




Paper Type: Original Article

## Database Security in Psychiatry: Leveraging Large Language Models and Blockchain for Secure Data Management

Joel Nithish Kumar Murugan<sup>1,\*</sup> , Padmavathi Vyshnavi Madarampalli<sup>1</sup>, Shashikant Ramesh Yadav<sup>1</sup>

<sup>1</sup> Illinois Institute of Technology, Chicago, Illinois, United States of America; jmurugan@hawk.iit.edu; pmadarampalli@hawk.iit.edu; syadav15@hawk.iit.edu.

### Citation:

Received: 26 April 2024

Revised: 7 July 2024

Accepted: 21 September 2024

Kumar Murugan, J. N., Madarampalli, P. V., & Yadav, Sh. R. (2025).

Database security in psychiatry: leveraging large language models and blockchain for secure data management. *Metaversalize*, 2(1), 1-10.


### Abstract


In this digital era, secure management of psychiatric data has become a key challenge due to the highly sensitive nature of the information it encompasses- from personal histories to therapeutic notes and behaviors up to diagnostic findings. Its unauthorized access or inappropriate handling might lead to privacy breaches, discrimination, and further erosion of trust in these mental health systems. This paper discusses how two disruptive technologies, Large Language Models (LLM) and blockchain, come together to address these challenges. The LLM is particularly good at analyzing unstructured data and, as such, provides deep, insightful clinical analytics for personalized mental health interventions while maintaining patient confidentiality. Blockchain technology ensures data integrity, immutability, and decentralized storage for the robustness of security and controlled access to sensitive psychiatric records. The combination of technologies will yield a secure, efficient, and privacy-preserving system for managing psychiatric data, advanced clinical decision-making, and trust protection of patients. The proposed framework will include a blockchain-based decentralized storage layer, a data analysis layer powered by LLMs, and a secure interface for controlled access to data with ethical and regulatory compliance. This integration is a significant step forward in attending to the special needs that psychiatric data management presents within healthcare.

**Keywords:** Large language models, Natural language processing, Blockchain, Data access control.

## 1 | Introduction

In the modern world, sensitive data in different fields are prone to data breaches [1], [2]. One such data source is patient data in healthcare. Health care is a field where sensitive data highly needs security and privacy; considering fields like psychiatry, the data is highly sensitive where the patient records containing health history, diagnostic evaluations, therapy notes, patient narratives, and session transcripts, which, when

 Corresponding Author: jmurugan@hawk.iit.edu

 <https://doi.org/10.22105/metaverse.v2i1.44>



Licensee System Analytics. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

neglected may lead to privacy violations, damage patients trust and affect clinical outcomes [2]. The healthcare industry faces major database security challenges driven by sensitive information and HIPPA regulations. Due to its highly sensitive nature, psychiatric data requires stringent security measures to prevent breaches and ensure confidentiality.

Advanced technologies and sensitive medical data present unpredicted challenges, which can be seen more evidently in different healthcare management systems but most prominently in psychiatric care. The combination of two cutting-edge technologies, Large Language Models (LLM) [3] and blockchain technologies [4]. The management of psychiatric data is one of the major concerns in health care. The patient records include sensitive information like personal histories, diagnoses, treatment plans, behavioral data, and notes from therapy sessions. Unauthorized access to such data can pose severe consequences to the patients, both physically and mentally. Traditional database systems that cannot manage such confidential information are functional and often can't provide a high level of data security and data privacy.

The two primary technologies, LLM's and blockchain technologies, when worked together, work as barriers for most prominent and sensitive data.

### **1.1 | Large Language Models**

- I. Interpret and analyze large unstructured data.
- II. Facilitate data analysis.
- III. Decision support by maintaining patient privacy.

### **1.2 | Blockchain**

- I. Handles immutable records keeping for data integrity.
- II. Provide decentralized data storage not relying on traditional systems.
- III. A secure foundation for storing and accessing sensitive data.

When both technologies work together, they form an effective system for managing psychiatric data and help prevent data breaches.

