

A FULLY SECURE SYSTEM TO TRANSPORT AND STORE DATA “NEWTECH”

Patented US
10,984,138

A fully-secured hardware system to encrypt data for transportation and storage. Once secured by NEWTECH, data are impervious to cryptographic attacks – including “brute force” and quantum computing methods.

INVENTORS

Daniel Esbensen

Steve Omohundro, Ph.D.

Data Creation's Rapid Growth

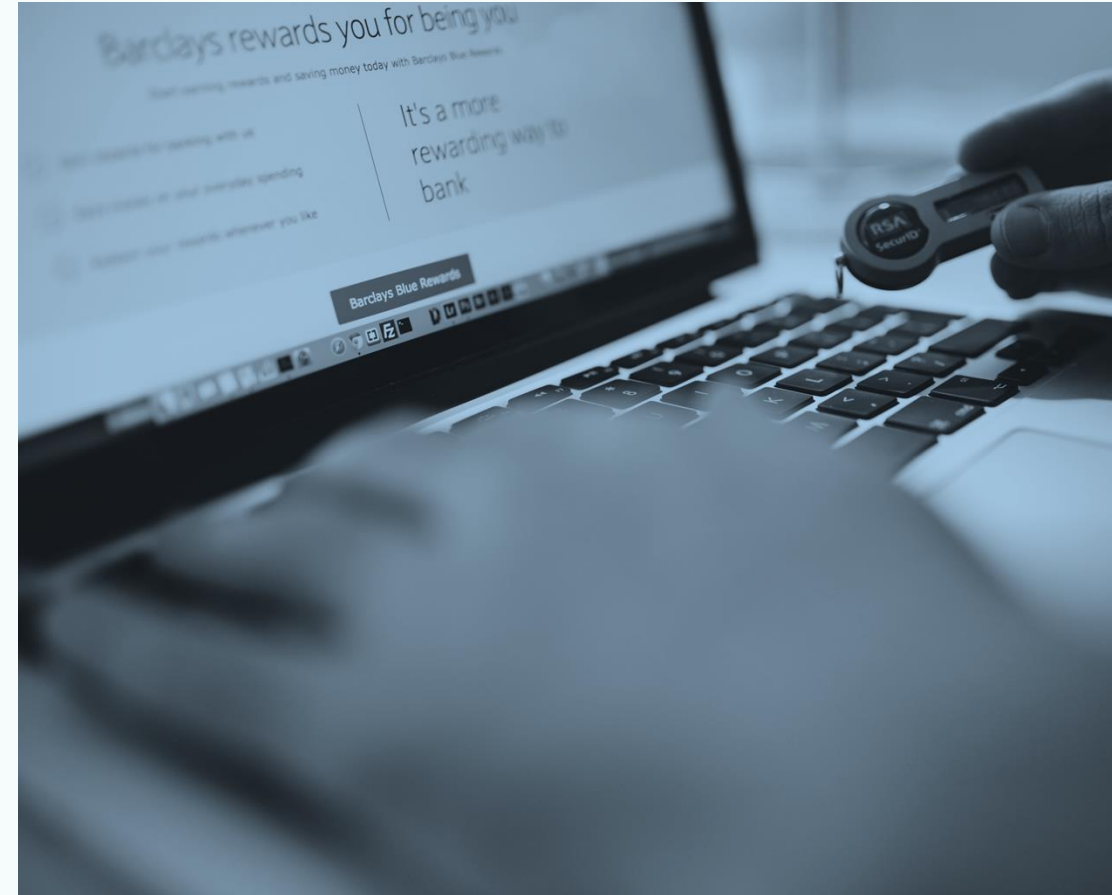
IBM found that humans now create
2.5 quintillion bytes of data daily

2,500,000,000,000,000,000



The Scope of the Problem

- Data sources are constantly under attack, and need forward security.
- They need to be secured now and for the future.
- State-of-the-art encryption methods can be broken given enough computing power. This is a mathematical truth.



Our Patented Solution NEWTECH

NEWTECH is a hardware data storage system that:

- Receives and assesses the source data to be encrypted
- Random encryption keys the same size of the data are generated. (One Time Pad)
- Applies the encryption keys to encrypt the data



How it Works

Simple Example: Encrypted data (two disks) need transport into long-term storage or moved to another site. NEWTECH allows for the two disks (one with the encrypted data and the other with the encrypted key) to become separated.

