사물인터넷 환경에서 하드웨어(FPGA)기반 암호가속기 사용 실시간 영상 데이터 암호화 시스템

김민재[1], 이준호[1], 김호원[2]
[1]부산대학교 정보융합공학과
[2]부산대학교 정보컴퓨터공학부
minjae@islab.re.kr, junho@islab.re.kr, howon@islab.re.kr

Real-time video data encryption system using FPGA-based crypto-accelerator in the Internet of Things environment

Min-Jae Kim[1], Jun-Ho Lee[1], Ho-Won Kim[2]
[1]Dept. of Information Convergence Engineering, Pusan National University
[2]Dept. of Computer Science and Engineering, Pusan National University
minjae@islab.re.kr, junho@islab.re.kr, howon@islab.re.kr

요 약

사물인터넷 기술이 활성화되면서 원격 접속 및 제어가 가능한 스마트 가전기기의 보급이 증가하고 있다. 이에 따라 스마트 가전 기기의 보안취약점을 이용하여 개인정보 유출, 프라이버시 침해 등 사이버 보안 관련 범죄도 같이 증가하는 추세이다. 최근 저성능 디바이스에서 경량 암호를 이용한 안전성 보장 방안에 대한 연구가 진행 중이나, 저성능 디바이스에서 4K/2160p 이상의 영상 데이터를 실시간으로 암·복호화하는 것은 높은 지연시간을 발생시킨다. 본 연구에서는 하드웨어 기반 암호 알고리즘 가속기를 이용하여 저성능 디바이스에서도 구현 가능한 대용량 영상데이터 실시간 암·복호화 시스템을 제안한다.

1. 서론

사물인터넷(Internet of Things) 기술이 활성화되면서 원격 접속 및 제어가 가능한 스마트 가전기기의 보급이 증가하고 있다. 이에 따라 스마트 가전기기의 보안 취약점을 이용하여 개인정보 유출, 프라이버시 침해 등 사이버보안 범죄도 같이 증가하는 추세이다. 이를 방어하기 위해 사물인터넷에 주로 사용되는 저성능 디바이스에서 경량 암호를 이용한 안전성 보장 방안에 대한 연구[1]가 진행 중이다. 그러나 저성능 디바이스에서 4K/2160p 이상의 영상 데이터를 실시간으로 암·복호화 하는 것은 높은 지연 시간을 발생시킨다.

암호 알고리즘의 가속화 및 신뢰성 보장 구조를 위해 디바이스에 외부모듈(HSM)을 연동하여 구현하는 경우, 모듈 및 프로세서 간 데이터 통신에 있어 대역폭으로 인한 오버헤드가 발생 하게 된다.

이러한 문제점을 개선하기 위해 프로세서에 연산 가속을 위한 모듈을 삽입해 암호 알고리즘 연산과 같은 암호 가속화 구조에 대한 연구가 활발히 진행 중에 있다.

대표적인 예로 AES 암호 가속을 위해 Intel에서는 AES-NI[2], ARM Arm v8 Cryptographic Extension의 Instruction Set Extension을 추가해 AES 알고리즘에 대한 암호연산을 가속하며, 소프트웨어 기반 암호가 가지는 단점을 제거했다.

본 연구에서는 사물인터넷 환경 디바이스에서 대용량 영상 데이터의 실시간 암·복호화 기능 제공을 위한 암호 가속기 및 디바이스 간 상호연동 구조를 제시한다.

