PoTS: Proof of Tunnel Signature for Certificate Based on Blockchain Technology

Dewi Immaniar[1], Nur Azizah[2], Dedeh Supriyanti[3], Nanda Septiani[4], Marviola Hardini[5]
University of Raharja[1,2,3,4,5]
Jenderal Sudirman No.40, Cikokol, Kota Tangerang[1,2,3,4,5]
Indonesia[1,2,3,4,5]
e-mail: dewi.immaniar@raharja.info[1], Nur.Azizah@raharja.info[2], dedeh@raharja.info[3], nanda.septiani@raharja.info[4], marviola@raharja.info[5]

Author Notification
April 2021
Final Revised
April 2021
Published
April 2021

To cite this document:
Immaniar, D., Azizah, N., Supriyanti, D., Septiani, N., & Hardini, M. (2021). PoTS: Proof of Tunnel Signature for Certificate Based on Blockchain Technology. *International Journal of Cyber and IT Service Management (IJCITSM)*, *1*(1), 101-114. Retrieved from https://iiast-journal.org/ijcitsm/index.php/IJCITSM/article/view/28

DOI:
https://doi.org/10.34306/ijcitsm.v1i1.28

Abstract

Proof of Tunnel Signature (PoTS) is designed to avoid the main problems found in certificates based on Blockchain technology. In this case, it is so closely related to Cybersecurity. A lightweight protocol such as a Certificate Authenticated Key Agreement (CAKA) is needed to reduce the vulnerability of a system's operation, namely overcoming management overhead by using a decentralized system according to the characteristics of Blockchain Technology. PoTS is the second stage after determining the Key Agreement (KA) or certificate hash in authenticating a node, and this is also a significant step in minimizing computation costs. The nodes generated after the signing process remain anonymous and can be verified optimally. Smart contracts are also used as a support so that this research can ensure transparency and openness of transaction nodes to maintain and improve the efficiency of transaction security for a certificate based on Blockchain Technology.

Keywords: PoTS, CAKA, Blockchain, Tunnel Signature, Smart Contracts

1. Introduction

By utilizing one part of Blockchain Technology [1], namely smart contracts, all information and communication in realizing the Authenticated Key Agreement (AKA) Protocol requires 3 (three) roles of cryptographic settings [2], namely: Identity Based (ID Card), certificate model, and also Private Key Infrastructure (PKI). Literally PKI will perform encryption directly by using 2 (two) cryptographic keys such as a public key and a private key [3]. Where the key digitally can emphasize trust in digital assets such as certificates. However, such heavy management can cause the standard of using public keys to decline, making it too risky. Therefore, the associated private key needs to be generated by a system called Key Generation Center (KGC) with a smart contract so that the user's security can be specifically guaranteed [4].

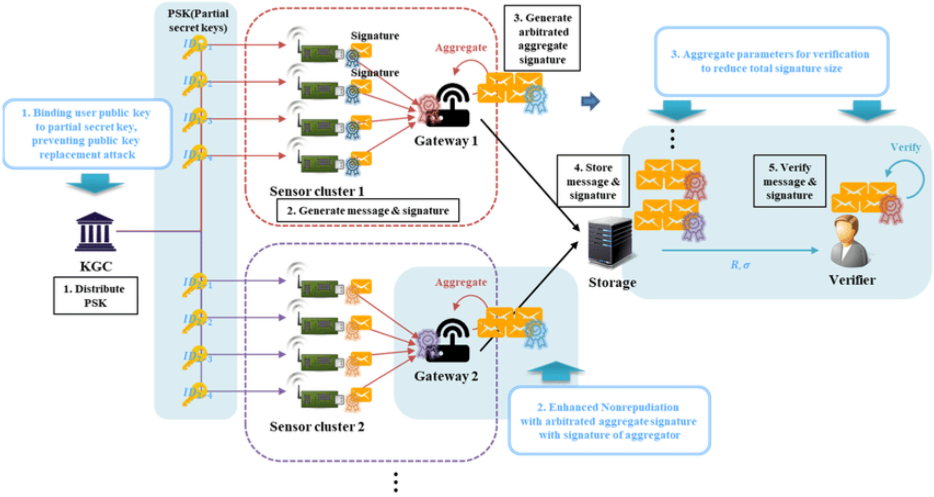
PSK(Partial secret keys)
ID_{1-1}
ID_{1-2}
ID_{1-3}
ID_{1-4}
ID_{2-1}
ID_{2-2}
ID_{2-3}
ID_{2-4}
1. Binding user public key to partial secret key, preventing public key replacement attack
KGC
1. Distribute PSK
Signature
Signature
Aggregate
Gateway 1
Sensor cluster 1
2. Generate message & signature
3. Generate arbitrated aggregate signature
Aggregate
Gateway 2
Sensor cluster 2
2. Enhanced Nonrepudiation with arbitrated aggregate signature with signature of aggregator
3. Aggregate parameters for verification to reduce total signature size
4. Store message & signature
Storage
5. Verify message & signature
Verify
R, σ
Verifier

Figure 1. Scheme Key Generation Center (KGC)

Theoretically, KGC is a robust system capable of monitoring all ID-based cryptographic activities [5]. The components that support the operation of cryptography consist of 2 (two) things, namely the partial private key of the ID-based KGC output, which has the function of an implicit certificate. To complete the private key requires an uncertified independent public key that is immune to user fraud, KGC and even changes to the public key.

Several attempts were made by previous researchers in building a secure CAKA protocol, but not a few also have computation and require a strong network. The efficiency level of CAKA is proposed through PoTS to improve blockchain technology-based security [6]. The protocol that operates applies a decentralized system where the server needs to manage the data generated by PoTS. The scheme is used to assign keys with light computation capability and remain anonymous. With this explanation, it can be said that PoTS synergizes in contributing to securing the interests of a decentralized blockchain technology certificate architecture through CAKA [7].