### **1.3 | LLM's and Blockchain Technologies**

These integrated advanced technologies provide significant development in healthcare, especially in psychiatry, where large amounts of complex and sensitive data can be found. Incorporating these technologies ensures proper management and analysis of large unstructured data. It also ensures privacy regarding behavioral data, diagnosis tests, unstructured therapy notes, and confidential patient information and helps provide proper clinical analysis for doctors.

These technologies are often distinct from traditional methods as they can effectively work with large amounts of unstructured data while maintaining privacy and high security.

Blockchain technology is uniquely distinguished for allowing secured storage, limited access to data, integrity, and transparency. On the other hand, LLMs are well known for their Natural Language Processing (NLP) capabilities, which ensure the analysis of large unstructured data, tracking the latest trends, and providing accurate treatment. When implemented together, both focus entirely on ensuring data storage, privacy, analytics, and proper meaningful insights.

When combined [5], these advanced technologies work as barriers to securing large amounts of data and confidential data, which are more prominent in the healthcare industry and, more specifically, in psychiatry.

## 2 | Literature Review

The intelligence era is upon us, and the LLM are storming worldwide. These models are revolutionizing how we interact with technology and have demonstrated exceptional capabilities in tasks such as reasoning, summarization, inference, etc. Due to this, they are widely applicable in fields like finance, healthcare, marketing, analytics, etc. Organizations are moving fast and waste no time incorporating these technologies into their products. Fundamentally, these models are trained on vast amounts of existing data. However, it is important to understand that the data security requirements vary across sectors, and some are more stringent than others. The healthcare sector is a highly regulated industry governed by stringent laws like the Health Insurance Portability Act (HIPAA). This ensures that high data security, confidentiality, and integrity standards are maintained for patient health information, and exposure to personal data could have serious consequences for the organization. Given the huge potential of LLMs in healthcare, the strict data security regulations cannot hold back its applicability in the industry. To address the security needs of the healthcare sector, incorporating blockchain with LLM has been recommended [6]. Further, this literature survey will examine current research on LLMs in mental health care and the challenges and ethical considerations surrounding their use.

LLMs have demonstrated remarkable abilities in comprehending human language and its sentiment, demonstrating huge potential for application in psychiatric care. The review by Smith et al. explored using LLMs like ChatGPT in psychiatric care. They noted the remarkable potential of LLMs in clinical reasoning and the ability to assist in diagnosing mental health disorders, managing depression, etc. LLMs could offer personalized assistance to patients and aid them in overcoming their clinical conditions. However, they also highlighted the limitations of these models in understanding complex cases and underestimating the suicidal risks in patients [7].

A systematic review of blockchain technology in healthcare was conducted by Agbo et al. [8], exploring the potential of blockchain in various healthcare-related fields. It highlighted blockchain's ability to enhance the confidentiality and security of healthcare data. Moreover, it could also facilitate the secure sharing of medical information amongst hospitals, thereby improving the interoperability of healthcare systems. This increases the transparency of the healthcare system and renders data tampering practically impossible. It also grants the patients greater control over their healthcare data. However, the review also identified challenges that may arise from adopting blockchain technology. The healthcare industry handles huge volumes of data stored in various formats. Implementing blockchain technology at this scale may lead to scalability issues and challenges from blockchain integration with existing systems. Given the industry's highly regulated nature, compliance with regulatory norms and data protection laws may pose a challenge. The immutable nature of blockchain records may be a drawback in specific scenarios as it may cause privacy concerns. Hence, there is a need to build consensus over the use of blockchain in healthcare and its implementation and integration with the existing systems.

The paper "future of digital health with federated learning" argued that the immense potential of machine learning models in healthcare was curtailed because huge volumes of data are restricted in silos, and privacy concerns often prevent their usage [9]. It proposes using federated learning to assuage data privacy concerns and simultaneously unlock the true potential of the data. Federated learning is a decentralized learning process where the machine learning models are trained on the data stored locally in the system. Hence, it satisfies the industry's data protection requirements and, at the same time, allows insights to be gained from the distributed datasets. As discussed, blockchain relies on the decentralization of data to ensure the entire system's security. Likewise, in federated learning, models are trained on the edge devices, and the data never leaves the local systems. A similar approach could be employed for language models that are developed using federated learning, thereby satisfying the data requirements of the industry and enabling insights to be gained from it.

