Delft University of Technology - Department of Software Technology

Security and privacy in medical data sharing through blockchain

Author: Karim Guettache | Supervisor: Chhagan Lal | Supervisor: Mauro Conti

Email: K.Guettache@student.tudelft.nl

Contribution

Blockchain (BC) can be used to realize a secure and trusted medical data sharing (MDS) system across different institutes. The main contributions of this research are as follows:

- A list of security and privacy (S&P) parameters desired for a MDS
- An analysis of the impact of BC and SCs to MDS systems, based on the S&P requirements

Blockchain based medical data sharing

1. **C**ertificate **A**uthority encrypts data, creates certificates for users for authentication and initializes metadata
2. **P**atient manage consent regarding data
3. **H**ealthcare and **R**esearch institutes query BC for data access, based on consent
4. Data can be downloaded from **D**atabase

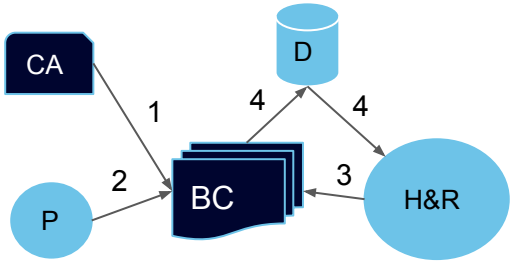

Figure 1: Blockchain based MDS

Security and privacy analysis on BC features

Authentication & unforgeability (A) Any interaction or exchange of data requires strong authentication of the institutes performing the action	**Confidentiality (B)** Sensitive data within the BCbmds should only be accessible by authorized and authenticated users
Integrity (C) Patient data, consent rules and data exchange txs should not be modifiable by unauthorized users	**Non-repudiation (D)** Any action performed; updating consent rules and data exchange txs, done by anyone, should be logged
Availability (E) Data retrieval and services should always be available to the institutes	**Access control (F)** Institutes can only perform the actions which they are authorized for	**Consent management (G)** Patients should be able to manage the consent rules regarding their data
Identity anonymity (H) The identities of the institutes should be anonymous when they perform actions	**Unlinkability (J)** Aggregating actions performed should not provide additional information on the action taker
Data anonymity (I) Patient data should not be able to identify the patient when this is specified in the consent rules	**Transparency & auditability (K)** Consent rules and data exchange txs should be fully transparent to the data owner and the institutes

Digital signatures	P2P network	Immutable ledger	Consensus	Smart contracts	Off-chain storage
(A) (B) (C) (D) (F) (K)	(E)	(B) (C) (D) (E) (F) (I) (K)	(B) (C) (D) (E) (F)	(F) (G) (I) (K)	(B) (C) (E)

Limitations & alternative solution

(H), (J) and parts of (B) are not supported well by BC and SC features. An alternative solution to (H) and (J) is identity mixer protocols. Identity mixers use *presentation tokens* based on *zero-knowledge proofs* as a proof of a digital signature on some attribute. The attribute and the signature themselves are not disclosed, providing anonymity. On each transaction a new token is generated, making them unlinkable.

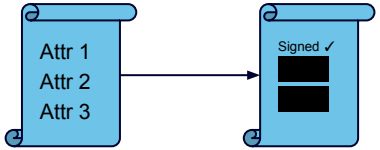

Figure 2: Certificate vs identity mixer

Conclusion

Inherent features of BC provide great support for security services in a MDS system. Privacy services are not supported well and require additional techniques to be achieved. Identity mixers are protocols that can be used to enhance the privacy of a BC based MDS.