Archives available at journals.mriindia.com

International Journal of Recent Advances in Engineering and Technology

ISSN: 2347-2812
Volume 12 Issue 02, 2023

Securing ATM Transactions Through Dual Channel OTP Verification: Mobile SMS and Gmail Integration

Shreyas Sudhakar Mohire[1], Amit Gupta[2] ,Tejashree Chalwadi[3], Navneet Jha[4], Ravindra Sugdeo Sonavane[5], Roopali Lolage[6] ,Surekha Mali[7],Swati Bhatt[8]

Department of Computer Engineering, Shree L.R. Tiwari College of Engineering, Mumbai[1,2,3,4]
Assistant Professor, Department of Artificial Intelligence & Data Science Thakur College of Engineering & Technology, Mumbai[5]
Professor, Department of Computer Engineering, Shree L.R. Tiwari College of Engineering, Mumbai[6]
Assistant Professor, Department of Computer Engineering, Shree L.R. Tiwari College of Engineering, Mumbai [7,8]

shreyas.s.mohire@slrtce.inthese[1],amit.r.gupta@slrtce.in[2],tejashree.h.chalwadi@slrtce.in[3], navneet.s.jha@slrtce.in[4],ravi.mergit16@gmail.com[5],roopali.lolage@slrtce.in[6],surekha.mali@slrtce.in[7],swatibhatt238@gmail.com[8]

Peer Review Information

Submission: 28 Aug 2023Revision: 26 Oct 2023Acceptance: 29 Dec 2023

Keywords

ATM, OTP, Security,System

Abstract

In today's date money is an essential thing to be carried out whether it is shopping, travelling or any health emergencies. But, at the same time it gets annoying when you need to carry huge amount of cash in your pockets. This is where ATM is important. Bank has provided ATM machines which can provide money anywhere you want. ATM is an easy way for withdrawal of money, just need to insert the card and enter the pin, after that the transaction proceeds. But what if someone will keep your card and somehow, he/she will know your password, it will grant him/her full access to your money. That raises question on present security and demands something new in the system that can offer second level of security. One-time password (OTP) is password that authenticates an authentic user for only one login to the respective system. This paper gives the new method towards the security of Automatic Teller Machine (ATM) system.

INTRODUCTION

Previously, individuals traded goods and services through barter, which is a direct exchange of goods without money. Subsequently, societies brought forth money in various forms to substitute the barter system and facilitate transactions. With time, paper and metal money began to give way to "plastic money," like credit and debit cards.

Consequently, Automated Teller Machines (ATMs) gained extensive usage globally. The usage of ATM cards continues to grow because of increased awareness of electronic payment and the

extension of ATM services by banks. This has, however, increased ATM fraud. Criminals including stealing cards, observing individuals entering their PINs, putting fake PIN pads on ATMs, and cheating individuals into divulging their PINs via emails and SMS. ATM fraud is problem not only for banks but also for customers and law enforcement. It results in financial losses and leads people to lose confidence in using ATMs, which might decrease their popularity. As ATMs are a major source of profit for banks, it is in their interest to prevent fraud. Banks must implement robust security measures to safeguard customers and their money.

To provide added security, most banks have instituted "two factor authentication" for web-based transactions The additional layer of security was originally employed by Google to protect email accounts. It asks users for a verification code as well as their password when they sign in. The verification code is automatically sent to the user's phone or produced by a special gadget. This way, even if a hacker gets a hold of a user's password, they will not be able to use the account without the verification code. This approach significantly decreases the risk of fraud and unauthorized access.

An ATM system, typically lacking an OTP feature for cash withdrawals, comprises several key components: a Card Reader that captures and transmits account information from a magnetic stripe to a host processor for transaction processing; a Keypad for users to input their PIN and select transaction types; a Display screen for viewing transaction details; a Speaker to provide auditory instructions or information; a Receipt printer for a printed record of the transaction, detailing the amount, account number, balance, and user name (though it's advisable to decline or tear up receipts); and finally, the Cash dispenser, the most crucial and sophisticated part, enabling users to withdraw cash.