Since artificial intelligence models rely heavily on data quality and representativeness, biases, and inaccuracies can be perpetuated [10]. Also, given that LLM are trained using neural networks, they operate as black boxes

having very low interpretability. Hence, it may be challenging for psychiatrists to understand the reasoning behind the AI-generated responses. Artificial intelligence systems may struggle to understand the minor nuances in human speech, such as sarcasm and exaggeration. Language models may not adequately capture the time-varying nature of mental disorders, and over-reliance on AI-generated responses may prove detrimental in critical situations. Also, the accountability for life-threatening events that AI-generated responses may cause is poorly defined. The loneliness caused by the digital revolution may be exacerbated by the use of AI, especially in situations where human experiences and empathy are paramount [10]. The immense potential of AI in healthcare is undeniable. However, at this stage, it may be prudent to use AI to help psychiatrists better understand their patients and help them diagnose rather than permitting the language models to provide unsupervised guidance to patients.

### 3 | Methodology

#### 3.1 | Data Collection in Psychiatry

Structured assessments, including specialized insight scales, psychological questionnaires, personality inventories, and clinical interviews are very important in the diagnosis of mental disorders and in gauging the patients' insight or awareness of their illness. These assessments enable clinicians to study the multiple dimensions within the patient's self-awareness of the mental state regarding his surroundings and the intent to learn about one's condition. For example, the insight scales elaborated for specific disorders, such as schizophrenia or depression, use detailed questionnaires to probe into awareness of hospitalization, attitude toward mental illness, and mastery over one's situation. In turn, insight assessment may give qualitative and quantitative information about patient improvement, allowing clinicians to monitor changes in self-concept and symptom awareness over time. These assessment findings also yield data on insight into an association with the severity of illness for an overall representation of a patient's mental health status and course [11].

Notes from the therapy sessions: unstructured data, such as the therapist session notes or therapy session transcripts, is full of sensitive information regarding patients and case histories and expressions about emotions, helping to understand the patient's mentality in a subjective manner.

Diagnostic tools and test results: examples include standardized diagnostic tools such as the DSM-5 and psychometric tests, like PHQ-9 and GAD-7 for depression and anxiety, respectively, that provide structured quantitative data on the status of mental health.

Behavioral data: behavioral data includes observed behaviors, treatment responses, and real-time monitoring when using digital tools or apps. This gives it a digital dimension, considering that it may come from wearables or mHealth applications.

Medication and treatment plans: medical and treatment plans will contain prescribed medication, including dosages and treatment outcomes. This information enables tracking of treatment effectiveness and adherence.

This is a very diverse type of data, adding to the psychiatrist's knowledge of the patient. Its sensitive nature, demanding storage securely and restricted access, makes management very complex.

#### 3.2 | Data Sensitivity and Security Needs

High sensitivity of psychiatric data: mental health data is highly personal [12]; it contains data about patients' trauma experiences, behavior, interpersonal relationships, and even mental states. This makes the data very sensitive because disclosing it improperly may affect a patient's privacy and security.

Vulnerability to abuse: psychiatric data, if accessed without authorization, could lead to severe impacts such as social ostracism, discrimination, or even harm to self or others. For example, disclosures on mental health may affect a person's chances of getting employment, insurance eligibility, or even their relationships.

Legal and ethical compliance: regulative frameworks, like HIPAA in the United States, raise the bar with strict protection of privacy for health care data, including those on mental health. Ethical standards in psychiatry

also require that the data not only be correct but also stored in a manner that respects patient confidentiality and protects it legally.

Secure data collection and storage: data sensitivity, vulnerability, and other compliances have created the need for secure data storage systems that offer controlled access, immutability, and transparency. Blockchain [13–15], combined with access controls and encryption, provides just the right solution. It provides data privacy on the one hand and enables authorized use to do analytics or even treatment monitoring on the other.

