

PharmaKrypt: Agentic AI-Powered Framework for Secure and Intelligent Medicine Verification

¹Dr. M.K. Jayanthi, ²Raaz Yadav, ³Vishwesh Singh, ⁴Pari Goel, ⁵Aryan Kumar Rai, ⁶Azaan Ahmed, ⁷Trisha Kapoor

¹ Professor, Computing Science Engineering and Artificial Intelligence, VIT Bhopal University, Bhopal Indore Highway, Kothrikalan, Sehore, Madhya Pradesh 466114

^{2,3,4,5,6,7} UG Student School of Computing Science Engineering and Artificial Intelligence, VIT Bhopal University, Bhopal Indore Highway, Kothrikalan, Sehore, Madhya Pradesh 466114

Abstract- PharmaKrypt is a Secure Supply Chain Verification System that aims to stop counterfeit drugs by utilizing a cryptographic serialization method, real-time geolocation locking, and a "One Scan" consumption policy. Counterfeit drugs cause over a million deaths a year because current technologies, such as holograms and standard QR codes, are ineffective since they are easily replicated. PharmaKrypt takes verification and makes it an active, state-aware process where one drug equals one identity, one successful scan. PharmaKrypt provides a multi-tiered architecture, a Manufacturing Hub for digital batch activation, a Secure Distribution module for geolocation-locked handshakes, a Pharmacy Portal for two-stage verification, and a Regulatory Oversight portal with a global "kill switch" feature. By utilizing modern web technologies, PharmaKrypt provides a streamlined, real-time tracking experience through ReactJS, TypeScript, and Firebase Firestore. PharmaKrypt eliminates the problems associated with offline, passive verification processes, bridges the physical-digital divide, and maximizes the reach of anti-counterfeit efforts, ensuring that no counterfeit drug reaches the patient.

Keywords: Anti-Counterfeiting, Cryptographic Serialization, Geolocation Locking, Supply Chain Security, Healthcare Technology.

I. INTRODUCTION

PharmaKrypt provides a revolutionary solution to protect the pharmaceutical supply chain through an active and state-aware verification system. Counterfeit drugs have become a crisis in the pharmaceutical industry worldwide, and no drug is safe from counterfeiting at any price point. The crux of the

problem is the "passive" nature of the current solutions in the pharmaceutical industry. Once a counterfeit drug manufacturer replicates a legitimate standard QR code or hologram, they can flood the pharmaceutical market with thousands of counterfeit drugs, which can be easily verified as legitimate through an offline verification system. PharmaKrypt resolves the "double-spend" problem through a revolutionary approach to the pharmaceutical industry by treating medicines as digital assets. PharmaKrypt's system is based on two main pillars of security: Digital Batch Activation and Location Locking. Digital Batch Activation ensures that newly generated codes remain entirely worthless or "Inactive" until a verified distributor scans and activates them. Location Locking ensures that these activated medicines are cryptographically locked to a specific pharmacy's geolocation before they are delivered. Additionally, PharmaKrypt also implements a "One Scan" policy for medicines; once a medicine is given to a patient, the ID is permanently flagged as "Consumed." If the ID is scanned again for the same medicine, a COUNTERFEIT SIGNAL IS IMMEDIATELY TRIGGERED.

II. LITERATURE REVIEW

The literature review section of this paper focuses on the existing supply chain systems and anti-counterfeiting systems. It identifies the limitations of the existing systems and the need for a more accessible, active, and state-aware system. Existing systems are passive systems that use physical identification and databases that do not offer real-time

geolocation tracking and do not stop the cloning of IDs. Recent studies highlight the need for an immutable ledger. For example, Prof. S. Patil et al. (2024) showed the high level of transparency and traceability offered by blockchain technology, but also the challenges faced in integrating it with legacy systems and the high initial cost for local pharmacies. In another study, Dr. S. Ellahham et al. (2024) emphasized the importance of integrating IoT with blockchain for the validation of product identity and physical state, thus eliminating blind spots in the supply chain. In the studies on "Proof of Ownership" (Perumalsamy et al., 2025), the importance of treating physical drugs as unique digital tokens to avoid the problem of "double spending" was also emphasized. The above studies also reflect the need for an innovative product such as PharmaKrypt, using real-time NoSQL databases (Firestore), cryptographic serialization, and geolocation locking, thus offering a highly efficient, scalable, and impactful product without the high initial cost associated with the use of heavy IoT hardware for low-cost generic drugs.

III. PROJECT FUNCTIONAL MODULES IMPLEMENTATION

The project is structured around several functional modules designed to ensure a seamless, secure and engaging user experience across the entire supply chain:

- **Manufacturing Hub (Admin):** Includes secure login and batch generation. The manufacturers create cryptographically secure high-entropy unique IDs such as PK 7X92 M4K1 for individual items and Master Cartons. It also includes live tracking to track the real-time status of all items (Inactive -> In Transit -> Stocked -> Sold).
- **Secure Distribution (The "Handshake"):** Facilitates parent child aggregation wherein the distributors scan a single Master Carton ID to verify multiple units in an instant. It also supports Location Locking, wherein the distributors can specify a target Pharmacy and City and update the batch status to "IN TRANSIT" and lock the batch to the destination.
- **Pharmacy Portal (Two Stage Verification):** Provides a Stock Intake module that verifies the medicine was for that particular pharmacy (status

set to STOCKED) and a Dispense module that sets the unique ID to SOLD when the product is sold. It also has a live inventory management view.

- **Regulatory Oversight (Super Admin):** Offers a Global Kill Switch, allowing you to "freeze" compromised batches or revoke credentials. It has a Counterfeit Radar, which monitors a "real time feed" of failed scans, including "Duplicate", "Theft", "Diversion", with exact time and location stamps.
- **Automated Alert System:** It generates instant notifications for anomalies, like trying to stock a medicine allocated to a different city or scanning an ID already marked as "Sold," and records them directly into the database.

