https://doi.org/10.33778/kcsa.2023.23.5.029

정보 공유를 위한 토큰 기반 KMS 연구

한 성 화*, 이 후 기**

요 약

KMS(Knowledge Management System)은 다양한 기관에서 정보 공유를 위해 사용하고 있다. 이 KMS는 각 기관에서 사용하는 기본 정보 뿐만 아니라, 중요 정보를 포함하고 있다. KMS에 저장된 중요 정보에 대한 접근을 통제하기 위하여, 많은 KMS는 사용자 식별 및 인증 기능을 적용하고 있다. 이러한 KMS 보안 환경은, KMS에 접근할 수 있는 사용자 계정 정보가 유출되면, 해당 계정 정보를 사용하는 악의적 공격자는 KMS에 접근하여 허가된 모든 중요 정보에 접근할 수 있는 한계점이 있다. 본 연구에서는 사용자 계정 정보가 유출되더라도 중요 정보를 보호할 수 있는 사용자 토큰(Token)을 적용한 파일 접근 통제 기능 적용 KMS를 제안한다. 제안하는 토큰 기반 KMS는 암호 알고리즘을 적용하여 KMS에 등록된 파일을 보호한다. 실효성 검증을 위해 목표하는 사용자 접근통제 기능에 대한 단위 기능을 확인한 결과, KMS에서 제공해야 할 접근통제 기능을 정상 제공하는 것을 확인하였다.

Study on Token based KMS for Information Sharing

Sung-Hwa Han*, Hoo-Ki Lee**

ABSTRACT

KMS (Knowledge Management System) is used by various organizations to share information. This KMS includes important information as well as basic information used by each organization. To protect infortant information stored in KMS, many KMS use user identification and authentication features. In such a KMS security environment, if the account information of a user who can access the KMS is leaked, a malicious attacker using the account information can access the KMS and access all authorized important information. In this study, we propose KMS with user access control function that can protect important information even if user account information is leaked. The KMS with the user access control function proposed in this study protects the stored files in the KMS by applying an encryption algorithm. Users can access important documents by using tokens after logging in. A malicious attacker without a Token cannot access important files. As a result of checking the unit function for the target user access control function for effectiveness verification, it was confirmed that the access control function to be provided by KMS is normally provided.

Key words : KMS, Information Sharing, Cryptography, Confidentiality, Access Control

접수일(2023년 09월 06일), 수정일(2023년 12월 07일), 게재확정일(2023년 12월 14일)

* 동명대학교/정보보호학과(주저자)
** 건양대학교/사이버보안학과(교신저자)

1. 서 론

기업은 물론, 공공기관이나 정부부처에서는 조직 구성원에게 특정 정보를 전달하거나 공유하기 위해 KMS를 사용한다[1]. KMS는 보통 Web 기반의 게시판 형태로 제공된다. 간단한 정보뿐만 아니라 업무 매뉴얼 등의 복잡한 정보를 포함할 수 있는 장점이 있다. 조직 구성원은 KMS에 접속하여, 필요한 정보를 검색하거나 조회하여 해당 정보를 확인할 수 있다[2].

KMS는 공개된 정보 외에 기밀 정보를 포함할 수 있다[3]. 특정 부서에게만 공유되는 정보뿐만 아니라, 특정 직급이나 등급에 해당하는 조직 구성원만 조회할 수 있는 정보가 등록될 수 있다. 이러한 정보는 허가되지 않은 사용자로부터 보호되어야 하므로, KMS는 식별 및 인증 과정을 적용하여 사용자의 접근을 통제하고 있다[4].

KMS는 조직 구성원만 접속을 허가하는 것이 일반적이지만, 필요한 경우 외부 이해관계자도 접속할 수 있다. 이때, 사용자의 식별 및 인증에 적용되는 계정 정보가 유출될 수 있다. 이때 악의적 사용자는 이 계정 정보를 사용하여 KMS에 접근 후 인가되지 않은 정보에 접근할 수 있다[5].

