**Blockchain: A Panacea for Healthcare Cloud-Based**

**Data Security and Privacy?**

**Algorithm**

**Advanced Encryption Standard** (**AES) using** **Searchable Symmetric Encryption Scheme**

**Algorithm Explanation**

The Advanced Encryption Standard, or AES, is a symmetric [block cipher](http://searchsecurity.techtarget.com/definition/block-cipher) chosen by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data.

**AES features**

The selection process for this new [symmetric key algorithm](http://searchsecurity.techtarget.com/definition/secret-key-algorithm) was fully open to public scrutiny and comment; this ensured a thorough, transparent analysis of the designs submitted.

NIST specified the new advanced encryption standard algorithm must be a block cipher capable of handling 128 bit blocks, using keys sized at 128, 192, and 256 bits; other criteria for being chosen as the next advanced encryption standard algorithm included:

* **Security:** Competing algorithms were to be judged on their ability to resist attack, as compared to other submitted ciphers, though security strength was to be considered the most important factor in the competition.
* **Cost:** Intended to be released under a global, nonexclusive and royalty-free basis, the candidate algorithms were to be evaluated on computational and memory efficiency.
* **Implementation:** Algorithm and implementation characteristics to be evaluated included the flexibility of the algorithm; suitability of the algorithm to be implemented in hardware or software; and overall, relative simplicity of implementation.

**Symmetric Encryption -**Symmetric algorithms use the same key for encryption and decryption and this is shared by both communicating parties. Sending party use the secret key to encrypt and receiving party use same key for decrypt.