Once separated, the original data cannot be recovered until the two disks are reunited; achieving unbreakable encryption for data transportation and storage.

NEWTECH also allows for virtually unlimited permutations of number of disks used. For example, requiring that two out of three disks be reunited to unencrypt the data, or three out of five, or other permutations as security needs require.

NEWTECH is mathematically shown to be unbreakable no matter how much computing power is employed.(OTP)



Benefits of Our Solution

- Data can be transported securely by shipping one disk, waiting for confirmation of receipt, and then shipping the second disk.
- Data can be safely stored in encrypted form forever, as long as the disks are not reunited.
- The data cannot be decrypted without the required number of disks – ever. The data is secured mathematically and is completely “future proof”!



Patent: Abstract of the Disclosure

A removable storage device system that encrypts storage data with random or pseudo random bits spread across multiple storage devices either in real time or in batch mode in a way that allows the storage devices to be removed from the system and separately stored or transported in a highly secured manner.

The encryption method provides that the original storage data can only be recovered by the recombination of specific subsets of storage devices. This system is not vulnerable to advances in cryptography, is robust against storage device failure, and is immune to side-channel attacks. A wide range of embodiments can be selected in order to balance the needs for low cost, high security, and robustness against failure or loss.



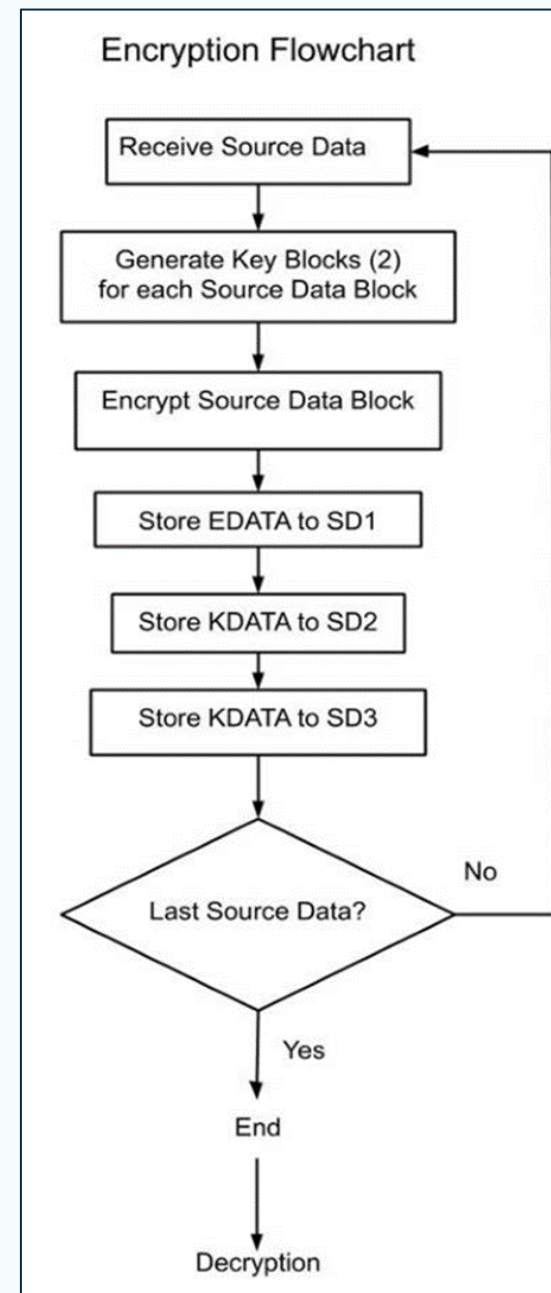
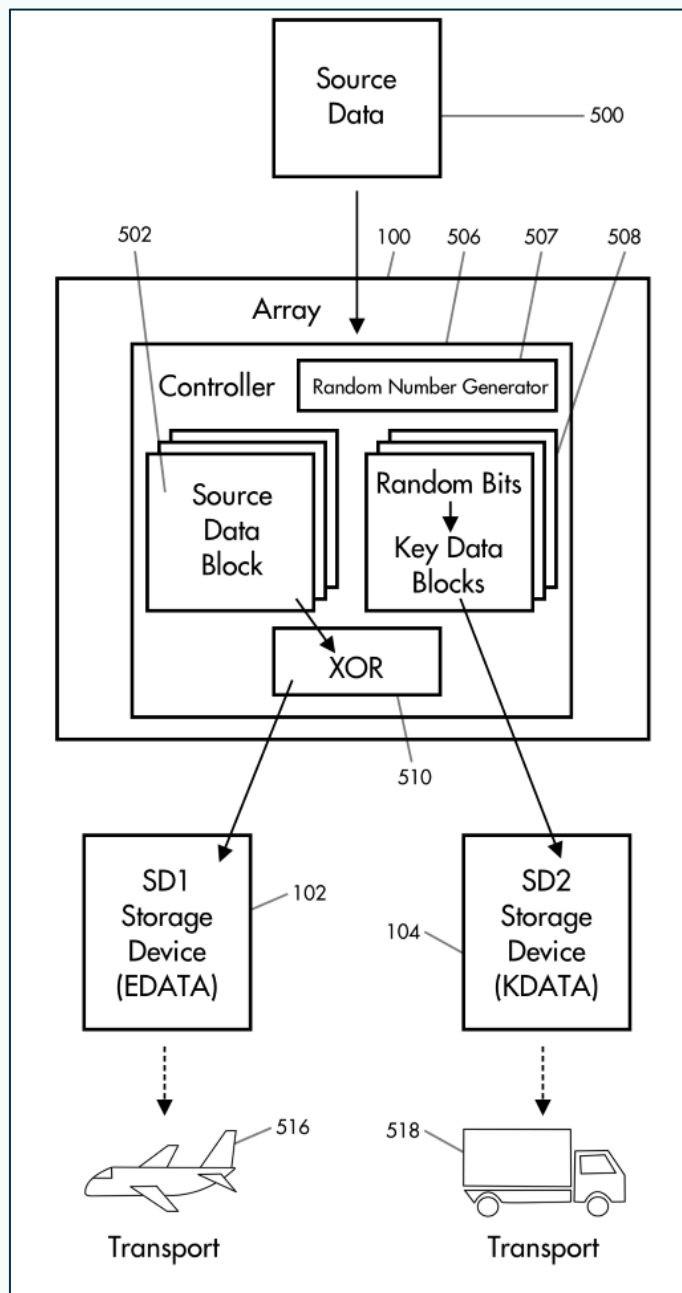
Patent: First Claim (of many...)

