2021 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo) | 978-1-6654-2652-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/UkrMiCo52950.2021.9716595

Securing Medical Data in 5G and 6G via Multichain Blockchain Technology using Post-Quantum Signatures

Lela Mirtskhulava
Department of Computer Science
Ivane Javakhishvili Tbilisi State University
lela.mirtskhulava@tsu.ge
0000-0003-4602-4967

Maksim Iavich
School of Technology
Caucasus University
Tbilisi, Georgia
miavich@cu.edu.ge
0000-0002-3109-7971

Marina Razmadze
School of Technology
Institute Techinformi
Tbilisi, Georgia
Razmadze.m@gsu.ge
0000-0003-1928-3330

Nana Gulua
Department of Computer Science
Sokhumi State University
Tbilisi, Georgia
ngulua@sou.edu.ge
0000-0001-6183-5632

***Abstract*—Slicing a network is a key innovative feature to deliver 5G (the fifth generation) services. 5G aims to enhance mobile broadband, deliver massive machine-type and low latency communications with ultra-reliability. This generation manages the huge scale of the devices of the Mobile Internet of Things (MIoT). 5G has been invented for controlling security addressed to the threats found in 2G/3G/4G networks consequently. 5G preventive measures include enhanced authentication capabilities, subscriber identity protection, and additional security techniques. New 5G network technologies introduced new threats for the industrial organizations. GSMA (The GSM Association) announced that Mobile Internet of Things (IoT) requires more security in 5G as the number of IoT devices and connections are exponentially increasing. "The IoT needs to be securely coded, deployed and managed throughout its lifecycle". Common IoT architecture is subjected to the following common attacks: 1) attacks on IoT devices through the running application; 2) remote attacks over the internet; 3) physical attacks; 4) attacks through the cloud 5) attacks through Wi-Fi or mobile air interface. Moreover, IoT devices are being used to form DDoS attacks where each IoT device forms the specific data resulting a volume-based attacks. Blockchains are considered as a main solution to solve various issues in 5G such as Mobile IoT security problems and Electronic Healthcare Records sharing problems. We analyse Hashing based Post-Quantum Signatures for enhancing blockchain security.**

Keywords—5G security, blockchain, Mobile Internet of Things, AI, post-quantum digital signatures.

I. Introduction

Google and Honeywell, two of the giant companies in computing, announced their improvements in quantum technologies. Google announced a slew of enhancements to its Sycamore processor. They have been making error corrections aiming to achieve one million physical qubit computers to be created by the end of the current decade. Honeywell presented its Model H1 with a quantum volume of 1024 this year and announced the path of continuous enhancement still is going [1].

The 5G standard relies on classical cryptography and does not consider the issues that can be caused by quantum computing. It is time to get prepared for the shift to the world of the post-quantum cryptography. The GSMA Security Team conducted a comprehensive threat analysis and posted that introducing and launching 5G systems by Mobile Network Operators (MPO) will bring new security threats and challenges around the globe. The GSMA has used this analysis for a "5G Cybersecurity Knowledge Base" to provide useful guidelines on 5G security risks and measures to mitigate them. There were threats faced in 4G/3G/2G networks and in order to address them 5G technology has developed security controls. This methodology includes new mutual authentication possibilities and enhanced customer identity protection. 5G offered additional security mechanisms to increase network security levels but adopting new technologies are introducing new threats. The Knowledge Base encourages giving step-by-step instructions to enhance 5G network security and build security assurance keeping in mind the 5G end-to-end networks' risk spectrum.

Mobile IoT is prevalent in 2G/3G/4G networks and the number of IoT devices are increasing exponentially in 5G. The diversity of new IoT devices will pose significant security and privacy threats as we are moving from 5G to 6G systems. The volume of novel IoT devices in the 6G network will increase 10 times (from 10 billion to 100 billion). Security controls need to be changed significantly [2-5]. Most of IoT services are sharing a common architecture where each service is subjected to three common attack scenarios: 1) Attacks on the devices through the applications running by the device; 2) Attacks on service platforms (the cloud); 3) Attacks on the communications links (WLAN, Cellular and BLE air interface etc.). IoT devices are launching DDoS attacks resulting in significant volume-based attacks [6-7].

