ZIROH Labs

PRIVACY MATTERS.

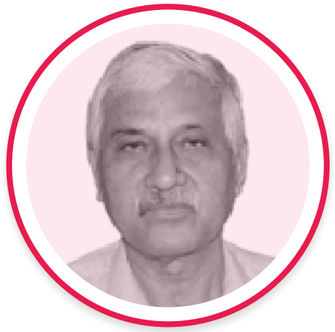
www.ziroh.com | contact@ziroh.com

Team

Distinguished Scientists, Top Engineers, Business Leaders & Innovators

Technical Advisory Team

Prof. Veni Madhavan
IISC, Bangalore
Advisor - Crypto



Prof. A K Gogoi
IIT - Guwahati
Advisor - Systems

Prof. N Sarda
IIT Mumbai
Advisor - DB

Prof. S Sadogopan
Former Director, IIIT-B
Advisor - Strategy.

Mr. Vipul Parekh
Co-Founder, BigBasket
Advisor

Locations:
US, India, Australia, Singapore, Hong Kong.

Total Employees: 82

Product Development & Engineering: 2016

HQ: US

Research Since: 2012

Team

Distinguished Scientists, Top Engineers, Business Leaders & Innovators

Executive Management Team

Dr. Whit Diffie
Turing Award, FRS
Chief Technologist

Hrishikesh Dewan
President & CEO
Former: DTH Labs, Siemens, Dell

Humphrey Polanen
Director Strategy
Led The Development Of World's First IDS

Dr. William Raduchel
Chairman, Board Of Governors
Former CFO: Sun Microsystems

Herman Collins
HR And Recruitment
Former: Sun Microsystems

Located In:
US, India, Australia, Singapore, Hong Kong.

Total Employees: 82

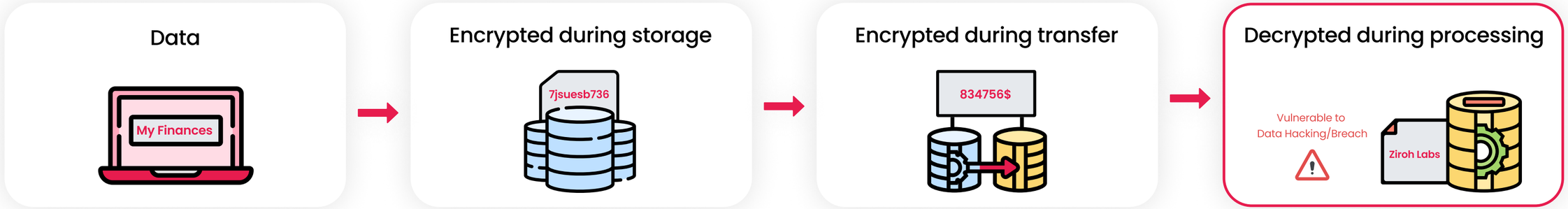
Product Development & Engineering: 2016

HQ: US

Research Since: 2012

Root cause of the problems - Decrypted Data Processing

ZIROH Labs



Eg. Data vulnerability during processing:

You Store a doc on Google Drive (encrypted)

You search for your social security number which is inside the document

Entire file is decrypted during serach

Vulnerable to hacks

You prepare a database on banking transactions by clients in 2020(encrypted)

You calculate the transactions in february

Entire table storing the transactions is decrypted during calculation

Susceptible to theft/hacking

You want to predict how many Californians travel to Cuba

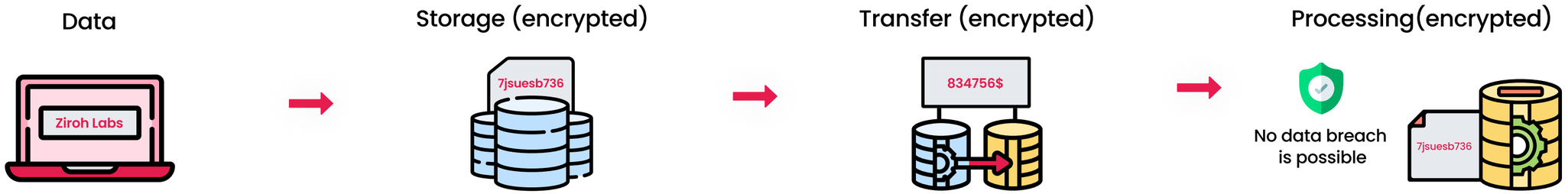
You source data from different databases to build your model