이러한 보안 문제점을 개선하기 위해 본 연구에서는 사용자 토큰(Token)과 암호 기술을 이용하여 인가된 사용자만 중요 정보에 접근할 수 있는 접근통제 기반 KMS 구조를 제안한다. 제안하는 KMS 구조는 사용자의 접근을 통제할 수 있을 뿐만아니라, 암호 기술을 적용하여 기밀성을 유지할 수 있다. 본 연구에서 제안하는 접근통제 기반 KMS 구조를 적용한다면, 계정 정보가 유출되더라도 KMS에 등록된 중요 정보를 보호할 수 있게 된다.

제안하는 접근통제 기반 KMS 구조는 실효성이 보장되어야 한다. 그러므로 이를 위해 KMS가 제공해야 하는 기능뿐만 아니라, 본 연구에서 목표하는 암호 기능 및 접근통제 기능을 단위 기능으로 선정하여 실효성을 확인한다.

2. 관련 연구

2.1 KMS

KMS는 지식관리시스템으로 기관에서 활용하는 정보를 저장하고 공유하는 시스템이다. KMS를 통하여 정보를 저장하고 전달할 수 있다. 조직 구성원은 KMS에 접근하여 공유된 정보를 조회, 검색하여 해당 정보를 획득할 수 있다[6].

KMS는 시스템 구성에 따라 다르지만, 대부분 <표-1>과 같은 기능을 제공한다[7-11].

<표 1> KMS 제공 기능

기능	설명
정보 공유	• 게시판 형태로 공유 대상 정보를 저장 • 사용자 조회 및 검색 기능 제공 • 정보 게시자 설정에 따른 사용자 그룹 대상 공지 • QnA 기능 제공
Biz 프로세스 관리	• 조직 목표 달성에 필요한 Task 및 프로세스, 산출물 정의 • 전자 결재 • KPI 관리 및 적용
Application 관리	• Text, Image, Audio, Binary File 등의 Application File 저장 • Application에 대한 SW Patch
형상 관리	• 저장된 File, Application에 대한 Revision 관리
접근통제	• 사용자 계정 관리, 권한 관리 • KMS 접근 사용자의 식별 및 인증 • DAC, MAC 기반 비인가자 접근 차단

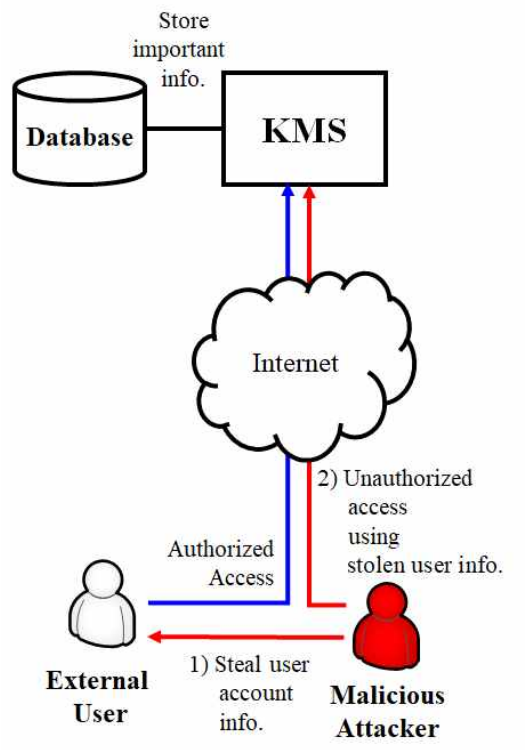
조직에서 KMS를 활용하는 수준은 다양하다. 기본적인 정보만을 공유할 수 있을 뿐만 아니라, 중요한 정보도 KMS를 통해 공유할 수 있다. KMS는, 등록된 계정 정보를 기준으로 MAC(Mandatory Access Control)이나 DAC (Discretionary Access Control)을 적용한다. 사용자의 신원이나 등급에 해당하는 권한이 없을 때는, 등록된 정보에 접근할 수 없다[12].

2.2 KMS 보안 위협

사용자는 등록된 계정 정보를 사용하여 KMS에 접근할 수 있다. 일반적으로 ID와 Password를 사용하며, 필요한 경우 OTP(One Time Password)나 생체인식 기술을 사용할 수 있다.

KMS에는 기관 내부의 사용자 뿐만 아니라, 협력기관소속 등의 외부 사용자도 접근할 수 있다. 외부에서 접속하는 사용자 또한 KMS의 식별 및 인증 체계를 적용하여 접근을 통제한다.