Access control and traceability: any secure system should log onto those who accessed data so that traceability is enabled only to authorized personnel, leaving clear touch points. This helps increase accountability, particularly when data is used for research or AI-based analysis.

### 3.3 | Implementing LLMs for Data Analysis in Psychiatry

With LLMs, the range of psychiatric data analysis is huge, clinical insight is enhanced, and patient care is enhanced [16]. The nature of data collection in psychiatry encompasses several unstructured forms, such as therapist notes, session transcripts, and assessment summaries. LLMs use NLP techniques to decode complex language forms and extract information, such as identifying the sentiment or emotional tone in a patient's speech, which is essential when monitoring mental health. For instance, LLMs may pick up minute linguistic cues of changing a patient's mental state, giving broader insight into the patient's emotional status [17]. With topic modeling and summarization, LLMs systematize information from several sessions to effectively allow clinicians to review patient history and symptom changes without going through vast notes. The synthesis and prioritization capability further enhances patient monitoring and allows practitioners to rivet their resources on a few important areas that really need intervention.

Privacy-preserving approaches can be integrated into LLMs using differential privacy techniques. These introduce controlled statistical noise, anonymizing individual data points but leaving the aggregate analysis intact. Therefore, such measures allow LLMs to generate insights without risking patient confidentiality, which is central to maintaining trust in AI-enhanced psychiatric tools. Using the former, through analyzing general patterns rather than specific ones and thus shielding sensitive information regarding patients, LLMs can significantly assist clinicians in grasping broad mental health trends and personalizing treatment. Applying LLMs in psychiatry would enhance the diagnosis and precision of therapy. At the same time, all benefits would be lucratively secured responsibly through given privacy safeguards.

Despite the advantages, implementing LLMs in psychiatry raises essential challenges concerning data bias, ethical considerations, and transparency [18]. LLMs would be trained on large datasets, which tend to expose models to socio-cultural biases that might afterward affect clinical acumen unintended and result in biased or unfair assessments. In mental health, this might be particularly problematic, as behavioral misinterpretation based on demographic or cultural variables may occur. Therefore, these LLMs in psychiatry should be trained on carefully curated data, reflecting balanced perspectives, so that bias becomes minimal and the model outputs align with accurate and just mental health assessments.

The sensitive nature of psychiatric data also builds up very strong demands regarding ethical practices concerning privacy and informed consent. Any unauthorized access or improper data handling might result in a serious breach of confidentiality for a patient. It might slowly lead to losing confidence in using AI technologies within healthcare. Psychiatric institutions must use robust anonymization processes and clearly inform patients about the usage and analysis their data will be put to. Similarly, building clinician confidence requires transparent and explainable AI practices. As many LLMs are black-box models, it might be non-intuitive for the clinician to understand how some conclusions have been derived. By using explainability techniques, such as summarized insight or confidence scores, clinicians will more easily validate and build trust in LLM output and thoughtfully integrate it into patient care.

Besides data privacy and transparency, patients' autonomy must be preserved by being entitled to consent to or opt out of analyses based on LLMs. Thus, the added advantage of accessing data with controls is that it

secures such information against unauthorized access, which also aligns the application of the LLM to privacy and ethical standards. These ethical measures form a basis for responsible use that, together with technical safeguards, enables AI to support mental health care in ways that put the welfare of patients first and uphold clinical integrity.

### **3.4 | Blockchain for Psychiatry-Ensuring Security of Data Storage**

Coupled with blockchain technology, which securely stores psychiatric data, is a revolution in the mental health sector's data management field. The decentralized and immutable nature of the blockchain especially applies to handling sensitive psychiatric information, where confidentiality and data integrity are the primary concerns. Psychiatric records often contain highly sensitive personal data; if unauthorized access or alteration occurs, it may interfere with the patient's privacy and trust. It enables blockchain technology to meet these challenges by storing data transparently and effectively controlling access based on cryptographic mechanisms and identification protocols.