OTP is a system-generated numeric string of characters that authenticates the user for a single transaction. Once you enter the amount that you wish to withdraw, the ATM screen will display the OTP screen. If an attacker manages to get hold of ATM card/Account number and the pin number he may easily use it to withdraw money. Firstly, the user will be asked with account number and ATM pin, after that the user will receive an OTP on his registered mobile number. After entering the OTP, the user will be asked for withdrawal or deposition of money. If he wants to withdraw money, the OTP will be verified then only further transaction can take place. Thus our system provides a totally secure way to perform ATM transactions with security structures. To overcome the security, this paper proposes second level security for ATM systems. An ATM is an IT enabled electromechanical system that has connectivity to the accounts of a banking system.

II. LITERATURE SURVEY

Enhancing security in Automated Teller Machine (ATM) transactions is a pressing issue, particularly given the rise in fraud and identity theft. Traditional PIN-based systems are vulnerable to a range of attacks including shoulder surfing, skimming, and phishing. As a result, integrating multi-factor authentication (MFA)—particularly through mobile-based One-Time Passwords (OTP) and email OTPs (e.g., via Gmail)—has emerged as a significant advancement in secure banking systems.

Krol et al. (2015) [1]conducted an influential study on the usability of two-factor authentication (2FA) in UK online banking. The research highlighted users' challenges with hardware tokens, emphasizing the need for streamlined authentication processes that do not compromise security.A notable ATM-specific implementation using QR and OTP mechanisms is proposed by Sumanth C (2019), who introduced a card-less secure authentication protocol. This system employed QR codes and dynamically generated OTPs, showcasing a robust defence against common ATM fraud techniques such as skimming and shoulder surfing.

Reese et al. (2019) [2] provided a comparative usability analysis of five 2FA methods, including SMS and email OTPs. Their results underscored that methods which balance security with user convenience—such as mobile and Gmail OTPs—tend to have higher acceptance and better compliance, an essential factor for ATM deployments.

Vassilev et al. (2020) [3]explored voice-enabled banking authenticated via 2FA using public cloud services, reinforcing the trend toward integrating multiple secure channels, such as mobile apps and email systems, for transaction validation.

Lastly, Shamdasani and Matte et al. (2014) combined biometric fingerprint scanning with OTP

sent to the user's mobile phone. Their dual-layered approach effectively mitigated risks associated with static PINs, and the OTP mechanism delivered via GSM—provided dynamic verification for every transaction.
Shaikh and Rabaiotti et al. [4] the United Kingdom (UK) Identity (Id) Card scheme. Their analysis approached the scheme from the perspective of high volumes of public deployment and they described a trade-off triangle model. They found that there are trade-offs between several characteristics, i.e. accuracy, privacy and scalability in a biometric based identity management system, where the emphasis on one undermines the other.

A Murthy and Reddy et al. [5]an embedded fingerprint system, which is used for ATM security applications. In their system, bankers collect customer's fingerprints and mobile numbers while opening accounts, and then customers only access the ATM. The ATM works in such a way that every time a customer places his/her finger on the printing module, the ATM automatically generates a different 4-digit code as a message to the mobile phone of the authorized customer through a GSM modem connected to the microcontroller. The code received by the customer is entered into the ATM machine by pressing the keys on the touch screen. After entering the received code, the ATM checks whether the code is a valid or not before allowing the customer further access and usage.

Schouten and Jacobs et al. [6] studied an evaluation of the Netherlands proposed implementation of a biometric passport, largely focusing on technical aspects of specific biometric technologies (such as face and fingerprint recognition) [7] but also making reference to international agreements and standards (such as ICAO and the EU's Extended Access Control) and discussed the privacy issue in terms of traditional security concepts such as confidentiality.

These studies collectively affirm the effectiveness of mobile and Gmail OTPs as secure, user-centric enhancements for ATM authentication systems. Their deployment can significantly reduce fraud, improve user trust, and align with global banking security standards.