그러나 이러한 보안 환경은 정보 유출에 취약하다. 외부 사용자의 계정 정보가 악의적 공격자에게 유출될 경우, 악의적 공격자는 이를 사용하여 KMS에 접근할 수 있다. (그림 1)과 같이 악의적 공격자는 KMS에 등록된 중요 정보에 접근한 다음, 중요 정보를 외부에 유출하거나 변조할 수 있다.

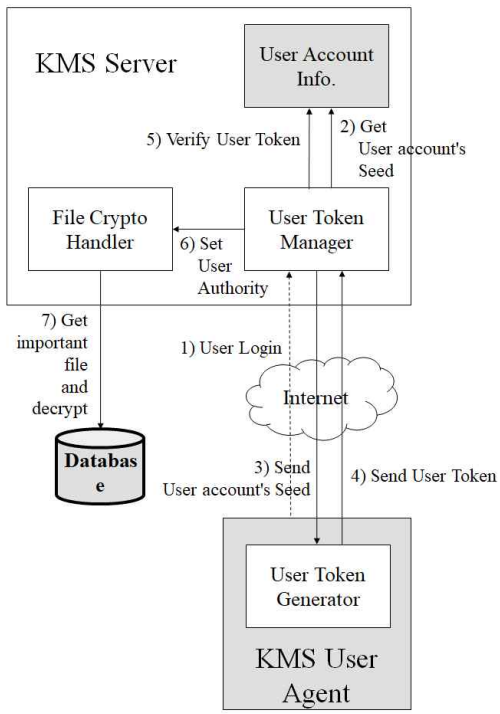


(그림 1) KMS 보안 취약점

3. 토큰 기반 KMS 구조

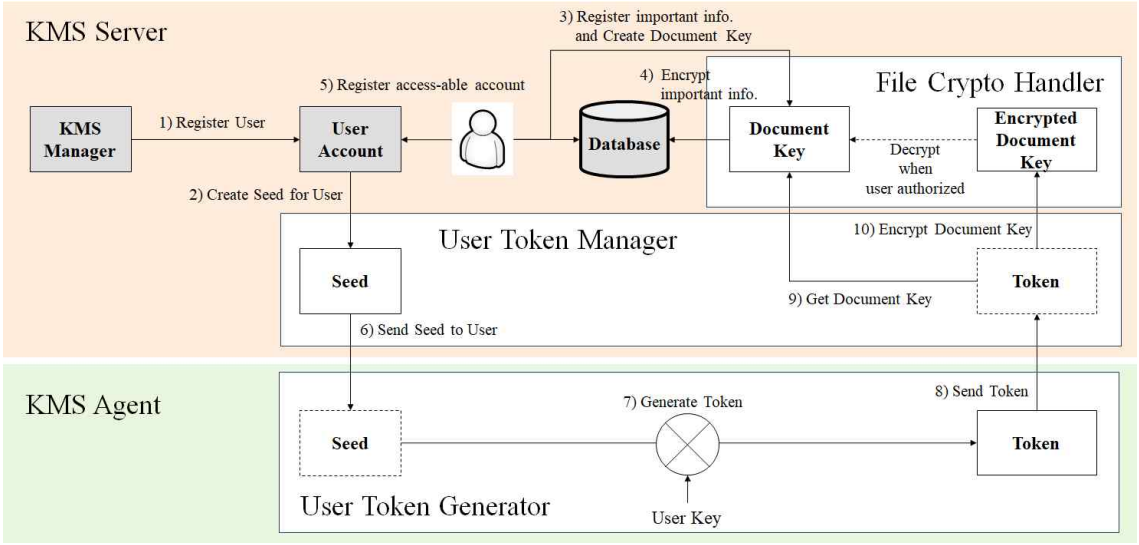
3.1 시스템 아키텍처

본 연구에서는 KMS 시스템에 대한 보안 위협에 대응하기 위한 사용자 접근통제 기반 KMS 구조를 제안한다. 제안하는 KMS 구조는 (그림 2)와 같다.



