

An introduction to using QR codes in web portals for synchronizing calendar events over phones

Inder Pal Singh Sethi, Om Pradyumana Gupta, Sulbha Bhaisare, Ritesh Kumar Dwivedi,
Misha Kapoor

Electronic Transaction Aggregation and Analysis Layer (eTaal), National Informatics Centre, Ministry of Electronics and Information Technology, Government of India, New Delhi, India

Article Info

Article history:

Received month dd, yyyy

Revised month dd, yyyy

Accepted month dd, yyyy

Keywords:

Mobile phone

One-time password (OTP)

Quick response code (QR code)

Secret data

Sensitive information

User authentication

ABSTRACT

An optical label with machine-readable information about the object it is attached to is called a quick response (QR) code. QR codes frequently hold information for a tracker, locator, or identifier that directs users to a website or application. To efficiently store data, a QR code has four standardized encoding modes: kanji, byte or binary, alphanumeric, and numeric. As a means of identifying a wide range of commercial goods, including transactions, ads, and other public notices, the QR code gained popularity. In our web portal, the proposed QR code model synchronizes all the event details synchronously in the mobile calendar. QR code is used for web-to-mobile data transfer, saving events or meeting details in the mobile calendar. Anyone with a smartphone can view the data encoded in a QR code by scanning it. Although it makes it easier for end users to decode QR codes, verifying access to the encoded data is a cause for worry. Our proposed model validates access to data through the QR code, allowing only authorized personnel to access data. To ensure accessibility control, the proposed model has the functionality of a one-time password (OTP) that enhances application security. The model achieved an average decoding speed of 157 milliseconds with an error rate of 0.38%.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Sulbha Bhaisare

Electronic Transaction Aggregation and Analysis Layer (eTaal), National Informatics Centre, Ministry of Electronics and Information Technology, Government of India, New Delhi, India

New Delhi, India

Email: sulbha.bhaisare@nic.in

1. INTRODUCTION

Quick response codes, also known as QR codes, are machine-readable optical labels that include information on the related item or product [1]. The automotive sector was the first to adopt the QR system because of its quick readability and larger storage capacity when compared to conventional UPC barcodes [2]. Product monitoring, item identification, time tracking, document management, and general marketing are a few examples of application.

Information is only coded in one dimension or one direction in barcodes. However, information is encoded in two directions when using a QR code: vertically and horizontally. It is easily readable and has a significant amount of storage capacity [3], [4].

A QR code is made up of black squares placed in a square grid on a white background. A camera or other imaging device can read this arrangement, and the Reed-Solomon error correction technique [5] is used to analyze the image until it can be understood correctly [6]. Next, the necessary information is taken out of patterns seen in the image's vertical and horizontal components [7].

This paper aims to provide OTP-based QR codes for web portals that contain all the event or meeting information for a day. Users need to scan the QR code that prompts them to enter the one-time password (OTP) to authenticate the users' phone numbers. On entering the OTP, all engagement information is synced and saved in the mobile's default calendar [8].

An application that allows users to manage engagements related to the user's daily activities is available on both desktop and mobile. Currently, most applications allow users to sync events and engagements on specific Calendars such as Google, Outlook, and iOS. However, syncing engagement details saved on the application with the default calendar app (mobile devices) has not been explored and remains a challenge [8], [9].

2. LITERATURE REVIEW

2.1. Quick response (QR) code

Japan's Denso Wave Incorporated invented QR codes for the first time in 1994 [10]. Toyota's parent business is Denso Wave. The purpose of QR codes was to help auto manufacturers keep track of their inventory of automotive parts. In an effort to encourage the widest possible use of QR codes, Denso Wave announced that it will not exercise its option to keep the patent rights to the code. Therefore, QR codes are becoming a widely used public code that may be utilized without expense or concern over patent issues.

A matrix code is a QR code. In order to match the efficiency of portable devices like smartphones, they must store a large volume of data and decrypt it quickly compared to one-dimensional barcodes. When creating two-dimensional matrix codes, these two factors are taken into account. The likelihood of security becomes crucial when a barcode holds sensitive data or private information. People don't know if a QR code will lead them to a website containing malware or trustworthy information because all they see is a square barcode with a unique design. Recently, a QR code has been used in many application streams, for example, related to lecturers, security, or advertising, and is rapidly gaining popularity. A growing number of people are becoming acquainted with this technology and utilizing it sensibly. As the number of smartphone users increases, so does the popularity of QR codes, which are quickly gaining widespread recognition. Given how widely used QR codes are, their protective aspect is essential for issues like data tampering and leaking [11].