You training data is decrypted

Susceptible to theft/hacking

ZIROH Labs

Data encryption at all stages



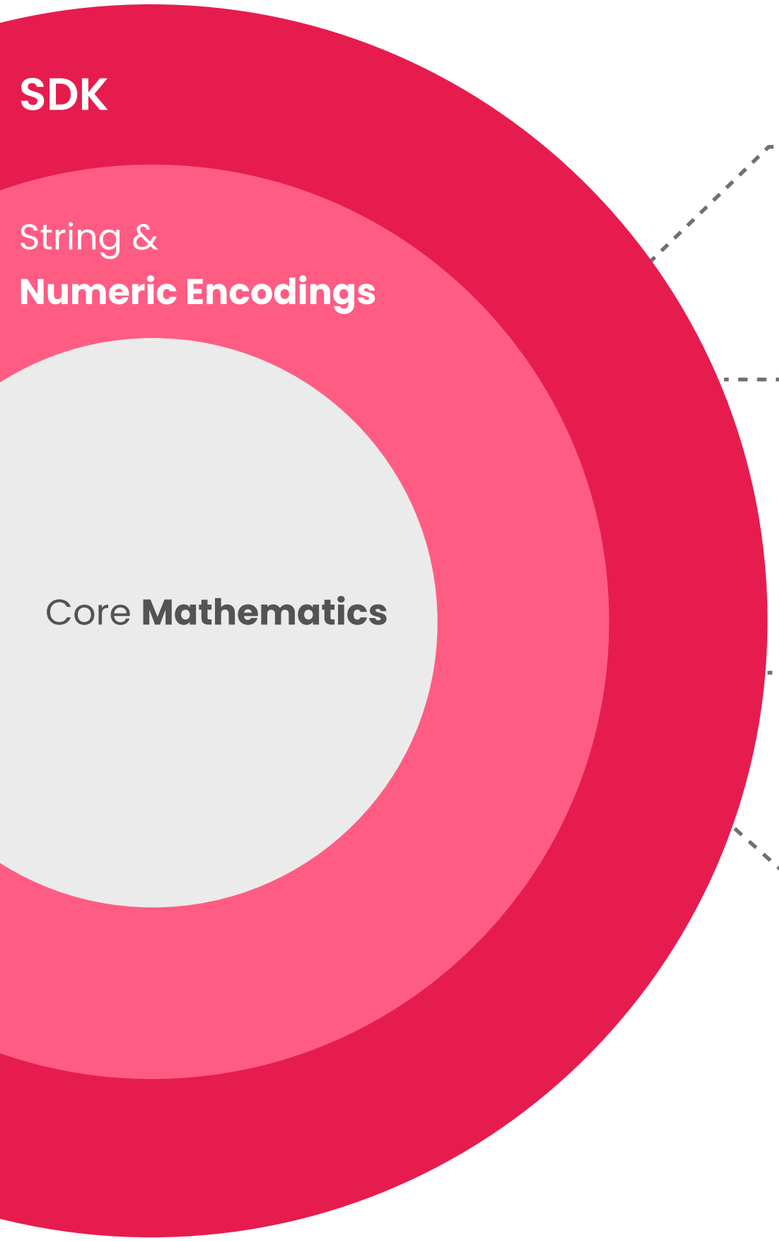
ALWAYS ENCRYPTED PARADIGM (FHE) Any device, Any storage, Any location, Any application

Ziroh Labs guarantees AN ALWAYS ENCRYPTED PARADIGM for Individuals & Businesses

- Data encryption at REST, TRANSFER & also PROCESSING
- User controlled encryption keys (decryption of data into plain text is impossible without user permission)
- Data collaboration while meeting Government data regulations.