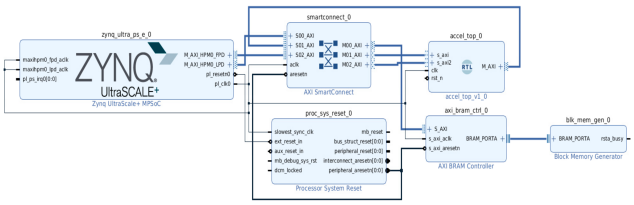
2. 배경 지식

ARIA[3]는 한국인터넷진흥원(KISA)에서 개발한 블록 암호화 알고리즘으로, 기본적으로 ISPN(Involution SPN)구조를 가진다. 일반적인 SPN(Substitution-Permutation-Networks) 구조인 AES와 다르게 별도의 복호화를 위한 함수가 필요로 하지 않는 장점이 있어 하드웨어 구현시 적은 면적으로 구현이 가능하다. ARIA의 암호키 크기는 128/192/256bit를 가지며 키 크기에 따라 12/14/16의 라운드를 가진다. 또한 블록 크기가 128비트이기 때문에 128비트 단위의 입출력으로 구성되어 있다. ARIA는 각각 Substitution Layer, Diffusion Layer, AddRoundKey로 구성

된다.

RTP[4](Real Time Protocol)는 IETF RFC 3350 A Transport Protocol for Real-Time Application 에서 정의된 오디오와 비디오 데이터를 네트워크 계층에서 전송하기위한 프로토콜이다. RTP는 UDP기반으로 동작하며, 타임스탬프 방식으로 전송하여 불규칙하게 수신되는 데이터를 순서대로 정렬하고 정렬된 데이터를 디코드 한다.

3. 시스템 설계



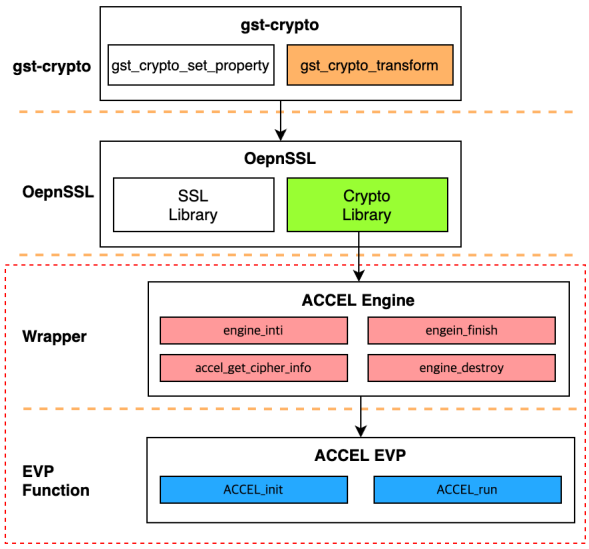
(그림 1) 암호가속기 사용 구조

그림 1은 암호가속기의 시스템 구조 이다. Zynq UltraScale + MPSoC는 PS(Processing System)영역으로 OS(Petalinux)가 프로세서를 실행한다. PS에서는 영상 데이터의 실시간 스트리밍, 영상데이터 암·복호화, RTP payload 인코딩/디코딩, 영상데이터 송/수신을 수행한다.

PL(Programmable Logic)영역은 AXI BUS에 accel top, AXI BRAM Controller로 구성 되어 있다. accel top은 암호가속기이며 암호화 수행후 AXI Master Interface가 Bram Controller를 통해 Bram에 연산 결과 값을 쓰는 구조다.

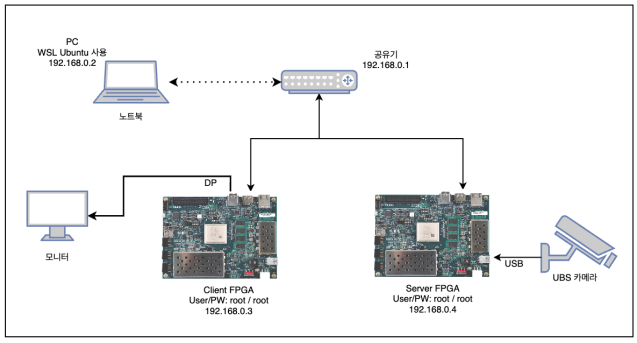
PS의 Petalinux에서는 실시간 스트리밍, 영상데이터 전송을 위해서 Gstreamer1.0을 사용하며, gst-crypto plugin을 사용해 영상데이터의 암·복호화를 수행한다.

