TITLE: IMPLEMENTATION OF SECURITY ALGORITHM FOR HEALTHCARE APPLICATION

Outline of this document: Research papers, AES algorithm, how does it works? Structure of AES Algorithm, Hardware and software used in AES, attacks that resistance AES algorithm and which are improved…

AES Algorithm:

We use AES algorithm to improve the security in healthcare system

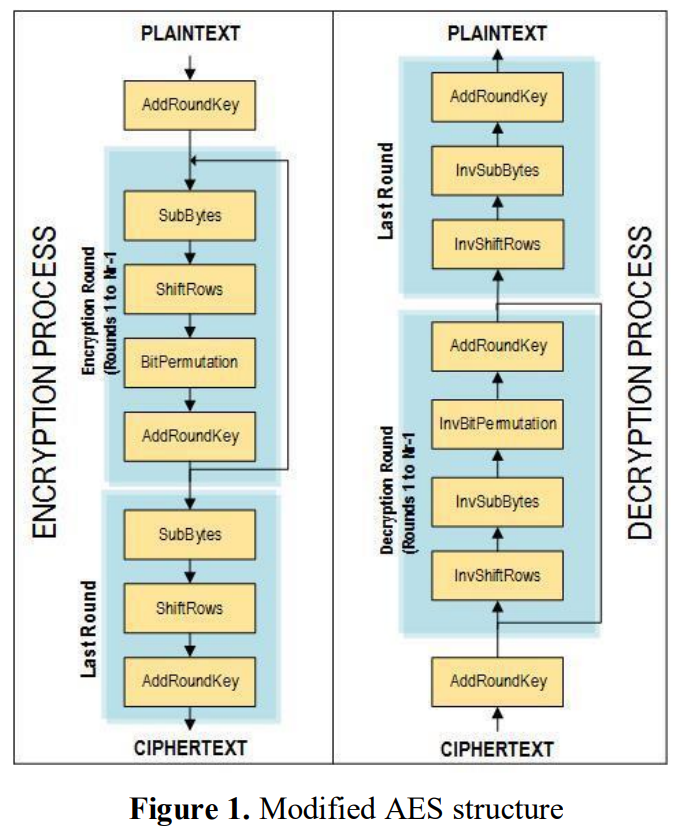
The cyberattack is improved nowadays in electronic devices in healthcare while checking heartbeat, X-rays, scanning etc.,

To avoid that AES algorithm used.

**How AES algorithm works??**

1. **Key Expansion**: AES uses keys of 128, 192, or 256 bits. It generates a series of round keys from the original key using a key schedule process.
2. **Initial Round**: Plaintext is arranged in a 4x4 matrix called the state. The initial round key is added to the state using bitwise XOR.
3. **Main Rounds (9, 11, or 13 rounds)**: Each round consists of four steps:
   * **Sub Bytes**: Each byte in the state is substituted using a substitution box (S-box).
   * **Shift Rows**: Rows of the state are shifted left by different offsets.
   * **Mix Columns**: Columns of the state are mixed using matrix multiplication.
   * **Add Round Key**: The current round key is added to the state.
4. **Final Round**: Like the main rounds, but without the Mix Columns step.
5. **Output**: The final state matrix is converted back into the encrypted ciphertext.

AES’s strength comes from its complexity and resistance to various cryptographic attacks,making it a standard choice for encrypting sensitive data.



**Links for reference paper**:

1. [Enhanced **AES algorithm**based on 14 rounds in securing data **and**minimizing processing time](https://iopscience.iop.org/article/10.1088/1742-6596/1793/1/012066/meta)
2. [On the implementation **and**performance evaluation of **security algorithms**for **healthcare**](https://link.springer.com/chapter/10.1007/978-981-15-0829-5_59)
3. [**Healthcare data security**in cloud **storage using**light weight symmetric key **algorithm**.](https://www.iajit.org/upload/files/Healthcare-Data-Security-in-Cloud-Storage-Using-Light-Weight-Symmetric-Key-Algorithm.pdf)
4. [**Health records**database and inherent **security**concerns: A review of the literature](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9647912/)

**How can we improve Hardware and software in healthcare system using AES:**

**1. Hardware Security Enhancements:**

* **Secure Hardware Modules (HSMs):** Implement HSMs to manage AES encryption keys securely. These modules are designed to protect cryptographic keys from physical and software-based attacks.
* **Trusted Platform Modules (TPMs):** Use TPMs for secure boot processes and to store sensitive information securely on devices.
* **AES-enabled Hardware Encryption:** Use processors and devices that support hardware-accelerated AES encryption to enhance performance and security.

**2. Software Security Enhancements:**

* **Data Encryption:** Implement AES encryption for data at rest (stored in databases and storage devices) and data in transit (communications over networks).
* **Encryption Libraries:** Use well-vetted cryptographic libraries for implementing AES, such as OpenSSL or Bouncy Castle, to avoid vulnerabilities in custom implementations.
* **Regular Software Updates and Patching:** Ensure all systems and applications are regularly updated to protect against known vulnerabilities.
* **Application-Level Encryption:** Encrypt sensitive data at the application layer before it's sent to the database, adding another layer of security.

**Attacks that resistance AES algorithm:**

1)**Brute-Force Attacks:** AES is resistant to brute-force attacks due to its large key sizes (128, 192, or 256 bits), which makes exhaustive key searches computationally infeasible.

2)**Differential and Linear Cryptanalysis:** AES has been designed to resist these attacks, which involve analysing the relationship between input plaintext and output ciphertext.

3)**Side-Channel Attacks:** While AES is inherently resistant to standard cryptographic attacks, side-channel attacks (such as power analysis or timing attacks) exploit hardware implementation flaws. However, hardware implementations can use countermeasures like masking and noise addition to mitigate these risks.

4)**Known-Plaintext and Chosen-Plaintext Attacks:** AES is secure against these attacks due to its complex key schedule and non-linear transformations.

**Hardware Used in AES:**

1. **FPGAs (Field-Programmable Gate Arrays):** Used for custom AES implementations that require high performance and low latency, often programmed using tools like Vivado.
2. **ASICs (Application-Specific Integrated Circuits):** These are custom-designed chips for efficient AES encryption in high-security environments.
3. **Microcontrollers and Processors:** Some processors have built-in AES instructions (e.g., Intel's AES-NI) to accelerate encryption tasks.
4. **Vivado:** Vivado can be used for implementing the AES algorithm, particularly in hardware design projects involving FPGAs (Field-Programmable Gate Arrays). Vivado, developed by Xilinx, is a tool used for hardware description languages like VHDL or Verilog, which are often used to design and simulate digital circuits**.**
5. By writing the AES algorithm in VHDL or Verilog, you can use Vivado to synthesize, simulate, and implement the AES encryption/decryption hardware, enabling efficient and secure cryptographic operations on FPGA platforms. This is useful for high-performance and secure embedded systems.

**Software Used in AES:**

1. **Programming Languages:** C, C++, Python, Java, and others with cryptographic libraries like OpenSSL, PyCryptodome, and Java's JCE (Java Cryptography Extension).
2. **Cryptographic Libraries:** Libraries like OpenSSL (C), Crypto++ (C++), PyCryptodome (Python), and Bouncy Castle (Java) are commonly used to implement AES in software applications.