Skysong Innovations
Advancing the Arizona State University Knowledge Enterprise

1475 N. Scottsdale Road, Suite 200
Scottsdale, AZ 85287-3538
Phone: 480 884 1996 Fax: 480 884 1984

Case ID:M20-009P
Published: 8/6/2020

Inventors

Jaejong Baek
Sukwha Kyung
Gail-Joon Ahn

Contact

Shen Yan
shen.yan@skysonginnovations.com

Blockchain-Based Automatic Key Generation from Dynamic Metadata

Background

Blockchain is a decentralized, shared system that records every transaction made by participating entities across the network so that any record cannot be altered retroactively. In private and permissioned Blockchain networks, Public Key Infrastructure (PKI) is adopted as a cryptographic key management technique that enables all components to securely communicate in an insecure public network and verify the identity of other entities via digital signatures. The certificates used in PKI are managed by a central management entity called Certificate Authority (CA) that verifies and signs the certificates. If a secret key is compromised or exposed accidentally, the secret must be shared again among all nodes to regenerate the new keys and certificates. The process of renewing and exchanging key secrets causes delay, which can jeopardize time-sensitive and mission-critical systems. In such systems, the devices and services (e.g., smart cars, financial, and medical) may not have sufficient time to generate new keys by communicating to the central server while maintaining the ongoing session. Thus, any delays incurred by key generation and sharing can interrupt the service provisioning and risk system failure.

Invention Description

Researchers at Arizona State University have developed a blockchain-based cryptographic key generation method for time-sensitive and mission-critical services such as military and healthcare systems. Instead of exchanging a secret before key generation, dynamic metadata of the shared ledger is used as a secret for the key generation. The metadata derived from shared ledgers typically share the features of the conventional seed used to generate the key, including randomness and uniqueness that arise from the decentralization, immutability, and transparency of blockchain technology. This innovation further enables the hyper-connected 5G vision, which supports high bandwidth and ultra-low latency for new applications including mobile, health, autonomous vehicles, and smart homes.

Potential Applications

- Cybersecurity
- Internet-of-Things (IoT) devices

- Mission-critical systems

Benefits and Advantages

- Key generation does not require a third party or central server
- Minimizes delay for real-time operation
- Can be implemented as a modular or minor modification

Faculty Profile of Professor Gail-Joon Ahn