정 보 보 호 학 회 지
제 32 권 제2호, 2022. 4

사물인터넷 디바이스 하드웨어 보안

지 장 현*, 박 우 정* , 문 재 근*

요 약

최근 많은 사물들의 센싱 정보를 인터넷을 통해 수집하고 가공 및 분석하는 사물인터넷 (Internet of Things, IoT) 서비스를 제공하고 있다. 2021년 기준 전세계 사물인터넷디바이스 수는 123억개로 사물인터넷 디바이스 수는 무서운 속도로 증가하고 있다. 사물인터넷 디바이스는 대체로 전력 및 비용의 문제로 저사양 디바이스를 사용하고 있고 다양한 구성요소를 가지고 있는 만큼 다양한 보안 취약성을 가지고 있다. 기존 IT 분야의 네트워크, 플랫폼, 서비스에서의 취약성은 모두 가지고 있으며, 사물인터넷 디바이스의 자원 제약성으로 인한 보안 결여 다양한 공격루트를 통한 공격자의 쉬운 접근 가능성으로 많은 보안 취약성과 높은 공격 가능성을 가지고 있다. 본 논문에서는 사물인터넷 하드웨어 보안 관점에서 살펴보고, 최근 오픈소스 하드웨어로 각광받고 있는 RISC-V를 활용한 사물인터넷 디바이스 보안 적용 방안을 보도록 한다.

키워드 : 사물인터넷 (Internet of Things), RISC (Reduced Instruction Set Computer)

Ⅰ. 서 론

최근 가정부터 산업 인프라까지 많은 사물들의 센싱 정보를 무선 인터넷을 통해 수집하고 가공 및 분석하여 각 분야의 필요한 서비스인 사물인터넷 (Internet of Things, IoT) 서비스를 제공하고 있고, 그 규모와 범위가 점차 확대되고 있다. 사물인터넷은 다양한 구성요소를 가지고 있고, 2021년 전세계 사물인터넷디바이스 수는 123억개로 연평균 22% 성장하고 있다 [1]. 사물인터넷 디바이스는 전력소모 및 비용의 문제로 저사양 디바이스를 사용하고 있어 높은 성능을 요구하는 보안 기술적용은 어려움이 있기 때문에 개인정보 및 서비스에 대한 보안의 취약성 등에 대한 연구가 활발히 진행되고 있다. 사물인터넷은 다양한 구성요소로 구성된 만큼 다양한 보안 취약성을 가고 있다. 기본적으로 네트워크, 플랫폼, 서비스에서의 취약성은 기존 IT 분야에서 연구되는 보안 취약성과 크게 다르지 않지만, 사물인터넷 디바이스는 자원 제약성과 다양한 루트를 통한 공격자의 쉬운 접근 가능성으로 많은 보안 취약성과 높은 공격 가능성을 가지고 있다. 본 논문에서는 사물인터넷 디바이스 보안을 하드웨어 디바이스 보안 관점에서 살펴보고자 하고, 최근 오픈소스 하드웨어로 각광받고 있는 RISC-V를 활용한 사물인터넷 디바이스 보안 적용 방향을 보고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존 사물인터넷 디바이스 소프트웨어 보안을 알아보고, 그에 따른 문제점에 대해서 알아본다. 3장에서는 하드웨어 기반 사물인터넷 디바이스 보안 방안 알아보고, 4장에서 RISC-V를 활용한 사물인터넷 디바이스 보안 연구에 내용을 알아본다. 마지막으로, 5장에서는 본 논문의 결론을 내린다.

Ⅱ. 기존 사물인터넷 디바이스 보안

대량의 데이터를 상호 교환하는 사물인터넷의 보안을 위해서는 기밀성, 무결성, 가용성, 인증, 부인 방지, 프라이버시 등의 보안 요구사항을 필수적으로 제공해야 한다. 이전에는 보안 요구사항을 만족하기 위한 방법으로 소프트웨어를 통한 암호학적 메커니즘을 적용하는 경우가 많았다. 그러나 사물인터넷은 연산 능력, 메모리, 에너지에 대한 자원 제약성을 가질 뿐만 아니라, 높은 이기종성과 큰 연결 규모를 가져 이러한 기존 솔루션을 그대로 적용하기에는 어려운 점이 있다.

본 장에서는 먼저 기존의 소프트웨어 기반 암호 기술과 그 한계에 관해 알아보고 앞으로의 방향성에 관해

* ㈜스마트엠투엠 하드웨어 보안팀(선임 연구원, jjh0819@smartm2m.co.kr, 연구원, wjpark@smartm2m.co.kr, 선임 연구원, jaekun34@smartm2m.co.kr)

언급한다. 다음으로 사물인터넷이 직면한 보안 문제들을 알아보고 그에 관한 기존 연구들을 제시한다.

