소프트웨어 정의 차량(SDV)의 무선 소프트웨어 업데이트를 위한 동적 속성 기반 접근제어 기법

박승현

한성대학교

sp@hansung.ac.kr

Dynamic Attribute-Based Access Control for OTA Updates in Software-Defined Vehicles (SDVs)

Seunghyun Park

Hansung University

요 약

소프트웨어 정의 차량(Software-Defined Vehicle, SDV)의 확산으로 무선 소프트웨어 업데이트(Over-the-Air, OTA)의 중요성이 커지고 있다. 그러나 기존 OTA는 차량 모델이나 ECU 식별자와 같은 정적 속성만을 고려하여, 보증기간 만료나 서비스 구독 해지 등 시간 및 상태에 따른 동적 속성을 반영하지 못하는 한계가 있다. 본 논문은 이러한 문제를 해결하기 위해 동적 속성 기반 접근제어 기법을 제안한다. 제안 기법은 정적 속성과 동적 속성을 분리하여 관리하고, 속성 만료와 속성 수준 키 갱신을 결합함으로써 실시간 권한 철회와 효율적 키 관리를 구현한다. 컨테이너 기반 모의 실험 결과, 제안 기법은 기존 정적 CP-ABE 방식 대비 권한 철회 지연을 최소화하고 키 갱신 속도와 네트워크 효율을 크게 향상시켰다. 본 연구를 통해 SDV OTA 환경의 동적 상태 변화를 반영한 접근제어 모델을 체계적으로 설계하고, 그 실효성을 실험적으로 검증할 수 있다.

I. 서 론

소프트웨어 정의 차량(Software-Defined Vehicle, SDV)의 확산은 자동차 산업의 구조를 소프트웨어 중심으로 전환시키고 있다. SDV는 하드웨어에 종속되지 않고 무선 소프트웨어 업데이트(Over-the-Air, OTA)를 통해 기능을 확장하지만, 이 과정에서 무결성 훼손, 무단 업데이트, 불법 소프트웨어 설치 등 다양한 보안 위협이 발생할 수 있다. 이에 UN R156과 ISO 24089 등 국제 표준은 OTA 과정에서의 무결성, 인증, 접근제어 및 권한 관리의 필요성을 강조하고 있다.

기존 OTA 보안 방식은 중앙 서버 기반의 일괄 접근제어나 정적 속성 중심의 암호화 방식에 의존하여, 보증 기간, 서비스 구독, 자율주행 모드와 같은 동적 속성의 변화를 실시간으로 반영하지 못하는 문제가 있다 [1]. 특히 SDV는 서비스와 차량 상태가 지속적으로 변하기 때문에, 이러한 한계는 실시간 권한 철회와 세분화된 보안정책 구현을 어렵게 한다.

본 연구는 이러한 문제를 해결하기 위해 동적 속성 기반 접근제어 기법을 SDV OTA 권한 관리에 적용한다. 제안 기법은 정적 속성과 동적 속성을 분리 관리하고, 속성 만료와 속성 수준 키 갱신을 통해 차량 상태 변화를 실시간으로 반영함으로써 기존 정적 CP-ABE [2, 3] 방식의 한계를 극복한다. 본 논문은 SDV OTA 시나리오를 기반으로 제안 기법의 구조와 효용을 분석하고, 향후 국제 표준 대응 및 실차 적용 가능성을 논의한다.

II. 동적 속성 기반 접근제어 기법

본 연구는 SDV OTA 업데이트의 보안성을 강화하기 위해 동적 속성 기반 접근제어 기법을 제안한다. 기존 CP-ABE 기반 접근제어는 차량 모델명이나 ECU 식별자 등 정적 속성만을 고려하여, 보증기간 종료나 서비스 구독 해지와 같은 시간, 상태 변화에 따른 권한 제어가 불가능하다. 이를 개선하기 위해 본 연구는 정적 속성과 동적 속성을 분리 관리하고, 속성 만료와 속성 수준 키 갱신을 결합하여 실시간 권한 제어와 효율적 키 관리를 구현한다.

1) 동적 속성 표현 모델

기존 CP-ABE는 시간에 따라 변화하는 속성을 처리하지 못하므로, 본 연구에서는 속성 유효성 함수를 도입하여 속성의 시간과 상태 의존성을 모델링한다.