Wide AI employment in 5G networks will benefit 5G security. ML (Machine Learning) and DL (Deep Learning) will automate threat detection. Using AI is significant when it comes to the volumes of data generated in 5G networks. AI is more feasible to mitigate unknown attacks and threats in real time. 5G networks are still evolving and it is reasonable to think that they will rely on smart AI-enabled applications. On other hand, AI development can blur the difference between real and fake contents making it possible to create new intelligent attacks.

GSMA developed the three-layered 5G security model (Fig.1.). ***First Layer*** – Product Security Layer is the responsibility of network equipment suppliers. Network devices security assurance is a main tool capable of evaluating whether network elements have been implemented according to main security requirements and adhere to globally recognized standards. The Network Equipment Security Assurance Scheme (NESAS), defined by 3GPP (The 3rd

978-1-6654-2652-7/21/$31.00 ©2021 IEEE

Generation Partnership Project) and GSMA, specifies security requirement and assessment.

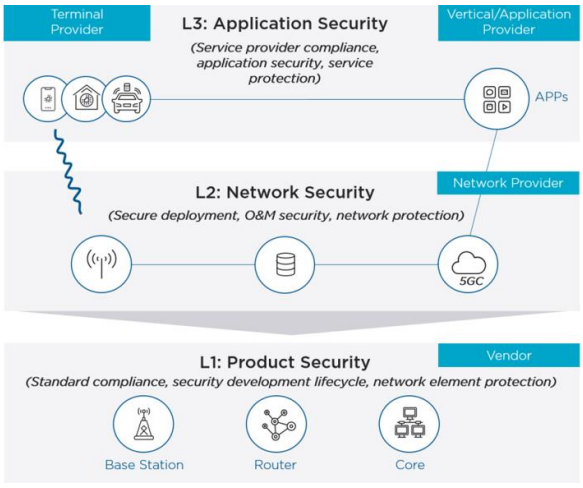

Fig.1. 5G Cybersecurity – a layered security model by GSMA [1].

Second Layer – Network Security Layer is controlled by the MNOs. They perform a continuous risk assessment including network elements, network functions and networks architecture for effectively managing security threats. The threats include network service disruption, malware, command-and-control, application layer attacks.

Third Layer – Application Security Layer include mobile device users (UEs) and vertical industries using a range of applications. Application security can be provided by joint collaboration between UE vendors, MNOs, service providers and application developers to ensure 5G network security through filtering, authentication and authorization controlled by the Service Level Agreement between all the parties to avoid data breaches.

Another potential solution is the use of blockchain technology (Distributed Ledger Technology -DLT). Blockchain enables use the trustless computing between parties and offers privacy protection technique in the network. The security and privacy features provided by blockchain includes: transparency, anonymity, immutability pseudonymous and verifiability and etc.

II. The Blockchain in IoT

A. Blockchain Anatomy

Blockchain technology is getting very popular in the information technology sector. Blockchain security relies on cryptographic digital signatures for the authentication of the blocks or transactions. Blockchain digital signatures are prone to cyberattacks by quantum computers. Key management encounters serious security risks in blockchain technology. Holding someone's private key means owing the ultimate key to obtain someone's information and identity. Blockchain is a decentralized network with a trustless mechanism allowing consensus between nodes and keeping privacy and truthfulness among them. All transactions or data transferred between nodes have to be secured to avoid attacks. It's known that 51% of Sybil attacks are carried out on the blockchain networks. We can consider blockchain as a peer-to-peer (P2P) system. It requires an explicit certificate between different remote nodes since the P2P system is susceptible especially to Sybil attacks. In IoT, we have to consider the appropriate protocols between nodes and applications very carefully.

Cryptographic hash functions are the significant elements when it comes to blockchain security. Hush calculation is the main aspect in order to prevent the attacks. The hash is calculated having three inputs (Fig.1): 1) previous block hash, 2) the Merkle root hash, and 3) the nonce. and using the cryptographic hashing algorithm (SHA-256). The output block hash represents the contents of all the blocks with a fixed size (Fig.2).

