I. J. Computer Network and Information Security, **2023, 1, 14-25**
Published Online on February 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2023.01.02

Revamped Dual-key Stealth Address Protocol for IoT Using Encryption and Decentralized Storage

Justice Odoom*
Southwest University of Science and Technology/Department of Computer Science and Technology, Mianyang, 621010, China
E-mail: odoom.justice@ieee.org
ORCID iD: https://orcid.org/0000-0003-2765-6977
*Corresponding Author

Huang Xiaofang
Southwest University of Science and Technology/Department of Computer Science and Technology, Mianyang, 621010, China
E-mail: huangxiaofang@swust.edu.cn
ORCID iD: https://orcid.org/0000-0002-9710-2171

Samuel Akwasi Danso
Ghana Communication Technology University/Faculty of Engineering, Accra, PMB 100, Ghana
E-mail: sdanso@gtuc.edu.gh
ORCID iD: https://orcid.org/0000-0002-9757-9527

Richlove Samuel Soglo
Southwest University of Science and Technology/Department of Computer Science and Technology, Mianyang, 621010, China
E-mail: richlovesoglo@gmail.com
ORCID iD: https://orcid.org/0000-0001-9988-4106

Benedicta Nana Esi Nyarko
Southwest University of Science and Technology/Department of Information Engineering, Mianyang, 621010, China
E-mail: benedictanyarko41@gmail.com
ORCID iD: https://orcid.org/0000-0002-1738-6048

Received: 17 December 2021; Revised: 06 July 2022; Accepted: 14 September 2022; Published: 08 February 2023

Abstract: Blockchain technology unarguably has over a decade gained widespread attention owing to its often-tagged disruptive nature and remarkable features of decentralization, immutability and transparency among others. However, the technology comes bundled with challenges. At center-stage of these challenges is privacy-preservation which has massively been researched with diverse solutions proposed geared towards privacy protection for transaction initiators, recipients and transaction data. Dual-key stealth address protocol for IoT (DkSAP-IoT) is one of such solutions aimed at privacy protection for transaction recipients. Induced by the need to reuse locally stored data, the current implementation of DkSAP-IoT is deficient in the realms of data confidentiality, integrity and availability consequently defeating the core essence of the protocol in the event of unauthorized access, disclosure or data tampering emanating from a hack and theft or loss of the device. Data unavailability and other security-related data breaches in effect render the existing protocol inoperable. In this paper, we propose and implement solutions to augment data confidentiality, integrity and availability in DkSAP-IoT in accordance with the tenets of information security using symmetric encryption and data storage leveraging decentralized storage architecture consequently providing data integrity. Experimental results show that our solution provides content confidentiality consequently strengthening privacy owing to the encryption utilized. We make the full code of our solution publicly available on GitHub.

Index Terms: Blockchain, Decentralized Storage, Encryption, Privacy, Stealth Address.

1. Introduction

Over the past decade, one technological invention that has gained unprecedented attention in academia and industry alike is Blockchain. It is the technological wonder which underpins Bitcoin [1], Ethereum [2], Hyperledger fabric [3] among others characterized by a publicly distributed transaction ledger with inherent traits of immutability, decentralization, consensus mechanism and transparency [4]. One key consequence of blockchain is disintermediation thereby causing rippling effects in virtually all spheres of life. It is therefore no surprise that this awesome technology has earned the enviable tag disruptive technology.

It is however worth pointing out that Blockchain technology is not challenge-free. [5-8] point out inherent challenges of the technology like Privacy leakages, Scalability, Selfish mining, Personal Identifiable Information, and Security. Note that privacy leakages on blockchain can have dire consequences [9, 10].

Privacy-preservation is one of the challenges that has garnered support in both academia and industry. Owing to its transparent nature, blockchain transactions are globally visible to all entities subsequently paving way for inferences to be made regarding transaction participants (senders and recipients) as well as transaction data. By carefully analyzing the blockchain, it is possible to discover payment patterns or relationships. Moreover, it becomes possible to deanonymize transaction participants by linking transaction participants to their real-world identities often using a combination of on-chain and off-chain data as evident in works including [11-13].