IV. PROPOSED RESEARCH METHODOLOGY

The methodology for developing PharmaKrypt involves a structured approach to ensure the platform's efficiency, security and user friendliness:

- **Requirement Analysis:** Identifying and documenting the software (ReactJS, TypeScript, Firestore) and hardware requirements (webcams for scanning, NFC capabilities for future scope) needed for the project.
- **System Design:** Creating detailed designs for the user interface, component architecture and NoSQL database schema, including data flow and state transitions (Inactive -> In Transit -> Stocked -> Sold).
- **Implementation:** Using technologies like ReactJS (Vite) for the frontend, Tailwind CSS for styling and Firestore for a robust, real-time backend. The project utilizes jsQR for real time video frame analysis and QR scanning.
- **Testing:** Conducting comprehensive testing strategies, including unit testing for cryptographic ID generation, integration testing for the Distributor to Pharmacy handshake and edge case testing for the "Double Spend" counterfeit alerts.
- **Deployment:** Launching the platform on secure hosting environments, ensuring all API keys are secured, authentication rules are strictly enforced and systems are fully operational for real time supply chain monitoring.

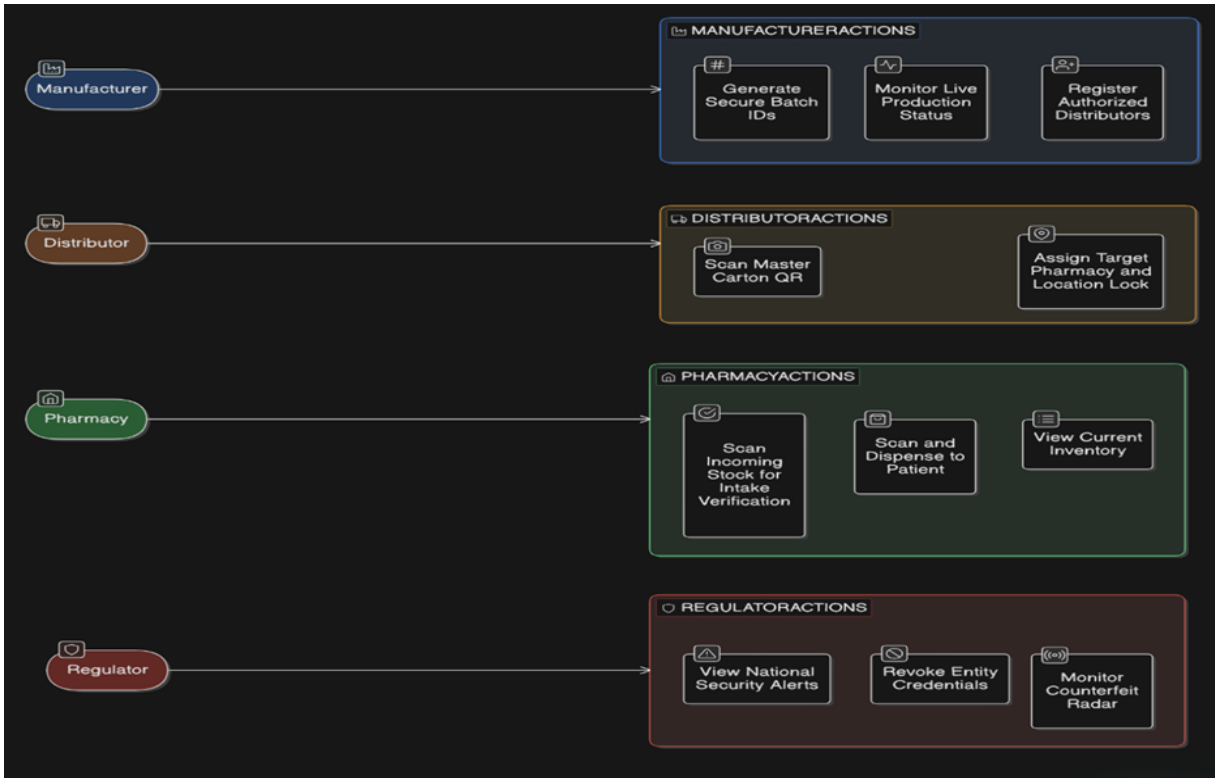


Fig. 1: Textual Representation of Use Case diagram for PharmaKrypt Verification System Home Page