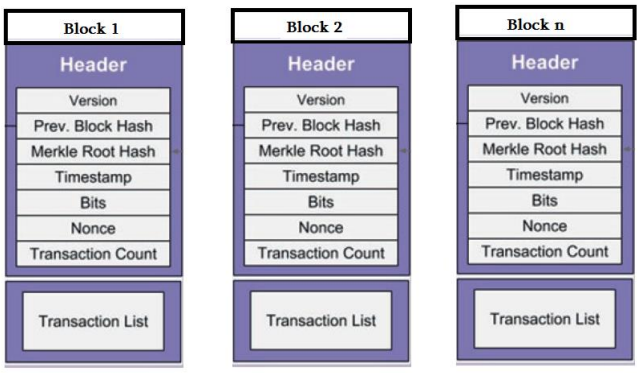

Fig. 2. Blockchain anatomy.

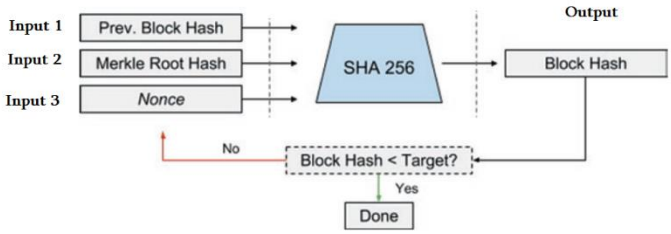

Fig. 2. Block Hash calculation.

B. Multichain Blockchains

Multichain platform provides private blockchains within and between organizations. Multichain blockchains (MB) can solve the problems of mining, openness and privacy. MB has three main features: 1) enables secure mining without proof-of-work; 2) ensures that the activities are only visible to the specific participants within blockchain; 3) introduces controls over permitted transactions. Private blockchain can solve the problems related to scale since the participants can control the block size. Private blockchain is a closed system which contains transactions that the participants are interested in.

In Multichain blockchain, each node generates its own private key randomly and doesn't reveal it to other nodes. MB uses this feature to limit blockchain access to the specific list permitted users, by using the "handshaking" process between two blockchain nodes where: 1) Each node has a public address as its own identity on the permitted list; 2) Each node can verify the address of other nodes within its own permitted list; 3) Each node can send a control message to the other nodes; 4) Each node will send back a signature of the control message, verifying its ownership of its own private key that corresponds to the presented public address.

III. Post-Quantum Digital Signatures

A. Post-Quantum Digital Signatures

NIST released (SP) 800-208 Recommendation for Stateful Hash-Based Signature Schemes which supplements FIPS 186 and approvs the usege of two stateful hash-based signature schemes such as the XMSS (eXtended Merkle Signature Scheme) and LMS (the Leighton-Micali Signature system) ((RFC 8391, and RFC 8554). Previous works have shown that stateful hash-based signatures are very effective to be used with a blockchain. In the given paper, we conducted our research on stateful hash-based signatures using a digital signature scheme specifically designed for multichain blockchains [10-13].

In Bockchained Post-Quantum Signatures (BPQS) is created for blockchain and other DLTs, based on by the based on XMSS-T. BPQS design focused on fast first time signatures. The size of the signature can grow linearly but can be decreased incorporating one authentication path on the blockchain. Two main building blocks are used by BPQS: 1) a few time (BPQS-FEW) and 2) an extensible many-time scheme (BPQS-EXT) (Fig.4). BPQS-FEW is a Merkle tree comprising of two nodes on each layer. The right leaf represents a compressed one-time schemes (OTS) key, and the left leaf represents the root of the two underlying nodes.

Efficient Secure Digital Signature Schemes were developed for Post Quantum Epoch and Digital Signature Scheme for Personal Data Security in Communication Network Systems were developed previously [8-9].

Root nodes are built using the internal node based on the techniques of XMSS-T. The authentication scheme of BPQS-EXT represents 2-leaf layered Merkle trees. The left-side leaf on each layer can be used as a fall-back key signing the root of the given tree on the next layer, and the right-side leaf can be used as an OTS key. In the BPQS scheme, BPQS-FEW are combined with one of HBS scheme and BPQS-EXT.

