

PRODUCT OVERVIEW

Securelay Services Overview

Protect sensitive data. Govern how it is used. Prove what happened.

Securelay helps organizations use sensitive data in applications, documents and AI while keeping access controlled and recorded.

Securelay Privacy Vault

Stores sensitive values in encrypted form. Applications use protected references instead of copying raw personal data everywhere.

Protected AI Runtime

Protects detected personal data before approved AI use. Every reveal is checked against policy, purpose, consent and usage limits.

SecureDocs

An organization-wide protected document workspace for using documents with approved AI workflows.

DPDP Implementation + DPO Support

Policy setup, consent and rights workflows, evidence preparation and ongoing privacy operations support.

HOW THE PLATFORM WORKS

1 PROTECT

Replace detected sensitive values with protected references.

2 DECIDE

Apply role, purpose, attribute and consent checks.

3 USE

Let approved apps, documents and AI continue their work.

4 PROVE

Create value-free receipts and verifiable audit evidence.

Why this matters now

India's privacy framework is moving into operational deadlines. Organizations need working controls, clear ownership and evidence - not only policy documents.

13 Nov 2026

Consent Manager registration provisions begin under the phased DPDP timetable. [\[6\]](#) [\[7\]](#)

13 May 2027

Core obligations covering consent, rights, safeguards, breach reporting and enforcement take effect. [\[6\]](#) [\[7\]](#)

72 hours

The final Rules require a detailed breach update to the Board within 72 hours, unless a longer period is allowed. [\[7\]](#)

FROM PRINCIPLE TO DAILY CONTROL

The final Rules name encryption, obfuscation, masking, virtual tokens, access controls, logs, monitoring and review as practical safeguards. [\[7\]](#) Securelay connects these controls to protected data use and evidence.

Operational work organizations must prepare

Data discovery and mapping

Know which systems, files, vendors and AI workflows handle personal data.

Clear notice and consent

Explain the data and purpose, record the decision and support withdrawal.

Purpose-bound access

Allow data use only for the approved person, role, purpose and request context.

Data rights workflows

Handle access, correction, erasure and grievance requests with reliable status.

Breach readiness

Keep owners, communication steps, facts and reporting evidence ready before an incident.

Logs and review

Record access and decisions so actions can be reviewed and independently checked.

Services that protect sensitive data

Keep original values under control while business systems continue to work with protected references.

Encrypted Privacy Vault

Keeps original sensitive values encrypted inside the vault. Other systems work with protected references.

PII Detection and Redaction

Finds supported personal-data types in text and files, then removes or protects the detected values. Detection is bounded and reviewed, not claimed to be perfect.

Pseudonymization and Tokenization

Replaces sensitive values with protected tokens. The original can be revealed only through approved controls. Tokens are pseudonyms, not anonymous data.

Data Masking

Shows only the approved part of a value, such as the last four digits or an email domain.

Protected File Processing

Protects detected sensitive content in PDF, DOCX, XLSX, JSON and supported image workflows before downstream use.

Audio Transcript Protection

Accepts recorded audio, creates a transcript through the configured service and protects detected PII in that transcript. It does not capture live voice.

SecureDocs

An organization-wide protected document workspace. The founder invites members through the Securelay Console; every admitted member receives the same fixed SecureDocs scope.

Services that govern access and AI

Securelay checks the person, purpose, request context, consent state and usage limits before a governed reveal.

AI Governance

Protects detected sensitive content before approved models or agents receive it. It records what the configured AI workflow received.

Controlled Reveal / Rehydration

Turns a protected reference back into the original value only after the required checks pass.

RBAC - Role-Based Access

Sets broad access from an assigned role, such as operator, privacy staff or auditor.

PBAC - Purpose-Based Access

Checks why the data is being used. A valid role can still be denied when the declared purpose is not allowed.

ABAC - Attribute-Based Access

Uses approved details about the request and record for more specific access decisions.

Consent Management

Records consent, checks whether it covers a purpose and supports withdrawal. Withdrawal blocks later governed reveals of consent-bound data.

Velocity Limits and Kill Switch

Limits how quickly protected data can be revealed. Operators can stop access when risk or unusual activity appears.