(그림 2) 접근통제 기반 KMS 구조

본 연구에서 제안하는 사용자 접근통제 기반 KMS는 3개의 컴포넌트로 구성된다. User Token Manager는 식별 및 인증된 사용자가 KMS에 등록된 정보에 접근할 때, 사용자에게 Seed를 전달하여 Token을 요청한다. User Token Generator는 Seed를 수신한 다음, Seed에 해당하는 Token을 생성하고 이를 다시 User Token Manager에 전달한다. File Crypto Handler는 사용자가 전달하는 Token으로 암호키를 획득한 후 등록된 정보를 복호화하는 역할을 한다.



(그림 3) Token 기반 KMS 암호기술 적용 방법

3.2 암호 기술 적용 방법

본 연구에서 제안하는 토큰 기반 KMS는 보호 대상 정보에 암호 기술을 적용한다. 중요 공유 정보가 암호화되는 과정은 (그림 3)과 같다.

KMS 관리자에 의해 사용자 계정이 등록되면, User Token Manager에 의해 사용자 계정에 대한 Seed가 생성된다. 생성된 Seed는 사용자(KMS Agent의 User Token Generator)에게 전달되며, 이를 이용하여 Token을 생성한다. Token은 다시 User Token Manager에 전달되고 Database에 저장된다.

KMS 사용자가 중요 정보를 등록할 때에는, Document Key에 의해 암호화 되어 저장된다. 중요 정보가 저장된 다음, KMS 사용자는 중요 정보에 접근할 수 있는 사용자를 설정한다. 이 과정에서 Document Key는 Token으로 암호화되어 Encrypted Document Key가 된다.

중요 정보에 접근할 수 있는 사용자는 여러명이거나 사용자 그룹일 수 있다. 이러한 경우 해당 사용자나 사용자 그룹에 대한 Token을 모두 적용하여 다수의 Encrypted Document Key가 생성될 수 있다.

4. 검증

본 연구에서 제안하는 토큰 기반 KMS는, 등록되는 공유 정보를 암호화하여 그 기밀성을 유지할 뿐만 아니라, 인가된 사용자의 접근을 허용할 수 있어야 한다. 그러므로 <표 2>와 같은 단위 기능 항목을 산정하여 본 연구에서 목표하는 기능이 정상 동작하는지를 검증한다.

<표 2> 토큰 기반 KMS 기능 검증 항목

Function ID	설명
Func_1	공유 정보에 대한 Random 암호키 생성 및 공유 정보 암호화
Func_2	사용자 계정에 대한 Seed 생성
Func_3	사용자에 의한 Seed 기반 Token 생성
Func_4	Token 전달 후 Document Key의 암호화
Func_5	사용자 로그인 후 공유 정보 접근 시 Seed 제출 및 Token 요청
Func_6	수신한 Token으로 Encrypted Document Key 복호화
Func_7	복호화된 Document Key로 암호화된 공유정보 복호화

Func_1를 확인한 결과, 공유 정보에 대한 Random 암호키 생성 및 공유 정보 암호화 기능이 정상동작하는 것을 확인하였다. 또 Func_2에서도 사용자 계정에 대한 Seed를 정상 생성함을 확인하였다. Func_3을 확인하였을 때, 사용자에 의한 Seed 기반 Token을 생성하였으며, Func_4에서는 Token 전달 후 Document Key를 암호화하는 것을 확인하였다. Func_5를 확인한 결과 사용자 로그인 후 공유 정보 접근 시 Seed를 제출 후 Token을 요청하는 것이 확인되었다. Func_6에서는 수신한 Token으로 Encrypted Document Key를 복호화 후, Func_7에서 복호화된 Document Key로 암호화된 공유 정보를 복호화하는 것을 확인하였다.

전체 기능을 검증한 결과, 각 단위 기능은 정상 동작함이 확인되었으며, 암호 알고리즘에 의해 공유 정보의 기밀성은 유지될 뿐만 아니라, 인가된 사용자에게는 그 접근을 허용하는 것이 확인되었다. 그러므로 본 연구에서 제안하는 Token 기반 KMS는 실효적이라고 할 수 있다.

5. 결 론

정보 서비스의 활용 범위가 확대되며, 비즈니스 프로세스의 복잡화, 광범위화가 진행되면서 공유해야 할 정보는 더 많아질 뿐만 아니라 중유한 정보도 증가하고 있다. 이러한 정보환경에서 KMS는 매우 큰 비중을 차지한다.

