IoT in healthcare

Presentations for the Bielefeld University course »Modern Data Science Technologies in Healthcare«






1. Alexander Stiebing: „A general overview“
2. Kyuri Kim: „Title here“
3. Bebeta Hoxha: „Data Security and Privacy in IoT“



23 July 2021

IoT in Healthcare

DATA PRIVACY AND SECURITY

Presentations for the Bielefeld University course
»Modern Data Science Technologies in Healthcare«

Bebeta Hoxha

23 July 2021

OUTLINE

- Security Requirements and Challenges
- Attacks and Consequences
- Security Solutions
- Cryptographic Algorithms
- Fog Computing

THE MAIN CONCERN

Over 68,000 medical systems exposed online
Cyber bugs in infusion pumps
Access to global information networks

Anesthesia equipment

Cardiology devices (ICD)

MRI scanners

Infusion systems

Insulin pumps

SECURITY ISSUES

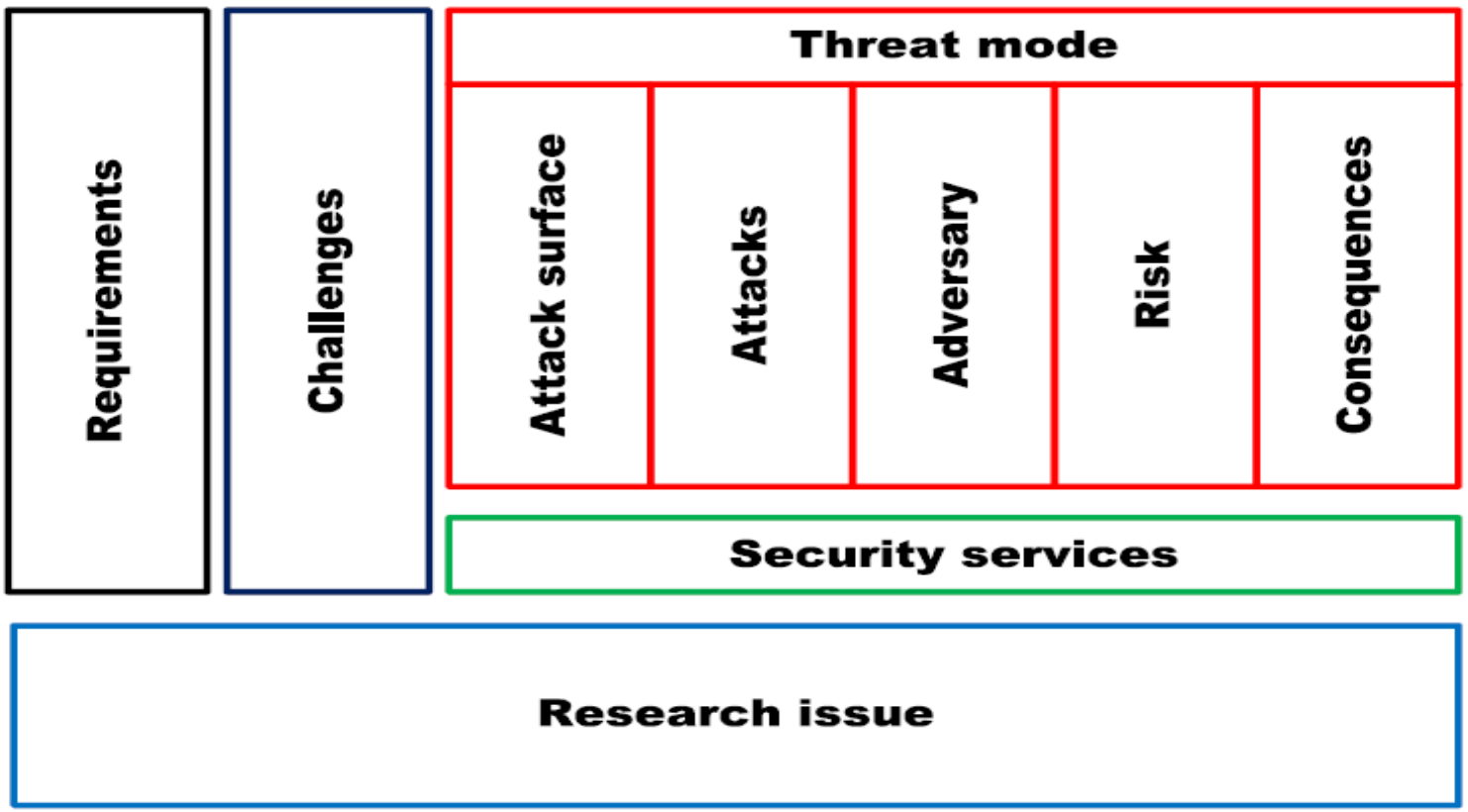


Figure 1. Security Issues in IoT-based health care (Islam et al, 2015)