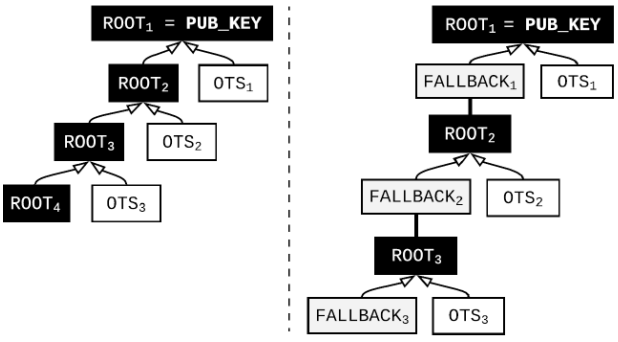

Fig. 4. Left-side: a few-time signature scheme (BPQS-FEW); Right-side, an extensible many-time signature scheme (BPQS-EXT).

IV. Blockchain Applications in Medical IoT

A. Security Risk to Patient Data

At present an electronic health records (EHR) are stored on centralized databases. Medical data remains largely non-portable. As cybercrime around the world is on the rise, healthcare systems are no exception as shown by recent high profile ransomware hacking. “Your medical information is worth 10 times more than your credit card number on the black market” [14].

Blockchain can transform the healthcare industry. Healthcare providers will be able to collect information directly from the patient. Patients' data are stored in existing hospitals' databases. A hash value (unique output) can be formed from each data source and then redirected to the blockchain. The patients can decide who will have access to their medical records. The stakeholders from the Healthcare industry will be able to query for access to the blockchain to obtain the medical information.

One of the good examples of blockchain used in medicine is a medicalchain [Fig.3].

Fig.3. Medicalchain.

The biggest problem in Healthcare today is that organization holds multiple and fragmented records about patients and in case of medical emergencies doctors are inclined to run a series of fresh tests and there is no way for a hospital to retrieve information from another hospital. With medicalchain a smart contract is launched to give time-limited access to patient’s electronic health records. The patients gives time-limited access to the insurer for verification of treatment and payment settlement (Fig. 4).

B. Our Proposed MIoT Architecture with Blockchain

Medical IoT architecture is using blockchain enabled home gateway. Home gateway is responsible for secure data transmission between IoT devices. Medical IoT was considered as a distributed ledger using blockchain through cloud layer. Smart IoT has three layers: device layer, gateway and cloud layers. At the device layer, sensors and wearable medical devices gather medical data from patients. Gateway layer is responsible for managing the obtained data. At cloud layer registers all blocks and transactio ns are registered and processed within the blockchain .

We have used the Mininet environment to test our proposed architecture. Mininet allowed us to use IoT devices. Gateways were configured by using virtual machines through Linux server. Ethereum blockchain configuration has been used. Amazon Elastic Compute Cloud was configured.

Centralized IoT architecture was built and compared to proposed distributed architecture in terms of performance and security. Security measurements showed that distributed architecture outperforms centralized one at security level.

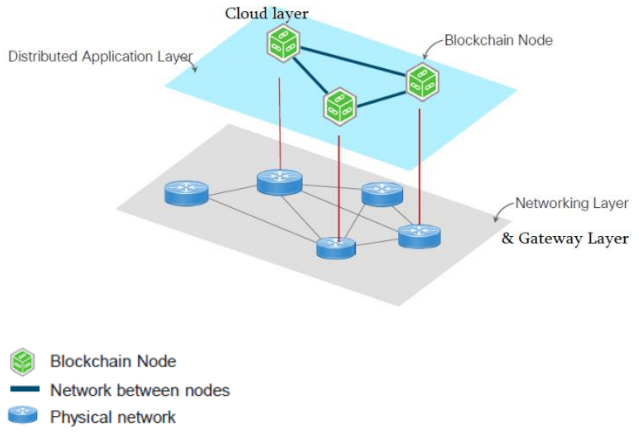

Fig. 4. IoT enbled Blockchain Architecture

V. Blockchain and Smart Contracts Provide Two Big Advantages

1) The system is Patient-centered: the patient owns his medical records though cannot modify or delete it but can decide who can have access; 1) Interoperability: The system acts as a catalogue, all records are stored and instead of having to do the entire test again the information can be accessed upon the patient's consent.

VI. How AI Can Change A Blockchain?

1. Optimising energy consumption
2. Scalability: AI can introduce new decentralized learning systems such as federated learning.
3. Security: AI is a fantastic ally for the blockchain to guarantee a secure applications deployment
4. Privacy: the privacy issue of owning personal data raises regulatory
5. Efficiency: better efficiency and a lower energy consumption may reduce the network latency allowing then faster transactions

VII. Conclusion

In the given paper, we proposed blockchain technology with hash-based Post-Quantum digital signatures as the best solution for securing MIoT. Main advantage of the proposed digital signature schemes is their key-generation speeds as they are faster than the others.