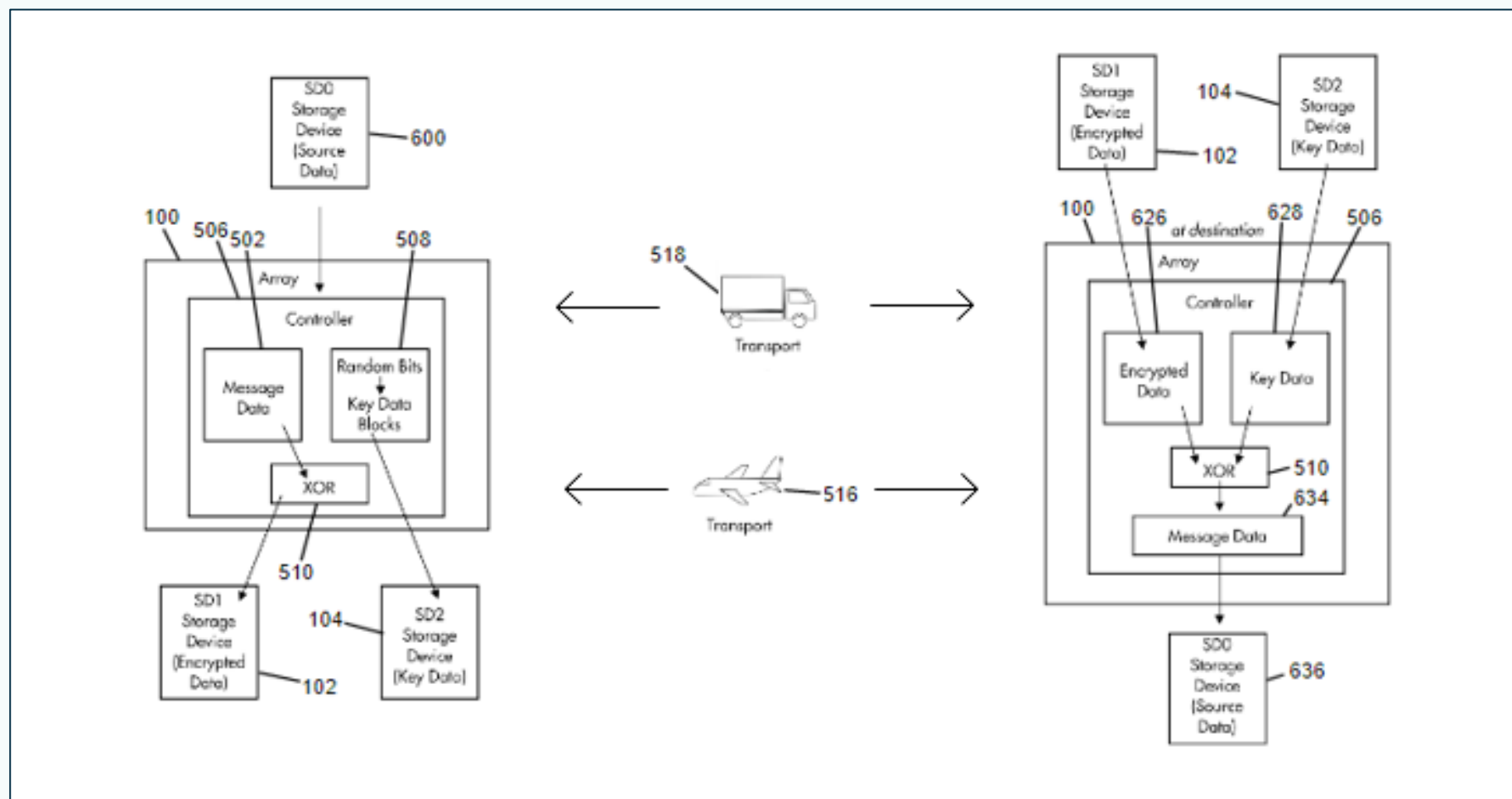
A system for generating secure data for transport comprising:

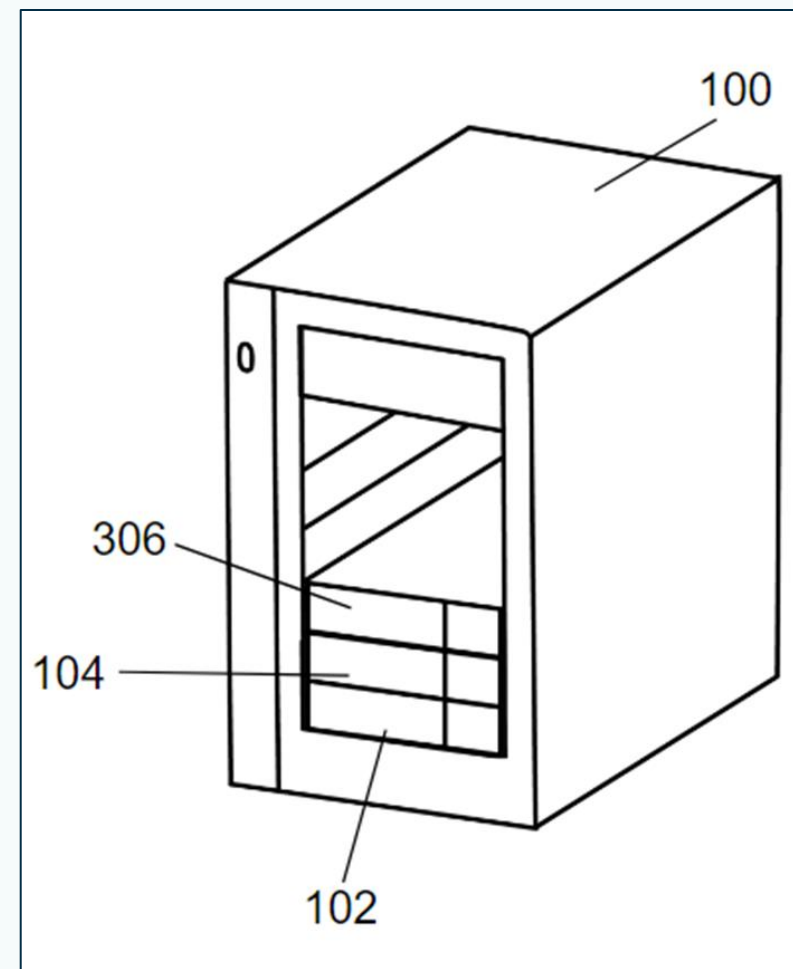
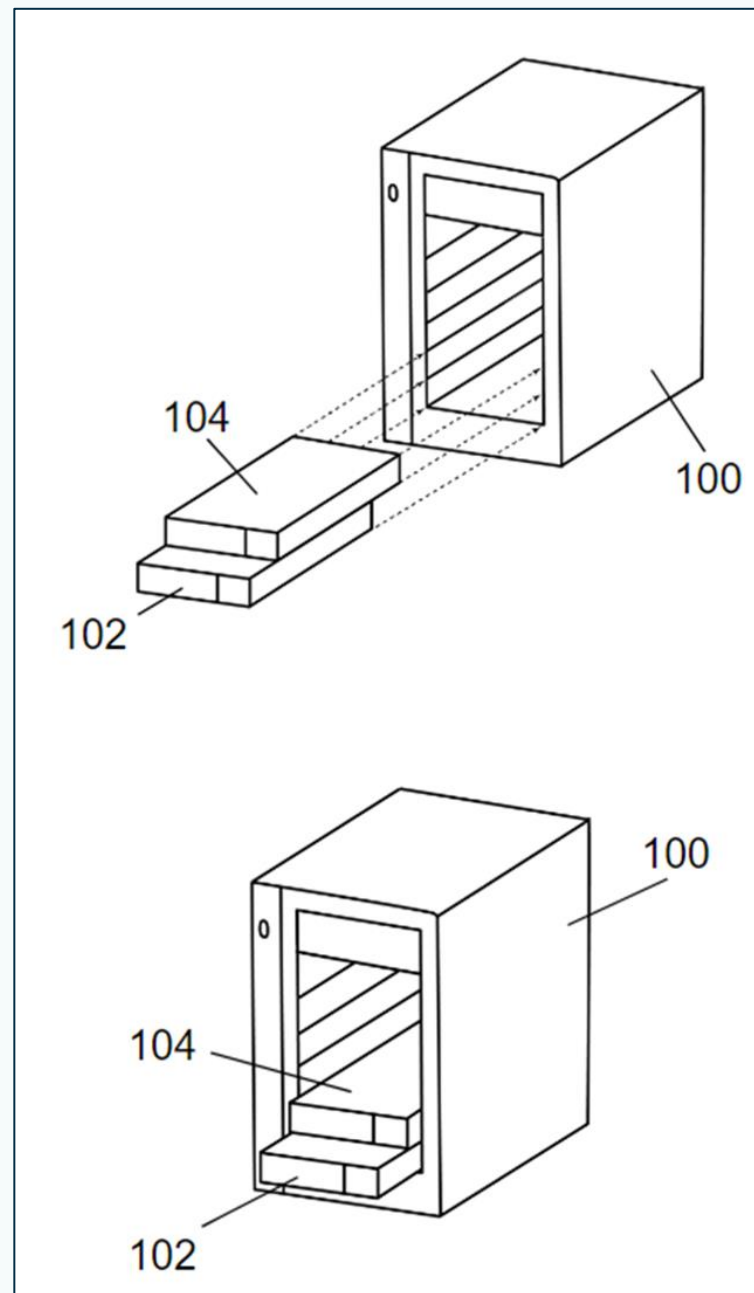
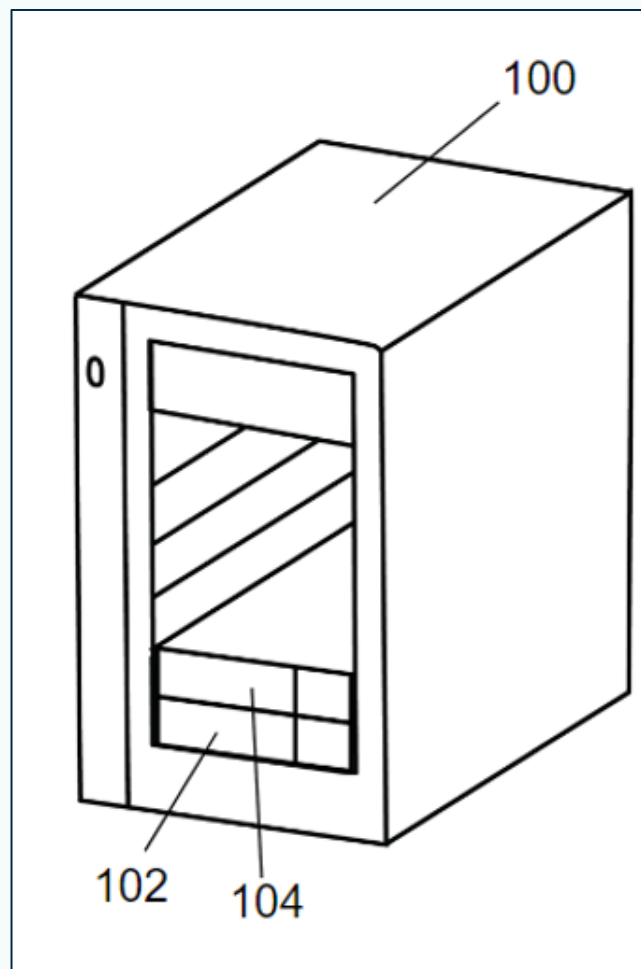
- a data source;
- a data storage controller electronically coupled with the data source;
- a first plurality of data stores electronically coupled with the data storage controller – the first plurality of data store configured to store encrypted data;
- a second plurality of data stores electronically coupled with the data storage controller – the second plurality of data stores configured to store key data;
- a random bit size generator for generating a random bit size corresponding with every write request of the data source of a size equal to the random bit size;
- a random key generator for generating a random key equal to or greater in size than the random bit size; and
- an encryption operator for encrypting the data source of the size with the random key.