SECURITY REQUIREMENTS

- CONFIDENTIALITY : Inaccessibility of medical information for unauthorized users.
- INTEGRITY: Received medical data are not altered in transit by an adversary.
- AUTHENTICATION: IoT health device to ensure the identity of the person with which it is communicating.
- AVAILABILITY: Survivability of IoT healthcare services to authorized parties when needed
- DATA FRESHNESS: Data freshness and key freshness.
- NON-REPUDIATION
- AUTHORIZATION: Only authorized nodes are accessible for network services or resources.
- RESILIENCY: Protection of the network/ device/information from any attack when interconnected health devices are compromised

SECURITY CHALLENGES

1. COMPUTATIONAL LIMITATIONS
   - Minimize resource consumption
   - Maximize security performance
2. MEMORY LIMITATIONS
   - low on-device memory.
   - not sufficient to execute complicated security protocols.
3. ENERGY LIMITATIONS
   - small health devices of limited battery power
4. MOBILITY
   - Different networks have different security configurations and settings.
   - mobility-compliant security algorithm development
5. SCALABILITY
   - designing a highly scalable security scheme

SECURITY CHALLENGES

6. COMMUNICATIONS MEDIA
   - Finding a comprehensive security protocol that can treat both wired and wireless channel characteristics equally.
7. THE MULTIPLICITY OF DEVICES
   - Designing a security scheme even for the simplest of devices.
8. A DYNAMIC NETWORK TOPOLOGY
   - Devising a security model
9. DYNAMIC SECURITY UPDATES
   - Designing a mechanism for the dynamic installation of security patches
10. TAMPER-RESISTANT PACKAGES

VULNERABILITY OF THE SYSTEM

INCREASED ATTACK SURFACE

SCENARIOS:

- Expansion of native networks, cloud networks, and cloud services
- Increased communication between IoT devices, networks, cloud services, and applications.
- In-device hardware and software limitations

ORIGIN OF THREATS:

- Inside and Outside of the Networks
- From a health device in a proximal network

ATTACKS BASED ON:

INFORMATION DISRUPTIONS

- Interruption
- Interception
- Modification
- Fabrication
- Replay

HOST PROPERTIES

- *User Compromise*
- Hardware Compromise
- Software Compromise

NETWORK PROPERTIES

- *Standard Protocol Compromise:*
- *Network Protocol Stack Attack*

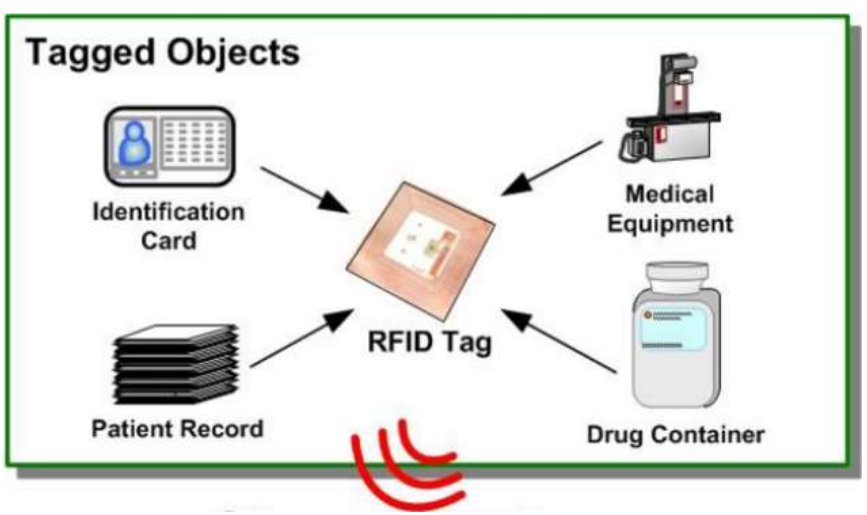
ATTACKS AND CONSEQUENCES

Table 1: Calculating IoMT security risk assessment (Sajitha et al, 2020)