Dual Approval for High-Risk Changes

High-risk actions can require a second authorized person before they are completed.

Important

RBAC, PBAC and ABAC are platform-wide policy controls. They are not separate membership levels inside SecureDocs.

Privacy operations, evidence and support

Connect day-to-day privacy work with technical evidence, so teams can move from written policy to governed operations.

Data Rights / DSAR

Tracks access, correction and deletion requests from filing through completion.

Correction Workflow

Applies approved corrections while keeping the action tied to the request and audit trail.

Crypto-Shred Erasure

Destroys the key material needed to recover a person's protected data and records the erasure action.

Retention Controls

Finds data that has reached its configured retention limit and supports governed deletion.

RoPA

Maintains a versioned Record of Processing Activities and a technical annex for evidence and review.

Breach Register

Records breach cases, status and reporting actions in one governed workflow.

Value-Free Audit Receipts

Records identifiers, scopes, counts and hashes without putting plaintext values or secrets into the receipt.

Offline Verification + AI Evidence

Lets an auditor verify an exported audit chain without trusting the live dashboard. Session evidence shows what the configured AI workflow received.

Integrations + Service Accounts

Connects through APIs, SDKs, CLI and MCP with least-privilege service accounts. The server applies the same policy and receipt rules.

DPDP Implementation + DPO Support

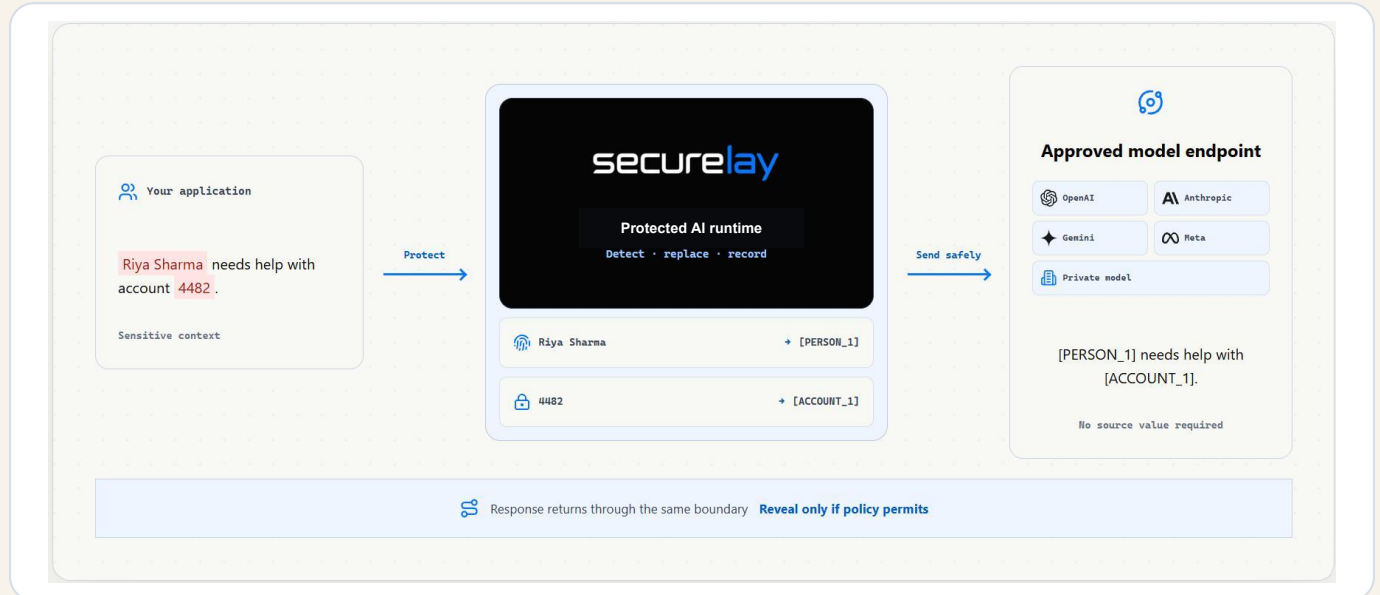
Helps teams map data, configure policies, set up consent and rights workflows, prepare evidence and run ongoing privacy operations.