Product Landscape

ZIROH Labs



Zunu DB

Stack to transform your database into an encrypted storage system with computing capabilities (unlimited SQL/NoSQL queries)

Zunu Drive

Stack to provide Privacy & Security of Unstructured Data in Cloud Storage Services

Zunu Mail

Stack to provide Privacy & Security of Emails

Zunu Analytics

Stack to provide Privacy & Securityof Data Sets and Model Parameters in Deep Neural Networks

- HealthVault
- FinVault
- Academic Vault
- CPAVault
- LegalVault

Built using Zunu Drive and Zunu Mail

Ziroh Core FHE

ZIROH Labs

Ziroh FHE Algorithms

ZFHE-1
(Based on RSA Assumption and Discrete Logs)

ZFHE-2
(RLWE)
{ Quantum Safe }

Our current focus is on ZFHE-1

Ziroh FHE Libraries

SecureString

Allows processing on top of encrypted string data.

SecureNumeric

Allows processing on top of encrypted numbers.

SDK's available in the following languages

ZIROH Labs

United States of America

To Promote the Progress of Science and Useful Arts

The Director

of the United States Patent and Trademark Office has received an application for a patent for a new and useful invention. The title and description of the invention are enclosed. The requirements of law have been complied with, and it has been determined that a patent on the invention shall be granted under the law.