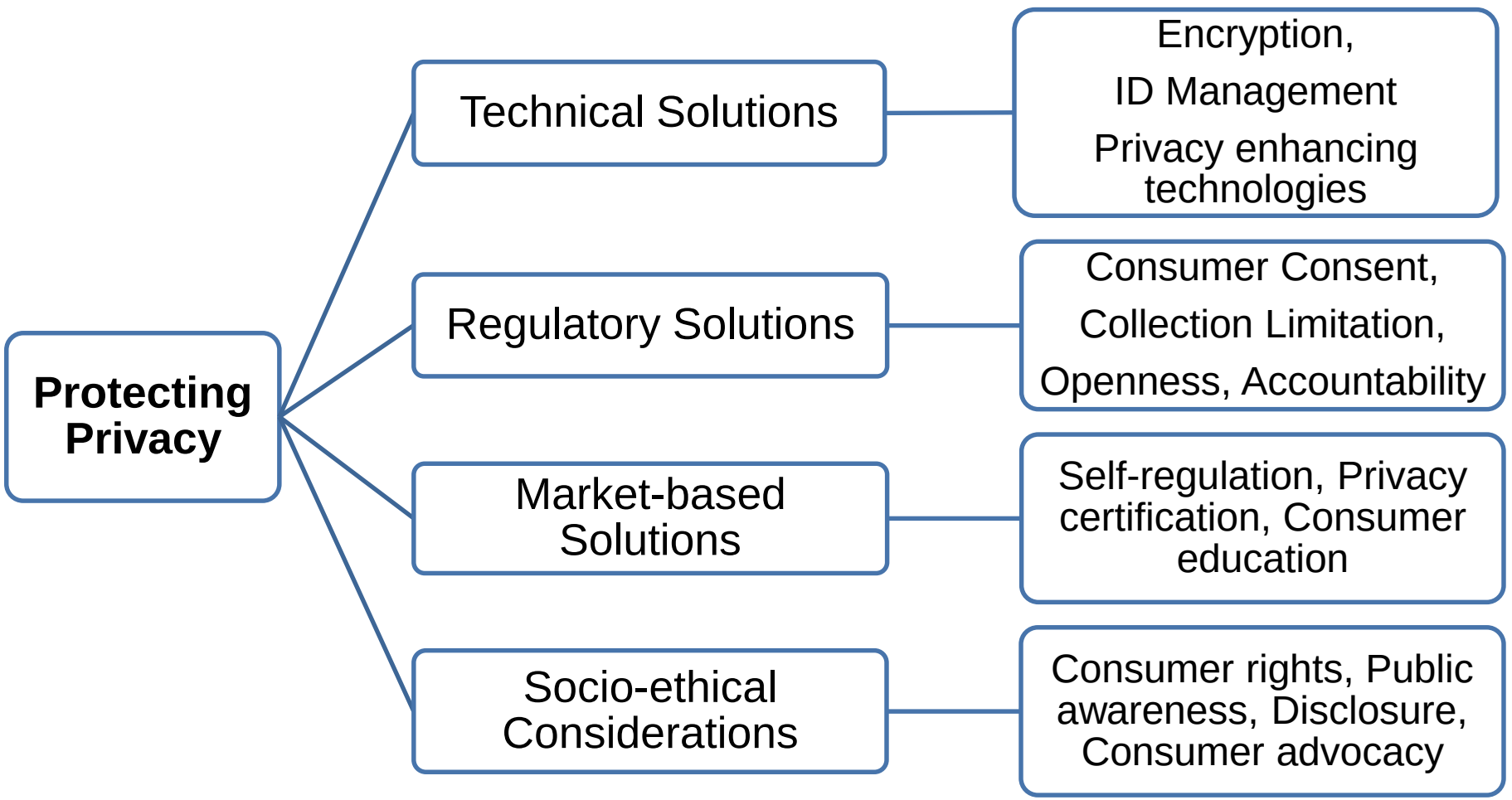
SN	IoMT	Attack	Difficulty	Awareness	Impact	Risk Factor (%)
1	ICDs	DDoS	W = 9	W = 9	W = 10	r = 94.00
2	GES	WA	W = 5	W = 4	W = 6	r = 29.00
3	Insulin Pump	DH	W = 7	W = 5	W = 9	r = 44.00
4	RFID Tags	UA	W = 10	W = 6	W = 5	r = 54.00