2. Related Works

Previous research has been designed but there are still deficiencies in privacy and security issues in cryptographic systems, where in the use of PoTS there is a management point that is vulnerable to being targeted by crime when entering the storage process. CAKA's decentralized system is required to promote PoTS privacy [8][9]. A key update between the PoTS clients was proposed based on the AKA pair, and it proved to provide more efficient robustness features [10]. So, starting to propose an anonymous authentication scheme based on pairs for PoTS because the system is lighter and more secure [11]. Introduced 3 (three) layer levels covering intermediate, sensor nodes and hubs, besides that, high costs are required to support infrastructure and minimize problems that arise [12]. Sensor nodes and intermediate nodes form the first tier. Intermediate nodes and hubs form the second tier. Hub and server nodes form the third tier.

The proposed protocol uses a tunnel to allow user authentication without disclosing identity, even though the server knows that the user is a member of the tunnel but the details of the identity remain unknown [13]. Provided many security and authentication requirements are carried out to be paired with Blockchain Technology-based IoT, to ensure that the protocol is safe and runs well on PoTS, performance evaluation is carried out [14].

Reference	PKC	Security novelty	ECC	Assumption and security model
Tong et al.	ID-based AKA	Key-update no repudiation	Pairing	CDH
Jiang et al.	ID-based AKA	Anonymity	Pairing	CDH
Shalif et al.	ID-based AKA	Avoid wrong session key attack	No Pairing	CDH in ROM
Jia et al.	ID-based AKA	Anonymous	Pairing	BDH, BRP Model
Saeed et al.	ID-based AKA	Light-weight	Pairing	CDH in ROM
Hassan et al.	ID-based AKA	Anonymity	Pairing	BDH in ROM
Li et al.	ID-based, PKI	Heterogeneous	Pairing	BDH in ROM
Gervais et al.	CLAKA	Blockchain	No Pairing	CDH in ROM
Dwivedi et al.	ID-based	Blockchain	No Pairing	DLP
Zhao et al.	ID-based	Key management	No Pairing	DLP
Mada et al.	ID-based	Off PAD AKA	No Pairing	AVISPA

Table 1. Evaluation of Protocol Work

As shown in Table 1. The certificate data is encrypted using the recipient's public key and decrypted using the recipient's private key. The digital tunnel signature is used for node authentication, this can be proposed to be efficient key management for the blockchain because in the PoTS protocol, the nodes generate backups and recover the keys used in the blockchain. Each block is encrypted with a different key to provide private data security [15].

2.1 Contributions and Inspirations

A lightweight CAKA is required in accordance with Blockchain Technology-based PoTS where authorized users can authenticate each other, besides that the blockchain also has various security features. Blockchain avoids the point of failure by utilizing blockchain nodes which can verify user data [16]. If it is not collaborated with Blockchain, PoTS will be vulnerable to activities that threaten security and privacy such as leakage of confidential information, impersonation and hacking from hackers. The problems that have been described have inspired to speed up the submission of the CAKA protocol so that the architecture can be decentralized [17].

1. The first step is to prevent major problems in PoTS by designing a new efficient CAKA protocol based on Blockchain Technology [18]. 2 (two) hash functions are used in one operation to improve protocol performance.
2. The second step was to introduce CAKA's decentralized architecture, PoTS is used between blockchain nodes. The signing nodes remain anonymous while the other nodes

totaling are tasked with verification, this is a tremendous advantage and benefit in reducing computation costs.

3. The final step is to carry out a thorough analysis of the security that meets the PoTS security requirements [19].

3. Research Methods

3.1 Flashback to Blockchain Technology

In the world of academia and industry, one of the important roles that a keyword can be found in Cryptocurrency, which is closely related is Bitcoin which has been famous for the size of the capital market because it became the world's first digital or e-cash system [20]. Bitcoin is an implementation of intermediate blockchain technology that has contributed to a breakthrough in the field of special data storage structures [21], blockchain is considered a general ledger where every transaction is stored in a distributed blockchain [22].

For user security which has the main characteristics of being decentralized, asymmetric cryptography is implemented with a distributed consensus algorithm [23][24]. It can be said that the existence of blockchain can increase efficiency and minimize costs, 2 (two) categories of Blockchain are:

1. Private Blockchain: A licensed blockchain is for example an intranet for institutions that use it for specific purposes and need to be monitored [25]
2. Public Blockchain: A permissionless blockchain where each node has participation in adding blocks

In accordance with the disruption that is currently being announced, Blockchain technology has experienced a very significant evolution, where there are 3 categories such as [26][27]: Financial transactions and money transfers using Blockchain 1.0, penetrating into bonds, stocks, loans and mortgages starting to adopt Blockchain 2.0, then public services, security systems and the Internet of Things are also starting to focus on Blockchain implementation [28].

3.2 Blockchain Architecture

Genesis Blockchain is the term used for the first block in Blockchain technology but does not have a parent block [29]. However, in general, a block consists of the hash of the parent block and the block header, which will be illustrated by the proposed Blockchain technology in Figure 2.

1. Block
   Figure 1 shows that to create a block, it must consist of a header and a block body. It can be said that the header must fulfill the following components:
   a. Merkle Root Hash: Shows the hash value in a block for all transactions [30].
   b. Timestamp: Shows the actual time in universal time.
   c. Block Version: In order to know which block validation to follow one should see this section.
   d. Nonce: This is a 4 byte field starting with 0 and increasing for each hash computation.
   e. nBits: indicates the target threshold of valid hash blocks.
   f. Parent Block Hash: This is a 256 bit hash value that points to the previous block.