#### **3.4.1 | Designing a blockchain solution for psychiatric data**

Psychiatric data stored using a blockchain solution provides security and tamper evidence through cryptographic techniques. Data about each patient can be encrypted and kept in a distributed ledger, with access controlled by cryptographic keys. Only the corresponding decryption keys, held by authorized parties such as designated clinicians or other authorized healthcare providers, could view or update the information and, therefore, keep patient information confidential [8]. This can be achieved by implementing asymmetric cryptography, in which one participant has a private key, kept secret, and a public key that lets others verify their identity without revealing the private information [19]. This creates opportunities for strict control over access on a very granular, role-based level, preventing unauthorized exposure or editing of sensitive data.

Moreover, immutability in blockchain means that data cannot be removed after being recorded or retroactively altered [20]. Any modifications are written as new entries, leaving the original recordings intact, thereby allowing for an audit trail that is quite transparent and really states who accessed or changed information related to a patient. In psychiatric contexts where data integrity bears consequences in clinical decision-making, this kind of auditability is demanded. In addition, permissioned blockchain architectures, such as Hyperledger Fabric, can be used interchangeably to introduce an additional layer of access control, allowing access to selected nodes within the network only to the owner. Thus, in such scenarios, only certified network participants, such as licensed psychiatrists or institutional administrators, would be authorized to participate and, by doing so, further minimize unauthorized access or potential data breach incidents.

#### **3.4.2 | Interfacing LLMs with blockchain**

Things become further complicated when LLM are given access to psychiatric data stored in blockchains. This requires creating a method that allows LLM to securely interface with blockchains, where data access and model analysis can only be performed with proper oversight [21]. This is the point at which a secure API or oracle would serve as a bridge between the LLM and the blockchain. This means that the oracles fetch only selected data from the blockchain, depending on what the AI model queries. This way, LLMs will not directly access raw blockchain data but get only relevant and authorized information. This structure will also ensure that data integrity is maintained and that the LLM is not allowed uncontrolled access to sensitive patient records.

To ensure that the data is kept secure during this interface, each data request by the LLM could be validated via a smart contract [22]. These smart contracts, baked into the blockchain, verify a requester's identity and permission level before divulging data. This approach avoids requests for unauthorized or unwarranted access and safely automates interaction with the blockchain and LLM. Additionally, methods of encryption and anonymization can be employed such that even LLMs receive data in de-identified form, according to privacy standards such as HIPAA.

Time-stamped and immutable records from blockchain further enhance the security of LLM integrations by providing tamper evidence logs for each access request and interaction. When training LLMs on trends in aggregate data is necessary, this may be done using privacy preservation techniques such as federated learning or differential privacy. While LLMs learn psychiatric data, they do so without compromising individual patients' privacy and also follow the ethical use of such data for mental healthcare.

## **4 | Integration of Blockchain and LLM for Psychiatry Medical Care**

This system will integrate blockchain technology with LLM to enable secure and efficient psychiatric care. The system's design should collect, store, and analyze sensitive psychiatric data with an emphasis on data privacy, integrity, and access authorization, furthering clinical insights through AI-driven data analysis.

### **4.1 | System Components**

Data collection and storage layer (blockchain): data come from psychiatric data, including structured assessments-for example, insight scales, and diagnostic questionnaires-unstructured sources, such as therapist notes and session transcripts, behavioral data, like real-time monitoring with wearable devices, and treatment records, such as lists of medications and dosages.

Storage: each entry will be encrypted and stored in a decentralized, tamper-proof ledger by a permission blockchain like Hyperledger Fabric. Because this is blockchain, any entry in the database is traceable and immutable, and each entry will show timestamp information about the identity of authorized personnel who accessed it.

Control access: asymmetric encryption only makes Patient information available to authenticated users, clinicians, and other caregivers. Data is protected by cryptographic keys in that no third party can access the data except a select few who have been allowed to decrypt the keys; thus, there is data confidentiality and consideration of privacy laws such as HIPAA.