Similar to OTP-based verification in ATM systems, IoT-based food spoilage detection systems employ automated real-time alerts to enhance safety and reliability in resource-sensitive environments [14]. In aquaponic farming, IoT-driven water quality prediction systems have demonstrated the effectiveness of real-time sensing and data validation, which can be mirrored in ATM security frameworks [15]. End-to-end encryption protocols used in 3G/4G mobile networks ensure data confidentiality during transmission and can support secure OTP delivery in ATM systems [16]. A topology-based IoT design for water parameter testing shows how network structures can support secure and seamless user authentication in decentralized systems [17]. Lightweight encryption algorithms with integrity validation can strengthen ATM communication links, much like they do in next-generation mobile networks [18]. Current ATM authentication lacks intelligent classification techniques such as SMOTE-based oversampling, which are known to improve performance in fraud detection systems [19]. Feature extraction methods like DCT-DWT-SVD have been used for secure data retrieval in multimedia systems, suggesting a similar approach can enhance biometric ATM authentication [20]. Hybrid biometric systems that utilize facial and iris recognition show promising results in multi-factor authentication and could complement traditional PIN-based ATM access. Real-time object detection algorithms used in video surveillance can be adapted for ATM terminals to track suspicious behavior or card misuse instantly [22]. Existing ATM systems do not account for dynamic routing or node-based verification methods like those analyzed in AODV protocol simulations for ad hoc networks [23]. Cloud-based frameworks such as Microsoft Azure offer scalable infrastructure that can support real-time OTP generation, delivery, and user behavior logging for ATMs [24].

III. THE EXISTING SYSTEMS

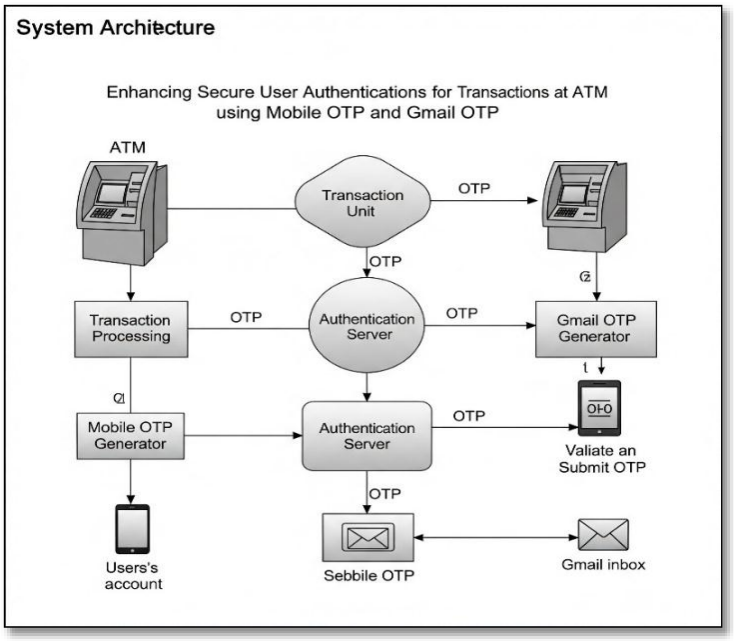
The existing ATM system authenticates transactions via the card and PIN-based system. Thereafter, it grants access to bank customers to several services such as cash withdrawal and deposits, account to account transfers, balance enquiry, top-up purchases and utility bills payment. The ATM system compares the PIN entered against the stored authorization PIN for

every ATM user. If there is a match, the system authenticates the user and grants access to all the services available via the ATM.

If there is a mismatch on the other hand, the user authentication process fails and the user is given two more opportunities to enter a correct PIN. If an incorrect PIN is entered for the third time, the card gets blocked and retained by the ATM. An instance of cash withdrawal on the existing system [8]. Entry of a correct PIN is adequate to authenticate a user to the bank system and thereafter grant access to the system for withdrawal as depicted in Figure The existing system also retains ATM cards after entry on an incorrect PIN thrice thereby eliminating further attempts to gain unauthorized access.

IV. System Architecture

The platform follows a structured approach to career guidance through the following key stages:



The block diagram of the system architecture is depicted in Fig. 1.

Fig 1. Block diagram of ATM using Mobile OTP and Gmail OTP

V. THE PROPOSED SYSTEM

The objective is to deliver second level security to the ATM systems, which can be done through OTP (One Time Password) which is secured and trusted way to add security to the systems. The OTP would be sent to user's registered mobile number and Gmail which would be present in the database. This system provides safest way to do ATM transactions. Whenever person enters account number onto the ATM machine, the system needs PIN to authenticate the user [9] If the PIN number gets verified, the OTP is generated and sent to user's mobile number and Gmail ID. The transaction will succeed only if the user enters valid OTP, otherwise transaction will fail. If the OTP entered is incorrect more than a particular limit the card will be blocked. At the period of opening account, the bank system will ask about mobile registration of the mobile number and Gmail ID of the user. This information will be kept in the bank database for further reference [10]. When User goes to any ATM machine, he/she has to swipe card to machine after that machine and bank server will check validation and authentication of that card, if card and its information is accurate machine will ask the PIN of the user. That card detail and PIN will be confirmed on the banking system. After verification of the card owner and PIN, system will access the user details from database and generate the OTP that will be further send to the mobile number and Gmail ID of the user. When user gets OTP code on mobile and Gmail, he/she has to enter that code on the screen in similar way as PIN. Here we can use this for Aadhar Card mobile OTP [21]11].