Product boundary

These controls support privacy operations and evidence. They do not by themselves prove legal compliance, certification or that every sensitive value was detected.

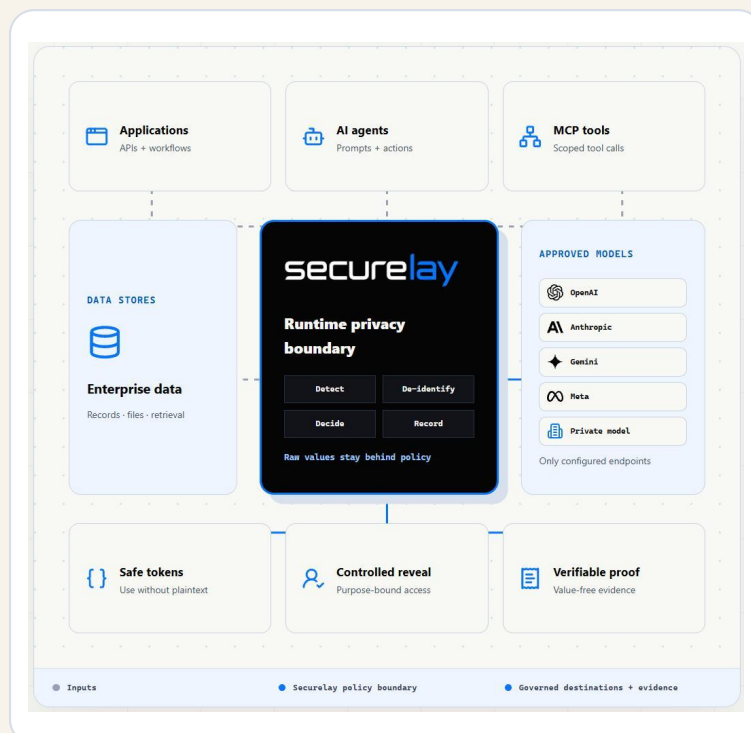
How the protected data path works

The diagrams below come from the current Securelay pitch deck and show the configured protection boundary and controlled AI flow.



Illustrative AI flow

Only configured paths are governed. Securelay is not a universal network gateway.



WHAT THE BOUNDARY DOES

- Detects supported sensitive values.
- Replaces them with protected references.
- Checks access, purpose and consent.
- Controls approved reveal operations.
- Records value-free evidence.

SecureDocs in action

The AI receives the protected view. An authorized user can view the real document locally after the configured controls pass.

PROTECTED VIEW SENT TO AI

File Edit Window Help

Securelay Harish11.pdf

Home Annotate Edit Pages View

Securelay AI Summarize AI Key Points Highlight Underline Strikethrough Search Edit text 1 of 2 155% Fit width Fit page Print Export images Properties

Securelay

PDF protected

Analyzing PDF context - 0%

AI reads only the configured protected view. Actual data comes from the locally opened PDF; reveal receipts validate every reversible token mapping.

Entity review What AI sees Actual data

2 protection receipts - 15 reveal receipts

Edit protection settings

Contextual identity review

Optional local alias/reference suggestions, defaults on: ☒

DATE_TIME Protection Tokenize Normalization Auto (case + gaps collap)

EMAIL Protection Tokenize Normalization Auto (email lowercase)

LOCATION Protection Normalization

Ask about this PDF

Summarize, explain, or find information in the document

Ask about this PDF...

Page 1 of 2

PERSON_OTK

Full Stack & AI Engineer - LLM & RAG Specialist - DevOps Engineer

EMAIL_OTK

PERSON_URL_OTK

PHONE_OTK

LOC_OTK

PERSON_URL_OTK

PROFESSIONAL SUMMARY

Results-driven Full Stack & AI Engineer with 3+ years building production-grade intelligent systems — LLM integrations, RAG pipelines, vector databases, and scalable web applications. Delivered 10+ live products across AI, SaaS, e-commerce, and academia for startups in India and the US. End-to-end ownership from architecture to cloud deployment. Open to full-time and contract roles in AI engineering, full-stack development, or DevOps.