먼저, 차량 V_i의 전체 속성 집합은 다음과 같이 정의된다.

$$A_i(t) = A_s \cup A_d(t) \tag{1}$$

여기서 A_s는 차량 모델, ECU 종류 등 변하지 않는 정적 속성의 집합이며, $A_d(t)$는 시간 t에서 유효한 동적 속성의 집합이다. 각 동적 속성 $a_j \in A_d(t)$의 유효성은 속성 만료 함수 $\mathrm{valid}(a_j, t)$로 표현한다.

$$\mathrm{valid}(a_j, t) = \begin{cases} 1, \text{ if } t < T_{\exp}(a_j) \text{ and } \mathrm{state}(a_j) = active \\ 0, \text{ otherwise} \end{cases} \tag{2}$$

여기서 $T_{\exp}(a_j)$는 속성 a_j의 만료시각, $\mathrm{state}(a_j)$는 속성의 현재 상태 $\{active, revoked, expired\}$를 의미한다.

유효 속성만을 포함하는 동적 속성의 집합은 다음과 같이 정의한다.

$$A_d(t) = \{a_j | \mathrm{valid}(a_j, t) = 1\} \tag{3}$$

즉, 차량의 구독 상태가 해지되거나 보증기간이 만료되면 해당 속성이 자동으로 무효화되어 접근정책에서 제외된다. 이를 통해 OTA 권한은 별도의 재암호화 없이 실시간으로 조정된다.

2) 동적 정책 기반 암호화

본 연구의 접근정책은 시간의 함수로 정의되며, 정적 속성 조건과 동적 속성 조건을 동시에 만족해야 복호화가 가능하다.

$$P(t) = f(A_s) \wedge g(A_d(t)) \tag{4}$$

여기서 $f(A_s)$는 정적 속성 조건, $g(A_d(t))$는 시점 t에 평가되는 동적 속성 조건이다. 예를 들어, 접근정책 $P(t)$에서 정적 속성을 $(MODEL \in X \wedge ECU \in GW)$으로, 동적 속성을 $(SUB = valid \wedge t < T_{exp})$으로 설정하면, 차량 모델과 ECU 조건과 같은 정적 속성을 충족하더라도 구독 만료나 보증기간 경과에 따라 동적으로 접근이 거부된다.

제조사 서버는 정책 $P(t)$에 따라 OTA 파일 M을 암호화하여 암호문 CT를 생성한다.

$$CT = Enc_{CP-ABE}(PK, M, P(t)) \quad (5)$$

차량 게이트웨이는 자신의 속성 집합이 정책를 만족할 경우에만 복호화에 성공한다.

$$Dec_{CP-ABE}(CT, SK_i) = \begin{cases} M, & A_i \models P(t) \\ \perp, & \text{otherwise} \end{cases} \quad (6)$$

이 과정을 통해 암호문 재배포 없이 정책이 자동으로 반영되며, SDV 상태 변화에 따른 실시간 접근제어가 가능하다.

3) 실험 설계

제안한 동적 속성 기반 접근제어 기법의 성능을 검증하기 위해 두 가지 실험을 수행하였다. 첫 번째는 속성 변경 시 전체 키 재발급 대비 부분 키 갱신의 효율성을 비교하는 단일 속성 갱신 효율성 실험이며, 두 번째는 속성 만료 시 복호화 권한이 즉시 철회되는지를 확인하는 시간 기반 접근제어 실험이다.

실험 환경은 컨테이너 기반 가상화 플랫폼을 사용하여 다수의 SDV 게이트웨이를 모사하였다. 제조사 서버는 OTA 업데이트 파일을 생성하고 CP-ABE 기반 접근정책을 적용하여 암호화하였으며, 각 차량 게이트웨이는 자신이 가진 속성 키를 이용하여 복호화를 시도하였다. 인증기관은 속성 키 발급 및 변경 이벤트를 관리하며, 실험 조건에 따라 전체 키 재발급 또는 속성 수준 키 갱신을 수행하였다.

단일 속성 갱신 효율성 실험에서는 속성의 총 개수를 1개에서 250개까지 변화시키면서 전체 속성의 만을 갱신 처리 시간을 측정하였다. 이 실험을 통해 속성 수 증가에 따른 처리 시간 변화와 제안 기법의 부분 키 갱신 메커니즘이 제공하는 효율성을 분석하였다. 시간 기반 접근제어 실험은 속성의 유효기간을 기준으로 시점을 변화시키며 복호화 성공 여부를 평가하였다. 유효기간 내에서는 정상적으로 복호화가 이루어져야 하며, 만료 시점 이후에는 즉시 복호화가 차단되어야 한다. 이를 통해 제안 기법의 실시간 권한 철회 성능을 검증하였다.