V. PHARMAKRYPT IMPLEMENTATION MODULES, OUTPUT ANALYSIS AND SCREENSHOTS

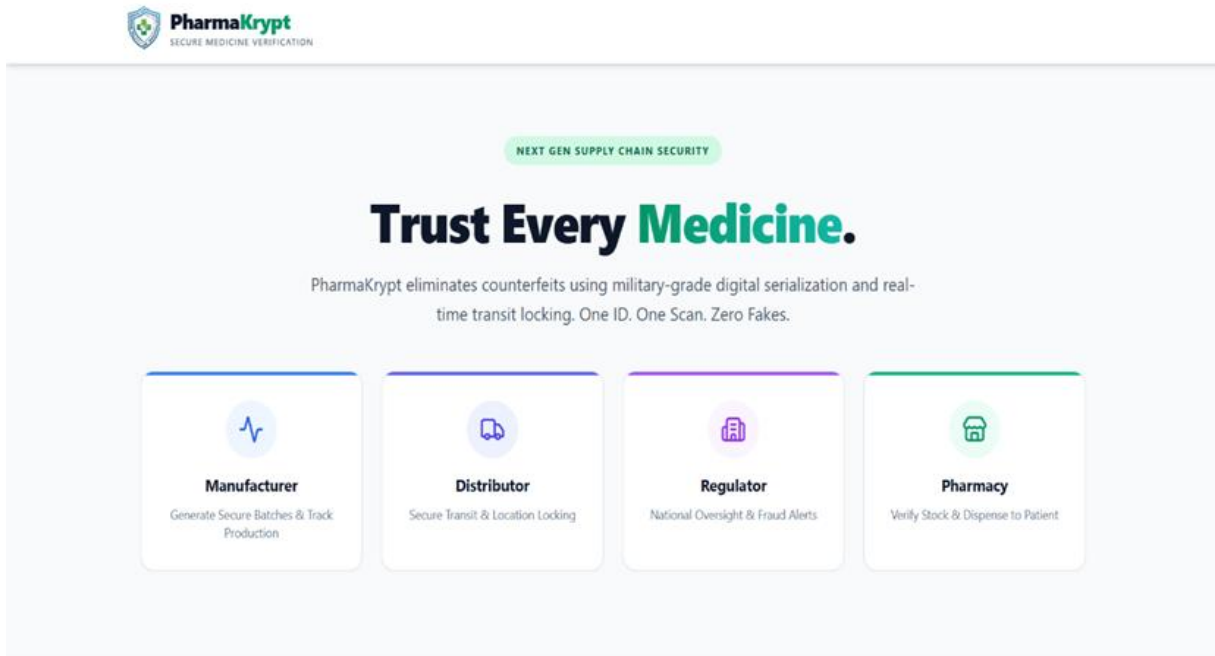


Fig. 2: PharmaKrypt Verification System Home Page

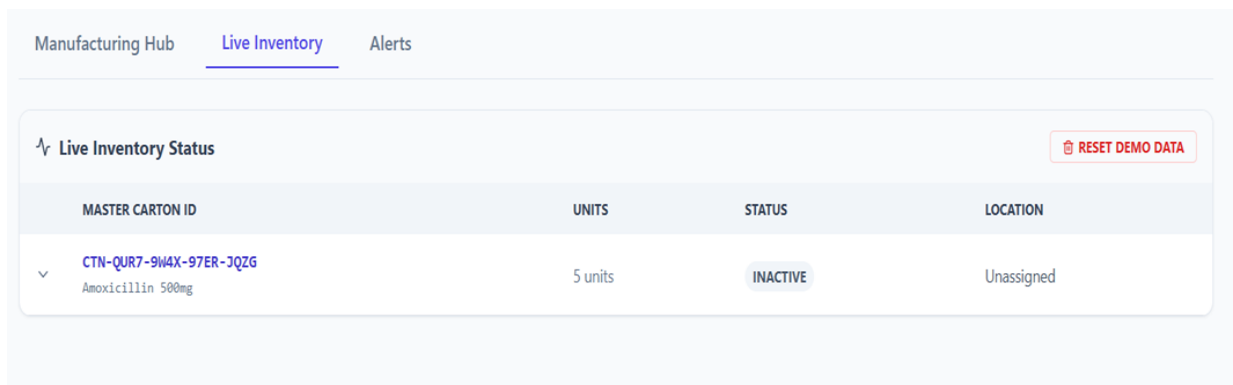


Fig. 3: PharmaKrypt Verification System Home Page

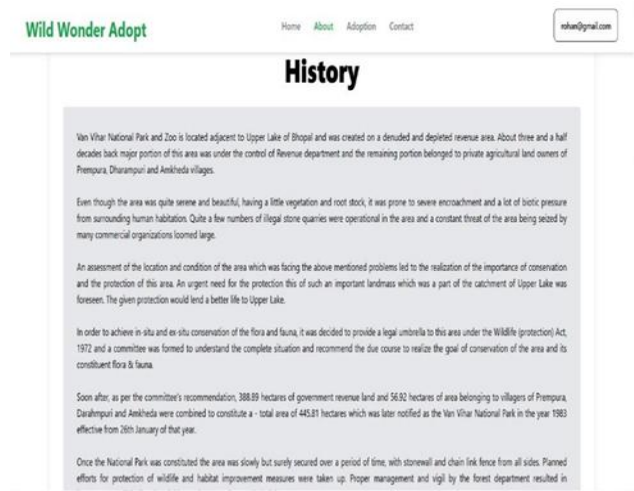
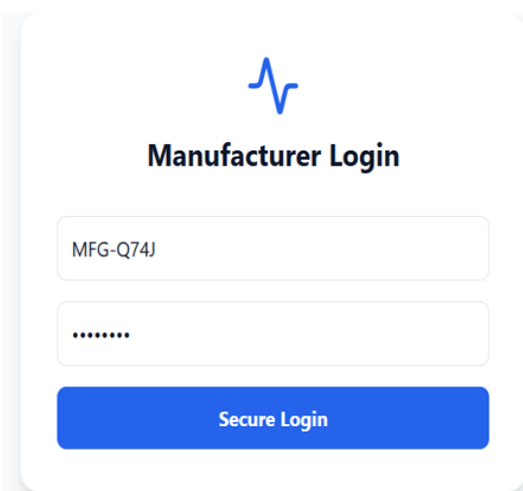


Fig. 4 & 5: Manufacture Login and History of PharmaKrypt Verification System Home Page