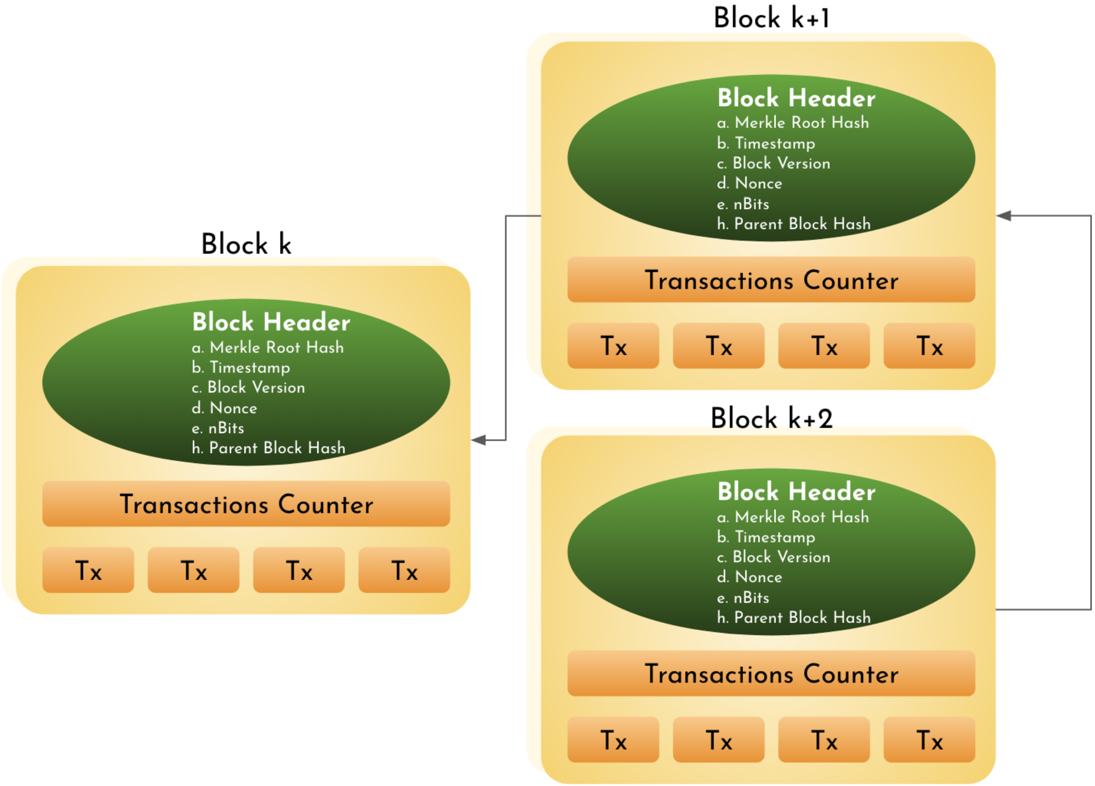

Figure 2. Simple Blockchain Framework

Transaction and block size affect the number of transactions contained in a block. To be able to validate the authenticity of transactions it is necessary to use an asymmetric cryptography system, because it uses a digital signature based on Blockchain Technology for legitimate nodes [31][32].

2. Digital signature
   Each node on blockchain technology has a private key and public key pair, and to maintain transaction security, the private key may not be used to sign transactions or be published [33]. Because essentially signed transactions are propagated to each node to verify the source. Digital signature consists of 2 steps, such as the signature process and the verification stage, this is to ensure that data is not tampered with or altered. In this research, Tunnel Signature is used to reduce computation costs and is considered more efficient [34]. Figure 3. is a Blockchain data stream illustrated with nodes and validation against the Blockchain chain.

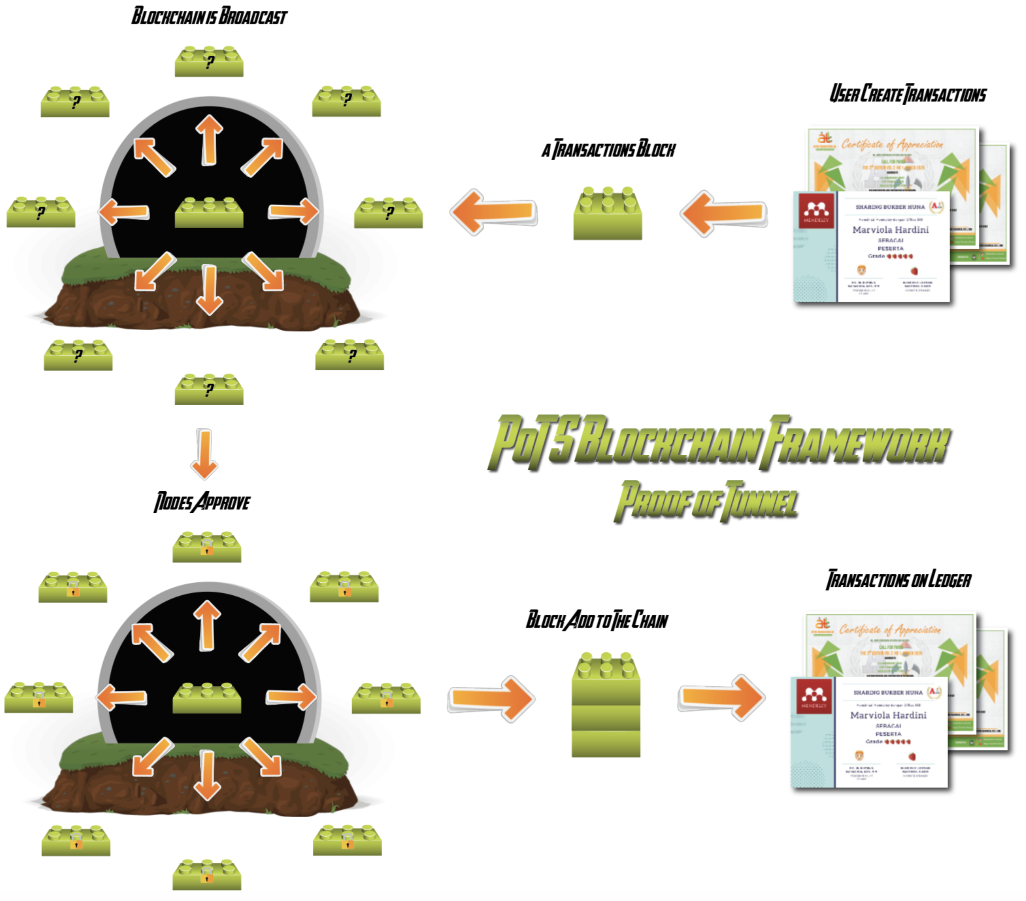

Figure 3. PoTS Blockchain Framework

In Figure 3. it is assumed that one node (Node A) records transactions and the other nodes verify the authenticity of transactions and approve them . It is sent to the blockchain node for each block of transactions that have been made, then the block is broadcast on the chain to be seen by all connected chains [35]. Validation can be performed by a number of nodes that are not on their behalf, then after validation the transaction will be entered into the general ledger [36]. Nodes cannot perform simultaneous transactions because there is node selection based on the Proof of Work (PoW), Proof of Stake (PoS) and Proof of Tunnel (PoT) mechanisms.