OTP adds next layer of security beyond pin. OTP generation algorithms typically make use of pseudo randomness or randomness, making a prediction of successor OTPs by an attacker

difficult, and also cryptographic hash functions, which can be used to derive a value but are hard to reverse and therefore attacker cannot retrieve the data that was used for hash. This is necessary because, it would be easy to predict future OTPs by observing previous ones.

The proposed system ensures secure user authentication by employing a dual-OTP verification mechanism — one OTP sent via SMS to the user's registered mobile number and another sent via Gmail to their registered email address. This two-channel OTP system significantly enhances security by reducing the risk of unauthorized access, as it requires possession of both the mobile device and access to the email account. The OTPs are time-sensitive and randomly generated, ensuring they are valid only for a short duration and cannot be reused. In case of a failed transaction due to incorrect OTP entry, network issues, or expiration of OTPs, the system provides a secure recovery mechanism. The user is prompted to re-authenticate and request new OTPs, which are freshly generated to prevent any misuse of previously issued codes [12]. Additionally, logs of failed attempts are maintained to detect suspicious activity and alert the user accordingly. This multi-factor authentication approach not only strengthens the transaction process but also ensures a user-friendly way to recover from failures without compromising security.

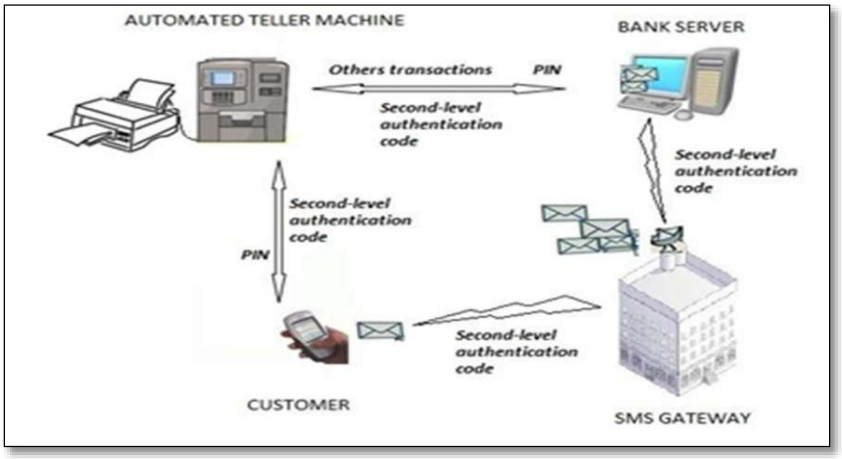


Fig 2. Flowchart of the Proposed System

For any bank transaction OTP is considered as most efficient way to do so. It is efficient because no one will be able to guess the OTP received on user's mobile number and Gmail ID. The OTP can be any random number sent by the bank to the user which is not easily crackable by any hackers.