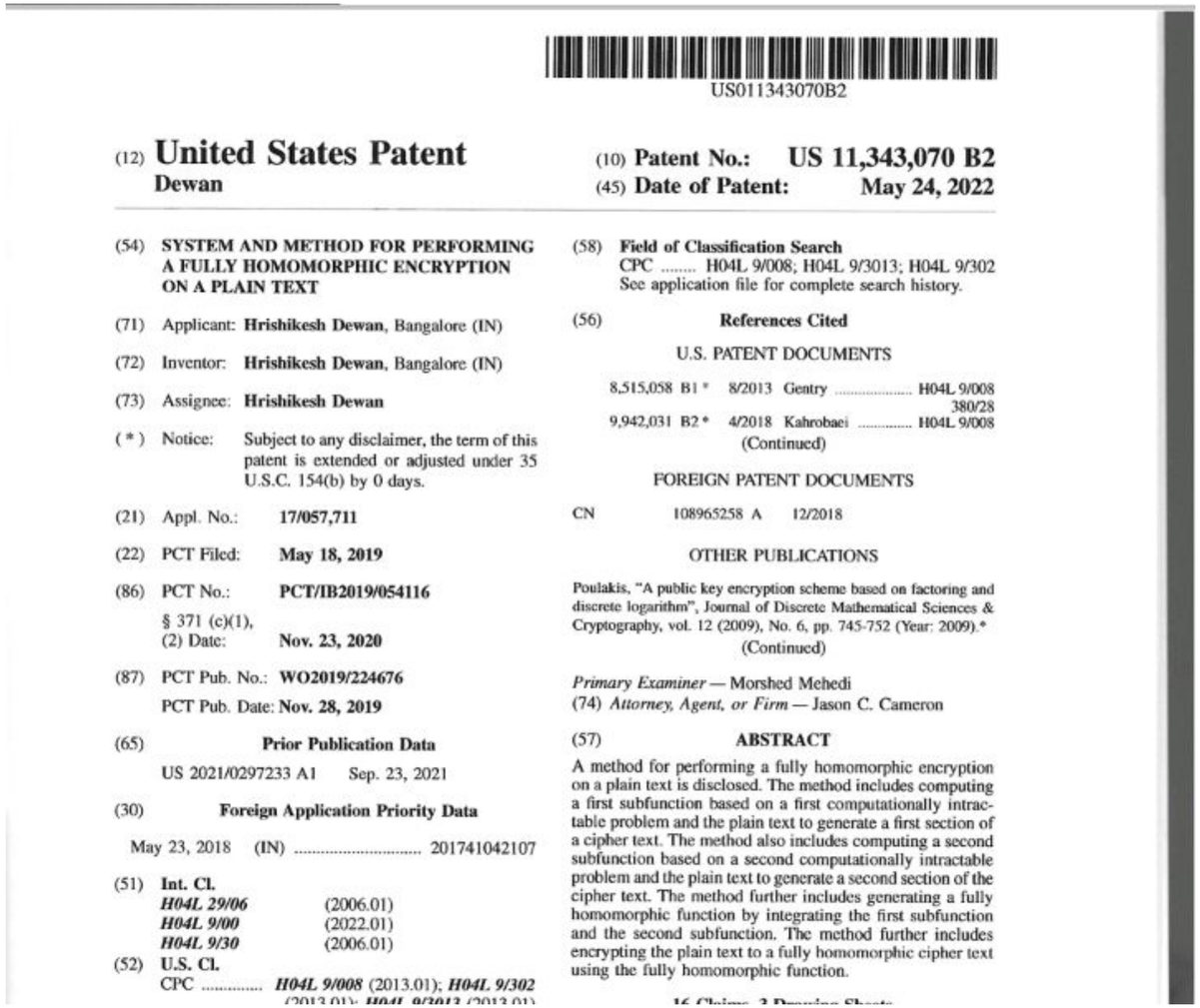
Therefore, this United States

Patent

grants to the person(s) having title to this patent the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States of America or importing the invention into the United States of America, and if the invention is a process, of the right to exclude others from using, offering for sale or selling throughout the United States of America, products made by that process, for the term set forth in 35 U.S.C. 154(a)(2) or (c)(1), subject to the payment of maintenance fees as provided by 35 U.S.C. 41(b). See the Maintenance Fee Notice on the inside of the cover.

Katherine Kelly Vidal

DIRECTOR OF THE UNITED STATES PATENT AND TRADEMARK OFFICE



US011343070B2

(12) **United States Patent**
Dewan

(10) **Patent No.: US 11,343,070 B2**
(45) **Date of Patent: May 24, 2022**

(54) **SYSTEM AND METHOD FOR PERFORMING A FULLY HOMOMORPHIC ENCRYPTION ON A PLAIN TEXT**

(71) Applicant: **Hrishikesh Dewan**, Bangalore (IN)

(72) Inventor: **Hrishikesh Dewan**, Bangalore (IN)

(73) Assignee: **Hrishikesh Dewan**

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **17/057,711**

(22) PCT Filed: **May 18, 2019**

(86) PCT No.: **PCT/IB2019/054116**
§ 371 (c)(1),
(2) Date: **Nov. 23, 2020**

(87) PCT Pub. No.: **WO2019/224676**
PCT Pub. Date: **Nov. 28, 2019**

(65) **Prior Publication Data**

US 2021/0297233 A1 Sep. 23, 2021

(30) **Foreign Application Priority Data**

May 23, 2018 (IN) 201741042107

(51) **Int. Cl.**
H04L 29/06 (2006.01)
H04L 9/00 (2022.01)
H04L 9/30 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 9/008*** (2013.01); ***H04L 9/302***

(58) **Field of Classification Search**
CPC H04L 9/008; H04L 9/3013; H04L 9/302
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

8,515,058 B1 * 8/2013 Gentry H04L 9/008 380/28
9,942,031 B2 * 4/2018 Kahrobaei H04L 9/008
(Continued)

FOREIGN PATENT DOCUMENTS

CN 108965258 A 12/2018

OTHER PUBLICATIONS

Poulakis, "A public key encryption scheme based on factoring and discrete logarithm", Journal of Discrete Mathematical Sciences & Cryptography, vol. 12 (2009), No. 6, pp. 745-752 (Year: 2009).*
(Continued)

Primary Examiner — Morshed Mehedi
(74) *Attorney, Agent, or Firm* — Jason C. Cameron

(57) **ABSTRACT**

A method for performing a fully homomorphic encryption on a plain text is disclosed. The method includes computing a first subfunction based on a first computationally intractable problem and the plain text to generate a first section of a cipher text. The method also includes computing a second subfunction based on a second computationally intractable problem and the plain text to generate a second section of the cipher text. The method further includes generating a fully homomorphic function by integrating the first subfunction and the second subfunction. The method further includes encrypting the plain text to a fully homomorphic cipher text using the fully homomorphic function.