ICD: Implantable Cardioverter-Defibrillator
GES: Gastric Electrical Stimulation
RFID Tags: Radio-Frequency ID

Difficult to attack (w = 1)
Easy to attack (w =9)



PRIVACY PROTECTION SOLUTIONS



HEALTHCARE PRIVACY ***REGULATIONS***

- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Office of the Australian Information Commissioner (OIAC)
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- ***Generation Data Protection Regulation (GDPR)***
  - ✓ Notification
  - ✓ Right to access
  - ✓ Right to be forgotten
  - ✓ Portability
  - ✓ Privacy by design
  - ✓ Data protection officer appointment

A DYNAMIC SECURITY MODEL

Security services designed with dynamic properties.

- Protection services reduce attacks.
- Detection services receive activity data from healthcare applications,
- Reaction services help health entities survive all attacks.

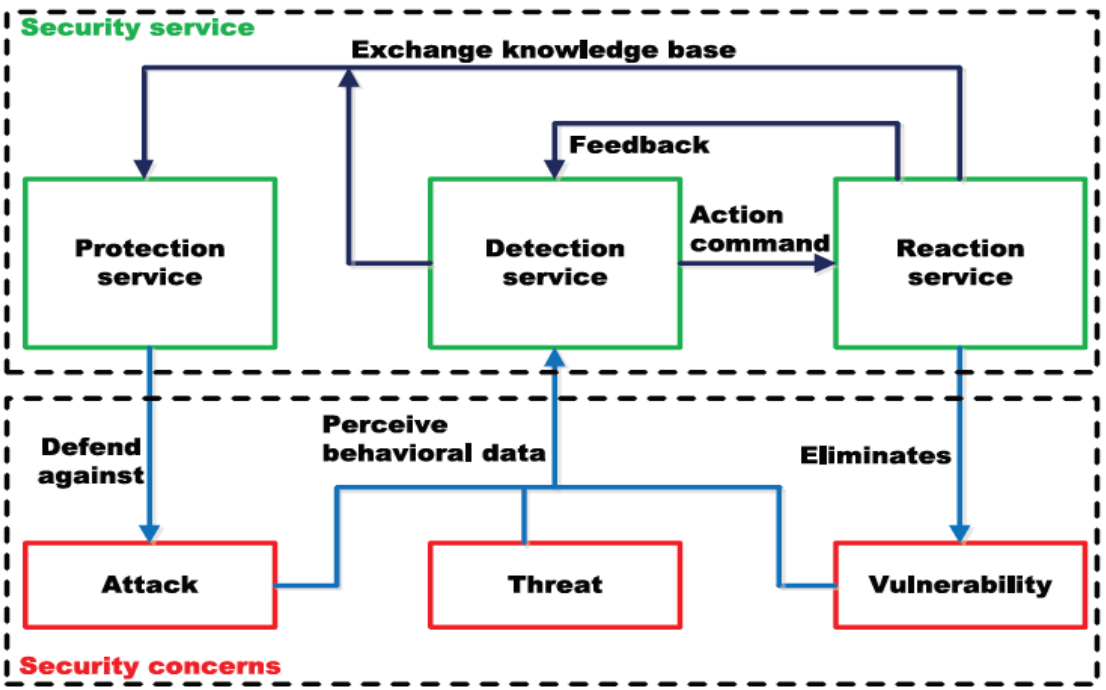


Figure 2. A dynamic security model (Islam et al, 2015)

FURTHER CONCEPTS

Table 2. Proposed concepts to mitigate security towards IoMT future (Sajitha et al, 2020)

SN	Level of Security	Security Goals	Key concepts to improve security
1	Device Level Security	Trusted public key infrastructure	Apply advanced authentication mechanism using Secure Socket Layer for authentication
2	Continues monitoring	Security monitoring	Monitoring spatial and temporal information.
3	Prevention	Threat prevention	Use packet filtering firewall to monitor incoming packets
4	Detection	Vulnerability management	Analysing data packets. Monitoring unusual data transmission
5	Response	Incident response	Immediate update about device fault to other devices and avoid results from faulted device