2.1. 소프트웨어 기반 암호 기술

소프트웨어 기반 암호 기술은 크게 대칭키 암호화 기술과 비대칭키 암호화 기술로 구분할 수 있다.

대칭키 암호화 기술은 암호화와 복호화에 동일한 키를 사용하는 암호 기술이다. 이는 계산량이 적고 구현이 쉬우나, 모든 연결에 대해 별도의 키가 요구되어 노드의 수가 많아질수록 확장성이 떨어지는 단점이 존재한다. 사물인터넷은 높은 연결 규모를 가지기 때문에 대칭키 알고리즘의 확장성은 응용에서 중요한 문제가 된다.

이에 비해, 비대칭키 암호화 기술은 암호화와 복호화에 별도의 키를 사용하는 암호 기술이다. 해당 기술은 유연하고 확장성이 높아 대칭키 암호화 기술의 단점을 보완하기 위해 많이 사용되지만, 비효율적이고 에너지 사용량이 높은 것이 단점이다. 따라서 사물인터넷 디바이스와 같은 자원 제약적인 환경에서는 실시간 통신에 사용될 수 없는 문제를 지닌다.

한편, 소프트웨어를 통해 암호화를 수행하면 사물인터넷 디바이스가 공격받을 경우에 메모리에 존재하는 키는 노출되기가 쉽기 때문에 키의 저장 및 관리가 어려워지는 문제도 존재한다.

최근에는 이러한 문제를 해결하기 위해 암호 및 키 관리 기능을 제공하는 별도의 하드웨어를 사용하여 연산 수행 능력을 높이고 에너지 사용량을 줄이거나 안전하게 키를 관리하기 위한 접근이 시도되고 있다. 이러한 하드웨어를 사용할 경우 검증된 기존 기술을 자원 제약적인 사물인터넷 환경에서 사용하는 것이 가능하며, 사물인터넷 디바이스가 취약점으로 인해 공격받을 경우에도 키가 별도의 저장소에 존재하여 안전한 장점을 가진다.

2.2. 사물인터넷의 보안 문제와 기존 연구

사물인터넷의 보안 문제를 해결하기 위해서는 사물인터넷의 개발 및 동작을 포함한 전체 생명 주기에서 적합한 보안 메커니즘이 적용될 필요가 있다. 이러한 사물인터넷의 보안 문제는 고유한 기술적인 특성에 의해 나타나는 문제를 제외하면, 기밀성, 무결성, 가용성, 인증, 경량 솔루션, 이기종성, 정책, 키 관리에 관한 문제로 구분될 수 있다. [2]

기밀성은 데이터가 인가된 사용자에게만 제공되는 것을 의미한다. 특히 사물인터넷에서 기밀성은 센서 노드의 데이터가 이외의 노드에 공개되거나, 태그 데이터가 인가되지 않은 리더에게 전송되지 않는 것을 의미할 수 있다. [3] 기밀성을 보장하기 위한 기존 연구로는 다양한 경량 암호 기술과 인증 기법, 하드웨어 기반 암호 가속 기술이 존재한다. [4, 5, 6]

무결성은 데이터가 변조되지 않음을 의미한다. 상대적으로 공격에 취약하고 네트워크의 품질이 낮은 사물인터넷 환경에서는 별도로 데이터의 무결성을 보장하기 위한 메커니즘이 요구될 수 있다. 무결성을 보장하기 위한 기술로는 에러 정정 코드(ECC) 등이 존재하지만, 높은 보안 요구사항을 달성하기 위해서는 암호 기술이 요구된다. 무결성을 보장하기 위해 해쉬 함수, 메시지 인증 코드 등과 같은 암호 기술을 적용하면 충분한 신뢰성을 제공하는 것이 가능하다.

가용성은 서비스나 데이터가 필요로 할 때 제공되어야 함을 의미한다. 서비스 거부 공격(DoS)으로 인해 사물인터넷 네트워크의 가용성이 저해될 수 있으며 이러한 공격을 탐지 및 대응하기 위한 방법들이 존재한다. [7]

인증은 접근을 시도하는 특정한 객체를 식별하거나 자격을 검증하는 것을 의미한다. 사물인터넷의 경우 제약된 자원과 높은 이기종성 등으로 인해 기존 시스템에 비해 인증을 제공하는 것이 어렵다. 공개키 암호 기술과 같이 충분히 검증된 인증 메커니즘을 사물인터넷에 적용하기 위해서는 TPM (Trusted Platform Module)과 같은 하드웨어 보안 모듈을 사용하는 것이 가능하다. [8]

경량 솔루션은 특히 사물인터넷 보안에서 필요한 요구사항으로, 사물인터넷의 자원 제약성으로 인해 적절한 보안 솔루션을 적용하기 위해서는 경량화가 필요함을 의미한다. 사물인터넷 디바이스에서 연산 능력, 메모리, 에너지에 대한 경량화를 달성하기 위해서는 사물인터넷 환경에 적합한 경량 솔루션을 설계하거나 소프트웨어적인 코드 최적화를 활용할 수 있으나, 특히 전용 하드웨어를 사용할 경우 소프트웨어 기반 솔루션에 비해 고도의 경량화가 가능하다.