WORK EXPERIENCE

Full Stack, AI & DevOps Engineer | DATE_TIME_OTK

Freelance Contractor - India & US Startups

- Designed and shipped end-to-end AI platforms integrating LLMs, RAG pipelines, and vector databases for ORG_OTK and ORG_OTK conferences.
- Built intelligent hiring workflows with semantic resume search and automated candidate screening, reducing manual review time significantly.
- Architected full-stack apps with React, Next.js, Node.js, and Python — REST & GraphQL APIs serving thousands of users.
- Owned deployments with Terraform, AWS EC2, Docker, CI/CD, and Supabase PostgreSQL.

FEATURED PROJECTS

VPIN4PDF	Private build	SEO AI	Private build
Document AI		AI Visibility Platform	
Localizes PDF, PPTX, and DOCX files with vision detection, generative edits, verification, and layout-preserving reconstruction.		Tracks brand mentions, citations, sentiment, competitors, and prompt performance across leading AI search engines.	
Stack: FastAPI, OpenAI GPT Vision, PyMuPDF, AWS EC2, Terraform, Supabase PostgreSQL, Docker		Stack: Next.js, DataForSEO, OpenAI, AWS EC2, Terraform, Supabase PostgreSQL, Docker	
Securelay Vault	Private build	Apranova	View live
Data Privacy & AI Security		E-Learning Platform	
Governed privacy vault for tokenization, consent-bound access, protected AI/RAG pipelines, and tamper-evident evidence.		Enterprise LMS with AI tutoring, RAG chatbots, coding workspaces, assessments, analytics, and AWS execution.	
Stack: Go, PostgreSQL, Cedar, AWS KMS/SEK, Kubernetes, Terraform, Docker		Stack: Next.js, LangChain, Gemini, OpenAI, AWS EC2, Terraform, Supabase PostgreSQL, Docker	
ORG_OTK AI	View live	Vibbillion AI	View live
AI Recruiting Platform		Agentic AI Search	
AI resume ranking, coding assessments, live proctoring, voice interviews, and recruiter analytics.		Cited web research, RAG knowledge bases, multi-model routing, specialized agents, and real-time chat.	
Stack: Next.js, Gemini, ORG_OTK, AWS EC2, Terraform, Supabase		Stack: LangChain, Gemini, OpenAI, AWS EC2, Terraform,	

AUTHORIZED USER VIEW

File Edit Window Help

Securelay Harish_Chattiboina_Resume_Updated.pdf

Home Annotate Edit Pages View

Securelay AI Summarize AI Key Points Highlight Underline Strikethrough Search Edit text 1 of 2 155% Fit width Fit page Print Export images Properties

Securelay

PDF protected

Authenticated tokens recovered - 15/15

AI reads only the configured protected view. Actual data comes from the locally opened PDF; reveal receipts validate every reversible token mapping.

Entity review What AI sees Actual data

2 protection receipts - 2 reveal receipts

Edit protection settings

Contextual identity review

Optional local alias/reference suggestions, defaults on: ☒

DATE_TIME Protection Tokenize Normalization Auto (case + gaps collap)

EMAIL Protection Tokenize Normalization Auto (email lowercase)

LOCATION Protection Normalization

Ask about this PDF

Summarize, explain, or find information in the document

Ask about this PDF...

Page 1 of 2

Harish Chittiboina

Full Stack & AI Engineer - LLM & RAG Specialist - DevOps Engineer

professor2004h@gmail.com

github.com/professor2004h

+91 7702304377 - Visakhapatnam, India

my-portfolio-ten-pl-vercel.app

PROFESSIONAL SUMMARY

Results-driven Full Stack & AI Engineer with 3+ years building production-grade intelligent systems — LLM integrations, RAG pipelines, vector databases, and scalable web applications. Delivered 10+ live products across AI, SaaS, e-commerce, and academia for startups in India and the US. End-to-end ownership from architecture to cloud deployment. Open to full-time and contract roles in AI engineering, full-stack development, or DevOps.