The data contained in QR codes can be extracted by mobile devices. However, when sending private information like coupons, e-tickets, and other sensitive data via QR codes, security concerns are raised despite the ease. Furthermore, because QR codes are module-oriented as opposed to pixel-oriented, current secret hiding techniques are inappropriate for use with QR codes. Any barcode decoder may accurately extract the ordinary data content (e.g., URL) from the generated QR code; this does not impact the scan ability of the code. Moreover, the secret key is the sole way for authorized people to access the hidden confidential data. Applications for the QR system that are trustworthy and safe can be obtained using this planned approach [12].

2.2. Password-based authentication

Three categories can be used to group the traditional user authentication factors: i) what you know (password and username), ii) what you have (smart cards), and iii) what you are (fingerprint information). One of the most popular and extensively used forms of authentication is password-based authentication, sometimes referred to as "one-factor authentication" [11]. It has certain inherent benefits and uses, but there are also clear drawbacks: Users frequently repeat their passwords on multiple websites and use passwords that are straightforward and quick to figure out [13], [14]. As a result, certain attackers may be able to obtain a user's password through phishing and offline guessing attempts. In the interim, the server keeps a lot of data unencrypted, which is easily taken by hackers. Consequently, the disclosure of the user's personal information could jeopardize the crucial security of the user [15]. Various efforts and attempts to improve password security, and the idea of OTP-based authentication were proposed [16]. As the name implies, an OTP authentication eliminates the need for the server to keep track of the user's password table by using a password that is only valid for a set period of time. It significantly increases security by thwarting dictionary and password-guessing attacks [17]. Nevertheless, a OTP is created in relation to particular difficult algorithms, serving as a support function to aid in the completion of the authentication procedure [18].

2.3. OTP-based authentication

An automatically generated secret word, either numeric or alphanumeric, known as an OTP, is used to verify a user's identity for a specific transaction or login session. OTP security tokens are pocket-sized key fobs or smart cards with microprocessors that generate an alphanumeric or numeric code to verify access to the framework or string [6]. Based on how the token is made, this secret code is reset every 30 or 60 seconds.

A device that can generate an OTP using an algorithm and cryptographic keys is delivered to the user. By using a comparable method and keys, a confirmation server on the server side can verify the validity of the secret key. Insider information that is communicated by the verification server and the user's OTP application is necessary for OTP-based validation techniques. The hashed message authentication code (HMAC) algorithm is used to generate OTPs along with a moving element, such as occasion counters or time-sensitive data: time-based one-time password (TOTP) and HMAC-based one-time password (HOTP). For more noticeable security, the OTP values have moment or second timestamps. A committed application on the endpoint, an email, or an SMS-based instant message are some of the ways that a client can receive the one-time secret word [19].

With secret key security, the one-time secret phrase keeps a strategic distance from common pitfalls acknowledged by IT chairmen and security directors. They do not have to worry about following structural guidelines, using weak or known passwords, exchanging login information, or using the same secret password across several databases and services. One more benefit of utilizing OTPs is that they expire in a matter of minutes, preventing hackers from obtaining the secret codes and using them again [20]–[22].

3. METHOD

For the mentioned problem we create a system or web portal that provides flexibility to the users to synchronize their events or meetings with the user's mobile without performing any login activity.

a. Login phase

There are three steps in the login phase.

- Step 1. Users send a login request with encrypted credentials to a server through a web portal (desktop).
- Step 2. The server authenticates the user
- Step 3. Users create engagements - events and meeting

Users want to synchronize their web portal meeting or events information with mobile devices without performing any login process. For the same case, the users have to authenticate their devices. For the device authentication mechanism whenever users start scanning the process of the QR code, they get OTP on their mobile device.

b. Authentication phase

- Step 1. On the web portal after successful login 'users' have to click a QR code button to generate a QR code as shown in Figure 1.