QUESTIONS?







APPENDIX

OTP: The ONLY Unbreakable Cryptography

- Mathematically proven secure against quantum computation
- Secure against side-channel attacks
- Previously regarded as impractical to implement at scale
- Our solution makes it practical and easy to use [implement]
- Our patented method is a storage system that incorporates OTP encryption while working around ALL the OTP limitations, achieving unbreakable encryption for data storage and data transportation
- [Cryptography - Limitations of the One-Time Pad](#)

Digital Data Storage is Undergoing Mind-Boggling Growth

By Dr. Lauro Rizzatti, Verification Consultant, 09.14.16  12

 Share Post



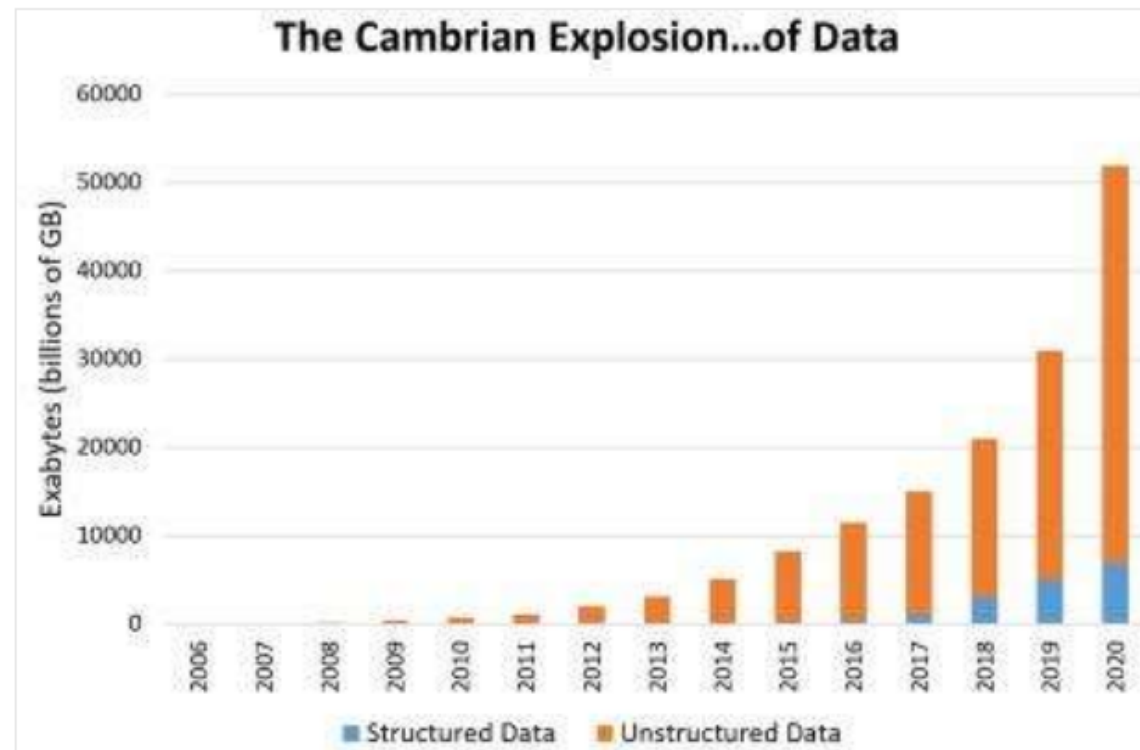
Share on Facebook



Share on Twitter



< [Previous](#) Image 3 of 7 [Next](#) >



https://www.eetimes.com/author.asp?section_id=36&doc_id=1330462#

IDC: Expect 175 zettabytes of data worldwide by 2025

By 2025, IDC says worldwide data will grow 61% to 175 zettabytes, with as much of the data residing in the cloud as in data centers.



- Small fleet of drones: 150 terabytes of data per day
- Sensors on an autonomous vehicle: 4 terabytes of data per day
- Animated movie files: 250 terabytes of storage.

<https://www.dronecommunity.biz/drones-data/>

<https://www.tuxera.com/blog/autonomous-cars-300-tb-of-data-per-year/>

<https://www.techrepublic.com/article/movie-animation-firms-big-data-challenges-present-lessons-to-learn/>

5 petabytes of data have been generated by
the European Sentinel 1A satellite

There are 4987 Satellites in orbit

<https://spaceflightnow.com/2016/04/28/europes-sentinel-satellites-generating-huge-big-data-archive/>

<https://www.pixalytics.com/satellites-orbiting-earth-2019/>

US HIPAA laws for Health Information Privacy

- **Health Insurance Portability and Accountability Act of 1996**
- According to the US Department of Health and Human Services Office for Civil Rights, between April 2003 and January 2013, it received 91,000 complaints of HIPAA violations, in which 22,000 led to enforcement actions of varying kinds (from settlements to fines) and 521 led to referrals to the US Department of Justice as criminal actions
- The largest fines of \$5.5 million levied against Memorial Healthcare Systems in 2017
- \$4.3 million levied against Cignet Health of Maryland in 2010

European GDPR

- General Data Protection Regulation 2016
- Controllers of personal data must put in place *appropriate technical and organisational measures* to implement the data protection principles.
- Sanctions: A fine up to €20 million or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater, if there has been an infringement of the following provisions: (Article 83, Paragraph 5 & 6^[34])

Today's Recommended Cryptography

- Symmetric Encryption: XSalsa20+Poly1305
- Symmetric Key Length: 256 bits
- Asymmetric Encryption: NaCl/Libsodium Curve25519 with ChaPoly
- Asymmetric Key Length: 256 bits

<https://latacora.micro.blog/2018/04/03/cryptographic-right-answers.html>

<https://en.wikipedia.org/wiki/EdDSA#Ed25519>

How a quantum computer could break 2048-bit RSA encryption in 8 hours

A new study shows that quantum technology will catch up with today's encryption standards much sooner than expected. That should worry anybody who needs to store data securely for 25 years or so.

NETWORKS / CYBER

DISA Seeks Encryption That Quantum Computers Can't Break

DISA will use OTA contracting to develop an encryption model that can't be broken by quantum computers.

<https://www.technologyreview.com/s/613596/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/>

<https://breakingdefense.com/2019/05/disa-seeks-encryption-that-quantum-computers-cant-break/>