3. 4 Characteristics of Blockchain There are 4 (four) main characteristics of Blockchain that are carried out in this research which can be seen as follows [37]:
   a. Anonymity: The identity of the interaction of each node with the Blockchain via the resulting address is undisclosed / confidential.
   b. Persistence: Where transaction validation is performed and any invalid transactions are not recognized. It is almost impossible to delete a transaction once it is entered on the blockchain, because blockchain has immutable characteristics [37].
   c. Decentralization: In blockchain, centralized work systems are no longer used, because no one has control over sensitive data. Each consensus algorithm is used to maintain data in a distributed network to maintain consistency [38].
   d. Auditability: Once the current transaction is recorded, the transaction status can be verified and tracked.

4. Implementation

4.1 CAKA Protocol Desain

The application of the certificate system faces various security problems such as wiretapping, data modification, impersonation and duplication [39]. So as a rejection step strong systems and security techniques (authentication, encryption, session keys) [13][2] are needed to prevent the mentioned threats. In this section, a system and security model for the CAKA protocol based on blockchain technology is presented [30].

1. System model

The model proposed for blockchain-based PoTS includes three entities (Controller C, KGC and Blockchain nodes). To control node N, KGC needs to identify entities and calculate private keys. After the session key has been completed, both users can authenticate with each other to secure data transmission [40]. It should be noted that Figure 4 illustrates the proposed system model when two entities communicate and avoid various attacks, as steps 1 and 2 represent the data transmission process during node authentication after key generation [41].

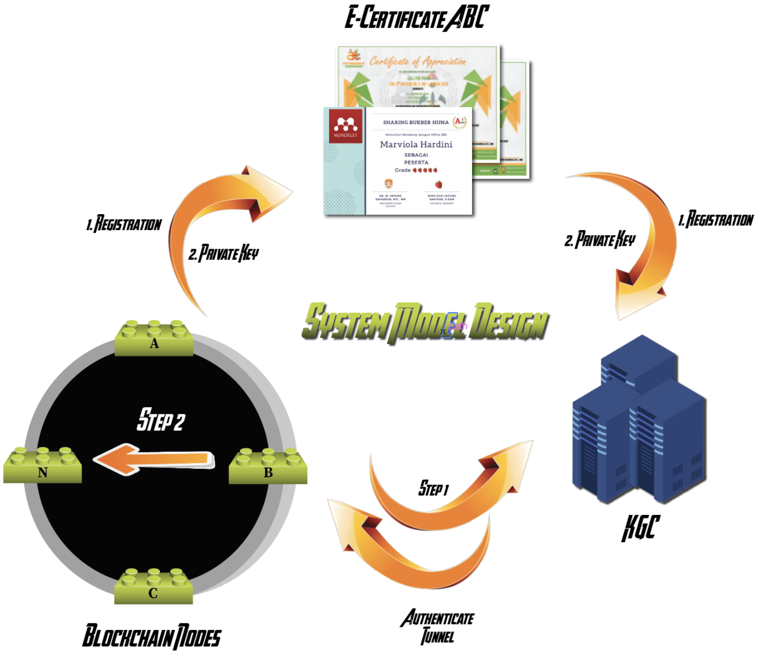

Figure 4. System Model Design

a. N blockchain nodes: In charge of collecting data from controllers and will broadcast to other blockchain nodes, also known as collector nodes.
b. The controller collects data from E-Certificate ABC and sends it to the blockchain node via the internet [27]. Before sending data to the blockchain, B performs calculations for the public key as data security with Blockchain N nodes. And in this session every data sent from B to blockchain N nodes will be encrypted [42].
c. KGC can generate a list of system parameters, so KGC is dedicated to registering N nodes as well as a decentralized B controller [43][44]. And it should be noted that KGC cannot know about the private keys of nodes N and B.
d. Before sending data to the Blockchain, a consensus message needs to be sent first to node N and broadcast to the Blockchain as stage 1. The session key is used to encrypt when B sends M messages to the Blockchain [15][45]. And at that time N will get a message using K's key session to restore the blockchain-permitting form, namely M.

In step 2 N broadcasts a consensus message to the Blockchain, each node can verify the authenticity of node N and get a message from node N. We have obtained two principles of security and privacy in PoTS according to the proposed protocol design for data protection [46]. As a requirement that must be considered, when the PoTS system is implemented with blockchain technology, it must meet the security properties of data integrity, authentication security, no rejection and also privacy [47][48].

4.2 Proof of Tunnel Signature (PoTS) Design

The author displays the tunnel signature and uses it to verify blockchain nodes with anonymity in mind. 3 (three) cryptographic hash functions H_1, H_2, and H_3 are selected for H_1: $\{0, 1\}^* \rightarrow \mathbb{R},^{*}$, $H_2 : \{0,1\}^* \rightarrow \mathbb{R},^{*}$ and $H_3 : \mathbb{N}_1 \rightarrow \mathbb{R},^{*}$ which is defined as the counter $f = e\ (P, P)$ to make a concrete signature.