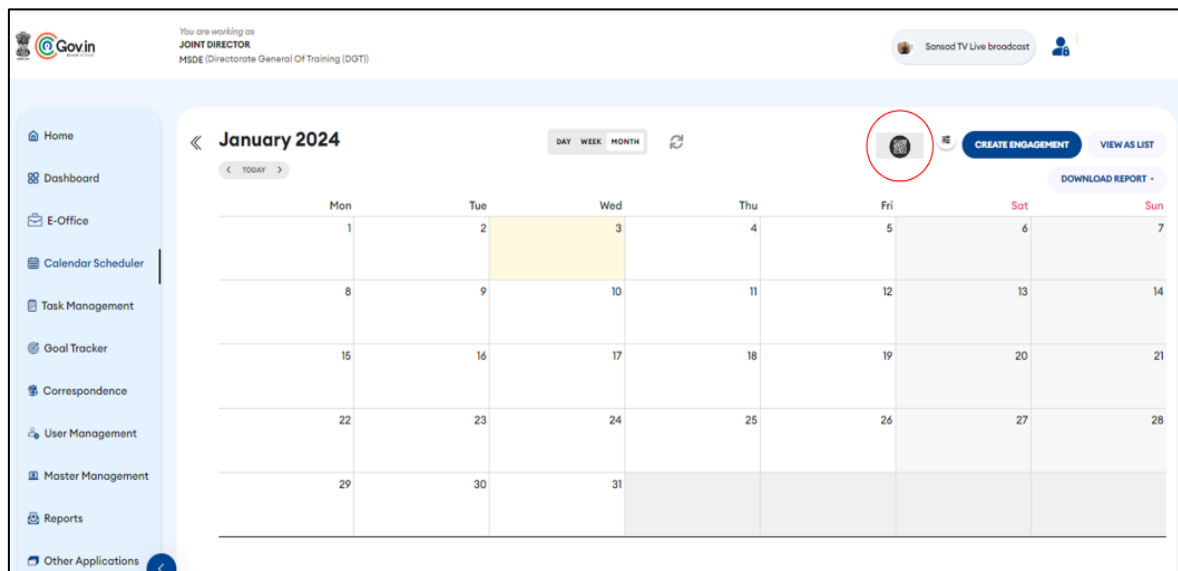


Figure 1. QR code button for generating and displaying QR code [23]

- Step 2. Users scan the OTP-based QR codes, as shown in Figure 2, as soon as the users scan the QR code using mobile devices ask for OTP then the users need to enter OTP which was sent to authenticate the devices as shown in Figure 3 [12].



Figure 2. OTP-based QR code for scanning

OTP Code Verification

Enter the OTP code sent to your phone:

Verify OTP Code

Figure 3. Portal screen on the mobile devices for OTP

- Step 3. After successful verification of OTP, users are able to download the file formatted ICS (.ics) [24].
- Step 4. After downloading the ICS files, users need to add subscription calendars on their mobile devices, as shown in Figure 4, and then the ICS files in the phone calendars ask to add all events or meetings, as shown in Figure 5. Figure 6 shows the phone calendar after adding an event or meeting [25].