"SYSTEM AND METHOD FOR PERFORMING A FULLY HOMOMORPHIC ENCRYPTION ON A PLAIN TEXT"

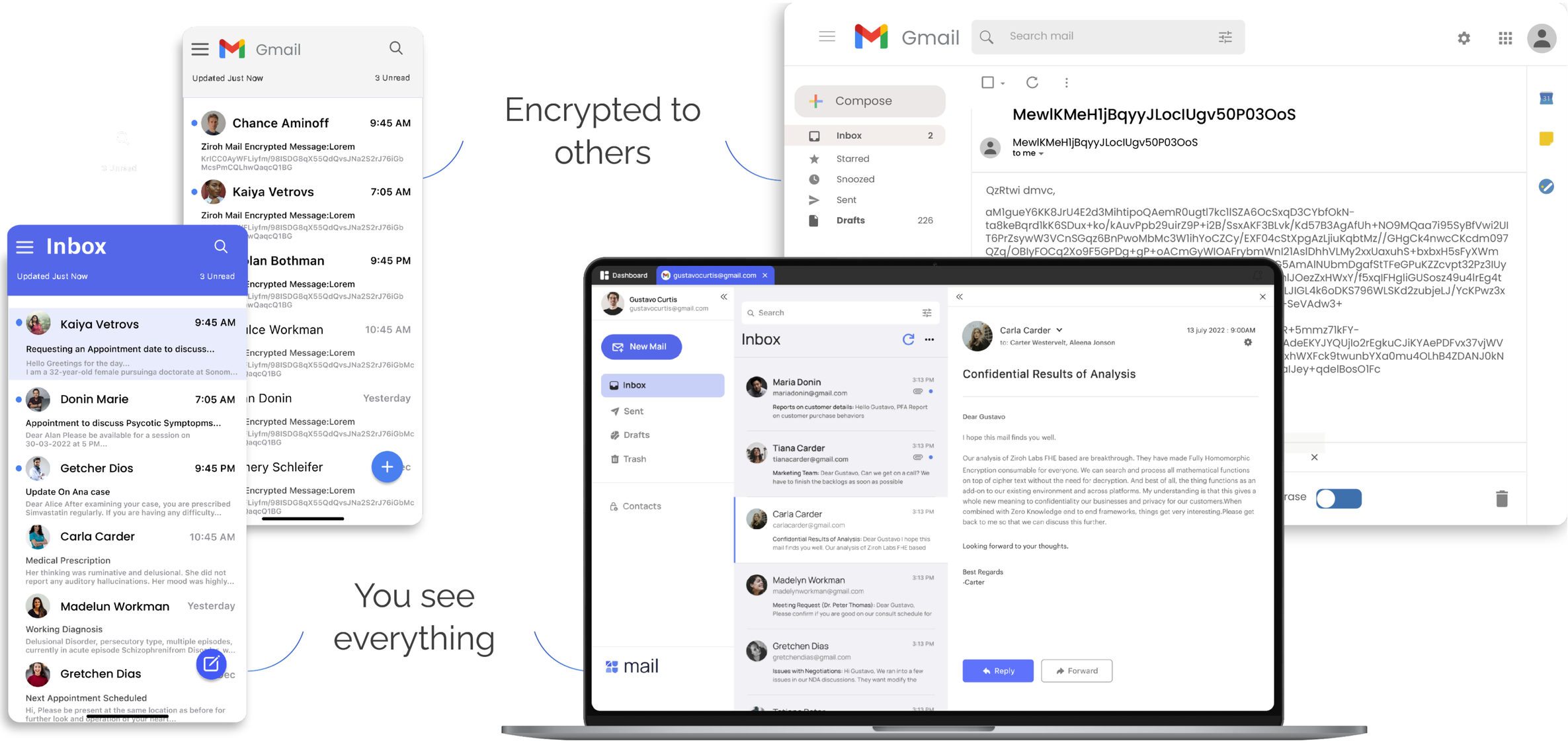
-Hrishikesh Dewan

Zunu Mail

ZIROH Labs

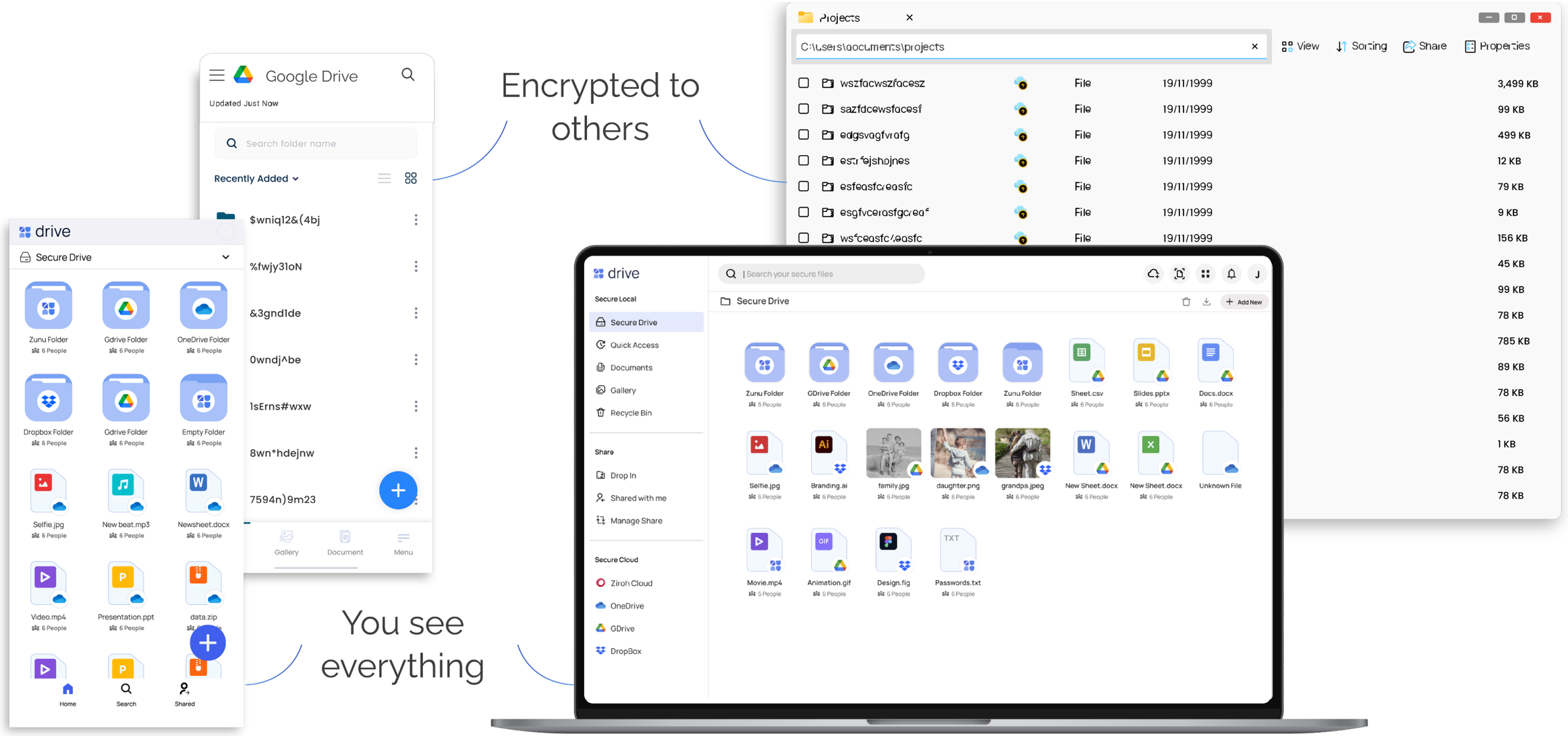
Encrypted to others

You see everything



Zunu Drive

ZIROH Labs



ZIROH Labs

Our USPs

Our products provide encryption to data during rest, transfer and also processing.

Encryption during Processing

Powered by Practical FHE

Our products are built using practical Fully Homomorphic Encryption technology (patent pending). FHE allows computations over encrypted data without decrypting it.

Guarantees full privacy from service providers

Our products provide complete privacy to user data from email/cloud/social messaging service providers.

Guarantees full privacy during hacking

Our products guarantee full privacy to user data even during hack.ing

Seamless integration to existing platforms

Our products integrate seamlessly into cloud platforms, databases, email platforms and devices without requiring any code changes

PRIVACY MATTERS.

Recognized by
Gartner
Hype Cycle 2021
Sample Vendor for
Digital Banking Transformation
Privacy Blockchain

Winner at
CISCO (LaunchPad Accelerator)
MassChallenge, Israel
Samsung Accelerator
Program

Member of
ICE71
NASSCOM (Deep Tech Club)
DSCI

Awarded
Best Papers
at IEEE

Published
6 Research
Papers

FHE Patented
by USPTO