이기종성은 기존의 인터넷에 비해 사물인터넷에 연

결되는 노드들이 다양한 종류와 특성을 가지는 것을 의미한다. 사물인터넷의 이기종성으로 인해 서로 다른 기기가 서로 다른 상황에서도 통신할 수 있는 프로토콜의 설계가 요구된다. [2]

정책은 데이터의 관리와 보호, 전송을 위해 필요한 표준 등을 의미하는 것으로, 사물인터넷에서 통일된 표준을 수립하고 정책을 시행하는 것은 중요한 보안 문제 중 하나이다.

마지막으로, 키 관리는 암호 기술을 사용하기 위해 필요한 키를 분배 또는 관리해야 하는 문제로, 사물인터넷의 자원 제약성, 높은 이기종성, 큰 연결 규모와 같은 특성으로 인해 중요한 문제 중 하나로 부각되고 있다. 자원이 제약된 상황에서 많은 노드 수에 대해서도 확장성을 가지는 키 관리 모델과 그 구현이 요구된다.

Ⅲ. 사물인터넷 디바이스 하드웨어 보안

본 장에서는 기존 사물인터넷 디바이스 보안 기술에서 생겼던 문제점을 보완하는 방법이나 저사양 사물인터넷 디바이스에서 성능향상을 위해 진행되고 있는 하드웨어 보안 기술에 대해서 설명하고 있다.

3.1. 사물인터넷 하드웨어 보안 기술 개념

하드웨어 보안 기술은 운용 시스템을 위한 특별한 서비스 구현하여 하드웨어 모듈을 제작하는 경우와 플랫폼 또는 소프트웨어 환경에서 보안을 위한 범용적으로 키 관리 기술이나 암호화 기능을 구현의 경우로 구분할 수 있고, 하드웨어 보안 기술의 구현은 크게 FPGA(Field Programmable Gate Array) 형태와 ASIC(Application Specific Integrated Circuit) 형태로 나눌 수 있다.

FPGA는 프로그래밍을 통해 내부 논리를 변경할 수 있어 범용성을 가지지만 효율성은 다소 떨어진다. ASIC는 범용 용도로 변경이 불가능한 특정 용도를 위해 맞춤 제작된 집적 회로이기 때문에 ASIC는 FPGA 또는 범용 프로세서상의 소프트웨어 구현보다 전력이나 성능면에서 고효율 특성을 만족한다. 이러한 특성으로 인해 사물인터넷 디바이스에 사용가능한 보안 모듈뿐만 아니라 비트코인 채굴이나 암호 크래킹 머신 등 하드웨어 보안 칩 적용하여 많이 활용된다.

또한, 프로세서, 메모리, 암호 모듈, 인터페이스 모듈을 단일 칩에 구현되는 SoC(System on Chip) 기술이 발전하여 칩 외부에 존재하는 메모리에 대한 물리적 탐침으로 발생하는 데이터 유출에 상대적으로 안전하고, 인증 또는 인가 서비스나 프로토콜 보안 제공을 위한 TLS 칩과 같이 중요 보안 서비스에서 하드웨어 보안이 활용되고 있다.

위에서 언급한 하드웨어 보안 기술을 제공하는 하드웨어 모듈을 대표적으로 HSM(Hardware Security Module)이라고 부른다. HSM은 암호 알고리즘에서 사용하는 암복호화 키, 서명 생성 키, 인증키 등, 중요한 키값을 안전하게 저장하는 장치이며, 일반적으로 암호 알고리즘을 처리할 수 있는 하드웨어 가속 모듈을 갖추고 있다. 하지만, ASIC은 변경불가능하기 때문에 사물인터넷 디바이스에서도 게이트웨이 또는 센싱 디바이스 등 목적에 맞춰 스펙을 조절하여 다양한 HSM 버전의 모듈이 있다.

사물인터넷 디바이스 뿐 만아니라 고성능 디바이스 및 전력 공급이 원할한 클라우드 서비스에서도 하드웨어 보안은 많이 활용되고 있다. 최근 대부분의 웹 서비스가 클라우드 인프라 기반으로 운용되고 있다.