Resolving the privacy challenge associated with blockchain technology has seen numerous propositions and solutions like ring signatures [14-18], zero knowledge proofs and their variants [19-21], commitment scheme as used in [19, 22] and secure multi-party computation [23, 24] etc. aimed at protecting transaction entities: transacting initiators (senders), transaction recipients, transaction data or their combination. Stealth address protocol [25] is one such solutions geared towards privacy-preservation for transaction recipients by guaranteeing transaction unlinkability and has undergone several transformations over the years as early variants were not secured in that among others, they were prone to privilege escalation attack [26, 27] bringing to the fore the issue of security.

Dual-key stealth address protocol for IoT (DkSAP-IoT) [28] although an improvement of the initial Dual-key stealth address protocol (DkSAP) [29] and is the state-of-the-art protocol regarding stealth address technology is not immune to security threats. This stems from the local storage of protocol-related data in the device. Over the years, data storage has been done using databases or cloud-based infrastructure and a merger of both technologies. Cloud-based storage has often been employed in extant works [30-34]. However, as noted in recent security reports by Verizon and Symantec [35, 36], cloud-based systems have inherent security vulnerabilities. In this paper, geared towards addressing the adverse effects of local storage of protocol-related data both on the existing protocol and subsequently the user, we adopt a different approach: the use of encryption and data storage on a decentralized platform. Concisely, we aim at designing a protocol allowing blockchain-based transaction recipients to receive payments in an anonymous fashion while making the protocol resource-constrained-friendly and at the same time adhere to core security requirements.

Security in designed protocols is essential and cryptographic protocols must align with and promote the well-known CIA triad denoting confidentiality, integrity and availability. It therefore becomes paramount to carefully implement such information security principles to be ingrained into protocols and existing ones for data and privacy protection [31]. It even becomes imperative in a dynamic environment to continually improve upon standards so as to meet specified expectations or specifications.

The primary contributions of our paper are summarized as follows.

- Encryption and decentralized storage-based DkSAP-IoT model is proposed.
- We provide algorithms and data flow diagram of our proposed solution.
- We present a proof-of-concept implementation and provide experimental results.
- A detailed mechanism for data retrieval including protocol-related data is shown in the event of loss or theft of the mobile device.
- We provide security and protocol analysis showing how our proposed solution satisfies fundamental security principles.

The rest of the paper is organized as follows: Section 2 reviews existing work on improvements to stealth address, data confidentiality, integrity and availability. Details regarding DkSAP-IoT is provided in section 3. In section 4, we provide details on methodology employed in the proposed solution and explicate on implementation details. In section 5, we present results pertaining to testing and validation whereas security and protocol analysis are presented in section 6. Section 7 concludes the paper.

2. Related Works

This section presents extant works pertaining to stealth address protocol, data availability and confidential that have relevance to our work.

A Stealth address provides a privacy-enhancing technique allowing payments to transaction recipients in an

anonymous manner and has seen a myriad of implementations [37]. In line with improving the efficiency and robustness of stealth address, the original idea [25] was improved to yield Dual-key stealth address protocol (DkSAP) [29] allowing a proxy entity like an auditor or law enforcement agent to scan the blockchain in order to establish coin ownership and has successfully been implemented in Aztec protocol [38]. However, the challenge with DkSAP is the requirement to constantly scan the blockchain and perform computationally expensive tasks of scalar multiplications hence not resource-constrained friendly.

In order to allow for usability of the protocol in mobile and resource constrained devices, [28] dubbed Faster Dual-key Stealth Address Protocol for IoT (DkSAP-IoT) drastically reduces the number of persistent computations to one by prolonging the lifetime of the shared secret to aid in locating the exact matched destination address. However, the shared secret is stored locally then continuously and pseudorandomly updated via a cryptographic hash function for the subsequent specified transactions. We adopt [28] in this work and modify the protocol given the fact that mobile, IoT and other resource constrained devices are akin to Cyber Physical Systems (CPS) hence prone to attacks [39] and theft. It becomes imperative for counter measures to be enforced to forestall any such security incidents. The National Institute of Standards and Technology (NIST) stipulates that such information security protection mechanisms must however be implemented so as to be commensurate with the assessed risks [40]. The assessed risks in the case of the deficiencies of DkSAP-IoT are CIA triad related.