I. OTP Working-

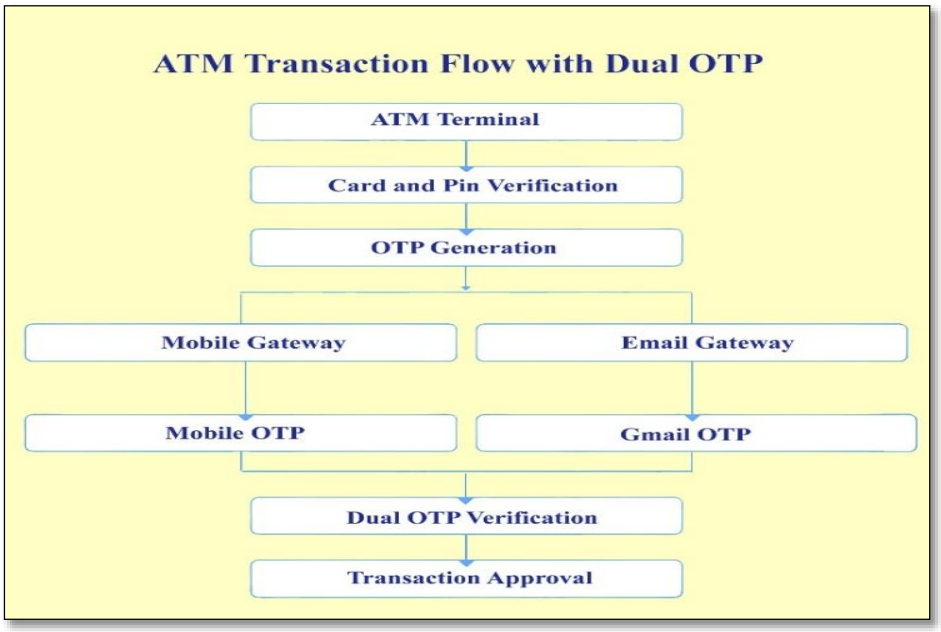


Fig 3. Proposed System Architecture for Enhanced ATM Security with Dual OTP Authentication

An OTP is a 4-digit number received on a user's registered mobile number and Gmail ID with the bank. OTP is preferred over an email because people staying in rural areas use simple phones, where internet connection may not be available and email facilities won't be available in some areas. Either they can use any one facility. The user will receive an OTP immediately after the pin verification. User needs to enter that 4-digit OTP into the system, if correct it will move on for the transaction process. If not, the system will give only 3 chances for the user to enter the OTP even after 3 attempts the OTP is incorrect the system will block that particular account and the notification will be sent to user's registered mobile number.

VI. FUTURE SCOPE

In this Paper, we are dealing with ATM System with OTP System for withdrawal of cash from account. Future scope can be a face recognition or Iris recognition to withdraw cash for more security. System when fully deployed will definitely reduce the rate of fraudulent activities on the ATM machines.

VII. CONCLUSION

The adoption of the ATM as an electronic banking channel has positively impacted the banking industry worldwide because it is very effective and convenient for bank customers. The advent of ATM fraud has however been a menace for many banks all over the world and many banks now aim to eradicate fraud costs to the bank. The proposed system can provide a practical and workable solution that addresses the requirements of the regulatory authority of the banks. The adopted technology of the proposed system is also cheaper to deploy than the biometric authentication technique because it utilizes the components of the existing system. The model can also provide for high withdrawal limits to cater for the demands of a cash-focused customer base. In general, it will positively impact the banking industry and the society by reducing the rising levels of crimes that are associated with ATM transactions. In the future, we will implement the proposed system using the second-level authentication model discussed in this paper.

Nowadays, ATM system is a key problem due to security issues and can be vulnerable too. Banks deliver four digits PIN to the user which can be changed later by the user. After first use, user generally changes the password and keeps password quite guessable. This is the main disadvantage of this PIN type ATM syste. Use of OTP is best and easy way to deal with these security threats. That OTP will be transfer on registered mobile number of the user. And that OTP will be used toward access ATM transactions. Another significant point in proposed system is that it demands lesser changes to the present system of Bank and ATM. That means minor overhead will be required to change the whole system with enhanced security.

VIII. REFERENCES

1. Sruthi. M; S. M. (2019). Secure and Smart Future ATM with One Time Password. IJESC, 1-3.
2. Aruna R; Sudha V; Shruthi G; Rani R; & Sushma V. (2018). ATM Security using Fingerprint Authentication and OTP. IFERP, 4.
3. Mr.S.Vijay sarathi; S.Akash; I.Nihilkumar; M.Nirmal; M.Muthukumaran.(2019). A Novel Methodology Of Integrated ATM Security. IJIRT, 7.
4. Leslie Lamport. (1981) Password Authentication with Insecure Communication Communications. ACM 24.11, 4
5. G.Jayandhi; S.Elphin Samuel; A.Govardhan; A.Logesh; A.Vishnukumar.(2018). Secure Pin Authentication as a Service for ATM. IJAREEIE, 7.
6. Shivam Kumar Rajput; Aniket R. Patne; Amit Varma; Girish Vishe. (2019). Enhanced fingerprint recognition and OTP to improve ATM Security. IJARIIT, 4.
7. Shyamsundar Bhairam; Deepak Agrawal.(2019). Method and System for Performing Card Less Cash Money Withdraws in ATM Machine. IJMERT, 4.
8. Bodagoddu Sharath Chandra Kumar; Jally Venkatesh. (2020). A Paper on Enhanced PIN Security for SBI ATM through Aadhaar Linked OTP or Biometric. IRJET, 5.
9. R. Aruna, V. Sudha, G. Shruthi, R. Usha Rani, V. Sushma, "ATM Security using Fingerprint Authentication and OTP", in International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE) , Volume 5, Issue 5, May 2018

