Personal data sharing model with legal validity in blockchain-based secure environment

Su Jin Shin*, Sang Uk Shin**

*Department of Information Security, Pukyong National University, Republic of Korea
**Division of Computer Engineering and Artificial Intelligence, Pukyong National University, Republic of Korea

inuin9014@gamil.com, shinsu@pknu.ac.kr

This paper proposes a data sharing model that ensures the legal validity of data provided by individuals as legal evidence within a blockchain environment. The proposed model applies Distributed Pseudo-Random Functions (DPRFs) to prevent all participants, except the data requester, from obtaining the original data. Based on these characteristics, the model guarantees integrity, confidentiality, and non-repudiation, thereby ensuring that data provided by individuals can possess legal validity as evidence.

(Pt9)Keyword—**Blockchain, Data sharing, MPC, Legal evidence, Data security**

Su Jin Shin received her B.E. degree in Dept. of Software and Artificial Intelligence from Pukyong University, Republic of Korea in 2023. She is currently a master course student in Department of Information Security, Graduate School from Pukyong National University. Her research interests are related with blockchain security, applied cryptography, and vehicle security.

Sang Uk Shin received his M.S. and Ph.D. degrees from Pukyong National University, Busan, Korea in 1997 and 2000, respectively. He worked as a senior researcher in Electronics and Telecommunications Research Institute, Daejeon Korea from 2000 to 2003. He is currently a professor in Division of Computer Engineering and Artificial Intelligence, College of Information Technology and Convergence, Pukyong National University. His research interests include cryptographic protocol, blockchain security, mobile and wireless network security, and digital forensics.