The quest to attain data availability has seen the reliance of several extant works on cloud-based infrastructure [30-34]. This is not surprising given performance or efficiency challenges, huge cost and blockchain blot pertaining to on-chain storage. It is however noteworthy that although cloud infrastructure meets the requirement of data availability, its challenges cannot be neglected. For instance, in recent security reports [35, 36], S3 bucket was an Achilles' heel in cloud and container-based infrastructure resulting in over 70million records been stolen or leaked. Moreover, the use of the cloud entails trusting the cloud service provider (CSP) to act honestly which is counter-intuitive to blockchain-based protocols. Notice that in such infrastructure, users have no way of detecting data tampering. The possibility of compromising data confidentiality and integrity cannot be relegated to the background. In this work, we take a different route by leveraging decentralized storage platform specifically Interplanetary File System (IPFS) [41] and its name system called Interplanetary Name System (IPNS) [42] thereby providing data availability with inbuilt data integrity check using a cryptographic hash function.

Achieving data confidentiality is paramount in any security-conscious infrastructure and has largely been realized via a plethora of technique paramount being encryption [34, 43, 44] encompassing both public key (asymmetric encryption) and symmetric encryption. Asymmetric encryption is usually slow and computationally expensive hence may not be ideal in resource-constrained environment.

3. Building Block

In this section, we provide basic knowledge and theory underlying the current implementation of DkSAP-IoT. Concisely, stealth address unlike the usual blockchain address utilizes a one-time address to guarantee privacy by disconnecting the link between the transaction initiator and receiver in a way that does not disclose the actual address of the recipient but rather the stealth address. The recipient of dual-key stealth address-based transaction possess a pair of private/public keys (v_B, V_B), (s_B, S_B). The algorithm for DkSAP-IoT [28] between two parties A and B follows.

3.1. Sending a Transaction

The Transaction initiator say A checks to find out if the transaction recipient B is in the receivers' locally stored list and if it does, A recovers the shared secret h_{cntB} and calculates the destination public key (Stealth Address) as:

$$T_A = h_{cntB} + S_B \tag{1}$$

If TR is not in the receiver's list of recipients, a new ephemeral public key R_A (see eqn. 2) followed by the shared secret h_o (see eqn. 3) are calculated where H denotes a cryptographic hash function and $r_A \in_R Z$.

$$R_A = r_A G \tag{2}$$

$$h_o = H(r_A V_B) \tag{3}$$

The destination public key or Stealth address is computed as follows:

$$T_A = h_o G + S_B \tag{4}$$

A sends a transaction including R_A and the stealth address T_A to B and then sets ephemeral public key counter

$cnt_B = 0$ and updates the shared secret h_{cntB}. Moreover, in both cases aforementioned the counter cnt_B is updated as:

$$cnt_B = cnt_B + 1 \tag{5}$$

$$h_{cntB} = H(h_{cntB-1}) \tag{6}$$

3.2. Receiving a Transaction

B verifies if the received transaction contains R_A. If it does, TR, computes the shared secret and the stealth address as:

$$h_o = H(v_B R_A) \tag{7}$$

$$T_A^{'} = h_o G + S_B \tag{8}$$

If $T_A^{'} = T_A$, B accepts the transaction from A and proceeds to calculate the corresponding private key for retrieval as:

$$t_A^{'} = h_o + _{SB} \tag{9}$$

B sets $cnt_A = 0$ and subsequently updates the counter and shared secret as well as precomputes the anticipated destination key pair or stealth addresses for the next transaction from A as follows:

$$cnt_A = cnt_A + 1 \tag{10}$$

$$h_{cntA} = H(h_{cntA-1}) \tag{11}$$

$$T_A^{'} = h_{cntA} G + S_B \tag{12}$$

$$t_A^{'} = h_{cntA} + _{SB} \tag{13}$$

If, however, the transaction from A has no R_A, it implies B has ever received a transaction from A hence B only retrieves the locally stored corresponding private key as explained above and performs the updates of counter and shared secret accordingly.