SECURITY SOLUTIONS

DATA ENCRYPTION

- Secret Key/ Symmetric Key
- Public Key/ Asymmetric Key
  - Key agreement, Encryption,
  - Digital Signature Algorithms

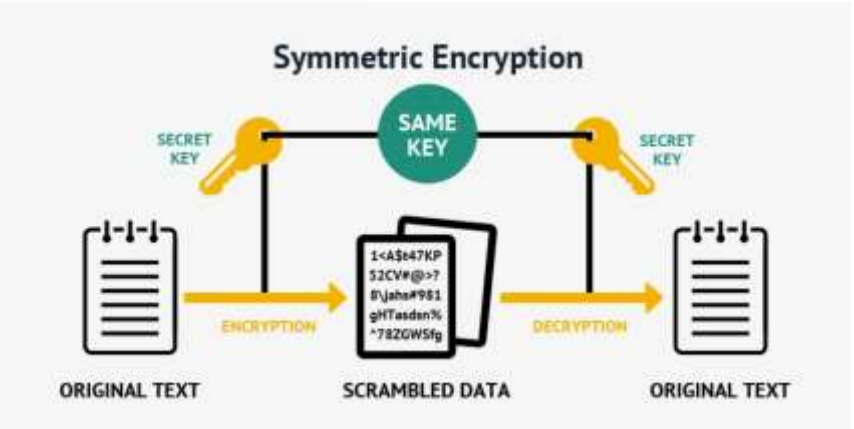


Figure 3. Symmetric Encryption
(retrieved from: *https://academy.ivanontech.com*

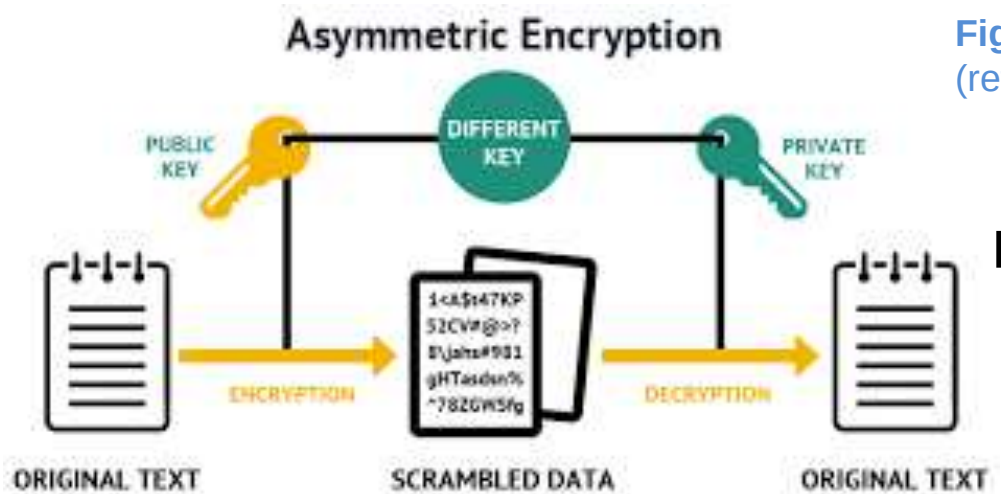


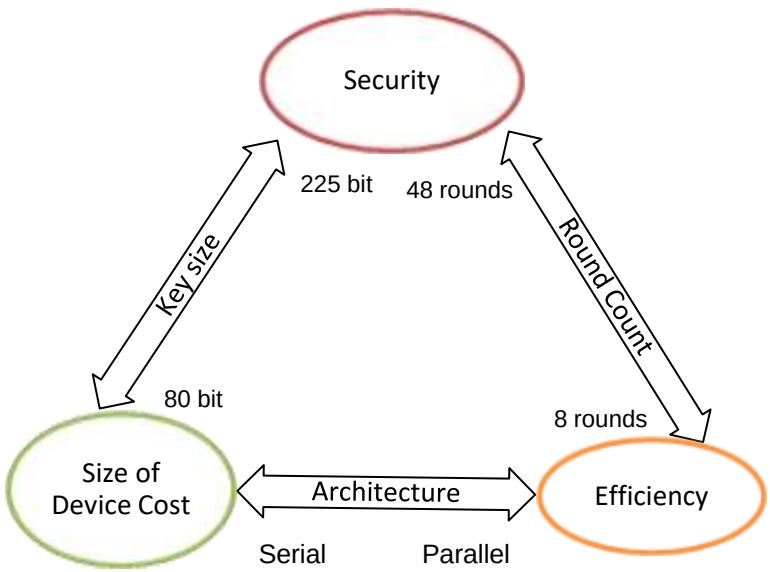
Figure 4. Asymmetric Encryption
retrieved from: *https://academy.ivanontech.com*