The computed Proof of Tunnel Signature:

$$\prod_{i}^{n} e(T_{IDi}, PK_{IDi} + y_{IDi}S_{IDi})$$

$$= e(T_{ID_A}, PK_{ID_A} + y_{IDi}S_{IDi}) \prod_{i, i \neq A}^{n} e(T_{IDi}, PK_{IDi} + y_{IDi}S_{IDi})$$

$$= ((h + r)\, PS_{ID_A}, x_{ID_A}(P_{pub} + H_2(ID_A)P) + y_{ID_A P} + y_{ID_A} + P_{pub} + H_2(ID_A)P)) \times \prod_{i, i \neq A}^{n} e(T_{IDi}, PK_{IDi} + y_{IDi}S_{IDi})$$

$$= e((h + r)\, PS_{ID_A}, (x_{ID_A} + y_{ID_A})\, (m + H_2(ID_A))P) \prod_{i, i \neq A}^{n} e(T_{IDi}, PK_{IDi} + y_{IDi}S_{IDi})$$

$$= e((h + r)\, P, P) \prod_{i, i \neq A}^{n} e(T_{IDi}, PK_{IDi} + y_{IDi}S_{IDi})$$

$$= f^{h+r} \prod_{i, i \neq A}^{n} e(T_{IDi}, PK_{IDi} + y_{IDi}S_{IDi})$$

$$= f^{h} f^{r} \prod_{i, i \neq A}^{n} e(T_{IDi}, PK_{IDi} + y_{IDi}S_{IDi}) = f^{H_2(M, u, L, PK)} .\, u$$

4.3 New Protocol Design Analysis

An analysis was performed for the performance of the new proposed protocol and various security properties by comparing it with other protocols.

Features	Fog-Driven IoT	WBAN	Akaiots	PoTS
Key Escrow	x	x	✓	✓
Anonymity	✓	✓	✓	✓
Key Compromise Impersonation	✓	✓	✓	✓
Immutability	x	x	x	✓

Verifiability	x	x	x	✓
Decentralized	x	x	x	✓
Consensus	x	x	x	✓

Table 2. Security Properties Collation

In Table 2. A comparison is made for the security properties between the PoTS protocol design with Fog-Driven IoT, WBAN, and Akaiots [49]. Comparison has also been made in Table 3. Including communication and computation costs, the proposed protocol design is represented by performing V_h: one-way hash function time, V_e: bilinear pair execution time, V_m: scalar multiplication time, and V_{se}: encryption / decryption execution time symmetrical.

Schemes	Communication Cost	Computations Cost	
		Client	Server
Fog-Driven IoT	$\lvert 6\mathbb{R}^*_q + 4G_1 + 4v_c \rvert$	$2V_m + 5V_h + V_e$	$2V_m + 4V_h + V_e$
WBAN	$\lvert 2ID + 2\mathbb{R}^*_q + 2G1 + 2v_c \rvert$	$V_{se} + 9V_m + 9V_h + V_{se}$	$2V_e + 5V_m + 10V_h + 2V_{se}$
Akaiots	$\lvert 4\mathbb{R}^*_q + 4G1 + 2v_c + 2ID \rvert$	$6V_m$	$6V_m$
PoTS	$\lvert 2ID + 2\mathbb{R}^*_q + 2G1 \rvert$	$V_e + 2V_m$	$V_e + 2V_m$