As briefly mentioned earlier in this paper, DkSAP-IoT in its original form does not satisfy the CIA triad in that, in the event of a hack or theft or loss of the device, the user has no way of recovering DkSAP-IoT stored data thereby defeating the very purpose of the protocol-storing such data for accelerated lookups and computations. Moreover, the data is stored in its raw or unencrypted form hence adversarial attacks would reveal the plain data consequently compromising the CIA tenets hence must be resolved.

4. Methodology

This section concisely describes the various techniques employed in revamping DkSAP-IoT dubbed Encryption and decentralized storage-based DkSAP-IoT. Furthermore, we demonstrate how we implement the prototype of the revamped protocol.

4.1. Encryption and Decentralized Storage-based DkSAP-IoT

In this section, we provide vivid details of our proposed enhancements to the current implementation of DkSAP-IoT. A high-level overview of the proposed architecture is pictorially represented in Fig. 1.

To ameliorate the weaknesses identified in the current DkSAP-IoT algorithm [28], we present an enhanced DkSAP-IoT to include encryption/decryption of data in the mobile device with an encrypted backup stored on the decentralized platform IPFS as a countermeasure against hack or theft of the mobile device as depicted in Fig. 1.

The choice of AES specifically AES-256 is due to its efficiency and security guarantees (we explicate on these in sections 6.4 and 6.5). It is one of the best symmetric encryption algorithms and mobile-friendly as well. We provide empirical evidence to buttress these assertions in section 6.4. We posit that key storage can be achieved through cold storage or stored using a secret sharing scheme (SSS) [45].

After updating the shared secret h_{cntB} in step (b) of section *3.1* in the original algorithm, we proceed to perform symmetric encryption followed by storage on IPFS or even better IPNS platform as evident in Fig. 2.