Plaintext is divided into b-bit blocks b = 64 or 128 bits

SECURITY SOLUTIONS

LIGHT-WEIGHT-CRYPTOGRAPHY (LWC)

- Suitable for limited source devices
- Amount of (80 to 128 bit) security
- Less energy consumption
- Less memory occupation
- Shorter time for algorithm execution



SECURITY SOLUTIONS

1. DATA ENCRYPTION
   - Link encryption
   - Node encryption
   - End-to-end encryption
2. ACCESS CONTROL
   - Various encryption methods applied in access control
3. TRUSTED THIRD PARTY AUDITING
   - The integrity and consistency of medical data stored in the cloud
4. DATA SEARCHING
   - Sensitive data are encrypted before outsourcing

FOG COMPUTING

Figure 5. Architecture of the proposed model (Winnie et al 2018)

FOG COMPUTING

Fake data in the Fog to trick the attacker

AES algorithm Implementation in the fog node.

- Symmetric block cipher technique to encrypt and decrypt the data
- Double security of the data
- Multiple rounds of transformation depending on the key size.

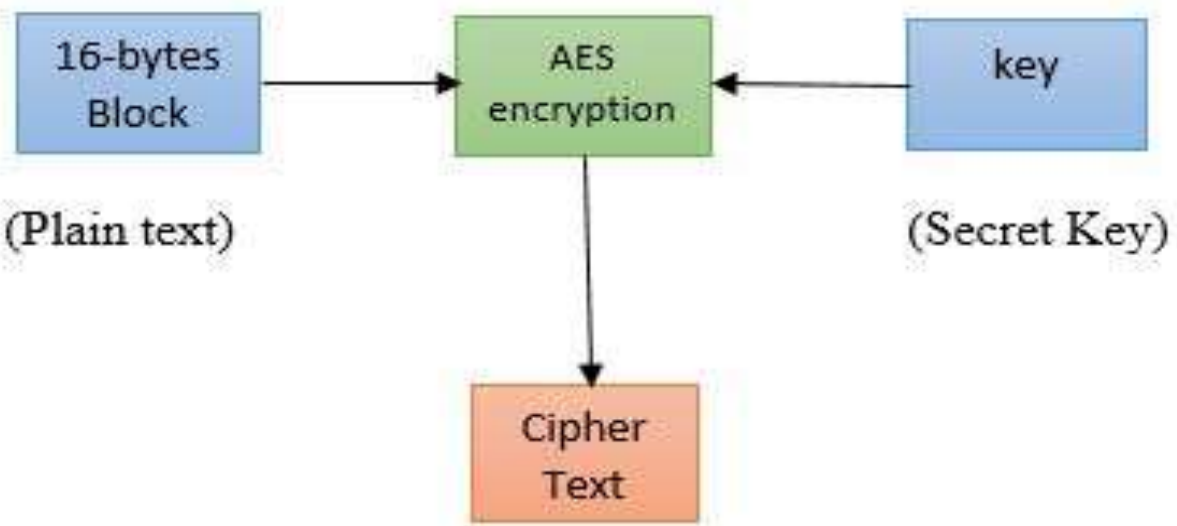
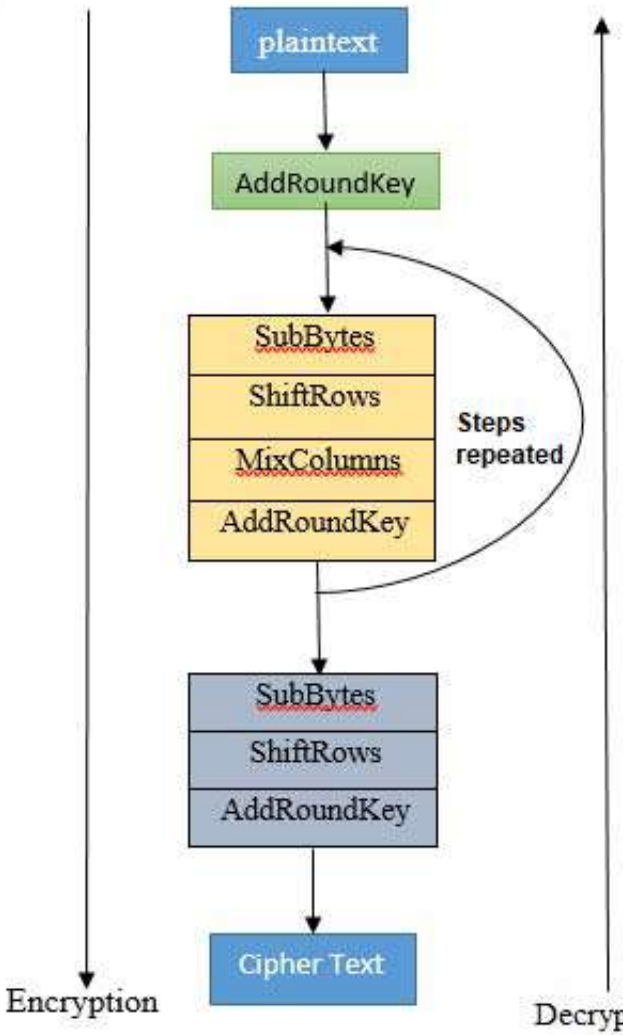


