Securing Data in the Cloud

Meeting the Challenges of Data Encryption and Key Management for Business-Critical Applications
Contents

Protecting Data in the Cloud: Executive Summary ........................................... 3
The Challenges of Securing Data at Rest in Private and Public Clouds ................ 3
Data Encryption: How Does It Work? ................................................................. 4
Managing the Encryption Keys in the Cloud ..................................................... 5
Your Private Swiss Banker .................................................................................. 5
Homomorphic Key Encryption: Protecting Keys in Use ..................................... 6
Understanding Threats in the Cloud ................................................................. 7
Conclusion: Porticor Virtual Private Data ........................................................ 7
Protecting Data in the Cloud: Executive Summary

There are many compelling reasons to migrate applications and data to private or public clouds: scalability, agility, cost savings – to name a few. But along with the benefits come increased risks to the safety of business-critical data. Any organization that is migrating data to the cloud needs to manage the risk to data at rest with a robust solution for data encryption and encryption-key management.

Securing data – at rest and in use – is simpler when the data is located within the four walls of a data center. Once data is moved to the cloud, it becomes vulnerable to a number of new threats ranging from stolen administrator credentials to new hacking techniques. In addition, new legislation, such as the US Patriot Act, is making it possible for competitors and governments to access data from cloud providers without the consent of the data owner.

For many organizations, keeping data private and secure has also become a compliance requirement. Standards including HIPAA, Sarbanes-Oxley, PCI DSS, the Gramm Leach Bliley Act and EU Data Protection directives all require that organizations protect their data-at-rest and provide defenses against threats. Cloud providers offering Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) offer a "shared responsibility" model for customer applications and data, so companies that are migrating to the cloud are responsible for finding a solution.

This whitepaper examines the risks to data in the cloud and introduces the Porticor® Virtual Private Data™ system, which combines state of the art encryption with patented key management to protect critical data in public, private and hybrid cloud environments. Porticor uses three core technologies to deliver trust in the cloud:

1. Robust, standards-based data encryption with a convenient, fast and simple management interface
2. Cloud-ready key management using patented Split-Key Encryption
3. Homomorphic key encryption techniques that protect keys even when they are in use

Each of these plays a vital role in ensuring that your data is safe and that your encryption keys are protected, both when in storage and when in use in the cloud. Together, they make Porticor Virtual Private Data the only solution that offers the convenience of encryption and key management in virtualized environments, without sacrificing trust.

The Challenges of Securing Data at Rest in Private and Public Clouds

Data encryption is one of the most important methods of protecting data at rest in the cloud and as a result, the number of solutions available – from open source APIs to proprietary turnkey projects – has mushroomed. In order to select the most effective solution for your needs, it’s important to understand the primary challenges of encrypting data in the cloud.

- **Managing the encryption process:** For complex applications with large amounts of data, the most time-consuming aspect of data encryption is management: deployment, set-up, adding and removing disks, etc. An effective encryption solution can reduce the time required for each of these tasks from hours to minutes.
- **Securing the data lifecycle:** Whether in use or at rest, both the data and the encryption keys must be handled and deployed correctly. An effective encryption solution must address every stage in the lifecycle.
- **Delivering high performance:** To ensure that the quality of service for your business applications meets expectations, the encryption solution must offer very high performance.
• **Ensuring trust in the cloud**: The problem with hosting key management in the cloud is one of trust. For both security and compliance reasons, you cannot allow a third party to manage your keys. In order to benefit from the convenience and low cost of cloud-based key management, you need a sophisticated solution that leaves the root of trust in your hands alone.

• **Storing and managing the encryption keys**: Every time the application accesses the data store, it needs to use encryption keys. There is generally one key per disk or data store and all of them must be managed on a key management server. Hosting a key management server in the data center is expensive, undermining the cost benefits of cloud projects. On the other hand, storing keys in the cloud raises the very important issue of trust.