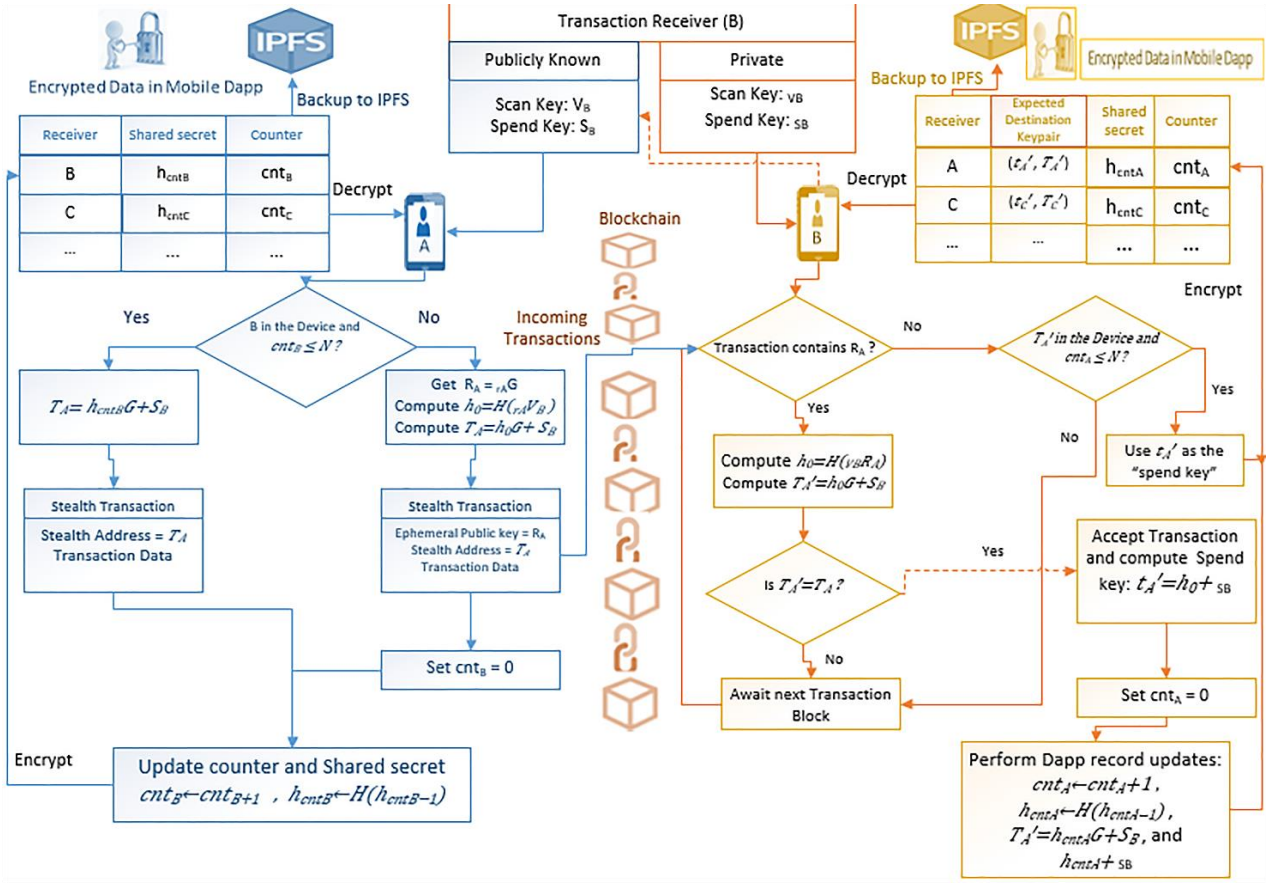

Fig.1. Architecture of Encryption and Decentralized Storage-based DkSAP-IoT.

Algorithm 1: Encryption and decentralized storage for sending transaction

Input: $cnt_B, h_{cntB}, B, userKey$
Output: IPFShash

```
MobileData ← (cnt_B, h_cntB, B)
k ← userKey
encryptedData ← Encrypt(MobileData,k)
encryptedData → IPFS/IPNS
IPFShash ← IPFS/IPNS
return IPFShash
```

Fig.2. Symmetric Encryption in the Improved Protocol.

In a similar fashion, in the course of receiving a transaction, after updating the counter cnt_A, shared secret h_{cntA} and precomputing the anticipated destination key pair or stealth addresses $T_A^{'}$ and $t_A^{'}$ for the next transaction, symmetric encryption followed by backup to IPFS/IPNS is performed demonstrated in Fig. 3.

Algorithm 2: Encryption and decentralized storage for receiving transaction

Input: $cnt_A, h_{cntA}, T'_A, A, userKey$
Output: IPFShash

```
MobileData ← (cnt_A, h_cntA, T'_A)
k ← userKey
encryptedData ← Encrypt(MobileData,k)
encryptedData → IPFS/IPNS
IPFShash ← IPFS/IPNS
return IPFShash
```

Fig.3. Symmetric Encryption and Data Backup Protocol to IPFS/IPNS.

The returned IPFS hash in both cases above can be stored using the same key management technique aforementioned for the AES key. With IPNS available on IPFS, the returned IPNS hash or address can still point to the updated or current encrypted user data stored on IPFS thereby alleviating the need for users to store multiple IPFS hashes hence further simplifying the process of data retrieval. Fig. 4 captures the augmentations to DkSAP-IoT.

Note that unlike the original protocol, our revamped DkSAP-IoT not only guarantees privacy protection or anonymity for transaction recipients but advances other unique features including making it possible for transaction recipients to recover protocol-related data on-the-fly. This way, protocol-related data becomes readily available even amid adversarial attacks. Moreover, our revamped DkSAP-IoT guarantees data integrity pertaining to protocol-related data, something conspicuously missing in the original protocol yet crucial in compliance to security requirements.

4.2. Retrieval of Stored User or Mobile Data on Decentralized Storage Platform

In the event of a hack or theft or loss of the mobile device, users can retrieve their encrypted data on IPFS with just a single query to IPFS as evident in Fig. 5 using the stored hash from the cold storage or reconstruction of the hash from the SSS scheme. The reconstruction process is beyond the scope of this paper hence we proceed on the assumption that users have accessed their required hash.