Table 3. The Collation Based on Communication and Computation Costs

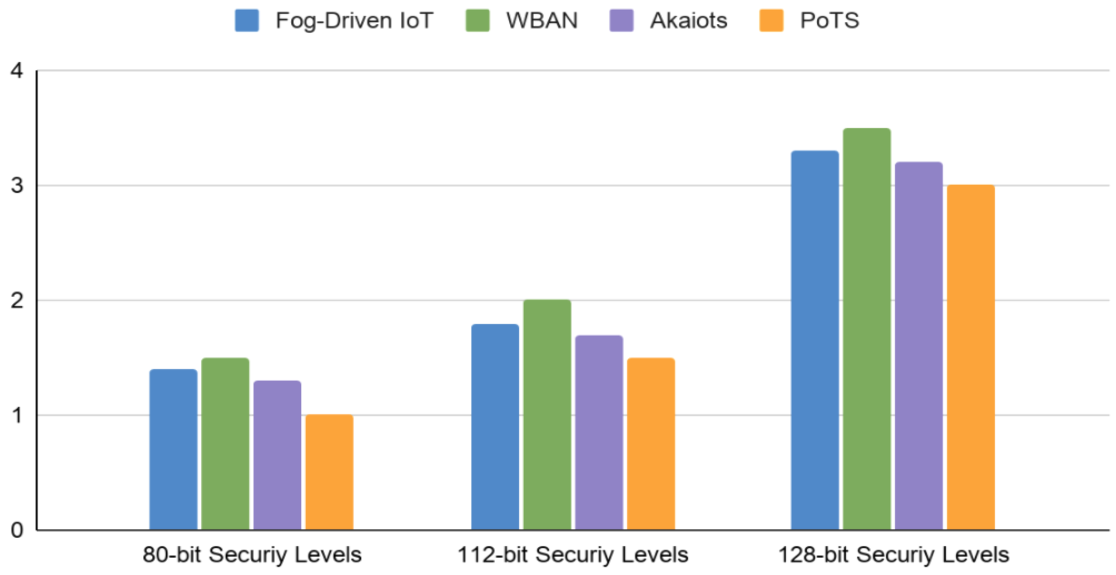

Figure 5. Computation Cost of Client

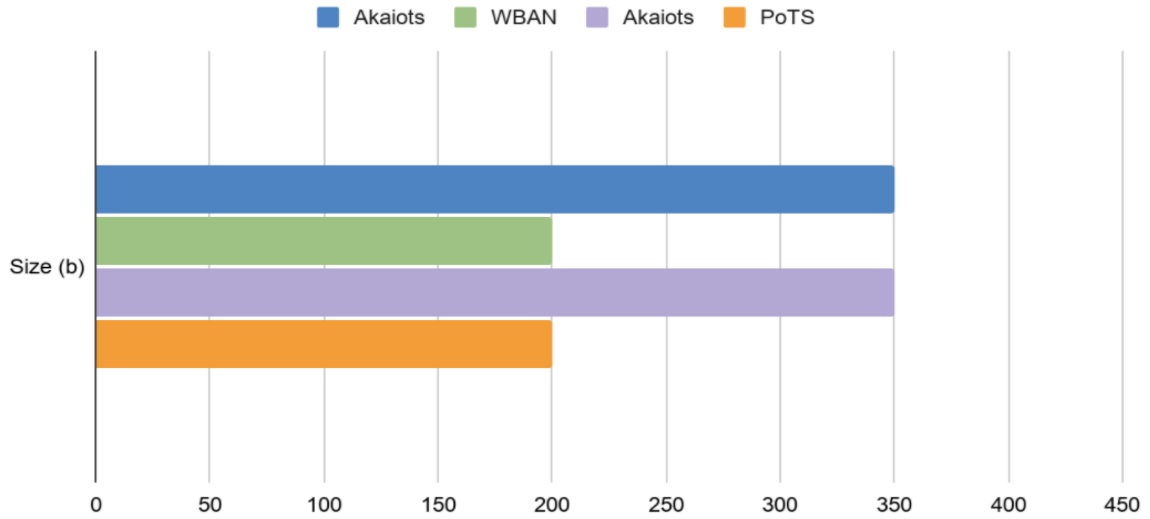

Figure 6. Communication cost on different protocols

The results of the implementation in Figure 5 and Figure 6 show the cost of computing the client / controller and server / node for the 4 (four) protocols being compared [50], this shows that the proposed PoTS protocol has lower computation costs than other protocols. Table 4. Shows the q and p sizes for the three security levels which are at 80-bit, 112-bit and 128-bit.

Security Level	Size of *q*	Size of *p*
80-bit	160	512
112-bit	224	1024
128-bit	256	1536

Table 4. Bits Size Levels of The Three Security

Formula	**Descriptions**
CAKA	Certificate Authenticated Key Agreement
KGC	Key Generation Center
ℕ	A cyclic additive group
q	A prime order of group ℕ

e	Bilinear Mapping
P_{pub}	A public key of KGC
i	An identity/user
IDi	A user identity
yi	A secret value of entity
PS_{ID}	Private key of entity
PS_{ID_A}	Private key for a signing node

Table 5. Notations Descriptions

5. Conclusion and Future Work

The proposed Blockchain Technology based CAKA protocol for PoTS has been successfully proposed, CAKA provides security features such as decentralization, immutability and anonymity. PoTS avoids management fraud, this is recognized by the performance evaluation which shows that PoTS is considered efficient and in accordance with CAKA. This research is adjusted to the development of blockchain which currently occupies Blockchain 3.0, and is starting to expand into various fields of science.

Judging from the research results obtained, it can be concluded that 7 Security Properties such as: Key compromise impersonation, Key escrow, Anonymity, Decentralized, Immutability, Verifiability, and Consensus, can be fulfilled with the implementation of Blockchain-based PoTS.

In the future there is a big possibility in this field to conduct further research on CAKA Design as an implementation of Blockchain-based PoTS. The CAKA protocol which is heterogeneous in nature can allow entities to have a key that is authenticated with a cryptographic system in a digital certificate.

Acknowledgments

The author would like to thank Ristek-Brin, Kominfo Tangerang, University of Raharja, Alphabet Incubator for their support and for providing a place to support this research through analysis of research systems.

Bibliography

[1] Q. Aini, U. Rahardja, and A. Khoirunisa, “Blockchain Technology into Gamification on Education,” *IJCCS (Indonesian J. Comput. Cybern. Syst.*, vol. 14, no. 2, pp. 1–10, 2020, doi: 10.22146/ijccs.53221.

[2] U. Rahardja, A. S. Bist, M. Hardini, Q. Aini, and E. P. Harahap, “Authentication of Covid-19 Patient Certification with Blockchain Protocol.”

[3] U. Rahardja, A. N. Hidayanto, T. Hariguna, and Q. Aini, “Design Framework on Tertiary Education System in Indonesia Using Blockchain Technology,” *2019 7th Int. Conf. Cyber IT Serv. Manag. CITSM 2019*, pp. 5–8, 2019, doi: 10.1109/CITSM47753.2019.8965380.

[4] Z. Fauziah, H. Latifah, X. Omar, A. Khoirunisa, and S. Millah, “Application of Blockchain Technology in Smart Contracts: A Systematic Literature Review,” *Aptisi Trans. Technopreneursh.*, vol. 2, no. 2, pp. 160–166, 2020.

[5] I. Amsyar, E. Christopher, A. Dithi, A. N. Khan, and S. Maulana, "The Challenge of Cryptocurrency in the Era of the Digital Revolution: A Review of Systematic Literature," *Aptisi Trans. Technopreneursh.*, vol. 2, no. 2, pp. 153–159, 2020.

[6] Q. Aini, A. Badrianto, F. Budiarty, A. Khoirunisa, and U. Rahardja, "Alleviate Fake Diploma Problem In Education Using Block Chain Technology," *J. Adv. Res. Dyn. Control Syst.*, vol. 12, no. 2, pp. 1821–1826, 2020, doi: 10.5373/JARDCS/V12I2/S20201225.

[7] L. Chandra, Amroni, B. Frizca, Q. Aini, and U. Rahardja, "Utilization Of Blockchain Decentralized System In Repairing Management Of Certificate Issuance System," *J. Adv. Res. Dyn. Control Syst.*, vol. 12, no. 2, pp. 1922–1927, 2020, doi: 10.5373/JARDCS/V12I2/S20201235.

[8] P. A. Sunarya, U. Rahardja, L. Sunarya, and M. Hardini, "The Role Of Blockchain As A Security Support For Student Profiles In Technology Education Systems," *InfoTekJar J. Nas. Inform. dan Teknol. Jar.*, vol. 4, no. 2, pp. 13–17, 2020.