• **Protecting the keys from theft when they are in use**: Encryption keys are vulnerable at two points – when in storage, and while in use. A truly effective key management solution will be able to protect the keys at both times.

### Data Encryption: How Does It Work?

The most secure data encryption solutions must support all of the major business use cases: full disk encryption, database encryption, file system encryption, distributed storage encryption and even row or column encryption. Porticor applies the same encryption technology to all of these needs.

Whenever an application (such as a database server) writes a disk block, it goes through the Porticor virtual appliance, where the data is encrypted and sent to the disk volume. The plain text data is never written to persistent storage. All requests to read data from the disk get sent to the Porticor virtual appliance, which reads the encrypted data blocks, decrypts them and then sends the plain text data back to the requesting application.

Porticor provides the unique ability to invisibly “hook” the encryption solution between your data storage and your application or database servers in the cloud. Once you grant permission, the encryption solution is transparent to the application and can be integrated quickly and easily without any application changes at all.

Porticor uses industry-standard high grade Advanced Encryption Standard (AES) encryption algorithm with a 256-bit key. Multiple blocks are chained using Cipher-Block Chaining (CBC), and the Encrypted Salt-Sector Initialization Vector (ESSIV) scheme is used to counter so-called fingerprinting attacks. It is also possible to configure the system to use alternate encryption algorithms as needed.

The Porticor solution can encrypt several different types of data on-the-fly:

• **Disk volumes**, which can be exposed to applications as Network File System (NFS) disks, or as Windows shares (CIFS volumes).

• **Disk volumes configured as a Storage Area Network (SAN)**. Porticor supports the iSCSI protocol for exposing these volumes. This is a common way to configure storage for database servers.

• **Distributed storage**, where applications normally write the whole file into a Web Service, and benefit from extremely high durability. Porticor supports the most popular implementation, Amazon’s Simple Storage Service (S3), and can integrate with other implementations.
Beyond encryption, Porticor features additional technologies to reinforce the security of your data:

- **Digital Signing**, to ensure data has not been altered
- **Patented data dispersion and deconstruction** technology, to ensure distributed storage data objects are difficult to find in the cloud
- **Logging and alerting on data-related events**, to support auditing and compliance with regulations

**Managing the Encryption Keys in the Cloud**

To encrypt data, Porticor performs the encryption algorithm on both the plain text and the secret key to obtain the cipher text: \( C = E_K(P) \). The best practice is to generate as many different random keys as practical - e.g. one key per disk volume or object - and to store them securely. You should never store the key next to the encrypted data, since it would be vulnerable to the same attacks as the data. This is a dilemma in the cloud: ideally, you do not want to store your keys in the cloud with your data, but of course you need them to access data stored on your application servers and database servers.

To address this issue, some security vendors require installation of a physical key management server in your data center. This is a resource- and cost-intensive solution that negates many of the benefits of migrating to the cloud in the first place. Other security vendors ask you to “trust” them and use their key management service. This approach violates the principle - and the compliance requirement - of keeping the keys under your own control.

Porticor Virtual Private Data is the only system available that offers the convenience of cloud-based hosted key management without sacrificing trust. Breakthrough split-key encryption technology protects keys and guarantees they remain under customer control and are never exposed in storage; and with homomorphic key encryption – even while they are in use.

**Your Private Swiss Banker**

Porticor split-key encryption is similar to the traditional practice used to protect private safe-deposit boxes at banks around the world. Each safe-deposit box has two keys: one is held by the customer, the other is kept by the bank. Neither the customer nor the banker can open the safe on their own; both keys are needed at the same time.

The Porticor key management solution also requires two keys. Each data object (such as a disk or file) is encrypted with a unique key that is split in two. The first part – the master key – is common to all data objects in the application. It remains the sole possession of the application owner and is unknown to Porticor. The second part is different for each data object and is stored by the Porticor Key Management Service. When the application accesses the data store, Porticor uses both parts of the key to dynamically encrypt and decrypt the data.