4) 실험결과 분석

실험 결과, 제안 기법은 기존 정적 CP-ABE 방식보다 보안성과 효율성 측면에서 우수한 성능을 보였다. 단일 속성 갱신 실험에서 기존 CP-ABE는 단일 속성 변경 시에도 전체 키를 재발급해야 하므로 속성 수 증가에 따라 처리 시간이 선형적으로 증가하였으며, 50개 속성 기준 평균 723.2초가 소요되었다. 반면 제안 기법은 변경된 속성만 선택적으로 갱신하여 속성 수와 무관하게 일정한 처리 시간을 유지하였고, 평균 90.3초로 약 8배의 효율 향상을 보였다. 이는 속성 수준 키 갱신 기법이 전체 재발급 대비 연산 부하와 네트워크 트래픽을 효과적으로 감소시킴을 의미한다. Fig. 1은 속성 수 증가에 따른 단일 속성 갱신 시간 비교 결과를 보여주며, 제안 기법의 일정한 처리 성능을 확인할 수 있다.

시간 기반 접근제어 실험에서는 유효기간 내 복호화가 정상적으로 수행되었고, 만료 시점 이후에는 즉시 거부되었다. 약 5만 건의 복호화 시도 중 유효기간 내 성공률은 99.99%, 만료 이후 실패율은 100%로 측정되었다. 만료 경계 구간에서 7건의 복호화 오류가 발생하였는데, 이는 복호화가 진행되는 리드 타임 동안 속성이 만료되어 복호화 완료 시 정책 유효성이 상실된 경우로 판단된다. 이러한 현상은 일시적 지연에 따른 미세한 오차로, 정책 평가 정확도에는 실질적 영향을 미치지 않았다. Fig. 2는 속성 만료 시점 이후 복호화가 즉시 실패함을 시각적으로 보여준다.

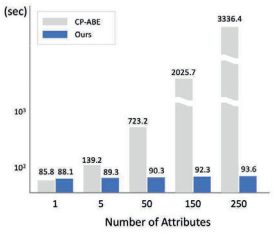

Fig. 1 Attribute Update Efficiency

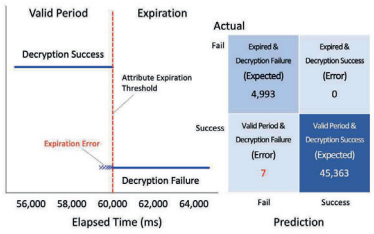

Fig. 2 Time-based Access Control

이 결과를 통해 제안 기법이 기존 CP-ABE의 비실시간성 한계를 극복하고, 속성 수준 키 갱신과 속성 만료 기반 권한 철회를 통해 SDV OTA 환경에서 요구되는 실시간성, 정확성, 효율성을 모두 충족함을 확인하였다.

Ⅲ. 결론 및 향후연구

본 연구에서는 SDV OTA 업데이트 과정에서의 보안 위협을 해결하기 위해 동적 속성 기반 접근제어 기법을 제안하였다. 제안 기법은 정적·동적 속성을 분리 관리하고, 속성 만료와 속성 수준 키 갱신을 결합하여 차량 상태 변화에 따른 실시간 권한 제어와 효율적 키 관리를 구현하였다. 실험 결과, 제안 기법은 기존 정적 CP-ABE 대비 평균 약 8배 빠른 속성 갱신 성능을 보였으며, 속성 만료 직후 복호화가 즉시 차단되어 실시간 권한 철회가 정상적으로 동작함을 확인하였다. 이러한 결과를 통해 제안 기법이 SDV OTA 환경에서 요구되는 보안성과 효율성을 동시에 충족함을 실험적으로 검증하였다.

본 연구는 SDV의 동적 상태 변화를 실시간으로 반영하는 접근제어 모델의 구현 가능성을 제시하였으며, 속성 만료와 부분 키 갱신의 결합이 기존 CP-ABE의 비실시간성과 비효율성 문제를 개선할 수 있음을 확인하였다. 향후 연구에서는 본 기법을 OTA 전 과정의 종단간 보안 체계로 확장하고, 실제 자동차 환경의 소프트웨어 업데이트 법규(UN R156) 및 국제 표준(ISO 24089)과의 정합성을 평가할 계획이다.

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2022R1A2C2005705, 분산 머신러닝 기반 지능형 플라잉 기지국을 위한 AI-MAC 프로토콜).

참 고 문 헌

[1] K. Routray and P. Bera, "Efficient and Secure Cloud Data Sharing Using CP-ABE Supporting Dynamic Attributes," *Proc. 30th Annu. Int. Conf. Mobile Comput. Netw. (ACM MobiCom '24)*, pp. 2245–2247, 2024.

[2] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," *Proc. IEEE Symp. Secur. Privacy (SP'07)*, pp. 321–334, May 2007.

[3] M. Xie, Y. Ruan, H. Hong, and J. Shao, "A CP-ABE Scheme Based on Multi-Authority in Hybrid Clouds for Mobile Devices," *Future Gener. Comput. Syst.*, vol. 121, pp. 114–122, 2021.