

Manish Kumar Yadav

Email ID: manishyy089@gmail.com

Phone: +91- 8961432377

PROFESSIONAL SUMMARY:

- A young IT professional with a total experience of 3.5 years in Backend Development, API Design, Application Integration, and Process Automation.
- Experienced in integrating and managing various payment gateways, ensuring secure, seamless transaction processing and compliance with industry standards.
- Technically conversant with **HTML, MySQL, PostgreSQL, Kotlin, Java, Spring Boot, Hibernate JPA, Micro Services & Rest APIs, Payment Gateway, Webhooks and SMS gateway, Third Parties API Integration.**
- Expertise in end-to-end payment gateway integration, including transaction flow, webhook handling, refunds, and secure tokenization.
- Quickly adapt to new technology and work environment.

QUALIFICATIONS:

- **B. Tech in Computer Science & Engineering** from Seacom Engineering College, (MAKAUT)
- Diploma in **Computer Science & Technology** from Bengal Institute of Technology.

EXPERIENCE:

- Working as Software Engineer in **StableOne Software PVT LTD**, Kolkata, from 01th Aug 2024 to Present.

TECHNICAL SKILLS:

- Operating System: Windows
- Languages: HTML, SQL, Kotlin, Java
- Database: MySQL, PostgreSQL, Redis
- Tools: Git, GitHub, Visual Studio, VS Code, Eclipse, IntelliJ IDEA
- Testing: Swagger, Postman, Junit 5

PROFESSIONAL EXPERIENCE:

- **Stableone Software PVT LTD, Kolkata** Aug 2024 – Till Now

Project Title	Novo Remitall
Clients	Internal
Duration	Mar 2025 – Till Now
Technology	Java 17, Kotlin, Spring Boot, Micro services, Hibernate JPA, Maven, PostgreSQL, Junit 5, RabbitMQ,
Database	PostgreSQL, Redis
Description	<p>Novo Remitall is a client project that integrates multiple essential services to provide a comprehensive solution. It utilizes ATLPay for its Payment System, ensuring secure and efficient financial transactions. For identity verification, it incorporates Liveness to handle KYC and facial recognition processes. The project also includes a Sanction Check module to screen customers for any criminal activity or legal restrictions. Additionally, Authentication is managed through a common login system, providing a unified and secure access mechanism across all services.</p>
Role / Responsibility	As part of the Novo Remitall project, my primary role was to integrate all associated modules —including ATLPay , Liveness , Sanction Check , and Authentication —into a unified system. I achieved this by using REST Template in a Spring Boot environment to enable seamless communication between services. My responsibilities included designing and implementing REST-based API calls , handling request/response transformations , and ensuring secure data transfer across services. Additionally, I performed code modifications and enhancements in individual projects where necessary to support integration, maintain data consistency, and optimize performance. I also implemented error handling, fallback strategies, and ensured proper logging to maintain reliability in service orchestration.

Project Title	AUTHENTICATION
Clients	Internal
Duration	Jul 2024 – Nov 2024
Technology	Java 17, Kotlin, Spring Boot, Micro services, Hibernate JPA, Maven, PostgreSQL, Junit 5, RabbitMQ,
Database	PostgreSQL, Redis
Description	Authentication is the process of verifying the identity of a user, application, or system before granting access to resources. It ensures that only authorized users can log in and perform actions by validating credentials like usernames, passwords, OTPs, tokens, or biometric data. In a multi-application environment, authentication can be centralized using methods like Single Sign-On (SSO), OAuth2, or JWT tokens to allow a user to log in once and securely access multiple connected applications without needing to authenticate separately each time.
Role / Responsibility	Design and develop secure authentication APIs to validate users and applications, ensuring only authorized access. Implement login, token generation (JWT), and user validation logic. Manage Single Sign-On (SSO) across applications, validate application credentials token expiration, and maintain authentication logs for security.