WORK EXPERIENCE

Full Stack, AI & DevOps Engineer | 2023 - Present

Freelance Contractor - India & US Startups

- Designed and shipped enterprise-grade AI platforms integrating LLMs, RAG pipelines, and vector databases for Vibbillion AI, Apranova, HireYouGo, and Intel Global Conferences.
- Built intelligent hiring workflows with semantic resume search and automated candidate screening, reducing manual review time significantly.
- Architected full-stack apps with React, Next.js, Node.js, and Python — REST & GraphQL APIs serving thousands of users.
- Owned deployments with Terraform, AWS EC2, Docker, CI/CD, and Supabase PostgreSQL.

FEATURED PROJECTS

VPIN4PDF	Private build	SEO AI	Private build
Document AI		AI Visibility Platform	
Localizes PDF, PPTX, and DOCX files with vision detection, generative edits, verification, and layout-preserving reconstruction.		Tracks brand mentions, citations, sentiment, competitors, and prompt performance across leading AI search engines.	
Stack: FastAPI, OpenAI GPT Vision, PyMuPDF, AWS EC2, Terraform, Supabase PostgreSQL, Docker		Stack: Next.js, DataForSEO, OpenAI, AWS EC2, Terraform, Supabase PostgreSQL, Docker	
Securelay Vault	Private build	Apranova	View live
Data Privacy & AI Security		E-Learning Platform	
Governed privacy vault for tokenization, consent-bound access, protected AI/RAG pipelines, and tamper-evident evidence.		Enterprise LMS with AI tutoring, RAG chatbots, coding workspaces, assessments, analytics, and AWS execution.	
Stack: Go, PostgreSQL, Cedar, AWS KMS/SEK, Kubernetes, Terraform, Docker		Stack: Next.js, LangChain, Gemini, OpenAI, AWS EC2, Terraform, Supabase PostgreSQL, Docker	
HireYouGo AI	View live	Vibbillion AI	View live
AI Recruiting Platform		Agentic AI Search	
AI resume ranking, coding assessments, live proctoring, voice interviews, and recruiter analytics.		Cited web research, RAG knowledge bases, multi-model routing, specialized agents, and real-time chat.	
Stack: Next.js, Gemini, Retell AI, AWS EC2, Terraform, Supabase		Stack: LangChain, Gemini, OpenAI, AWS EC2, Terraform,	

Token Studio and policy evidence

A real console view of tokenization and governed reveal. The refusal shown in the result is a recorded product outcome, not an error to bypass.

The screenshot displays the Securelay Token Studio interface, which is divided into several sections:

- Left Sidebar:** Contains navigation links for Overview, Dashboard, Data (Vault Browser, Token Studio, Classification, Connections, API Studio), Data Policy (Data Policies, Thresholds, Anomalies), Access (Roles & Grants, Approvals, Policy Simulator), AI & Agents (AI Redaction, RAG Privacy, Lineage & Sessions), Privacy Ops (Consent, DSAR, Erasure, Breach Notices), and Audit & Evidence (Audit Chain).
- Token Studio Header:** States "Mint and resolve tokens against the standalone vault. Every mint and every reveal — or refusal — is a receipt in the tamper-evident audit chain."
- Tokenize Section:**
 - Describes the POST /v1/tokenize endpoint: "seals each raw value into the standalone vault and returns a token. Detokenizing it later passes the same two-gate read path as any record — no console bypass."
 - Form fields include: Value (alice@example.com), dataType (email), tokenType (deterministic — same value, same to), Normalize (none — byte-faithful (default)), dataSubject (subject-42), and clientRef (crm:row:1042).
 - Buttons: "+ Add another" and "Mint tokens".
 - Status: "No tokens minted yet".
- Detokenize Section:**
 - Describes the POST /v1/detokenize endpoint: "resolves tokens back through Gate 1 (policy) and Gate 2 (AAD: purpose + consent) — per token. A denial arrives in-band with its own error code; the batch never fails wholesale."
 - Form fields include: Tokens (otk_ssduLmjjfcty4z7ee5yzdiqb4), Purpose (tokenize), and Redaction (Policy default).
 - Buttons: "Resolve tokens".
- RESULTS Table:**

TOKEN	OUTCOME	REDACTION
otk_ssduLmjjfcty4z7ee5yzd...	POLICY_DENIED	—

access denied by policy
- Search by value Section:**
 - Text: "Deterministic tokenization doubles as a lookup key: tokenize the plaintext you are searching for, and because the same value always mints the same token, use the result in your own WHERE clause or records filter — the search value itself never has to leave the vault boundary. Inside the vault, POST /v1/query performs the same equality lookup over a keyed blind."

