of account information by applying certain new restrictions on the software that the banks will be using. This will hopefully work out as a way to tackle the ever-growing problem of skimming.

III. PROPOSED ALGORITHM

The objective of our paper is to propose a method that could be possibly used to prevent the theft of information from Debit Cards with minimal or no change to the existing system. Every year, a very high amount of funds is stolen from accounts via skimming all over the world. This is a global problem and it is growing with each passing day. Therefore, it is the need of the hour to devise a mechanism to stop skimming from successfully retrieving all the data of a cardholder. The need for preparing this paper is the fact that it is essential to come up with a solution to the problem of skimming so that people feel safe while accessing their accounts from ATMs and performing transaction according to their requirements.

The proposed system is a simple modification of the existing system to reduce cost and time on the part of banks and organizations who will employ this technique to prevent skimming. In this technique, we simply make a change in the banking software. The change will not require the use of the PIN anymore for any transactions at the ATM.

Every cardholder has a registered mobile number with the bank account. Whenever a person needs to make a transaction, the person will go to an ATM and insert the card in the card reader. On inserting the card, there may be a false card reader present at the card slot which will pick up all the account details from the magnetic stripe. But this won't cause any security issues anymore. This is because, the user will not have to enter any PIN anymore to access the account. On entering the card in the card reader and pressing a button on the screen, the ATM will contact the host server stating that the person with the account number on the card wants to access the linked account. The host will contact the bank computer. This computer will generate an OTP (One Time Password) and will send this OTP to the user's registered mobile number and to the ATM machine through the host server. The user, on receiving the OTP will enter the OTP and carry out the transactions as required by him/her.

The advantage of using this method is that, the OTP will remain valid for just one transaction. So, even if the skimmer places a fake keypad and reads the OTP while the user enters it, it won't be valid for any other transactions anymore. Even though the skimmer picks up the information on the magnetic strip, they won't be able to access the linked account because the OTP will be invalid after one transaction and due to the fact that the OTP will always be sent to the user's mobile number which the user will always have with himself/herself.

IV. RESULTS AND DISCUSSION

In order to test the validity of the working of the proposed system, we created a dummy system. We implemented the bank server through MySQL and created an Admin Mode for related operations of a bank. We created a User Mode to test the basic operations that could be performed by a user at an ATM. The system has been coded using Java. All customer related information – customer name, card number, phone number, balance, account number are stored in a table called "Customers" that is implemented via MySQL.

The Admin Mode contains controls for adding, modifying and deleting records to and from the Customers table. This mode has been secured with a password which can only be accessed by the Admin.

The User Mode enables users to perform transactions similar to the ones carried out at an ATM outlet upon the swiping of the ATM card. Only valid cardholders can perform the transactions. The validity refers to the presence of data in the Customers table.

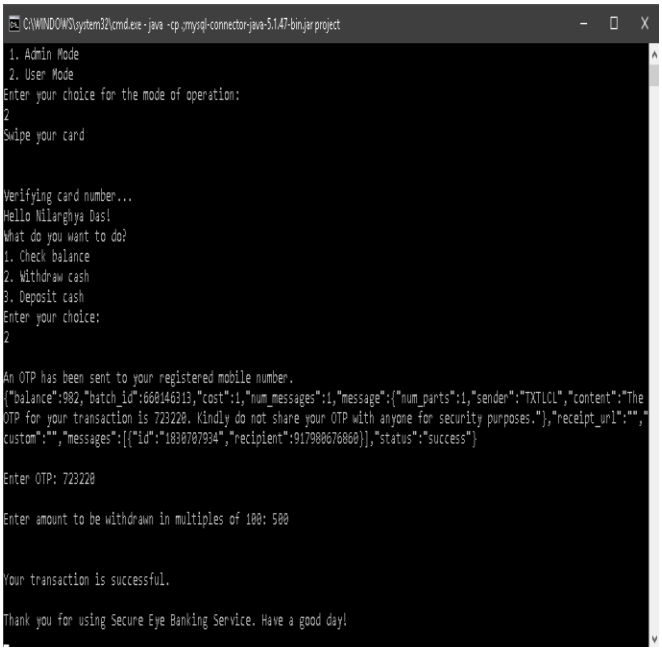


Fig. 3 Screenshot of cash withdrawal operation

The dummy system has been tested as per the algorithm proposed by us and it can be said that the system works properly and fulfills the task of validating customers based on an OTP. Snapshots of the test result for cash withdrawal and depostion are provided for better clarity.