[9] Q. Aini, N. Lutfiani, F. Hanafi, and U. Rahardja, "Application of Blockchain Technology for iLearning Student Assessment," *IJCCS (Indonesian J. Comput. Cybern. Syst.*, vol. 14, no. 2, 2020, doi: 10.22146/ijccs.53109.

[10] S. Sutirna, "TOTAL QUALITY MANAGEMENT THROUGH LECTURER ASSESSMENT WITH STUDENTS TO IMPROVE GRADUATE QUALITY," *ADI J. Recent Innov.*, vol. 2, no. 1 Sept, pp. 227–242, 2020.

[11] Henderi, Q. Aini, N. P. L. Santoso, A. Faturahman, and U. Rahardja, "A proposed gamification framework for smart attendance system using rule base," *J. Adv. Res. Dyn. Control Syst.*, vol. 12, no. 2, pp. 1827–1838, 2020, doi: 10.5373/JARDCS/V12I2/S20201226.

[12] A. Williams and E. Dolan, "Application of Blockchain Technology in e-LoA Technopreneurship Journal," *Aptisi Trans. Technopreneursh.*, vol. 2, no. 1, pp. 98–103, 2020.

[13] A. Adiyanto and R. Febrianto, "Authentication Of Transaction Process In E-marketplace Based On Blockchain technology," *Aptisi Trans. Technopreneursh.*, vol. 2, no. 1, pp. 68–74, 2020.

[14] R. Geethanjali, "Notice of Retraction Survey on Health Monitoring of Elderly Using IoT," *Aptikom J. Comput. Sci. Inf. Technol.*, vol. 2, no. 3, pp. 131–136, 2017.

[15] B. S. Riza, M. Y. Mashor, and E. V. Haryanto, "THE APPLICATION OF RSA AND LSB IN SECURITY OF MESSAGES ON IMAGERY," *ADI J. Recent Innov.*, vol. 1, no. 1, pp. 20–32, 2019.

[16] A. S. Bist, W. Febriani, C. Lukita, S. Kosasi, and U. Rahardja, "Design of Face Recognition AttendX for Recording Student Attendance Data Based on Artificial Intelligence Technology," *Solid State Technol.*, pp. 4505–4518, 2020.

[17] F. Agustin, S. Syafnidawati, N. P. Lestari Santoso, and O. G. Amrikhasanah, "Blockchain-based Decentralized Distribution Management in E-Journals," *Aptisi Trans. Manag.*, vol. 4, no. 2, pp. 107–113, 2020.

[18] P. P. S. Naik and T. V. Gopal, "BNIMS: Block-based Non-iterative Mean-shift Segmentation algorithm for Medical Images," *Aptikom J. Comput. Sci. Inf. Technol.*, vol. 1, no. 2, pp. 46–56, 2016.

[19] E. S. Aisyah, E. P. Harahap, and N. Salsabila, "The Effect Requirements Selling In The Marketplace For Security Against Buyer Trust," *Aptisi Trans. Manag.*, vol. 4, no. 1, pp. 67–75, 2019.

[20] N. K. Purnamawati, A. M. Adiandari, N. D. A. Amrita, and L. P. V. I. Perdanawati, "The Effect Of Entrepreneurship Education And Family Environment On Interests Entrepreneurship In Student Of The Faculty Of Economics, University Of Ngurah Rai In Denpasar," *ADI J. Recent Innov.*, vol. 1, no. 2 Maret, pp. 158–166, 2020.

[21] P. A. Sunarya, Q. Aini, A. S. Bein, and P. Nursaputri, "The Implementation Of Viewboard Of The Head Of Department As A Media For Student Information Is Worth Doing Final Research," *ITSDI J. Ed. Vol. 1 No. 1 Oct. 2019*, p. 18, 2019.

[22] A. Zainuddin, J. Junaidi, and R. D. Putra, “Design of E-Commerce Payment System at Tokopedia Online Shopping Site,” *Aptisi Trans. Manag.*, vol. 1, no. 2, pp. 143–155, 2017.

[23] U. Rahardja, “Artificial informatics,” *2009 4th IEEE Conf. Ind. Electron. Appl. ICIEA 2009*, pp. 3064–3067, 2009, doi: 10.1109/ICIEA.2009.5138764.

[24] R. Rojali and D. I. Sari, “Relationship Of Individual Characteristics, Physical Home Environment And Behavior With The Incidence Of Pulmonary Tb In Cijoro Pasir Village, Muara Village East Ciujung And West Rangkasbitung Village, Rangkasbitung Subdistrict, Lebak Regency 2019,” *ADI J. Recent Innov.*, vol. 1, no. 2, pp. 167–179, 2020.

[25] Q. Aini, T. Hariguna, P. O. H. Putra, and U. Rahardja, “Understanding how gamification influences behaviour in education,” *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 1.5 Special Issue, pp. 269–274, 2019, doi: 10.30534/ijatcse/2019/4781.52019.

[26] F. Sudarto and A. Yondari, “Web-Based Population Cencus Design In Neighborhood Building,” *Aptisi Trans. Technopreneursh.*, vol. 2, no. 1, pp. 18–24, 2020.

[27] I. Ilamsyah, A. Robertz, and R. R. Fitriani, “The Web-based Internet Cafe (RIC) Raharja Ordering System,” *Aptisi Trans. Technopreneursh.*, vol. 1, no. 1, pp. 93–100, 2019.

[28] C. Lukita, M. Hatta, E. P. Harahap, and U. Rahardja, “Crowd funding management platform based on block chain technology using smart contracts,” *J. Adv. Res. Dyn. Control Syst.*, vol. 12, no. 2, 2020, doi: 10.5373/JARDCS/V12I2/S20201236.

[29] F. P. Oganda, U. Rahardja, Q. Aini, M. Hardini, and A. S. Bist, “BLOCKCHAIN: VISUALIZATION OF THE BITCOIN FORMULA,” *PalArch’s J. Archaeol. Egypt/Egyptology*, vol. 17, no. 6, pp. 308–321, 2020.