대표적으로 아마존은 웹 서비스 기반 형태의 클라우드를 제공하고 이를 AWS(Amazon Web Service) 클라우드로 명명하였다. 이와 같은 환경에서 안전한 웹 서비스 운용을 위해서 데이터베이스 암호화와 같은 데이터베이스 보호, 통신 프로토콜의 적용과 같은 보안 요구 또한 증가하고 있기 때문에 보안 기술 고성능으로 동작이 필요해졌다.

이러한 보안 요구를 만족하기 위해 Amazon은 AWS Cloud와 HSM이 결합한 형태인 AWS Cloud HSM를 제공하고, AWS Cloud HSM은 AWS Cloud에서 자체 암호화키를 손쉽게 사용할 수 있도록 지원하는 Cloud 기반 하드웨어 보안 모듈로 키관리 기능 및 FIPS 140-2 레벨3 인증으로 안전성이 높은 보안 기능을 제공할 수 있다. AWS Cloud HSM은 PKCS#11, JCE(Java Cryptography Extensions), Microsoft CNG(CryptoNG)와 같은 표준 API를 활용하여 하드웨어 키 관리와 암호 알고리즘 가속 기능을 제공할 수 있다. [9]

특수 목적을 위해 설계된 하드웨어 기술도 존재한다. PUF(Physically Unclonable Function)와

TPM(Trusted Platform Module)이다.

PUF는 물리적으로 복제를 불가능하고, 랜덤성을 가지도록 설계가 되어 사람의 지문과 같은 역할을 할 수 있다. 해당 값을 통해 하드웨어 칩의 고유 ID값으로 사용할 수 있으며 Root 키로 사용할 수 있다.

TPM은 플랫폼의 신뢰성을 보장하기 위한 목적으로 다양한 보안기능을 제공하는 모듈이다. TPM 역시 HSM과같이 키 관리 및 암호 기능을 제공하고, 추가적으로 Secure Boot 기능을 제공할 수 있다. 하지만, HSM과 다르게 고속 암호화 처리는 불가능하다는 단점이 있어 플랫폼 신뢰성 및 안전성을 위해 사용할 수 있다.

3.2. 프로세서 명령어 확장기반 하드웨어 보안

하드웨어 보안에서는 프로세서 특수 목적의 ALU를 추가함으로써 특정 암호에 대한 프로세서에 내장된 대표적 암호 하드웨어 가속 기술로는 2008년에 인텔에서 제안한 x86 명령어 집합 확장을 이용한 AES 암호 가속기(AES-NI)를 예를 들 수 있다. 이는 암호화 및 복호화 수행 성능을 향상하는 기술이며, 인텔 프로세서의 명령어 형태로 사용자에게 제공된다.

AES-NI 명령어 집합은 암호화 라운드 수행, 복호화 라운드 수행, 라운드 키 생성, Inverse Mix Column 연산, 캐리 없는 곱셈 연산을 지원하기 위해 7개로 구성된다. AES-NI의 장점으로 빠른 연산 속도가 있다. 소프트웨어보다 AES-NI를 사용한 하드웨어 기반의 암호화가 8~10배 이상 빠르다.

AES-NI 명령어를 지원하는 Intel Core i7-4790K 프로세서에서 AES-NI를 사용할 경우비교 했을 때 인텔 프로세서와 같은 고성능 프로세서인 경우에도 하드웨어적인 AES 암호 가속기를 제공할 경우, 동작 모드(Mode of Operation)에 따라 약 1.6배에서 4.2배 정도의 성능 차이를 가지고 있다. [10]

암호 알고리즘을 소프트웨어 구현할 경우, 구현상에서 코드의 취약점을 가질 수 있고 운용 차원에서도 여러 취약점을 가질 수 있다. 예를 들면, 암호키 및 IV등 안전하게 저장되어야 하는 값을 메모리 저장하는 경우 다른 소프트웨어나 앱의 취약성을 이용해 메모리에 접근하여 메모리를 유출하거나 변조할 가능성이 존재한다. 다른 경우에는 연산 수행시간, 전력소모량, 캐시 메모리 히트율 및 메모리 접근 빈도등 부채널 분석 정보를 이용해서 부채널 공격을 실행할 수 있다. 이에 반해, AES-NI는 전용 암호화 가속을 위한 하드웨어를 사용함으로써 위의 소프트웨어 취약점을 보완 및 방지가 가능하고, 부채널 분석도 부채널 방지 기법 등을 하드웨어 모듈에 적용한다면 문제점을 보완할 수 있다.

이처럼 암호 가속 기술은 프로세서에 적용하기 위해 추가적인 모듈 혹은 명령어가 필요하다. 이는 미적용 대비 하드웨어 면적, 전력 소모가 증가하게 된다는 의미로 볼 수 있지만 실제 운용하는 관점에서는 연산 축소로 전력소모나 속도 측면에서 이득을 볼 수도 있다.