The combination of the Blockchain, IoT, and AI technologies can be done in multiple dimensions. Blockchain is expanding and promising new opportunities to move IoT forward. This potential of blockchain is directly connected to cryptography. Blockchain presents main features like decentralization, trust and security needed for IoT solutions. Blockchain will meet General Data Protection Regulation's (GDPR) to protect EHRs and will be handful in healthcare. So, Blockchain is the best solution to solve the issues in 5G and 6G technologies caused by IoT devices.

Blockchain offers a decentralized, transparent and secure ledger through the users. This is a new approach via a combination of smart contracts and IoT offered to enhance 5G security. The blockchain technology can manage data sessions between the user devices, such as a laptop, a smartphone and the virtual networks via its own (blockchain) interface. Artificial Intelligence (AI) employment in 5G networks will benefit its security. Deep Learning (DL) can automate threat detection and mitigate new attacks in real time. To apply these both technologies such as blockchain technology and AI for enhancing 5G security is our purpose in this work.

References

[1] https://www.idquantique.com/quantum-computing-review-q3-2021/?fbclid=IwAR27lZyfJHH_smLHhv2aXKIgC25IV6PGBOw845MP6z-P-cJxGrRVqgSLPzU

[2] https://www.gsma.com/security/securing-the-5g-era/

[3] https://www.gsma.com/security/5g-cybersecurity-knowledge-base/

[4] https://www.gsma.com/security/network-equipment-security-assurance-scheme/

[5] 6g White Paper: Research Challenges For Trust, Security And Privacy by Editor in chief: Mika Ylianttila and Section editors: Raimo Kantola, Andrei Gurtov, Lozenzo Mucchi, Ian Oppermann. 2020

[6] L. Mirtskhulava, N. Meshveliani, N. Gulua and L Globa, "Cryptanalysis of Internet of Things (IoT) Wireless Technology," IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics – UkrMicO. Odessa, Ukraine, 2019

[7] L. Mirtskhulava, L. Globa, L. Gulua, Meshveliani, "Complex Approach in Cryptanalysis of Internet of Things (IoT) Using Blockchain Technology and Lattice-Based Cryptosystem". In: Ilchenko M., Uryvsky L., Globa L. (eds) Advances in Information and Communication Technology and Systems. MCT 2019. Lecture Notes in Networks and Systems, vol 152. Springer, Cham. https://doi.org/10.1007/978-3-030-58359-0_4. 2021

[8] M Iavich, G Iashvili, SGnatyuk, A. Tolbatov, L. Mirtskhulava. "Efficient and Secure Digital Signature Scheme for Post Quantum Epoch". Information and Software Technologies. ICIST 2021. Communications in Computer and Information Science, vol 1486. Springer, Cham. https://doi.org/10.1007/978-3-030-88304-1_15. (2021)

[9] M. Iavich, G. Iashvili, R. Bocu R, S. Gnatyuk, "Post-quantum Digital Signature Scheme for Personal Data Security in Communication Network Systems," Advances in Artificial Systems for Medicine and Education IV. AIMEE 2020. Advances in Intelligent Systems and Computing, vol 1315. Springer, Cham. https://doi.org/10.1007/978-3-030-67133-4_28. 2021

[10] W. Fang, W. Chen, W. Zhang, et al., „Digital signature scheme for information non-repudiation in blockchain: a state of the art review," Wireless Com Network 2020, 56 (2020) https://doi.org/10.1186/s13638-020-01665-w

[11] https://bisontrails.co/digital-signatures/

[12] T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks," in IEEE Access, vol. 8, pp. 21091-21116, 2020, doi: 10.1109/ACCESS.2020.2968985.

[13] K. Chalkias, J. Brown, M. Hearn, T. Lillehagen, I. Nitto and T. Schroeter, "Blockchained Post-Quantum Signatures," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1196-1203, doi: 10.1109/Cybermatics_2018.2018.00213.

[14] https://medicalchain.com/en/whitepaper/