The first three snapshots of the dummy system testing are for user operations corresponding to balance checking, money withdrawal and money deposition respectively. The last two snapshots show the SMS received by the corresponding user on his registered mobile phone after the deposition and withdrawal transactions respectively. All the snapshots show successful working of the proposed algorithm.

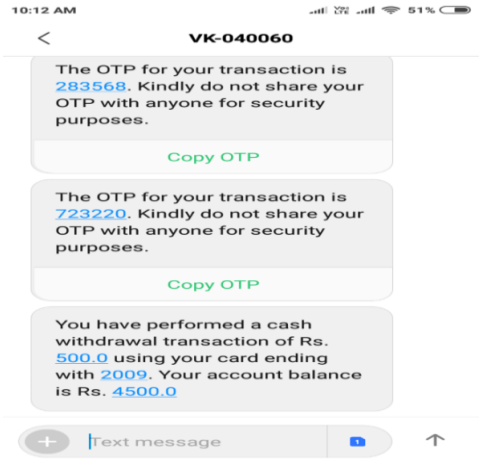


Fig. 4 Snapshot of SMS stating cash withdrawal from account linked with the respective mobile number.

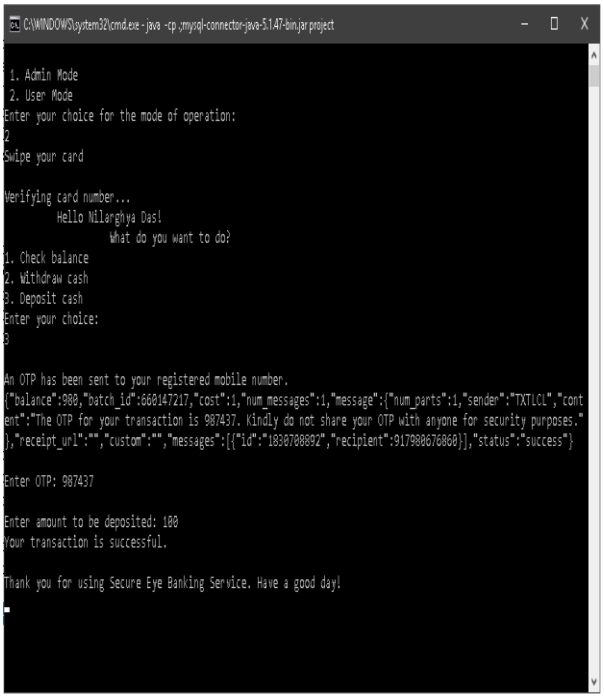


Fig. 5 Screenshot of cash deposition operation

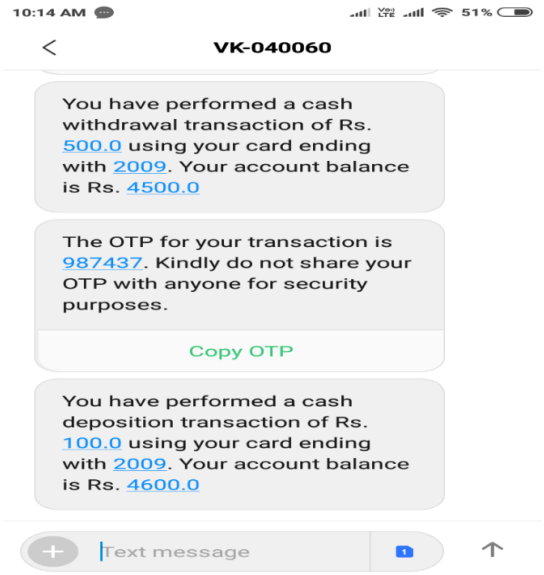


Fig. 6 Snapshot of SMS stating cash deposition from account linked with the respective mobile number.

V. CONCLUSION AND FUTURE SCOPE

In our paper, we have proposed one of the many solutions possible, the entire explanation and design of the new system.

The above discussed system and design will have to be implemented into the banking system software of different banks for its use by the general people. Once implemented on a large scale, this system will help to prevent skimming largely. The system will not allow a person to withdraw money without entering a random One Time Password (OTP) generated during the process of withdrawing money itself. We hope that the system will work as per the discussion made in this research paper and will provide us with the appropriate results once implemented and established in its relevant compatible software spaces.

With time, new flaws are being discovered, and accordingly measures are taken to make the system more secure. But that doesn't stop the criminals from pursuing their search for new loopholes and committing illegal activities. Thus, the effort to make these systems more and more secure to save them from the growing advance threats should never cease.