명령어 확장 기반 암호 가속 기술 적용 시의 성능 향상 혹은 추가 모듈 혹은 구조의 최적화 연구를 통해 암호 가속 기술의 효율성을 높이는 방향의 연구가 진행되고 있지만, 인텔 프로세서나 ARM 프로세서에 모듈을 직접 추가하기에는 어려운 상황이다.

하지만, 4장에서 설명되는 RISC-V는 이러한 명령어 확장 하드웨어 가속 기술을 적용 연구도 가능하고 많은 연구가 진행되고 있다.

3.3. PUF

PUF는 물리적 복제방지 기능을 제공하는 하드웨어 모듈로 일종의 사람의 지문과 같이 디지털 지문으로 볼 수 있다. 일반적으로 하드웨어 회로는 하드웨어 기능을 복제할 수 있어 복제하는 사례가 있었다. 하지만, PUF는 논리 수준의 회로가 복제하더라도 공정상 발생하는 물리적인 특성 차이에 의해 다른 결과값을 가지는 기술이다. 즉, PUF 하드웨어 모듈을 생산했을 때 각기 다른 출력값을 가지기 때문에 하드웨어 모듈의 고유값을 생성하는 기술로 볼 수 있다.

현재 사용되는 PUF는 대부분 반도체 제조 공정에서 자연적으로 발생하는 고유한 물리적 차이를 기반으로 만들어진다. 예를 들어, 반도체 공정을 사용하여 특정 로직을 구현했을 경우 실제 같은 기능을 하지만, 오차가 존재하므로 특정 로직의 지연시간은 모두 미세하게 차이가 날 수밖에 없다. 이는 반도체 공정의 고유한 성질이다. PUF는 일반적으로 아날로그 회로의 특성에 의존한다는 특성이 있다.

최근에도 새로운 물리적인 특성을 활용한 PUF 기술이 많이 개발되고 있다. PUF는 기본적으로 복제 불가

능한 특징을 가지며 이러한 복제 불가능한 특징을 이용하여 다양한 보안 목적으로 사용할 수 있다. PUF는 고유한 키값 생성(Secret Key Generation), 인증 디바이스(Authentication Device)로도 활용할 수 있다.

PUF는 안전성을 위해 활용을 많이 되는 하드웨어 모듈이지만 PUF에 대한 공격 기법도 존재한다. Modelling Attack과 Differential Template Attack, EM Attack 등이 존재하지만 PUF 공격에 대응하기 위한 기술이 존재한다. Reconfigurable PUF와 Erasable PUF가 대표적인 PUF 공격 대응 기법이며 PUF의 고유성을 공격 하는 방법과 공격에 대응하여 고유성을 유지하는 연구가 계속해서 진행되고 있다.

3.4. TPM

TPM은 Trusted Computing을 달성하기 위한 목적으로 만들어졌으며 Trusted Computing은 사용자의 비밀 데이터 및 개인 정보를 보호하기 위한 목적을 가지고 있다. 일반적으로 TPM은 HSM이 포함한 기능을 포함하고 있다. 단, TPM은 고속으로 암호 데이터 처리를 위한 HSM과 같은 경우와 달리 신뢰성등 플랫폼 보안을 초점되어 설계되었다고 볼 수 있다. 따라서 TPM이 HSM을 대체 완벽하게 대체한다고 볼수는 없다. TPM은 고속 데이터 암호화 및 복호화 기능을 제공하지 않는다.

TCG(Trusted Computing Group)에서는 Trust Computing을 위한 표준을 제안하였고, 여기서 정의된 구조가 TCG 구조이다. TCG 아키텍처의 주된 기술 특성은 Secure I/O, 메모리 Curtaining, 저장 공간 봉인, 원격 증명기술 특성을 포함하는데 TPM이 바로 이러한 TCG 아키텍처의 기반이 되는 모듈이다.

TPM은 암호화에 필요한 키를 안전하게 생성 및 관리하는 기능을 제공함하고 있어 디바이스 식별과 인증, 암호화 장치의 무결성 보장을 위한 Secure Boot 기능을 제공할 수 있고, 이러한 기능을 이용하여 플랫폼 무결성 검증, 디스크 암호화 등 다양한 컴퓨팅 응용 환경에 적용된다.

플랫폼 무결성 검증은 PC나 특정 운영체제 국한되지 않는 모든 컴퓨터 플랫폼에 대해 신뢰할 수 있는 상태에서 부팅을 수행하고, 그 신뢰성이 운영체제가 완전히 부팅될 때까지 유지되는 것으로 TPM 내 PCR(Platform Configuration Register)를 통해 제공된다.