### **4.2 | Layer of Data Processing and Analysis**

Unstructured data NLP: the LLM will process unstructured text from the therapy notes, session transcripts, and patient self-assessments; perform the overall sentiment and topic modeling to provide insight into the patient's state of mind, their behavioral modifications, and improvement that the clinicians review for temporal monitoring of mental health.

Data summarization and prioritization: LLM summarizes patient history to identify symptoms or areas that need intervention, saving clinicians the work of going through voluminous notes manually. It will also track subtle linguistic changes that may signal shifts in mental health features, which will be particularly useful for early detection and response to changes in mental health conditions.

Privacy-preserving data processing: a classic example is differential privacy, a technique that allows LLM to analyze the trend across patients with assurance that individual patient data is anonymous and, hence, confidential while supporting personalized and population-level insights.

### **4.3 | Secure API/Oracle**

Data bridge: an intermediary could allow controlled data access based on pre-defined permissions in the interaction between the blockchain and the LLM. This oracle fetches relevant data fields from the LLM but does not reveal raw data from underneath the blockchain.

Smart contracts for validation: each request for data is first validated by smart contracts, which ensure that only the authorized queries are returned. This would prevent unauthorized access because smart contracts impose permissions and audit each interaction with the LLM.

Anonymization and encryption: the interfacing layer further anonymizes data as required and ensures that all privacy standards are satisfied without exposing sensitive identifiers to the LLM's data processing pipeline.

#### 4.4 | Audit and Compliance Module

Access logs: the blockchain log's immutable record logs each access or modification request, leaving a clear audit trail that traces data interactions. This level of transparency enhances accountability and can be reviewed against compliance or auditing purposes.

Real-time alerts: each unauthorized attempt to access or modify data will trigger alerts to the administrator for timely responses in case of a possible security breach. This ensures that psychiatric records remain intact and unviolated.

Patient consent management: the patient may grant or revoke consent to perform certain analytics on their data. The system will register the patient's preferences transparently using the blockchain. This gives the patient control over how their data are used and adheres to ethical guidelines related to informed consent.