Project Title	LIVENESS (Liveness Check)
Clients	Internal
Duration	Oct 2024 – Jan 2025
Technology	Java 17, Kotlin, Spring Boot, Micro services, Hibernate JPA, Maven, PostgreSQL, Junit 5, RabbitMQ,
Database	PostgreSQL, Redis
Description	A KYC Liveness Check is a process used to verify whether the person undergoing identity verification is a live human and not a robot, fraudster, or impersonator. It typically involves biometric checks like facial recognition or live video capture , where the user may be asked to perform certain actions (e.g., blinking, smiling, or turning their head) to prove they are a real person. The system detects if the video is real-time, ensuring that it is not a pre-recorded or manipulated video, preventing fraud and ensuring the identity is genuine. This process is crucial for preventing identity theft, synthetic fraud, and bot-related activities in remote onboarding and verification systems.
Role / Responsibility	Design and implement KYC Liveness Check processes to ensure users are real and not fraudulent. Develop APIs for real-time video or image capture, integrate facial recognition or biometric validation, and implement anti-fraud measures such as detecting spoofing or robot behavior. Ensure that the system can accurately verify user authenticity, prevent identity theft, and maintain compliance with security standards and regulations.

Project Title	SANCTIONS (Sanctions Check)
Clients	Internal
Duration	Jan 2025 – May 2025
Technology	Java 17, Kotlin, Spring Boot, Micro services, Hibernate JPA, Maven, PostgreSQL, Junit 5, RabbitMQ
Database	PostgreSQL
Description	Sanction Check is a process used to verify if a customer or individual is listed in any sanction or watch list databases, typically maintained by government agencies or international organizations. The system checks for keywords or flags related to criminal records, fraudulent activity, or terrorism associations . The process involves querying external databases or websites to determine if the individual or entity matches any records. If a match is found, the system alerts the relevant authorities or the organization, ensuring compliance with legal and regulatory requirements. This process helps prevent conducting business with individuals or organizations involved in illegal or unethical activities.
Role / Responsibility	Design and implement the Sanction Check process to ensure customers or individuals are not flagged for criminal, fraudulent, or prohibited activities. Integrate APIs to query sanction lists from external sources (e.g., OFAC, UN, World Bank), and develop automated systems for real-time checks. Ensure accurate detection of flagged entities, alerting the system when a match is found, and maintaining compliance with regulatory and legal requirements. Also responsible for regular updates to sanction list data and ensuring the security and integrity of the check process.

- **Agpaytech India PVT LTD, Kolkata**

Dec 2023 – Jul 2024

Project Title	ATLPAY (Payment Aggregator)
Clients	Internal
Duration	DEC 2023 – Jul 2024
Technology	Java 11, Kotlin, Spring Boot, Hibernate JPA, Maven, PostgreSQL, Native Query (SQL), Junit 5, RabbitMq
Database	PostgreSQL, Redis
Description	ATLPAY is a payment aggregator offering UK-based clients access to multiple payment gateways with multi-currency support. Based on merchant we provide payment gateway through payment like Volume, PayDough, ECP, Ryvyl, Nuvie Payment and Cryptonix. It is one kind of Payment Gateway.
Role / Responsibility	As a developer, my role involves designing and developing secure, scalable RESTful APIs using the Spring Boot framework to integrate various payment gateways (such as Paydough, Volume, ECP, Ryvyl, Cryptonix, and Nuvie). I am responsible for implementing payment initiation, transaction processing, refunds, and webhook handling to capture real-time payment events. My responsibilities also include storing transaction and webhook data efficiently in PostgreSQL. I maintain clear API documentation and implement testing strategies (unit and integration tests), ensure PCI DSS compliance, and set up monitoring and alert systems to ensure the reliability and security of payment operations.

- Sigmen Technologies Solutions PVT LTD, Kolkata

Jun 2022 – Nov 2023

Project Title	Sigma Patient Portal
Clients	Internal
Duration	Jun 2022 – Nov 2023
Technology	Java 8, Spring Boot, Hibernate JPA, Spring MVC, Maven, MySQL, Native Query (SQL).
Database	MySQL
Description	Patient Portal - is a Hospital Information Management System that can perform any Hospital-related functionalities like Lab Booking, OPD Appointment Booking, Billing and Payment, Patient Medical history, Payment Gateway Integration, webhook, SMS gateway Integration, JWT token, Blog Posting and Comment Features for Patient, Authentication, Spring Security seamlessly.
Role / Responsibility	Design and develop RESTful APIs using Spring Boot framework to provide seamless access to patient-related functionalities. Utilize Spring MVC architecture to structure the application, ensuring efficient routing and handling of requests. Integrate web services for communication with external systems and services, enhancing the portal's capabilities. Utilize Hibernate JPA to manage interactions with the MySQL database, ensuring efficient storage and retrieval of patient information.

PERSONAL DETAILS:

- Name Manish Kumar Yadav
- Date of Birth 02 August 1997
- Language Known Hindi, English & Bengali