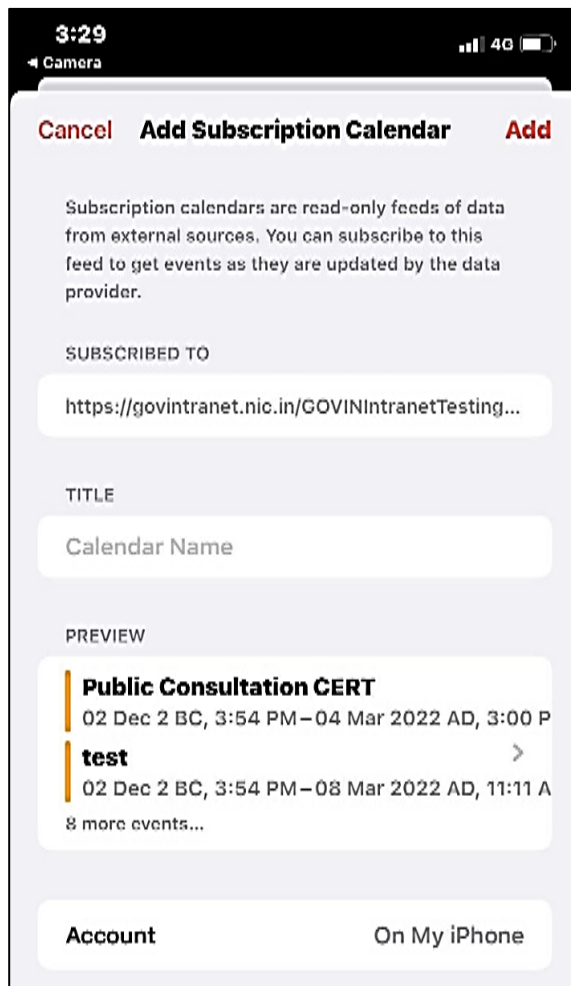


Figure 4. Add subscription calendar to the mobile device

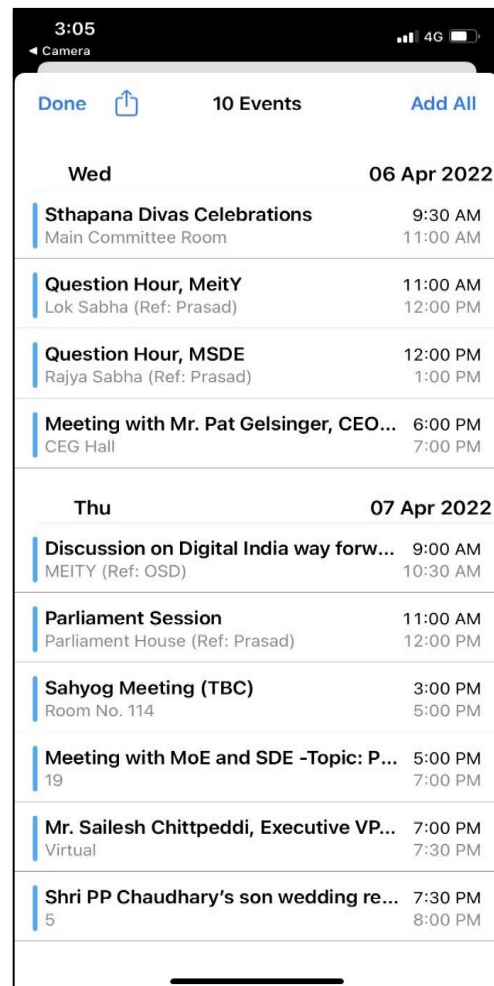


Figure 5. An ICS file in the phone calendar to add all events or meetings

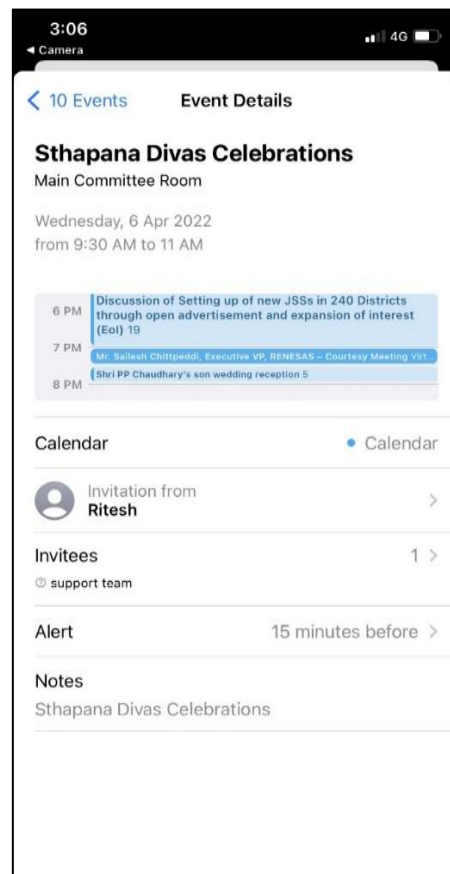


Figure 6. Phone calendar after adding an event or meeting

4. CONCLUSION

In this paper, an authentication technique based on OTP QR code is provided. A computer, a user, a mobile phone, and a remote server are the four entities involved in the scheme. The solution adopts an OTP QR code to improve the security of authentication. Our method is more user-friendly, safe, and straightforward, and it has great practical value.

In our web portal, the OTP authentication-based QR code is used to provide all the event details and add all events or meetings to a mobile device calendar, QR code used for web portals to mobile device data transfer saves event or meeting details to the mobile calendar without using any portal authentication on a mobile device. Any user can access the data stored in a QR code by scanning it with a smartphone or other mobile device. Although it makes decoding QR codes easier for end users, it is also a worry if you wish to limit who can access the encoded data. Your QR code's data is restricted by our system so that only authorized workers can access it. Through the use of OTP-protected QR codes, our web portal successfully enables users of the portal to scan OTP-protected QR codes and synchronize all their meeting or event details in their mobile device calendar and send user notifications about the event fifteen minutes before the meeting or events.