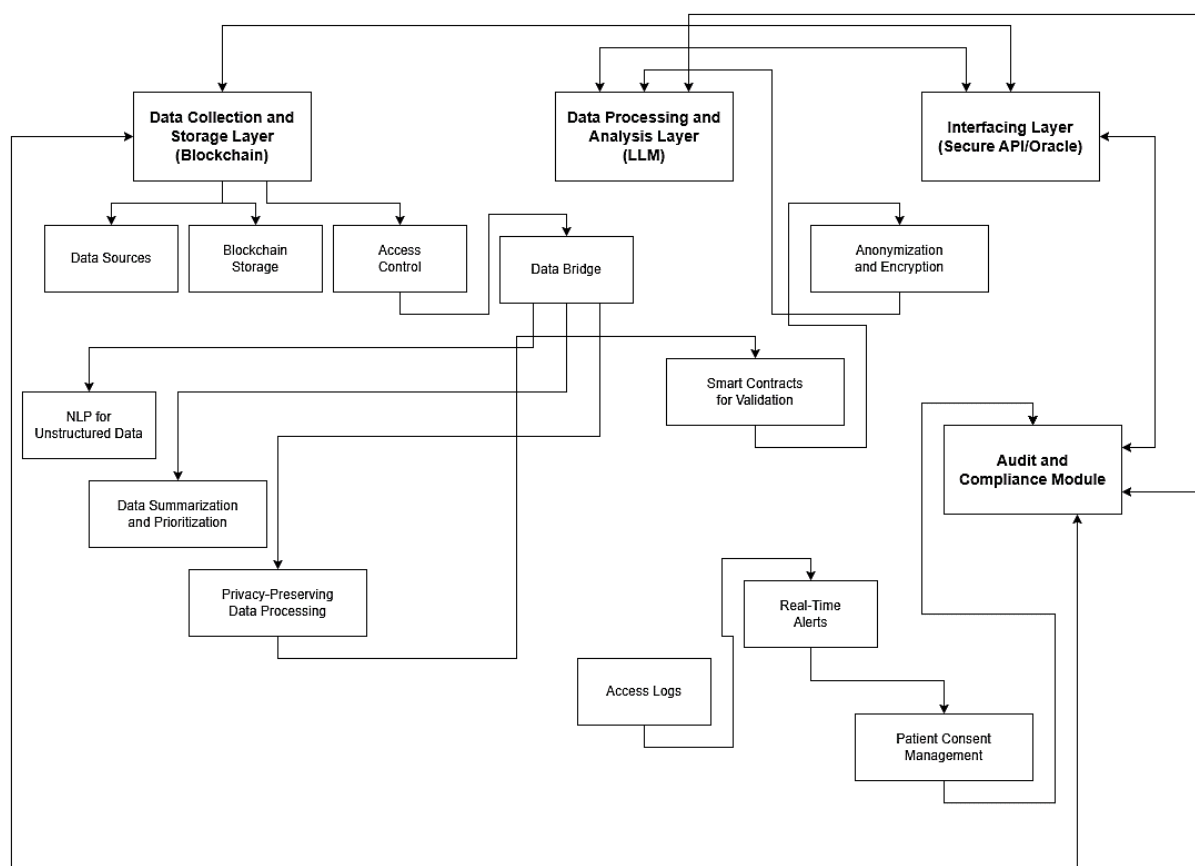


Fig. 1. System design.

## 5 | Conclusion

Integration of blockchain and LLMs for sensitive psychiatric data: blockchain is a decentralized, immutable ledger that allows unparalleled security, transparency, and access to data, while LLMs are advanced in uncovering meaning from unstructured data and providing clinical insights. Put together, these technologies meet the challenges of protecting psychiatric data from breaches, ensuring regulatory compliance, and protecting patient confidentiality.

A synergy that offers a better guarantee of security and integrity for psychiatric records and advances quality in care through data-driven, personalized interventions. The sensitive data analytics are done responsibly and

ethically as the proposed system design incorporates secure APIs, techniques that preserve privacy, and real-time monitoring. This integration is poised to disrupt psychiatric data management by empowering clinicians with actionable insights while ensuring patient privacy, enabling trust, improving outcomes, and setting a new standard in innovation for mental health.