Whenever you create a new project (application), you generate a single Master Key and back it up securely on your own premises. The Master Key is used by the Porticor virtual appliance which resides in your own cloud, but it is never transferred into Porticor’s key management service. When you encrypt a disk volume or an object, it receives a new key that is a mathematical combination of the Master Key and a unique random key created by the Porticor Appliance and stored in an encrypted form in the Porticor Key Management service.
Porticor Virtual Key Management is the only solution that keeps your data and encryption keys safe at all times – even when they are in use in the cloud. Homomorphic encryption is a technique that enables mathematical operations to be performed on encrypted data. Porticor has developed a patent-pending technology that implements homomorphic techniques for combining and splitting encryption keys. It enables the Porticor Virtual Appliance to give the application access to the data store without ever exposing the master keys in an unencrypted state.

As explained above, with Porticor, each data object is encrypted with a key that has two parts: the Master Key and the second (“banker”) key. When the application needs to access the data store, the Porticor Virtual Appliance combines both parts of the key in a mathematical operation. Ordinarily, this would require both parts of the key to be exposed (unencrypted). However with Porticor, both parts of the key are encrypted before and during their use in the virtual appliance. As a result, the keys are fully encrypted when they are resident in in your cloud account. Porticor homomorphically encrypts the master key differently for each instance of the Porticor Virtual Appliance. So even if your cloud account is breached or attacked, and the encrypted master key is stolen, it can never be used to access your data.
With Fully Homomorphic Encryption, all mathematical operations can be performed on encrypted data, but since it requires an enormous amount of computational resources, it isn’t yet feasible for a real-world system. With Partially Homomorphic Encryption, only select mathematical operations are supported, dramatically reducing the computational overhead. Porticor has developed a patent-pending implementation of Partially Homomorphic Encryption so that the most critical link in the encryption of data in the cloud – the master key – is also encrypted and secure. At the same time, you benefit from fast, reliable performance for your business-critical applications.

Understanding Threats in the Cloud

In order to manage and mitigate risk, you need to understand it. Threats to cloud security are widely publicized and they are real; but with Porticor, you get a level of data protection that is unavailable even in on-premise encryption solutions.

All data encryption systems, both in the cloud or in a physical data center, share a common vulnerability – they need to use the encryption keys. When the keys are in use, they can, in theory, be stolen. Porticor takes every known precaution, and has invented several new ones, to mitigate this risk.

Porticor appliances are designed for security. The disks never contain the encryption keys and the memory (where the encryption keys are stored) is inaccessible – even to Porticor. Nevertheless, in the highly unlikely event that a Porticor Virtual Appliance is breached and the encryption key is stolen, only the one data object that is in memory at that time is exposed. In order to access the rest of your data storage, the thief would need your Master Key. Thanks to homomorphic key encryption, your Master Key can never be stolen and used. As a result, the breach of a single object cannot lead to a breach of your entire system. This is a level of protection that even on-premise encryption solutions cannot offer.

Conclusion: Porticor Virtual Private Data

Data encryption is critical to protecting the security of data at rest in the cloud. But when it comes to the cloud, encrypting the data is only the beginning – managing and protecting the encryption keys effectively is vital. An effective data encryption solution must include:

- Robust, fast, yet easy to use data encryption
- Reliable, cloud-based key management that is cost-effective, but trustworthy
- Key encryption technologies to protect your encryption keys as well as your data – both in storage and in use

Porticor Virtual Private Data is the first solution to offer cloud-based key management without sacrificing trust. Like a Swiss banker, Porticor requires two parts of a split key to access every disk. Each part of the key is encrypted to protect it while it is resident in your cloud account using patent-pending homomorphic key encryption technology. With the Master Key, you retain control of your encrypted data, without having to install and maintain key management servers on premise.

Try Porticor today or contact us for more information.