그림 2는 영상 데이터 암·복호화를 위한 API 구조다. gst-crypto plugin은 OpenSSL Lib를 사용해 Gstreamer의 영상 데이터를 ARIA-CBC를 이용해서 암호화를 수행한다. OpenSSL Lib는 crypto engine을 사용하는 설정을 통해 PL의 암호가속기를 사용한 암·복호화를 수행할 수 있다.



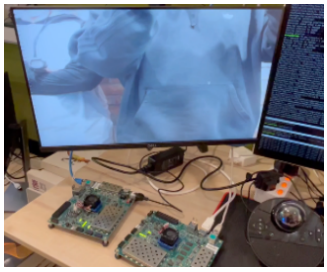
(그림 2) 영상 데이터 암/복호화 API 구조

4. 시험 결과

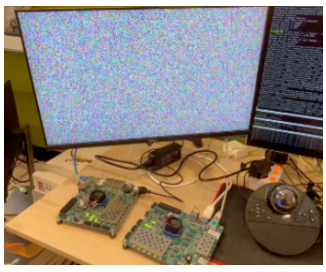


(그림 3) 시험 환경 구성

시험 환경은 그림 3과 같이 구성했다. Client FPGA에서 Server에서 보내는 RTP packet을 받고 이를 모니터에 출력한다. 송신측과 수신측이 정확하게 암호화, 복호화를 수행했을 경우와 복호화를 수행하지 못했을 경우 2가지로 시험을 수행했다.



(그림 4) 영상 출력



(그림 5) 암호화된 영상 출력

암호화한 영상데이터를 송신하고 복호화를 정상적으로 수행해서 그림 4와 같이 영상데이터를 확인했

다. 복호화를 정확하게 수행하지 않은 경우 그림 5처럼 영상 데이터가 암호화 되어 물체 식별이 불가능한 것을 확인 했다.

입력데이터 길이	SW(Mbps)	HW(Mbps)
16Kbytes	27.791	44.501
32Kbytes	27.766	45.852
64Kbytes	27.774	45.877
평균	**27.777**	**45.410**

<표 1> OpenSSL ARIA-CBC 성능 비교 시험결과

OpenSSL의 암호화 수행 속도 검증 기능을 사용해 ARIA-CBC-128의 입력데이터 길이대비 속도 측정 수행결과는 표 1과 같으며, 4K/2160p급의 영상품질의 데이터를 무리없이 암호화가 가능하다.

5. 결론

암호가속모듈을 프로세서와 연결하고, 프로세서에서 이를 사용해 영상데이터의 암·복호화에 사용하기 위해 gst-crypto plugin, crypto engine을 수정 및 개발했다. 성능 측정결과 하드웨어기반의 암호화가 소프트웨어 기반의 암호보다 63.4%의 성능 향상을 확인했고, 복호화를 수행하지 않은 경우 암호화한 영상데이터를 정확하게 식별하지 못하는 것을 확인했다.

6. Acknowledgement

이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2019-0-00097,스마트공장 네트워크 인프라용 보안 칩 및 실시간 제어프로토콜 보안 기술 개발)

참고문헌

[1] Seo, Hwajeong, and Howon Kim. "사물인터넷을 위한 경량 암호 알고리즘 구현." Review of KIISC 25.2 12-19, 2015.

[2] Uskov, Alexander, Adam Byerly, and Colleen Heinemann. "Advanced Encryption Standard Analysis with Multimedia Data on Intel® AES-NI Architecture." International Journal of Computer Science & Applications 13.2, 2016.

[3] Kwon, Daesung, et al. "New block cipher: ARIA." International conference on information security and cryptology. Springer, Berlin, Heidelberg, 2003.

[4] Schulzrinne, Henning, et al. "RFC3550: RTP: A transport protocol for real-time applications.", 2003.