OmniIndex FHE: Encrypted Search & Analytics

Five examples of the security, privacy and productivity benefits of OmniIndex's patented ability to search & analyze fully encrypted data.

OmniIndex

White Paper

OmniIndex

FHE Overview

OmniIndex's patented fully homomorphic encryption provides the only commercial solution for searching and performing computations on fully encrypted data in real-time.

It is based on Synchronous AES 256 using the CryptoPP libraries which are deemed uncrackable through brute-force attacks.

This means data does not have to be decrypted and left vulnerable to exposure through accidental or deliberate actions.

OmniIndex's technology is protected by a number of international patents. These include:

Secure Database Searching (US10346633B2)

This patent describes a method for enabling secure searches on encrypted data. It employs element-wise encryption and a specialized comparison technique to match encrypted search queries with encrypted data, preserving data confidentiality throughout the search process.

Search Index (US10552466B2, US9519665B2, and US20140324877A1)

These patents disclose a system for creating searchable indexes for encrypted data. The system utilizes a function to transform data elements into a searchable encrypted form, allowing users to query the encrypted index without decrypting the underlying data.

> "The problem with encrypted data is that you must decrypt it in order to work with it. By doing so, it's vulnerable to the very things you were trying to protect it from by encrypting it.
>
> There is a powerful solution to this scenario: homomorphic encryption."

FORBES

OmniIndex

OmniIndex: Confidential Data Solutions

OmniIndex's fully homomorphic encryption is a key technology in all of its confidential data solutions. This includes the Dropblock file store and the award-winning Web3 data platform PostgresBC.

This paper explores five use cases of how OmniIndex's patented FHE technology has been used by their customers and partners, focusing on the real-world benefits of this technology today:

Threat Intelligence
Zero-Trust Privacy Controls
DICOM Image Analytics
Financial Data Analysis
PII Redaction

Zero-Trust Access

Real-Time Integration

Homomorphic Encryption

Blockchain Storage

OmniIndex

OmniIndex

Threat Intelligence

Unlike other log management and analysis tools, OmniIndex uniquely ensures log files are never left vulnerable to attack through decryption. This is because OmniIndex enables data to remain encrypted at rest, in transit, and in use. What's more, log files are inoculated from ransomware attacks due to OmniIndex's secure systems.

Our native and private AI, Boudica, then analyzes the encrypted log files in real-time to identify patterns, threats & vulnerabilities in the system. For example, an AI risk assessment of 1.5 million encrypted records pulling back 200,000 rows can be done in under 400 milliseconds.

Potential Security Insights Include:

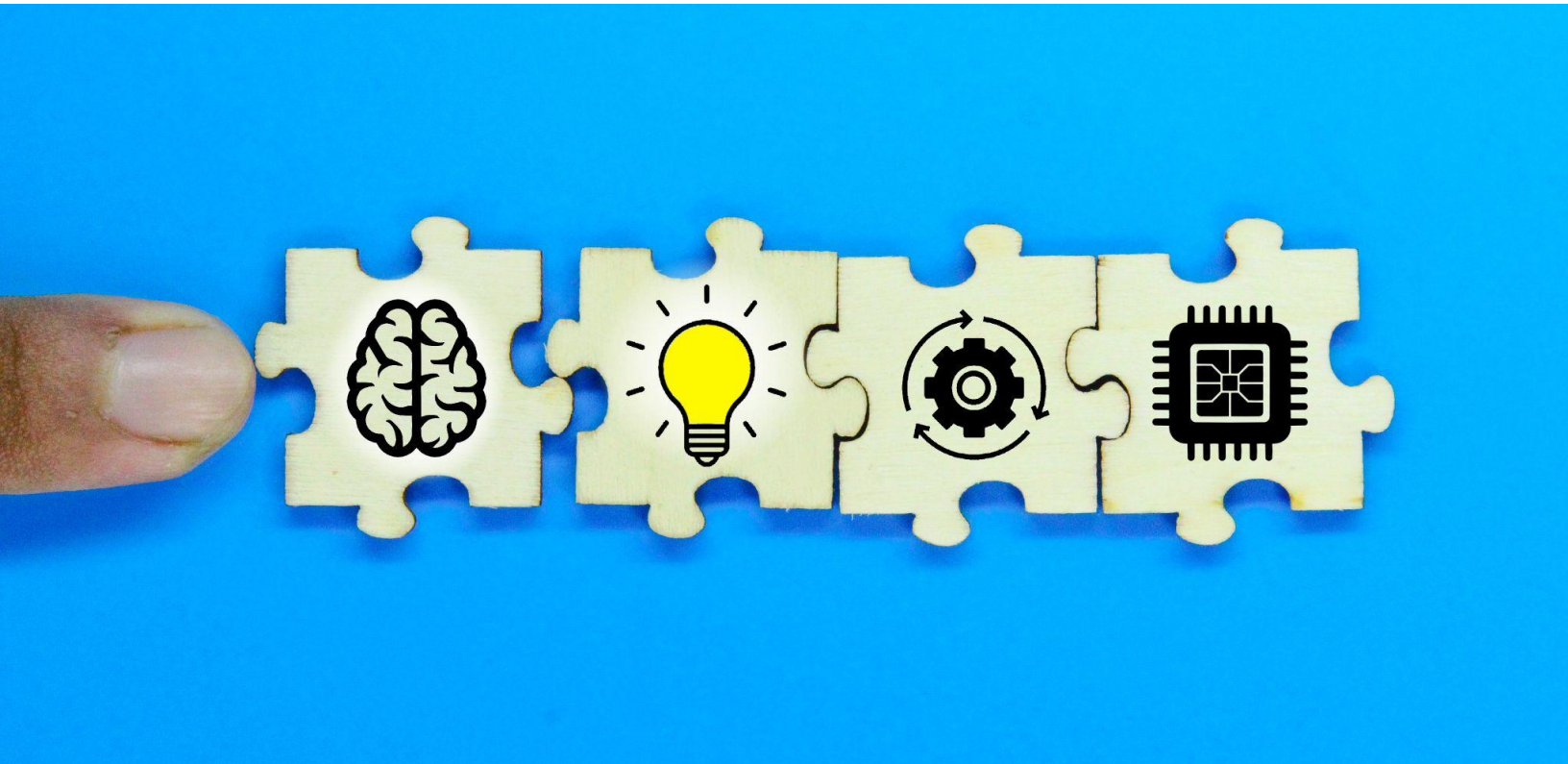
Brute Force Attacks:
Frequent failed login attempts from unusual IP addresses or locations could suggest a brute force attack is underway.

Unauthorized User Access:
Detection of logins by users who should not have access to the system or attempts to access restricted resources.

Unknown Processes or Files:
Detection of unknown processes or files running on the system, which could be signs of malware infection.

Network Traffic Anomalies:
Unusual network traffic patterns, such as excessive outbound connections or suspicious DNS requests.

Unusual Access Patterns:
Detecting unusual access patterns from trusted users, such as accessing sensitive data outside of normal working hours or from unusual locations.



OmniIndex

Zero-Trust Privacy Control

Super user and admin accounts pose a significant risk to data security and privacy. This has been an historic issue with traditional data and file systems, and remains a concern with contemporary zero-trust systems too.

This is because a compromised super user account can render perimeter security measures ineffective due to their vast access levels across the system.

The challenge is that these users require full access to the data due to the types of administrative tasks they need to perform. As such, systems are either having to accept the risk, or lose the ability to perform these tasks.

Homomorphic encryption offers a powerful solution. This is because the technology allows users to do crucial tasks without the data being decrypted & exposed. Examples include:

Troubleshooting performance issues:
Super users can analyze query execution plans and identify bottlenecks without accessing sensitive data within those queries, ensuring efficient database operation while preserving confidentiality.

Performing data migrations:
Super users can migrate data between different databases or systems without exposing sensitive information, ensuring data integrity and confidentiality throughout the migration.

Auditing user activity:
Super users can analyze audit logs and monitor user actions without accessing the underlying sensitive data, enabling effective security monitoring & compliance auditing.