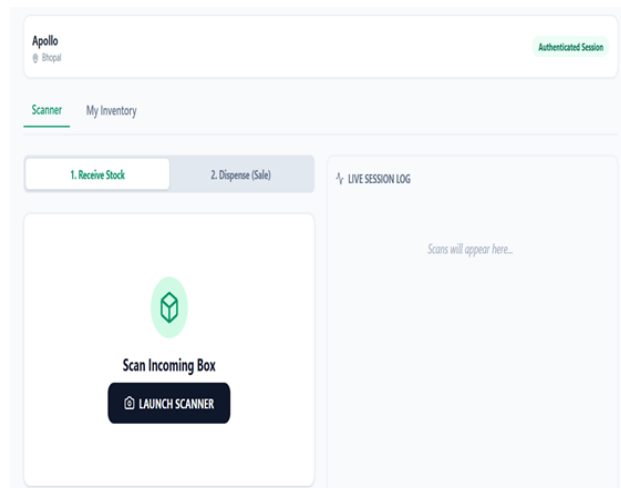
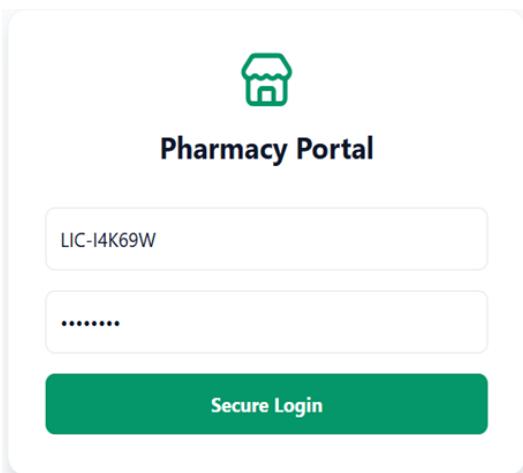


Fig. 6: Manufacturing Pharmacy Portal PharmaKrypt Verification System Home Page

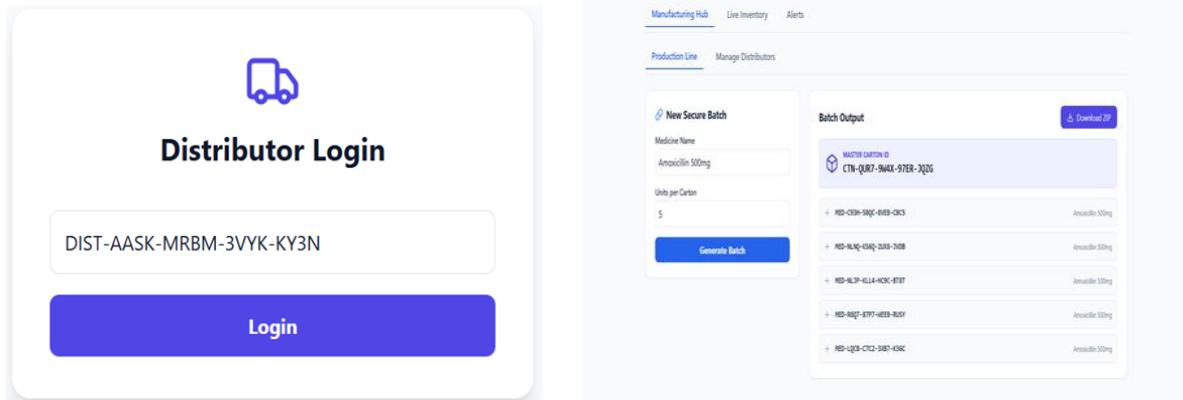


Fig. 7 & 8: PharmaKrypt Verification System Distributor Activation (Adoption/Handshake)