REFERENCES

- [1] P.-Y. Lin, W.-S. Lan, Y.-H. Chen, and W.-C. Wu, "A confidential QR code approach with higher information privacy," *Entropy*, vol. 24, no. 2, p. 284, Feb. 2022, doi: 10.3390/e24020284.
- [2] A. Mishra and M. Mathuria, "A review on QR code," *International Journal of Computer Applications*, vol. 164, no. 9, pp. 17–19, Apr. 2017, doi: 10.5120/ijca2017913739.
- [3] K. Krombholz, P. Fruhwirt, T. Rieder, I. Kapsalis, J. Ullrich, and E. Weippl, "QR code security -- how secure and usable apps can protect users against malicious QR codes," in *2015 10th International Conference on Availability, Reliability and Security*, Aug. 2015, pp. 230–237. doi: 10.1109/ARES.2015.84.
- [4] L. Várallyai, "From barcode to QR code applications," *Journal of Agricultural Informatics*, vol. 3, no. 2, Jan. 2013, doi: 10.17700/jai.2012.3.2.92.
- [5] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *Journal of the Society for Industrial and Applied Mathematics*, vol. 8, no. 2, pp. 300–304, Jun. 1960, doi: 10.1137/0108018.




- [6] L. N. Childs, "An introduction to Reed–Solomon codes," 2019, pp. 259–272. doi: 10.1007/978-3-030-15453-0_15.
- [7] M. Eminagaoglu, E. Cini, G. Sert, and D. Zor, "A two-factor authentication system with QR codes for web and mobile applications," in *2014 Fifth International Conference on Emerging Security Technologies*, Sep. 2014, pp. 105–112. doi: 10.1109/EST.2014.19.
- [8] M. Alajmi, I. Elashry, H. S. El-Sayed, and O. S. Farag Allah, "Steganography of encrypted messages inside valid QR codes," *IEEE Access*, vol. 8, pp. 27861–27873, 2020, doi: 10.1109/ACCESS.2020.2971984.
- [9] M. M. Din and A. Fazal Fazla, "Integration of web-based and mobile application with QR code implementation for the library management system," *Journal of Physics: Conference Series*, vol. 1860, no. 1, p. 012018, Mar. 2021, doi: 10.1088/1742-6596/1860/1/012018.
- [10] "QR Code development story," *Denso Wave*. <https://www.denso-wave.com/en/technology/vol1.html> (accessed Sep. 11, 2024).
- [11] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The quest to replace passwords: a framework for comparative evaluation of web authentication schemes," in *2012 IEEE Symposium on Security and Privacy*, May 2012, pp. 553–567. doi: 10.1109/SP.2012.44.
- [12] S. H. Seo, C. Y. Choi, G. Y. Lee, and H. K. Choi, "QR code based mobile dual transmission OTP system," *The Journal of Korea Information and Communications Society*, vol. 38B, no. 5, pp. 377–384, May 2013, doi: 10.7840/kics.2013.38B.5.377.
- [13] M. B. Barcena and C. Wueest, *Security response: insecurity in the Internet of things*. Mountain View: Symantec, 2015.
- [14] P. Kieseberg *et al.*, "QR code security," in *Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia*, Nov. 2010, pp. 430–435. doi: 10.1145/1971519.1971593.
- [15] A. Gupta, A. Singh, A. Tripathi, and S. Sharma, "Two-factor authentication using QR code and OTP," 2024, pp. 105–114. doi: 10.1007/978-981-99-6906-7_10.
- [16] H. Kanakia, S. Shaikh, Y. Koyande, and H. Jain, "Secure authentication via encrypted QR code," in *2024 IEEE 9th International Conference for Convergence in Technology (I2CT)*, Apr. 2024, pp. 1–5. doi: 10.1109/I2CT61223.2024.10544035.
- [17] Miss. Shweta Kamble, Miss. Pooja Kendre, Miss. Ayesha Siddiqua, and Mr. Deshpande G. R., "E-authentication system using QR code and OTP," *International Journal of Advanced Research in Science, Communication and Technology*, pp. 24–28, Dec. 2023, doi: 10.48175/IJARSCT-14204.
- [18] Young Sil Lee, Nack Hyun Kim, Hyotaek Lim, HeungKuk Jo, and Hoon Jae Lee, "Online banking authentication system using mobile-OTP with QR-code," in *5th International Conference on Computer Sciences and Convergence Information Technology*, Nov. 2010, pp. 644–648. doi: 10.1109/ICCIT.2010.5711134.
- [19] J. Rajendran and M. H. I. Hamzah, "QR code based event management system," *Applied Information Technology And Computer Science*, vol. 2, no. 1, pp. 124–143, 2021.
- [20] B. Rodrigues, A. Chaudhari, and S. More, "Two factor verification using QR-code: a unique authentication system for Android smartphone users," in *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)*, Dec. 2016, pp. 457–462. doi: 10.1109/IC3I.2016.7918008.
- [21] S. K. Choudhary, R. Temkar, and N. R. Bhatta, "QR code based secure OTP distribution scheme for authentication in net-banking," *International Journal of Information Science and Intelligent System*, vol. 2, no. 4, pp. 115–121, 2013.
- [22] R. Danthy, K. Pratham Pai, and V. Rao, "Secure online banking authentication system using time bound password," in *2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT)*, Feb. 2024, pp. 130–135. doi: 10.1109/IC2PCT60090.2024.10486295.
- [23] "Gov.in secure intranet." <https://govintranet.nic.in/GOVINtranet/Login.aspx> (accessed Feb. 01, 2024).
- [24] C. Branden, *QR codes - The ultimate guide book*. QReactive Studios, 2011.
- [25] "How to use QR codes for business effectively," *Bitly*, 2024. <https://bitly.com/blog/qr-code-for-business/> (accessed Sep. 11, 2024).