In our paper, we have proposed one of the many solutions possible. We consider this solution as a step towards the betterment of the existing banking system. If this system is properly built, maintained and incorporated into existing system, it will be able to save lots of money from getting stolen by skimmers through the various known ways also discussed in our documentation. If proper precautions are taken while using the ATM with an OTP requirement, no

skimmer will ever be able to crack the security mechanism employed in this system.

We see in today's advanced world, that with every passing day, criminals are coming up with new ways to crack the latest security measures. Thus, after implementing the system designed by us, proper maintenance of the same is required. If done so, this mechanism will work in people's favor and will prove to be of great use.

We can say that the limitation to our proposed algorithm is the fact that while making transactions, the card holder must always have his/her mobile phone with him/her having the SIM card bearing the number which is registered with bank corresponding to the Debit Card. This is because, the OTP for each transaction will be sent to the customer's registered mobile number. But that should not be a problem, considering the wide use of mobile phones and smartphones in today's world. Another problem is that the OTP must be entered within a stipulated amount of time into the ATM to perform a transaction. So, if the OTP takes more time than the stipulated time to get delivered to the registered mobile number of the customer due to network problems or any other problem, the session will time out. We hope to solve this problem of OTP delivery in the next version of our algorithm by finding a means to generate the OTP from the customer's registered mobile number and then forwarding the OTP to the bank server so that it can verify the customer when the OTP is entered by the customer at an ATM portal. Also, once people start getting comfortable with the use of this system with time, the length of the OTP generated can also be increased, which will make it almost impossible for a skimmer to even guess the OTP and try and access a victim's account.

REFERENCES

[1] Khalifa, Salem S.M, and Kamarudin Saadan, "The Formal Design Model of an Automatic Teller Machine (ATM)." *Lecture Notes on Information Theory*, vol. 1, no. 1, Mar. 2013.

[2] Mrunal A. Mahajan, "An approach for securing Swiping Machine transactions", Journal Paper (IJSRCSE), Volume 06 , Special Issue.01 , pp.68-72, Jan-2018.

[3] Omari, Richard Kwaku Bamfo, "An assessment of the use of Automated Teller Machine (A.T.M) of Barclays Bank Ghana Limited Akim Oda Branch", Institute Of Distance Learning, Kwame Nkrumah University of Science and Technology, September 2012.

[4] Mukesh Sharma and Shailendra Jha, "Digital Data Stealing from ATM using Data Skimmers: Challenge to the Forensic Examiner", Journal of Forensic Sciences and Criminal Investigation, Volume 1, Issue 4, January 2017.

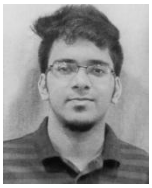
[5]Dhanush J.Nair and Sunny Nahar. "ATM Transaction : A New Time Based Approach Research paper", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 6, June 2015.

[6] Yekini N.A., Itegboje A.O., Oyeyinka I.K. and Akinwole A.K., "Automated Biometric Voice-Based Access Control in Automatic Teller Machine (ATM)", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No.6, 2012.

[7] Kavita Hooda, "ATM Security", International Journal of Scientific and Research Publications, Volume 6, Issue 4, April 2016.

Author's Profile

Dr. Asoke Nath is working as Associate Professor in the Department of Computer Science, St. Xavier's College (Autonomous), Kolkata. Apart from his teaching assignment he is also engaged in doing research work in the field of Cryptography and Network Security, Steganography, Green Computing, Big data analytics, Li-Fi Technology, Mathematical modeling of Social Area Networks, MOOCs etc. He has delivered Keynote speech, invited lectures in various International conferences in India and in abroad. He has published more than 245 research articles in different Journals and conference proceedings.



Mr. Sourya Saha completed his Bachelor of Science (B.Sc.) degree in Computer Science from St. Xavier's College (Autonomous), Kolkata in 2017 and his Master of Science (M. Sc.) degree in Computer Science from St. Xavier's College (Autonomous), Kolkata in 2019. He is currently pursuing Master of Technology (M. Tech) degree in Computer Science and Engineering from University of Calcutta.

Mr. Sarthak Gupta completed his Bachelor of Science degree in Computer Science from St. Xavier's College (Autonomous), Kolkata in 2017 and his Master of Science degree in Computer Science from St. Xavier's College (Autonomous), Kolkata in 2019. He is currently preparing for appearing in the Union Service Public Commission examination in 2020.

Mr. Nilarghya Das pursued his Bachelor's of Science degree in Computer Science from Asutosh College, Kolkata in 2017 and his Masters of Science degree in Computer Science from St. Xavier's College (Autonomous), Kolkata in 2019. He is currently working as a Consultant Analyst in Nielsen India Pvt. Ltd.