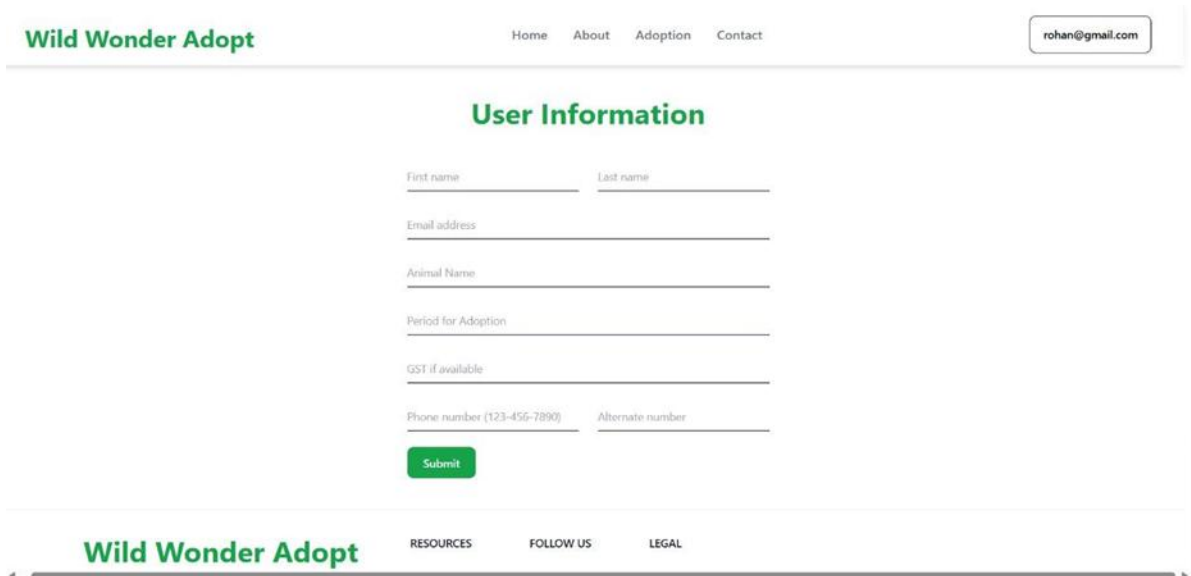


Fig. 9: PharmaKrypt Verification System Home Page

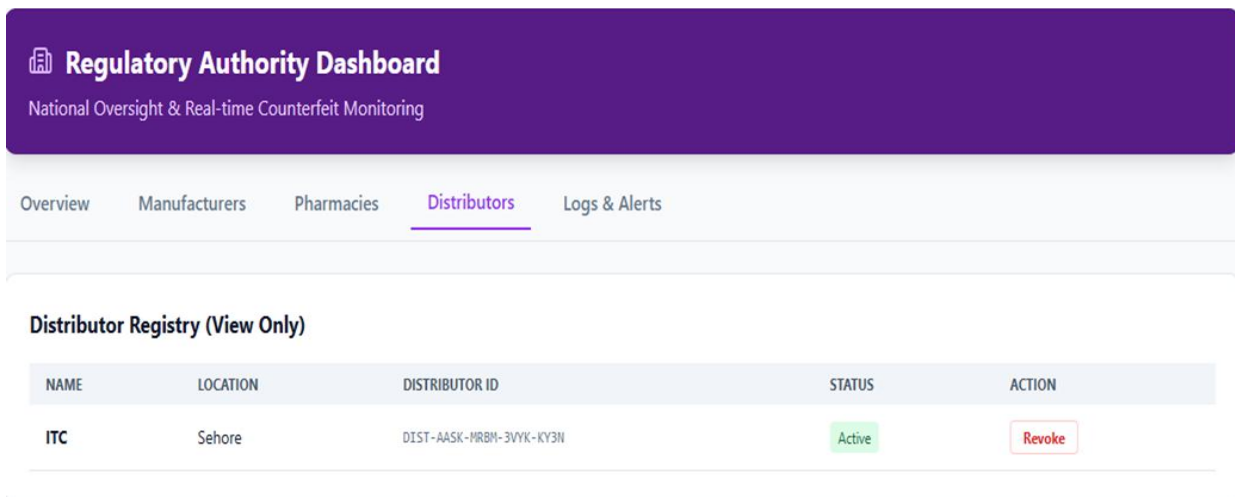


Fig. 10: Contact Us PharmaKrypt Verification System Home Page

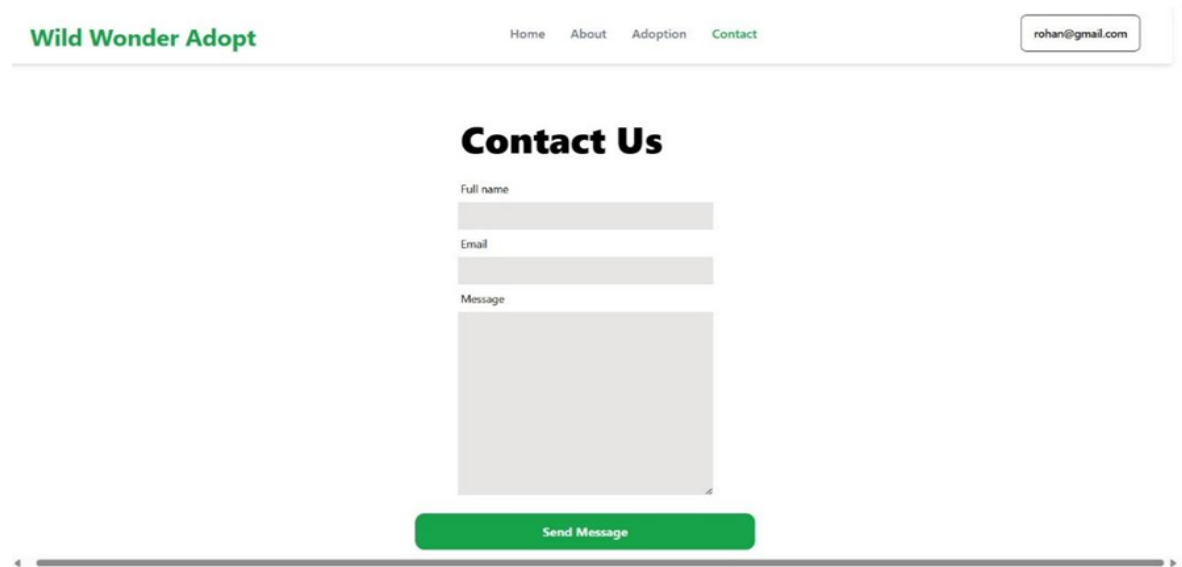
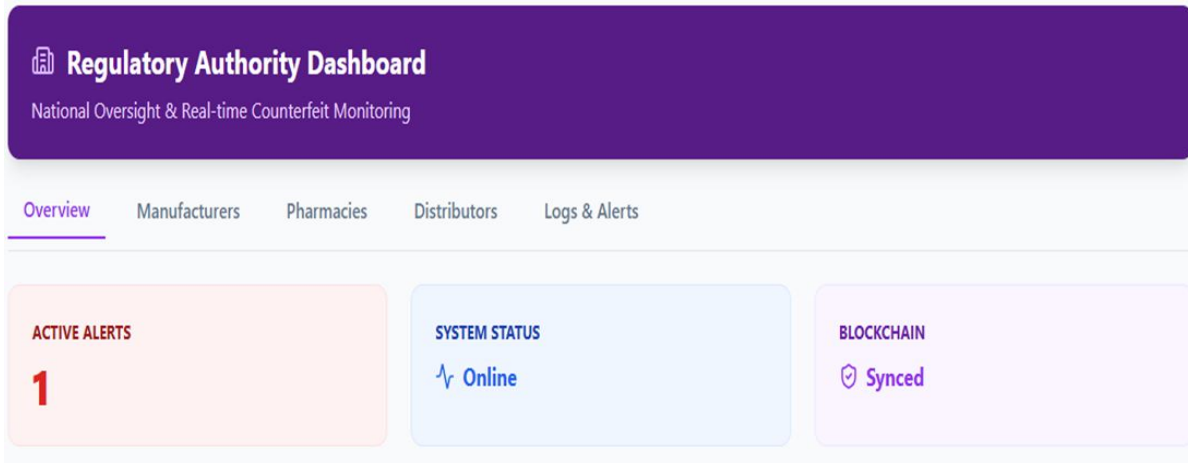
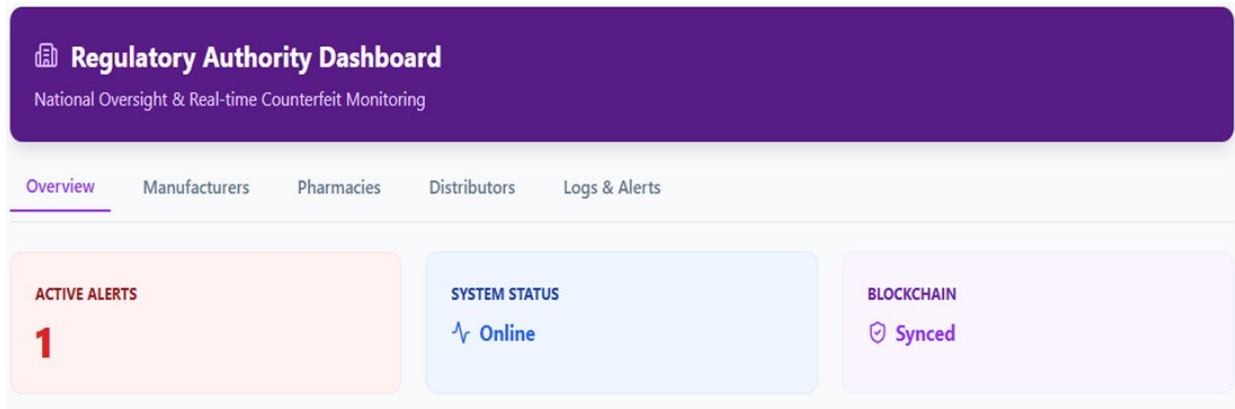