Figure 6: Block Diagram of AES (Winnie et al 2018.

AES ALGORITHM STEPS



Plain text divided into 16-byte block, represented into 4×4 matrix.

1. *Byte Substitution*

   Input is substituted by using the S-box table

2. *Shift Rows*

   Each row of the matrix is shifted to the left cell at every row.

3. *Column mix*

   Using a mathematical technique.

4. *Add Round key*

   The new 16-byte (128 bits) matrix is XOR-ed to the 256 bits of the round key.

Figure 7: Flow Diagram of AES algorithm (Winnie et al 2018)

CONCLUSION

- **PROBLEMS RISING:**
  - Resource-efficient Security
  - Secure Routing
  - Data Transparency
  - The Security of Handling IoT BIG DATA
- **SOLUTIONS**
  - Strict policies and technical security measures
  - Data Encryption using Light Weight Cryptography
  - Solution Proposed: Fog Computing + AES Algorithm

DISCUSSION

Ethical approach of the Data Privacy, Sharing and Vulnerability in Medical IoT networks

REFERENCES

1. Anil Chacko, T. H. (2018). Security and Privacy Issues with IoT in Healthcare. *EAI, 4*(14).
2. Bitchkei, S. (2019, November 7). *Healthcare Data Privacy Overview: From HIPAA To HITECH*. Retrieved from Hitachi systems security : https://hitachi-systems-security.com/healthcare-data-privacy-overview-from-hipaa-to-hitech/
3. Mirjana Maksimovic, V. V. (2015). A Custom Internet of Things Healthcare System. *10th Iberian Conference on Information Systems and Technologies - CISTI'2015*, (pp. 653-658). Agueda, Portugal.
4. S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain and K. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," in *IEEE Access*, vol. 3, pp. 678-708, 2015, doi: 10.1109/ACCESS.2015.2437951
5. Shanagoda Sajitha, D. A. (2020). Analysis of Security issues in Healthcare systems using Internet of Things. *IJARESM*, 298-301.
6. Tech, I. o. (2020, May 24). *IvanOnTech Academy*. Retrieved from The Complete Guide to Cryptography – Asymmetric vs. Symmetric Encryption: *https://academy.ivanontech.com/blog/the-complete-guide-to-cryptography-asymmetric-vs-symmetric-encryption*
7. Yumnam Winnie, U. E. (2018). Enhancing Data Security in IoT healthcare services using FOG Computing. *International Conference on Recent Trends in Advanced Computing (ICRTAC-CPS 2018)* (pp. 200-205). IEEE.
8. Wencheng Sun, Z. C. (2018). Security and Privacy in the Medical Internet of Things: A Review. *Hindawi*, 9 pages.