OmniIndex

Medical Image Analytics

OmniIndex uniquely enables organizations to analyze fully encrypted health records and medical images; including DICOM.

DICOM stands for Digital Imaging and Communications in Medicine. These images contain many different types of data including device usage and patient information. This data is crucial in Healthcare and Life Science, however due to the strict regulations around patient data & the difficulty in using this type of data DICOM images are vastly underutilized.

OmniIndex enables organizations to utilize this information in their workflow due to the ability to keep the data encrypted at all times. Potential benefits include:

Improved Diagnostics:
Analyze encrypted DICOM images to identify patterns and anomalies, potentially aiding in faster & more accurate diagnoses without compromising patient privacy.

Efficient Collaboration:
Securely share DICOM images with specialists & healthcare providers for consultations and second opinions, improving patient care and streamlining the process for efficiency.

Regulatory Compliance:
Ensure adherence to strict healthcare data privacy regulations (e.g HIPAA) by keeping patient data encrypted at all times: in storage, in transit, and in use.

Device Utilization and Management:
Gain insights into machine utilization & maintenance needs without exposing any regulated data or PII. This can aid efficiency and optimize patient care.

OmniIndex

Financial Data Analysis

Financial institutions face a growing challenge: balancing the need to extract valuable insights from sensitive customer data with the critical imperative to protect that data from fraud while complying with stringent regulations & defending it from ransomware attacks.

Traditional data security measures often result in data silos to keep the most regulated data away from the main workflow, hindering analysis and limiting the potential for innovation & insights.

Homomorphic encryption offers a groundbreaking alternative, keeping this data secure without removing it from the workflow. This enables institutions to:

Derive actionable insights without compromising data security:
Analyze encrypted data to identify patterns, anomalies, and trends that can inform strategic decision-making.

Enhance fraud detection capabilities:
Utilize AI and machine learning algorithms to detect fraudulent activities in real-time by analyzing encrypted transaction data.

Improve risk management and regulatory compliance:
Perform risk assessments and ensure compliance with data protection regulations while keeping data encrypted.

Gain a deeper understanding of customer needs:
Analyze encrypted customer data to personalize services, improve customer satisfaction, and develop targeted products.

OmniIndex

PII Redaction

OmniIndex Dropblock enables users to automatically redact PII data (telephone numbers, social security numbers, zip codes, email addresses) in their files to ensure none of this regulated and confidential information is exposed when a file is shared or analyzed.

The redacted data is encrypted with FHE and stored in the user's own blockchain storage. Only authorized users are then able to unredact that data, meaning they can share the file with others with complete confidence the redacted information cannot be exposed.

This not only provides the security and privacy needed for such sensitive data, but also unlocks a number of secure productivity options too due to the homomorphic nature of the encryption. Including:

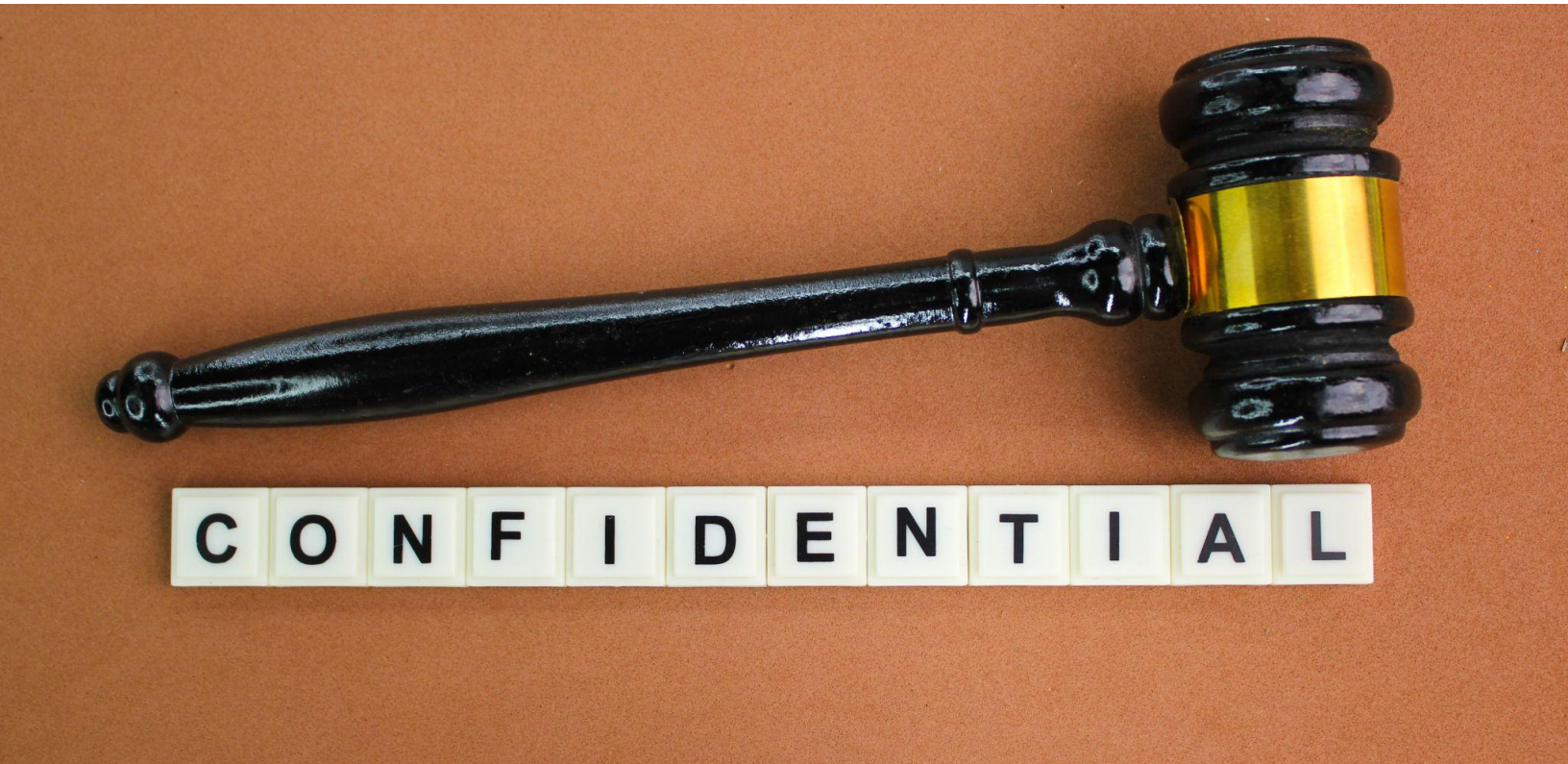
Customer Sentiment Analysis:
Analyze feedback containing PII (names, emails) without exposing it, ensuring compliance while extracting insights.

Medical Research:
Share patient data with researchers without compromising privacy, allowing analysis of clinical information for crucial insights.

Financial Audits:
Verify transactions containing account numbers without exposing sensitive data, ensuring audit integrity & privacy standards.

Human Resources Analytics:
Analyze employee data (performance reviews, salary etc)) to identify trends & improve HR processes without exposure.

Legal Discovery:
Share sensitive documents (contracts, emails) with legal teams while redacting PII, enabling efficient legal proceedings without compromising confidential information.



OmniIndex

OmniIndex's FHE solutions are available in a number of different plans to suit all needs. This includes a **free Developer account** of Dropblock for a single user to test and try our confidential file store.

Other Dropblock plans include:

Small Business – 250 Users – $1250 monthly subscription

Medium Business – 1,500 Users – $6,375 monthly subscription

Enterprise – Unlimited Users – $25,125 monthly subscription

Please visit our website or get in touch with us today to book a discovery meeting and learn more about the OmniIndex solutions for confidential data. Including our Web3 Data Platform, PostgresBC.

Zero-Trust Access

Real-Time Integration

Homomorphic Encryption

Blockchain Storage

OmniIndex

www.omniindex.io +1 (650) 297-4682