Fig. 11& 12: RAD PharmaKrypt Verification System



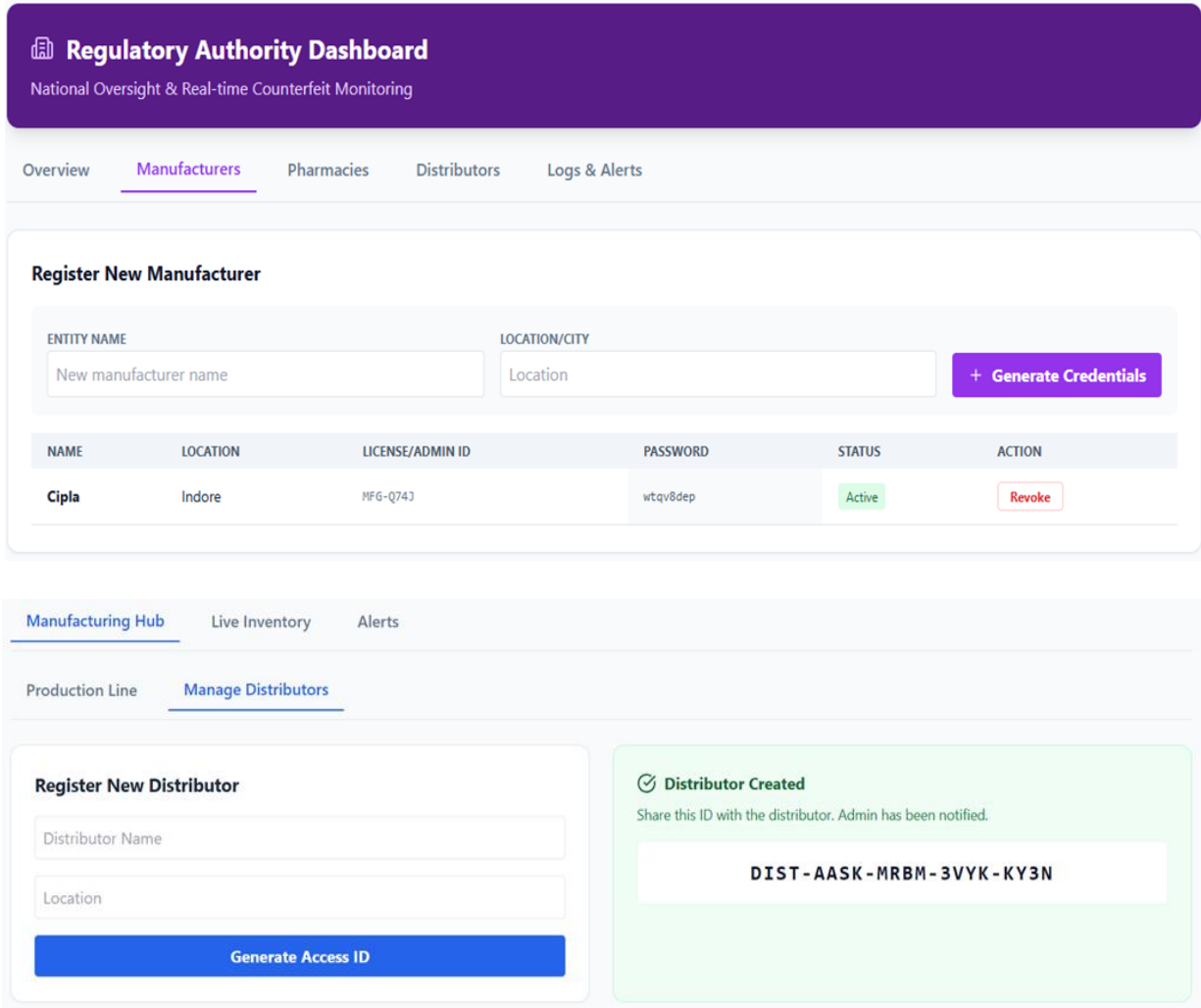


Fig. 13, 14 and 15: PharmaKrypt Verification System RD Dashboard

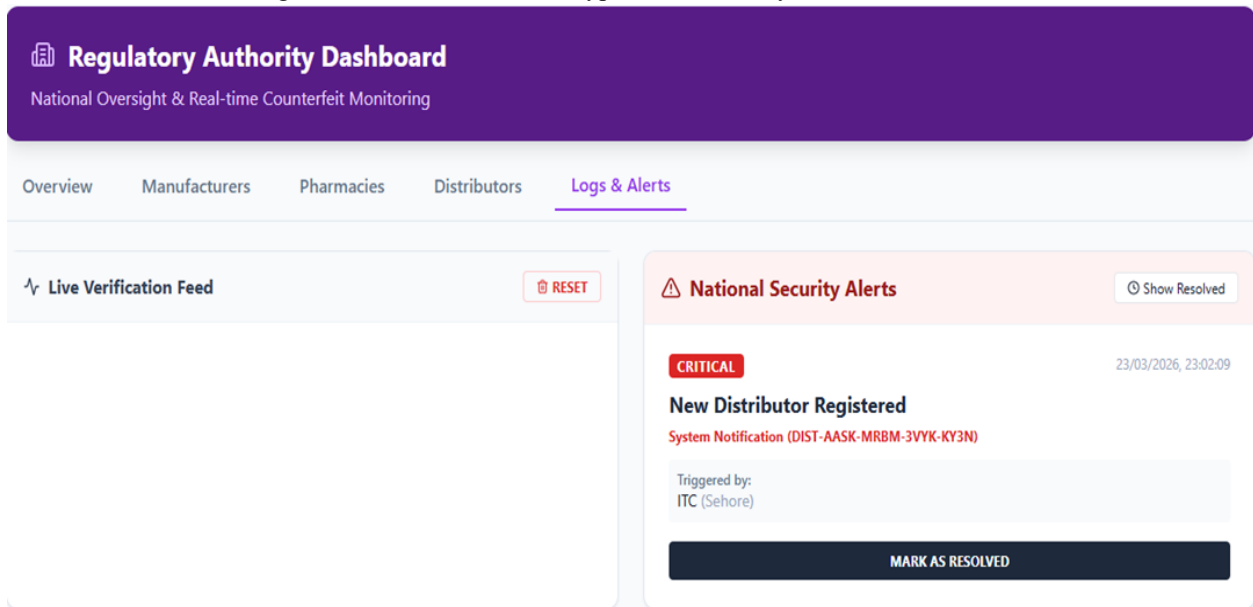


Fig. 16: PharmaKrypt Verification System Home Page

VI. CONCLUSION

The conclusion highlights PharmaKrypt's success in redefining supply chain security from a passive checklist to an active, impenetrable defense network. By implementing Location Locking and Digital Batch Activation, PharmaKrypt effectively addresses the limitations of traditional offline verification processes. The strict "One Scan" consumption policy mathematically eliminates the "Double Spend" problem, ensuring that a cloned QR code becomes instantly useless the moment the genuine product is sold. The platform fosters immense transparency, promotes regulatory accessibility and ensures sustainable, real time support for pharmaceutical security. Future plans include expanding the ecosystem with a dedicated Consumer App for patient verification, integrating Hyperledger Fabric for decentralized, trustless blockchain infrastructure and deploying AI Risk Scoring models to predict counterfeit hotspots based on scan anomalies. These developments aim to further increase the platform's impact, ensuring that medicines globally are always trusted, never guessed.

REFERENCES

- [1] Counterfeit Pharmaceutical Product Detection Using Blockchain Technology" by A. Kanaji, Prof. S. Patil, et al., 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), IEEE Xplore, 2024
- [2] A Pharmaceutical Supply Chain Management using Blockchain and IoT" by Dr. S. Ellahham et al., 2023 Global Conference on Information Technologies and Communications (GCITC), IEEE Xplore, 2024.
- [3] G., D. K., Singh, M. K., & Jayanthi, M. (Eds.). (2016). Network Security Attacks and Countermeasures. IGI Global. <https://doi.org/10.4018/978-1-4666-8761-5>
- [4] Blockchain Non-Fungible Token for Effective Drug Traceability System" by S. Perumalsamy & V. Kaliyamurthy, Engineering, Technology & Applied Science Research, 2025.