또한 TPM은 리눅스 커널의 Secure Doc, Dm-crypt 및 Microsoft의 BitLocker와 같은 FDE(Full Disk Encryption) 응용 기술에서 컴퓨터의 하드 디스크를 전체 암호화하는데 사용되는 키 안전하게 보호하고, 암호화 기능을 제공할 때 사용되고 있으며, 이 외에 DRM(Digital Right Management), 소프트웨어 라이선스 보호 등 암호 응용이 가능한 모든 프로그램과 연동하여 TPM을 이용 할 수 있다.

TPM은 사물인터넷 디바이스에서 키 관리 목적 또는 사물인터넷 플랫폼 신뢰성을 위해서 사용될 수 있지만 많은 센싱 데이터를 보내고, 고속 암호화 기능을 필요로하는 사물인터넷 디바이스에서는 하는 사용하기 어려울 수 있다.

3.5. HSM

HSM은 보안과 관련된 기능을 수행하기 위한 물리적 컴퓨팅 디바이스로, 키의 안전한 생성, 저장 및 관리 기능과 대칭키 암복호화, 비대칭키 서명, 인증, 그리고 해쉬 함수 등 암호 연산에 대한 가속 기능을 제공한다. 이러한 하드웨어 기반 컴퓨팅 디바이스는 소프트웨어에 비해 연산 능력이 높고, 에너지, 메모리와 같은 자원을 더욱 효율적으로 사용하기 때문에 사물인터넷 환경의 보안을 위해 다양한 용도로 사용될 수 있다.

먼저, 사물인터넷 환경에서 키의 관리 및 분배 문제를 해결하기 위해 HSM을 사용할 수 있다. 사물인터넷은 많은 수의 이기종 디바이스가 상호 연결되는 환경이므로 키 관리 문제를 효율적으로 해결하는 것이 중요하다. 이러한 문제의 해결을 위해서는 안전한 키 생성 및 저장, 비대칭키를 기반으로 한 키 교환 알고리즘 등의 수행이 요구되며 이는 HSM을 통해 적합하게 수행될 수 있다. 특히, 사물인터넷 디바이스가 공격의 대상이 되어 메모리에 있는 정보가 노출되는 경우에도, HSM을 사용하면 인터페이스를 통한 키의 출력을 방지하여 별도의 저장소에 키를 안전하게 보관하고 필요 시 삭제하는 것이 가능하다.

또한, 사물인터넷 환경에서 실시간 암호 연산을 위한 자원 활용 문제를 해결하기 위해 HSM을 활용할 수 있다. 예로, DTLS (Datagram Transport Layer Security)와 같은 보안 통신 프로토콜은 계산 집약적인 암호 연산의 수행을 요구한다. 이러한 경우 전용 하드

웨어 보안 모듈을 소프트웨어와 연계하여 에너지, 메모리, 실행 시간을 사물인터넷 환경에 적합한 수준으로 효율화하는 것이 가능하다. [6]

Ⅳ. RISC-V 기반 사물인터넷 디바이스 보안

4.1. RISC-V

RISC-V는 사물인터넷뿐만 아니라 스마트폰, 웨어러블 디바이스등 다양한 분야에서 하드웨어 프로세서가 전반적으로 활용되고 있다는 점에서 시작됐다. 하드웨어 프로세서는 인간의 두뇌 역할을 하는 칩으로 중앙처리장치(CPU)로 불린다.

현재 저사양 프로세서를 많이 활용하는 사물인터넷과 웨어러블 디바이스의 프로세서는 약 90%가 ARM사의 프로세서를 사용있어 해당 프로세서를 사용하는 경우 설계 수정이 거의 불가능하고 로열티 부담으로 비용적인 측면에서도 문제가 많다. 이에 최근 오픈소스 기반 RISC-V 프로세서가 제조 및 설계업체들의 주목을 받고 있다.

RISC-V 프로세서의 기본 사양을 정하는 명령 세트 아키텍처(ISA)를 미국 캘리포니아 대학 버클리 캠퍼스의 연구자가 2010년부터 개발을 시작하고, 2015년 RISC-V 파운데이션이 공식 오픈하면서 연구가 활발하게 진행되었다. RISC-V는 오픈소스이므로 누구나 무료로 설계에 활용할 수 있다. RISC-V 프로세서는 미국 사이파이브와 같이 RISC-V 기반으로 설계된 회로의 지적재산(IP)을 외판하는 기업도 생겨나고 있다.

4.2. RISC-V Ibex 코어

Ibex는 HDL(Hardware Description Language)언어 중 시스템 베릴로그(System Verilog)로 개발된 32비트 RISC-V 프로세서이다. Ibex는 저전력/저면적 특성으로 임베디드 사용을 위한 요구사항에 적합하며, 소스코드가 공개되어 있어 추가적인 커스터마이징이 가능하다.