10. V. Prasanan, R. Sandeep Kumar, C. Deepak, R. Deepak Kummar, S. Navin Kumar, “Iot Based Atm Maintenance And Security System” in International Journal of Applied Engineering Research ISSN 0973-4562, Volume 14, Number 6, 2019 (Special Issue).
11. Kavita Hooda, “ATM Security”, in International Journal of Scientific and Research Publications, ISSN 2250-3153, Volume 6, Issue 4, April 2016.
12. Archana et al., International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, October-2013’
13. Nemade, B. P., K. Shah, B. Marakarkandy, K. Shah, B. C. Surve, and R. K. Nagra. "An Efficient IoT-Based Automated Food Waste Management System with Food Spoilage Detection." International Journal of Intelligent Systems and Applications in Engineering 12 (2024): 434-449.
14. Nemade, B. P., K. Shah, B. Marakarkandy, K. Shah, B. C. Surve, and R. K. Nagra. "An Efficient IoT-Based Automated Food Waste Management System with Food Spoilage Detection." International Journal of Intelligent Systems and Applications in Engineering 12 (2024): 434-449.
15. Nemade, Bhushankumar, and Deven Shah. "An IoT-based efficient water quality prediction system for aquaponics farming." In Computational intelligence: select proceedings of InCITe 2022, pp. 311-323. Singapore: Springer Nature Singapore, 2023.
16. V. Kaul, B. Nemade, V. Bharadi, and S. K. N. Khedkar, “Next Generation Encryption Using Security Enhancement Algorithms for End to End Data Transmission in 3G/4G Networks,” Procedia Comput. Sci., vol. 79, pp. 1051–1059, 2016, doi: 10.1016/j.procs.2016.03.133.
17. B. Nemade and D. Shah, “IoT based Water Parameter Testing in Linear Topology,” in 2020 10th Int. Conf. Cloud Comput., Data Sci. Eng. (Confluence), Noida, India, 2020, pp. 546-551. doi: 10.1109/Confluence47617.2020.9058224.
18. V. Kaul, B. Nemade, and V. Bharadi, “Next Generation Encryption using Security Enhancement Algorithms for End to End Data Transmission in 3G/4G Networks,” in Procedia Computer Science, vol. 79, pp. 1051-1059, 2016. [Online]. Available: https://doi.org/10.1016/j.procs.2016.03.133
19. B. Nemade, V. Bharadi, S. S. Alegavi, and B. Marakarkandy, “A Comprehensive Review: SMOTE-Based Oversampling Methods for Imbalanced Classification Techniques, Evaluation, and Result Comparisons,” Int. J. Intell. Syst. Appl. Eng., vol. 11, no. 9s, pp. 790-803, 2023.
20. Sai, N. S. T., Ravindra Patil, Shailesh Sangle, and Bhushan Nemade. "Truncated DCT and decomposed DWT SVD features for image retrieval." Procedia Computer Science 79 (2016): 579-588.
21. Kekre, H. B., V. A. Bharadi, V. I. Singh, V. Kaul, and B. Nemade. "Hybrid multimodal biometric recognition using kekre’s wavelets, 1d transforms & kekre’s vector quantization algorithms based feature extraction of face & iris." In International Journal of Computer Applications (IJCA), Special Issue for ACM International Conference ICWET, pp. 29-34. 2011.
22. Nemade, Bhushan, and Vinayak Ashok Bharadi. "Adaptive automatic tracking, learning and detection of any real time object in the video stream." In 2014 5th International Conference-Confluence The Next Generation Information Technology Summit (Confluence), pp. 569-575. IEEE, 2014.
23. P. Patel, R. Bansode, and B. Nemade, “Performance evaluation of MANET network parameters using AODV protocol for HEAACK enhancement,” in Procedia Computer Science, vol. 79, pp. 932-939, 2016.