- [5] <https://firebase.google.com/docs/firestore>
- [6] M.K. Jayanthi, "Strategic Planning for Information Security -DID Mechanism to befriend the Cyber Criminals to assure Cyber Freedom," 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), Abha, Saudi Arabia, 2017, pp. 142-147, doi: 10.1109/Anti-Cybercrime.2017.7905280.
- [7] Detecting Counterfeit Medicines Utilizing Artificial Intelligence Technique by A. Soy et al., International Journal of Creative Research Thoughts (IJCRT), 2025.
- [8] Kavitha, E., Tamilarasan, R., Baladhandapani, A., Kannan, M.K.J. (2022). A novel soft clustering approach for gene expression data. Computer Systems Science and Engineering, 43(3), 871-886. <https://doi.org/10.32604/csse.2022.021215>
- [9] Naik, Harish and Kannan, M K Jayanthi, A Survey on Protecting Confidential Data over Distributed Storage in Cloud (December 1, 2020). Available at SSRN: <https://ssrn.com/abstract=3740465> or <http://dx.doi.org/10.2139/ssrn.3740465>
- [10] Shree Nee, T. R., Kannan, M. K. J., & Mariyappan, K. (2025, April). Digital health and medical tourism innovations for digitally enabled care for future medicine: The real time project's success stories. In Navigating innovations and challenges in travel medicine and digital health (pp. 325–344). IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3693-8774-0.ch016>
- [11] Kavitha, E., Tamilarasan, R., Poonguzhali, N., Kannan, M.K.J. (2022). Clustering gene expression data through modified agglomerative M-CURE hierarchical algorithm. Computer Systems Science and Engineering, 41(3), 1027-141. <https://doi.org/10.32604/csse.2022.020634>
- [12] Kumar, K.L.S., Kannan, M.K.J. (2024). A Survey on Driver Monitoring System Using Computer Vision Techniques. In: Hassanien, A.E., Anand, S., Jaiswal, A., Kumar, P. (eds) Innovative Computing and Communications. ICICC 2024. Lecture Notes in Networks and Systems, vol 1021. Springer, Singapore. https://doi.org/10.1007/978-981-97-3591-4_21
- [13] M. K. J. Kannan, A bird's eye view of Cyber Crimes and Free and Open Source Software's to Detoxify Cyber Crime Attacks - an End User