[표 1] 는 RISC-V 기반 코어 간의 에너지 효율성 비교를 나타낸다. 각 측정값의 분자(Iteration)는 CoreMark 벤치마크 상에서의 반복 횟수를 의미하며, 분모(mJoule)는 에너지 소비량(전력)을 의미한다. 측정결과 Ibex_IMC 코어가 가장 높은 에너지 효율성을 나타내고 있다. [11]

〔표 1〕 RISC-V 프로세서간 에너지 효율성

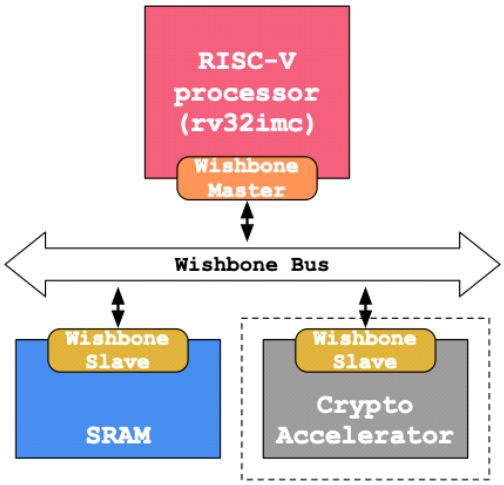
	Iteration/mJoule
E20	4.328
E21	2.583
SCR1_EC	5.611
SCR1_IC	3.159
SCR1_IMC	5.551
N22	7.94
Ibex_IMC	8.714
Ibex_EC	3.64
CV32e40p	5.5
RpcoRV	4.44

본 논문에서 사물인터넷 디바이스 보안을 위한 RISC-V 프로세서 소프트웨어 및 하드웨어 성능 연구를 위해서 사물인터넷 디바이스에 적합한 저전력 조건을 만족하는 후보 중 위와 같이 가장 높은 에너지 효율성을 보이는 Ibex RISC-V 코어를 연구 대상으로 선택하였으며, 이후 연구 내용의 RISC-V 프로세서는 해당 프로세서를 기반으로 설계 및 개발을 진행하였다.

4.3. Ibex 기반 사물인터넷 디바이스 보안 성능 연구

본 연구에서는 RV32IMC 기반 RISC-V Ibex 프로세서를 활용한 성능 비교 연구를 진행해 보았다. 기본 RISC-V 프로세서에 소프트웨어 및 하드웨어 성능비교를 위해 국내에서 많이 사용하고 있는 블록암호인 ARIA를 국내 표준 기반으로 HDL 언어로 개발을 진행하였다. 또한, 성능 비교를 위해 사물인터넷 디바이스를 위해 최적화는 저면적 버전으로 개발한 ARIA 하드웨어 가속기를 연동하여 FPGA를 통해 소프트웨어 및 하드웨어 성능 검증을 진행하였다.

저전력 RISC-V 프로세서 기반 소프트웨어 암호화 수행과 동일한 FPGA에 올려진 하드웨어 암호 가속기 구현에 대한 성능 평가를 수행하였다. 동일한 조건에서 하드웨어 ARIA 모듈은 RISC-V 코어와 동일한 클럭 주파수를 통해 동작하였다. 해당 시험은 Wishbone 인터페이스를 통해 제어 신호를 전달하였고, 데이터 입출력은 RISC-V에서 제공하는 Load 및 Store 명령을 통

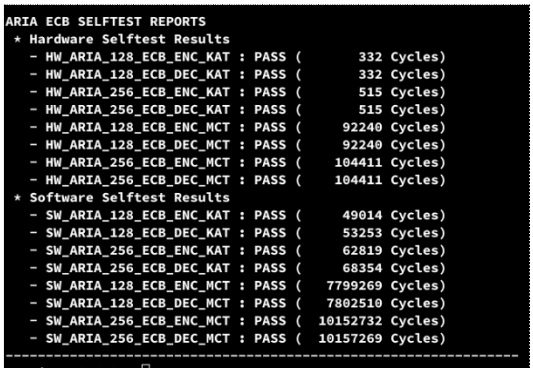


〔그림 1〕 RISC-V 활용한 암호 가속기 구조

해 수행하였다.

성능 비교에 활용된 소프트웨어 버전 ARIA 코드는 한국인터넷진흥원(KISA)에서 제공하는 Reference 코드를 활용하여 컴파일을 진행하였다. Ibex 프로세서 상에서 소프트웨어와 하드웨어 동작 시켰을 때 암호화 성능을 측정하였을 때 하드웨어 기반 블록 암호의 성능은 약 100~150배의 성능 차이를 보였다. 이러한 성능 차이는 키 초기화 및 생성에서 가장 많이 성능 차이가 나타났으며 암호화 과정에서도 소프트웨어 대비 하드웨어 성능이 월등히 빠른 것을 알 수 있었다.