## References

- [1] Balajee, R. M., Mohapatra, H., & Venkatesh, K. (2021). A comparative study on efficient cloud security, services, simulators, load balancing, resource scheduling and storage mechanisms. *IOP conference series: materials science and engineering* (Vol. 1070, p. 012053). IOP Publishing. <https://doi.org/10.1088/1757-899x/1070/1/012053>
- [2] Swain, B., Raj, P., Singh, K., Singh, Y., Singh, S., & Mohapatra, H. (2025). Ethical implications and mitigation strategies for public safety and security in smart cities for securing tomorrow. In *Convergence of cybersecurity and cloud computing* (pp. 419–436). IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3693-6859-6.ch019>
- [3] Act, A. (1996). Health insurance portability and accountability act of 1996. *Public law*, 104, 191. <https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996>
- [4] Zhou, B., Yang, G., Shi, Z., & Ma, S. (2022). Natural language processing for smart healthcare. *IEEE reviews in biomedical engineering*, 17, 4–18. <https://doi.org/10.1109/RBME.2022.3210270>
- [5] Hasselgren, A., Kravlevska, K., Gligoroski, D., Pedersen, S. A., & Faxvaag, A. (2020). Blockchain in healthcare and health sciences—A scoping review. *International journal of medical informatics*, 134, 104040. <https://doi.org/10.1016/j.ijmedinf.2019.104040>
- [6] Kumar, S., Lim, W. M., Sivarajah, U., & Kaur, J. (2023). Artificial intelligence and blockchain integration in business: trends from a bibliometric-content analysis. *Information systems frontiers*, 25(2), 871–896. <https://doi.org/10.1007/s10796-022-10279-0>
- [7] Heston, T. F. (2024). *Perspective chapter: integrating large language models and blockchain in telemedicine*. IntechOpen. <https://www.intechopen.com/chapters/1176440>
- [8] Omar, M., Soffer, S., Charney, A. W., Landi, I., Nadkarni, G. N., & Klang, E. (2024). Applications of large language models in psychiatry: A systematic review. *Frontiers in psychiatry*, 15, 2003–2024. <https://doi.org/10.3389/fpsy.2024.1422807>
- [9] Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: A systematic review. *Healthcare*, 7(2), 56. <https://doi.org/10.3390/healthcare7020056>
- [10] Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H. R., Albarqouni, S., ... & Cardoso, M. J. (2020). The future of digital health with federated learning. *NPJ digital medicine*, 3(1), 1–7. <https://doi.org/10.1038/s41746-020-00323-1>
- [11] Terra, M., Baklola, M., Ali, S., & El-Bastawisy, K. (2023). Opportunities, applications, challenges and ethical implications of artificial intelligence in psychiatry: A narrative review. *The egyptian journal of neurology, psychiatry and neurosurgery*, 59(1), 80. <https://doi.org/10.1186/s41983-023-00681-z>
- [12] Marková, I. S., & Berrios, G. E. (1992). The assessment of insight in clinical psychiatry: a new scale. *Acta psychiatrica scandinavica*, 86(2), 159–164. <https://doi.org/10.1111/j.1600-0447.1992.tb03245.x>
- [13] Luxton, D. D., June, J. D., & Fairall, J. M. (2012). Social media and suicide: A public health perspective. *American journal of public health*, 102(S2), S195–S200. <https://doi.org/10.2105/AJPH.2011.300608>
- [14] Radanović, I., & Likić, R. (2018). Opportunities for use of blockchain technology in medicine. *Applied health economics and health policy*, 16(5), 583–590. <https://doi.org/10.1007/s40258-018-0412-8>
- [15] Awotunde, J. B., Jimoh, R. G., Folorunso, S. O., Adeniyi, E. A., Abiodun, K. M., & Banjo, O. O. (2021). Privacy and security concerns in IoT-based healthcare systems. In *The fusion of internet of things, artificial intelligence, and cloud computing in health care* (pp. 105–134). Springer. [https://doi.org/10.1007/978-3-030-75220-0\\_6](https://doi.org/10.1007/978-3-030-75220-0_6)
- [16] Kim, S. K., & Huh, J. H. (2020). Autochain platform: expert automatic algorithm blockchain technology for house rental dApp image application model. *EURASIP journal on image and video processing*, 2020(1), 47. <https://doi.org/10.1186/s13640-020-00537-z>

- [17] Nicholas, J., Onie, S., & Larsen, M. E. (2020). Ethics and privacy in social media research for mental health. *Current psychiatry reports*, 22(12), 1–7. <https://doi.org/10.1007/s11920-020-01205-9>
- [18] Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). *On the dangers of stochastic parrots: can language models be too big?* [presentation]. FAccT 2021 - proceedings of the 2021 ACM conference on fairness, accountability, and transparency (pp. 610–623). <https://doi.org/10.1145/3442188.3445922>
- [19] McCradden, M., Hui, K., & Buchman, D. Z. (2023). Evidence, ethics and the promise of artificial intelligence in psychiatry. *Journal of medical ethics*, 49(8), 573–579. <https://doi.org/10.1136/jme-2022-108447>
- [20] Zyskind, G., Nathan, O., & others. (2015). Decentralizing privacy: using blockchain to protect personal data. *2015 IEEE security and privacy workshops* (pp. 180–184). IEEE. <https://doi.org/10.1109/SPW.2015.27>
- [21] Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., & Ni, W. (2020). PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Computers and security*, 88, 101653. <https://doi.org/10.1016/j.cose.2019.101653>
- [22] Yaqoob, I., Salah, K., Uddin, M., Jayaraman, R., Omar, M., & Imran, M. (2020). Blockchain for digital twins: recent advances and future research challenges. *IEEE network*, 34(5), 290–298. <https://doi.org/10.1109/MNET.001.1900661>
- [23] Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: concept and applications. *ACM transactions on intelligent systems and technology*, 10(2), 1–19. <https://doi.org/10.1145/3298981>