- Perspective, 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), Abha, Saudi Arabia, 2017, pp. 232-237, doi: 10.1109/Anti-Cybercrime.2017.7905297.
- [14] Verma, D., Kannan, M. K. J., Barnwal, S. K., Barve, A., & Swaminathan, R. (2022, September). Multimodal sentiment sensing and emotion recognition based on cognitive computing using hidden Markov model with extreme learning machine. *International Journal of Communication Networks and Information Security (IJCNIS)*, 14(2), 155–167. <https://doi.org/10.17762/ijcnis.v14i2.5496>
- [15] MK J Kannan, Shree Nee T R (2025, November). Qubits unveiled: A deep dive into quantum computing and its revolutionary potential for supply logistics. In P. Gaba, A. Panwar, V. Jain, & R. Kannan (Eds.), *Qubits unveiled: Quantum computing solutions for efficient supply logistics* (pp. 273–293). Nova Science Publishers. <https://doi.org/10.52305/WSXW8884>
- [16] Learning React: A Hands On Guide to Building Web Applications Using React and Redux" by Kirupa Chinnathambi, Addison Wesley Professional, 2020.
- [17] P. Jain, I. Rajvaidya, K. K. Sah and J. Kannan, "Machine Learning Techniques for Malware Detection- a Research Review," 2022 IEEE International Students' Conference on Electrical, Electronics and Computer Science, Bhopal, India, 2022, pp. 1-6, doi: 10.1109/SCEECS54111.2022.9740918.
- [18] Firebase Essentials Web Edition: Get to Know Firebase Realtime Database and Firebase Authentication" by Neil Smyth, CreateSpace Independent Publishing Platform, 2017.
- [19] B. R. M, M. M. V and J. K. M. K, Performance Analysis of Bag of Password Authentication using Python, Java and PHP Implementation, 2021 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2021, pp. 1032-1039, doi: 10.1109/ICCES51350.2021.9489233.
- [20] "Software Engineering: A Practitioner's Approach" by Roger S. Pressman, McGraw Hill Education, 2019.
- [21] Dr. Sunil Kumar Dr. P. T. Kalaivaani, Dr. M K Jayanthi Kannan, Dr. Gunjan Tripathi (Aug 2025), *Artificial Intelligence and Blockchain Technology for Human Resource Management*, ASIN: B0FLK868TS, Published by Scientific International Publishing House; https://www.amazon.in/gp/product/B0FLK868TS/ref=ox_sc_act_title_1?smid=A1UBZVVGJOLJ UJI&pssc=1
- [22] Aaijaz, N., Grace Mani, K., Kannan, M. K. J., & Tewari, V. (2025, February). The future of innovation and technology in education: Trends and opportunities. S&M Publications. <https://www.amazon.in/gp/product/B0DW334PR9>
- [23] Shukla, S. K., Dwivedi, U., Kannan, M. K. J., & Sarvani, C. (2024, October 23). *Python for data analytics: Practical techniques and applications*. JSR Publications. <https://www.amazon.in/gp/product/B0DMJY4X9N>
- [24] <https://tailwindui.com/components>
- [25] Harish Naik, B. M., & Kannan, J. (2023). Research on various security aware mechanisms in multi-cloud environment for improving data security. In 2023 2nd IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE) (pp. 1–6). IEEE. <https://doi.org/10.1109/ICDCECE57866.2023.10151135>
- [26] <https://github.com/cozmo/jsQR>
- [27] Harish Naik B M and M K J Kannan and (Aug 2024), "Secure Cloud Storage for Sensitive Data based on Authentication and Encryption Algorithms", *International Journal of Advanced Technology and Engineering Exploration (IJATEE)*, paper Id: IJATEE.2024.111101510, ACCENTS, www.ijateeditor@gmail.com
- [28] <https://reactjs.org/docs/getting-started.html>
- [29] Object-oriented analysis and design of learning objects and applications of agent based reusable learning objects in e-learning system design, JM. K. (2009). [Doctoral dissertation, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya]. Shodhganga. <http://hdl.handle.net/10603/125448>
- [30] Alshahrani, M. S. M., & Kannan J M. K. (2026, February). Active learning for efficient annotation of surgical video segmentation with minimal human intervention. *ICTACT Journal on Image and Video Processing*, 16(3), 3821–3829. <https://doi.org/10.21917/ijivp.2026.0539>
- [31] J Kannan, M. K., TR Shree Nee., & Mariyappan, K. (2026). Ethics and regulations in AI-driven

ophthalmology. In B. K. Mishra, A. Kumar, K. Mariyappan, V. Tiwari, P. S. Rathore, & G. H. Das (Eds.), *Generative artificial intelligence in ophthalmology* (pp. 331–386). Scrivener Publishing.

<https://www.scrivenerpublishing.com/cart/title.php?id=1341>,<https://doi.org/10.52305/WSXW8884>

- [32]MK J Kannan, Satyajit Patel (2024). Sustainable Information Retrieval Techniques for Onion Market Instability Prediction using Machine Learning and Deep Learning Approaches. *International Journal of Advance Research, Ideas and Innovations in Technology*, 10(6) www.IJARIT.com. <https://www.ijariit.com/manuscripts/v10i6/V10I6-1455.pdf>