블록암호에서 키 설정이후에는 고정된 키를 사용하므로 메시지 사이즈가 커질수록 차이는 줄어들었지만 60~70배 정도의 성능차이를 보여주고 있었다.



〔그림 2〕 SW 및 HW 암호화 테스트

〔표 2〕 메시지 사이즈에 따른 RISC-V 암호화 성능 결과

	SW(kbps)	HW(kbps)
16Byte	127	18997
1KByte	744	62728
32KByte	896	65152

V. 결 론

본 논문에서는 사물인터넷 디바이스 보안을 위해서 진행되고 있는 소프트웨어와 하드웨어 보안 방향성 및 RISC-V 프로세서를 활용한 사물인터넷 하드웨어 보안 관점에서 연구해보았다. 소프트웨어 대비 하드웨어 성능은 기존 많은 연구에서도 많은 성능 향상이 있어왔다. 현재 보안을 적용한 많은 사물인터넷 디바이스는 ARM사의 프로세서를 사용하고 있지만 비용이나 프로세서 설계 수정에는 제약사항이 많아 일반적으로 불가능하다고 볼 수 있다. 고성능 프로세서 및 전력을 충분히 공급하기 어려운 환경의 저전력을 요구하는 사물인터넷 디바이스에서는 RISC-V 프로세서를 활용하고, 보안 솔루션을 적용하기 위해서는 하드웨어 기술을 적용한다면 사물인터넷 뿐만 아니라 드론, 커넥티드 카 등 고신뢰성을 가진 고성능 저전력 SoC 프로세서 적용 가능할 것으로 보인다. 따라서, RISC-V 암호 가속기 뿐만 아니라 추후 RISC-V를 활용한 안전한 TEE(trusted execution environment) 환경 구성을 위한 기술 등 다양한 보안 솔루션 연구를 하고자 한다.

참 고 문 헌

[1] Global IoT market size grew 22% in 2021 – these 16 factors affect the growth trajectory to 2027 (IoT Analytics , Available online) : https://iot-analytics.com/iot-market-size/(30 Mach 2022).

[2] Mahmoud, Rwan, et al. "Internet of things (IoT) security: Current status, challenges and prospective measures." 2015 10th international conference for internet technology and secured transactions (ICITST). IEEE, 2015.

[3] Khairi, Anjum, et al. "A Critical Analysis on the Security Concerns of Internet of Things

(IoT)." Perception 111 (2015).

[4] Dhanda, Sumit Singh, Brahmjit Singh, and Poonam Jindal. "Lightweight cryptography: a solution to secure IoT." Wireless Personal Communications 112.3 (2020): 1947-1980.

[5] Purohit, Kamlesh C., et al. "Hybrid approach for securing IoT communication using authentication and data confidentiality." 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall). IEEE, 2017.

[6] Banerjee, Utsav, et al. "An energy-efficient reconfigurable DTLS cryptographic engine for End-to-End security in iot applications." 2018 IEEE International Solid-State Circuits Conference-(ISSCC). IEEE, 2018.

[7] Muzammal, Syeda M., Raja Kumar Murugesan, and N. Z. Jhanjhi. "A comprehensive review on secure routing in internet of things: Mitigation methods and trust-based approaches." IEEE Internet of Things Journal 8.6 (2020): 4186-4210.

[8] Kothmayr, Thomas, et al. "A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication." 37th Annual IEEE Conference on Local Computer Networks-Workshops. IEEE, 2012.

[9] AWS Cloud HSM 주요 기능 : https://aws.amazon.com/ko/cloudhsm/features/.

[10] 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).

[11] RISC-V Resource-Constrained Cores: A Survey and Energy Comparison

〈저자소개〉

지 장 현 (JangHyun Ji)

2016년 2월 : 부산대학교 컴퓨터공학과 졸업
2021년 2월 : 부산대학교 컴퓨터공학과 석박통합과정 수료
2020년 4월~현재 : 스마트엠투엠 재직
<관심분야> 하드웨어 보안, 정보보호

박 우 정 (Woojung Park)

2021년 2월 : 부산대학교 컴퓨터공학과 졸업
2021년 3월~현재 : 스마트엠투엠 재직
<관심분야> 하드웨어 보안

문 재 근 (Jaegeun Moon)

2015년 8월 : 경북대학교 전자공학과 졸업
2017년 8월 : 경북대학교 전자공학과 석사 졸업
2021년 2월 : 국민대학교 금융정보보안학과 박사과정 수료
2021년 10월~현재 : 스마트엠투엠 재직
<관심분야> 하드웨어 보안, 부채널 분석, 정보보호