Securelay Console - Token Studio

Tokenize

Seal a sensitive value and return a protected reference for applications to use.

Governed reveal

Resolve a reference only when the configured policy, purpose and consent state permit it.

Start with one controlled workflow

Connect one real data path, agree the roles and purposes, then verify the evidence before expanding.

Future scope

More connectors, partner delivery tools, localized notice experiences and additional capture interfaces remain roadmap options until shipped and verified.

Latest DPDP developments

Recent government, procurement and court activity shows that DPDP preparation is active now. Checked 2 September 2026.

1 27 Aug 2026 | Times of India

Government departments put on a DPDP implementation timeline

The Cabinet Secretary directed central ministries, states and UTs to prepare time-bound plans and appoint senior nodal officers. Why it matters: The work now needs named owners, inventories, consent review, safeguards and processor-contract review. [Open source](#)

2 12-13 Aug 2026 | NeGD, Government of India

Gujarat workshop focused on implementation roadmaps

The workshop covered notice and consent, data lifecycle, breach handling, grievances, privacy by design and security safeguards. Why it matters: Readiness is being translated into departmental gap lists and action plans. [Open source](#)

3 7 Aug 2026 | Business Standard

Supreme Court sought the Centre's reply on the DPDP-linked RTI amendment

The petitions concern the balance between personal-information protection and public-interest transparency. Why it matters: Privacy governance must stay adaptable as legal interpretation develops. [Open source](#)

4 29 Jun 2026 | Bank of Baroda

Bank issued an enterprise privacy-governance platform RFP

The tender sought supply, implementation and maintenance of a DPDP-aligned enterprise data privacy governance and compliance platform. Why it matters: Large institutions are turning privacy requirements into concrete technology procurement. [Open source](#)

5 May 2026 | MeitY

Recruitment opened for the Data Protection Board

MeitY invited applications for one Chairperson and four Members of the Data Protection Board of India. Why it matters: The digital-by-design adjudicatory institution is moving toward operational staffing. [Open source](#)

THE SIGNAL

Organizations are moving from awareness to owners, roadmaps, platform selection, operating controls and evidence. Securelay is designed for that operational layer.

Sources

Fresh developments are listed first, followed by the official Act, Rules and Government backgrounder. Every link is clickable.

1 DPDP compliance gets Cabinet Secretary's push

Times of India | 27 Aug 2026

Used for: the latest government-wide implementation direction

[Open source](#)

2 DPDP implementation workshop

NeGD, Government of India | 12-13 Aug 2026

Used for: current readiness topics and departmental roadmaps

[Open source](#)

3 Supreme Court seeks reply on DPDP-linked RTI change

Business Standard | 7 Aug 2026

Used for: active judicial interpretation

[Open source](#)

4 Enterprise data privacy platform RFP

Bank of Baroda | 29 Jun 2026

Used for: a current institutional procurement example

[Open source](#)

5 Data Protection Board appointment notice

MeitY | May 2026

Used for: Board mandate and staffing process

[Open source](#)

6 DPDP compliance deadlines

India Data Law | verified Aug 2026

Used for: current phased deadlines with source tracking

[Open source](#)

7 Digital Personal Data Protection Rules, 2025

MeitY / Gazette of India | 13 Nov 2025

Used for: safeguards, consent, breach and audit requirements

[Open source](#)

8 Digital Personal Data Protection Act, 2023

MeitY | official Act text

Used for: rights, duties and statutory framework

[Open source](#)

9 DPDP Rules, 2025 backgrounder

Press Information Bureau | 17 Nov 2025

Used for: plain-language official context

[Open source](#)