[30] A. I. L. Wibowo, A. D. Putra, M. S. Dewi, and D. O. Radianto, “Study of Divergence of Go Public Company’s Financial Performance Based on Website Before and After Merger Using Window Period Method TIME Frame 2015-2017,” *Aptisi Trans. Technopreneursh.*, vol. 1, no. 1, pp. 27–51, 2019.

[31] K. O. Ogbeide and E. M. EJ, “Path-Loss Prediction for UHF/VHF Signal Propagation in Edo State: Neural Network Approach,” *Aptikom J. Comput. Sci. Inf. Technol.*, vol. 1, no. 2, pp. 77–84, 2016.

[32] U. Rahardja, S. Sudaryono, N. P. L. Santoso, A. Faturahman, and Q. Aini, “Covid-19: Digital Signature Impact on Higher Education Motivation Performance,” *Int. J. Artif. Intell. Res.*, vol. 4, no. 1, May 2020, doi: 10.29099/ijair.v4i1.171.

[33] Sudaryono, U. Rahardja, and E. P. Harahap, “Implementation of Information Planning and Strategies Industrial Technology 4.0 to Improve Business Intelligence Performance on Official Site APTISI,” *J. Phys. Conf. Ser.*, vol. 1179, no. 1, pp. 0–7, 2019, doi: 10.1088/1742-6596/1179/1/012111.

[34] M. S. Shaik, K. S. Prasad, R. A. Shaik, and D. V. Rao, “Acoustic Echo Cancellation using Computationally Efficient Adaptive Algorithm Techniques,” *Aptikom J. Comput. Sci. Inf. Technol.*, vol. 1, no. 2, pp. 57–62, 2016.

[35] G. N. B. Safrizal and G. N. Budiadyana, “Analysis Application Design Career Development Center In The STMIK Insan Pembangunan and (Case Study: Information Study Program),” *IAIC Trans. Sustain. Digit. Innov.*, vol. 1, no. 1, pp. 66–77, 2019.

[36] U. Rahardja, T. Hariguna, and Q. Aini, “Understanding the impact of determinants in game learning acceptance: An empirical study,” *Int. J. Educ. Pract.*, vol. 7, no. 3, pp. 136–145, 2019, doi: 10.18488/journal.61.2019.73.136.145.

[37] S. Watini, Q. Aini, M. Hardini, and U. Rahardja, “Improving Citizen’s Awareness in Conserving Diversity of Malay Traditional Dances in Malaysia through the Art Appreciation Performed by Students of Early Childhood Education Study Program,” *Int. J. Psychosoc. Rehabil.*, vol. 24, no. 8, pp. 2730–2737, 2020, doi: 10.37200/IJPR/V24I8/PR280292.

[38] P. A. Sunarya, F. Andriyani, Henderi, and U. Rahardja, “Algorithm automatic full time equivalent, case study of health service,” *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 1.5 Special Issue, pp. 387–391, 2019, doi: 10.30534/ijatcse/2019/6281.52019.

[39] U. Rahardja, C. Lukita, F. Andriyani, and Masaeni, “Optimization of marketing workforce scheduling using metaheuristic genetic algorithms,” *Int. J. Adv. Trends Comput. Sci. Eng.*,

vol. 9, no. 1.2 Special Issue, pp. 243–249, 2020, doi: 10.30534/IJATCSE/2020/3691.22020.

[40] P. Ramanathan, “Implementation of PC Controlled Wireless Video Transmitting Vehicle,” *Aptikom J. Comput. Sci. Inf. Technol.*, vol. 2, no. 2, pp. 63–67, 2017.

[41] U. Rahardja, E. P. Harahap, and S. R. Dewi, “The strategy of enhancing article citation and H-index on SINTA to improve tertiary reputation,” *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 17, no. 2, pp. 683–692, 2019, doi: 10.12928/TELKOMNIKA.V17I2.9761.

[42] M. Soltani and A. K. Bardsiri, “Notice of Retraction A New Secure Hybrid Algorithm for QR-Code Images Encryption and Steganography,” *Aptikom J. Comput. Sci. Inf. Technol.*, vol. 2, no. 2, pp. 86–96, 2017.

[43] B. S. Riza, “Blockchain Dalam Pendidikan: Lapisan Logis di Bawahnya,” *ADI Bisnis Digit. Interdisiplin J.*, vol. 1, no. 1, pp. 41–47, 2020.

[44] S. Kosasi, “Karakteristik Blockchain Teknologi Dalam Pengembangan Edukasi,” *ADI Bisnis Digit. Interdisiplin J.*, vol. 1, no. 1, pp. 87–94, 2020.

[45] K. Arora, A. S. Bist, R. Prakash, and S. Chaurasia, “A Novel Approach for Facial Attendance: AttendXNet,” *Aptisi Trans. Technopreneursh.*, vol. 2, no. 2, pp. 104–111, 2020.

[46] P. A. Sunarya, F. Andriyani, Henderi, and U. Rahardja, “Algorithm automaticPrawira, M., Sukmana, H. T., Amrizal, V., & Rahardja, U. (2019). A Prototype of Android-Based Emergency Management Application. 2019 7th International Conference on Cyber and IT Service Management, CITSM 2019. https://doi.org/10.1109/CI,” *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 1.5 Special Issue, pp. 387–391, 2019, doi: 10.30534/ijatcse/2019/6281.52019.

[47] W. Zulkarnain and S. Andini, “Inkubator Bisnis Modern Berbasis I-Learning Untuk Menciptakan Kreativitas Startup di Indonesia,” *ADI Pengabdi. Kpd. Masy.*, vol. 1, no. 1, pp. 77–86, 2020.

[48] A. K. Yaniaja, H. Wahyudrajat, and V. T. Devana, “Pengenalan Model Gamifikasi ke dalam E-Learning Pada Perguruan Tinggi,” *ADI Pengabdi. Kpd. Masy.*, vol. 1, no. 1, pp. 22–30, 2020.