다만 비즈니스 환경의 확대에 따라 보안 위협은 증가하며, 이에 따라 악의적 사용자에 의한 정보 유출 및 비인가 변조 가능성이 있다.

본 연구에서는 이러한 보안 문제점을 해결하기 위하여 토큰 기반 KMS 시스템 구조를 제안하고, 그 실효성을 검증하였다. 본 연구에서 제안하는 구조를 KMS에 적용한다면, KMS를 통해 공유하는 정보의 기밀성은 보장될 뿐만 아니라, 인가된 사용자의 접근만을 허용하게 된다.

본 연구는 사용자 계정에 대한 Token으로 공유 정보를 암호화하는 암호키를 암호화하는 단순한 방식을 적용하였다. 그러므로 사용자 계정에 대한 Token을 안전하게 생성하고 배포하기 위한 추가적인 연구가 필요하다.

참고문헌

[1] M. Alavi and D. E. Leidner, "Knowledge management and knowledge management systems: Conceptual foundations and research issues," MIS quarterly, pp.107-136, 2001.

[2] H. A. N. Sulaiman, "Knowledge Management System Service Center Berbasis Web," Faktor Exacta, vol.8, no.3, pp.220-230, 2015.

[3] P. Tyndale, "A taxonomy of knowledge management software tools: origins and applications," Evaluation and program planning, vol.25, no.2, pp.183-190, 2002.

[4] H. Wang, X. Guo, Y. Fan, and J. Bi, "Extended access control and recommendation methods for enterprise knowledge management system," IERI Procedia, vol.10, pp.224-230, 2014.

[5] E. Randeree, "Knowledge management: securing the future," Journal of knowledge management, vol.10, no.4, pp.145-156, 2006.

[6] K. Iskandar, M. I. Jambak, R. Kosala and H. Prabowo, "Current issue on knowledge management system for future research: a systematic literature review," Procedia computer science, vol.116, pp.68-80, 2017.

[7] R. J. Ong, R. A. A. Raof, S. Sudin and K. Y. Choong, "A review of chatbot development for dynamic web-based knowledge management system (KMS) in small scale agriculture," In Journal of Physics: Conference Series, vol.1755, no.1, pp. 012051, Feb. 2021.

[8] S. Chatterjee, S. K. Ghosh and R. Chaudhuri, "Knowledge management in improving business process: an interpretative framework for successful implementation of AI - CRM - KM system in organizations," Business Process Management Journal, vol.26, no.6, pp.1261-1281, 2020.

[9] H. Jiang, C. Liu and Z. Cui, "Research on knowledge management system in enterprise," In 2009 International Conference on Computational

Intelligence and Software Engineering, pp.1-4, IEEE, Dec. 2009.

[10] M. Wang, M. Zheng, L. Tian, Z. Qiu and X. Li, “A full life cycle nuclear knowledge management framework based on digital system,” Annals of nuclear energy, vol.108, pp.386-393, 2017.

[11] J. Peng, D. Jiang and X. Zhang, “Design and implement a knowledge management system to support web-based learning in higher education,” Procedia Computer Science, vol.22, pp.95-103, 2013.

[12] P. N. Mustafa Kamal, A. Osman and N. Buniyamin, “An overview of industrial Knowledge Management System and a review of Access Control Methods,” Journal of Electrical and Electronic Systems Research (JEESR), vol.16, pp.10-18, 2020.

〔저 자 소 개〕

한 성 화 (Sung-Hwa Han)
동명대학교 정보보호학과 교수
숭실대학교 공학박사
관심분야 : IT융합보안, 시스템보안, 인공지능, 악성코드 탐지, 제로트러스트 보안
email :shhan@tu.ac.kr

이 후 기 (Hoo-Ki Lee)
건양대학교 사이버보안학과 교수
숭실대학교 공학박사
KY 창업보육센터장, 정보보호영재교육원 부원장, 사이버미래혁신융합연구회 회장
관심분야 : 사이버보안 침해지표 연구, 제로트러스트 보안, 보안관제시스템
email : hk0038@konyang.ac.kr