BIOGRAPHIES OF AUTHORS






Inder Pal Singh Sethi    is one of the prominent senior scientists of Govt. of India. Presently he is working as Deputy Director General (DDG) in the National Informatics Centre, Ministry of Electronics and Information Technology, Govt. of India. He is a master's in computer (MCA) from Thapar Institute of Engineering and Technology, Patiala. He has been working for over 35 years in the National Informatics Centre with a demonstrated history of handling important IT and e-governance projects. He has demonstrated his excellence in the field of Digital India Program of Govt. of India. His areas of interest include artificial intelligence, enterprise architecture design, and business process reengineering. He can be contacted at sethi@gov.in.






Om Pradyumana Gupta    is working as Scientist-E in the National Informatics Centre, Ministry of Electronics and Information Technology, Govt. of India. He has 22 years of vast experience in the field of research and development in Information Technology. He is also pursuing his Ph.D. in the field of artificial intelligence. Earlier he received the degree of M.Tech in Information Technology and MCA. He is actively spearheading very critical and national-level projects like Gov. in Secure Intranet, Dididhan Dashboard, and eTaal. His areas of interest include robotics, artificial intelligence, computer vision, and deep learning. He can be contacted at op.gupta@gov.in or op.gupta@nic.in.






Sulbha Bhaisare    is a Deputy Director (IT) at the National Informatics Center, New Delhi, India, she holds a Bachelor of Engineering in Computer science and Engineering from RGPV University, Madhya Pradesh, India; a Master of Engineering in Computer Engineering from RGPV University, Madhya Pradesh, India; Post Graduate Diploma in Embedded Systems and Design (PG-DESD) from Centre for Development of Advanced Computing (C-DAC), Noida. Her research interests include machine learning, deep learning, information security, artificial intelligence (neural networks, fuzzy logic, genetic algorithm, data mining, information science, and human-computer interaction. She can be contacted at sulbha.bhaisare@nic.in.



Ritesh Kumar Dwivedi    is working as Scientist-D in the National Informatics Centre, Ministry of Electronics and Information Technology, Govt. of India. He has 18 years of experience in IT. He is also pursuing his Ph.D. in the field of Artificial Intelligence, Neural Machine Translation for Indian Regional Languages. Earlier he received the degree of M.Tech. in Information Technology and MCA. He is actively spearheading very critical and national-level projects like Gov.In Secure Intranet, and Dididhan Dashboard. His areas of interest include NLP, artificial intelligence, computer vision, and deep learning. He can be contacted at ritesh.dwivedi@nic.in.



Misha Kapoor    is a senior scientist working as a joint director with the Government of India. She is working on some research in computational intelligence, e-governance, and digital payment Systems. She likes to study and work in India. She has a talent for learning languages. She likes to study e-governance, algorithm designs, and computational intelligence. Her main research directions include artificial intelligence, digital payment systems, e-governance computational intelligence, intelligent control systems, and network optimization. She can be contacted at misha.kapoor@nic.in.