Using this improved protocol for DkSAP-IoT, the transaction recipient can receive transactions (Data or coin) from the transaction initiator along with secured data retrieval in the event of loss or theft of mobile devices coupled with guaranteed data security courtesy the encryption and decentralized storage mechanism employed.

The transaction recipient also enjoys privacy, extremely strong anonymity and unlinkability of the diverse transactions received [26, 46] since the actual destination of the transaction was a Stealth Address as seen in Fig. 1.

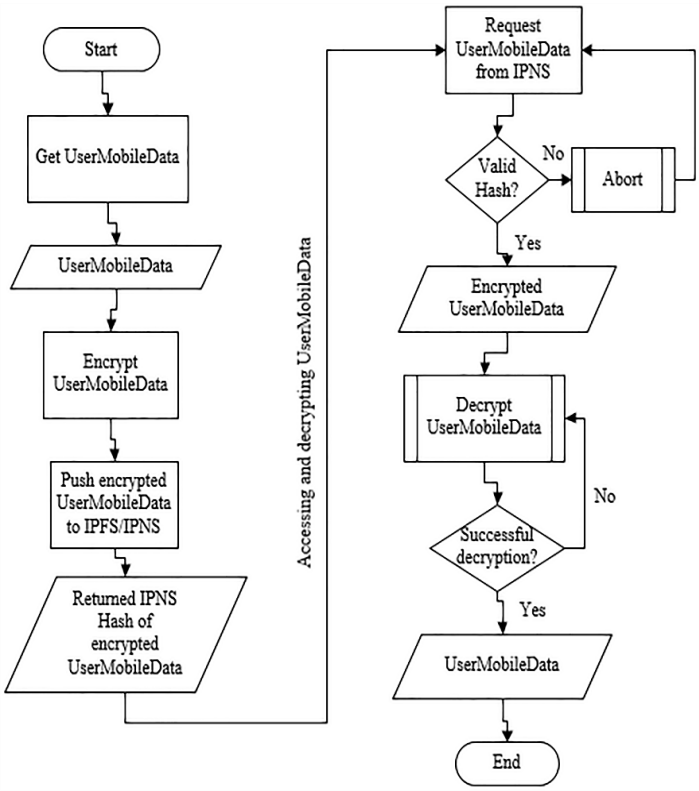

Fig.4. Improvements Made to DkSAP-IoT.

Algorithm 3: Retrieve User Mobile data from IPFS/IPNS

Input: IPFShash, $userKey$ as k
Output: MobileData

```
procedure getUdata():
if IPFS(IPFShash)==True then
    encryptedData ← IPFS/IPNS
    MobileData ← Decrypt(encryptedData,k)
    return MobileData
else
    return 0
end
```

Fig.5. Data Retrieval Protocol from IPFS/IPNS.

4.3. Implementation Details

We implement our proposed encryption and decentralized storage-based DkSAP-IoT by way of developing a web-based application using a JavaScript framework known as Vue.js [47] which provides flexibility for mobile integration as well as script implementation of IPFS and IPNS without the need for users to have a local running instance of IPFS on their devices. The AES encryption and decryption are implemented using Crypto-Js [48] which is a standard and secure cryptographic library implemented in JavaScript. The GitHub link to our solution is *https://github.com/JustNETOrgani/improvedDkSAP-IoT*. The web-based application implies accessibility to all devices (mobile and IoT) with browser capabilities that wish to use the solution.

5. Testing and Validation

This section provides thorough test and validation procedures performed on the proposed solution. We provide experimental results conducted in the Chrome browser on an intel 2.90 GHz processor running on a Windows 10 OS.

5.1. Receiving a Transaction

We proceed to test our solution by mimicking a sent transaction from test data using input fields in the designed application (see Fig. 6). Transaction recipients accept the transaction by on-click of a button (see "Receive transaction" button on Fig. 6) consequently triggering the proposed encryption and decentralized storage as could be seen in Fig. 6 and Fig. 7.

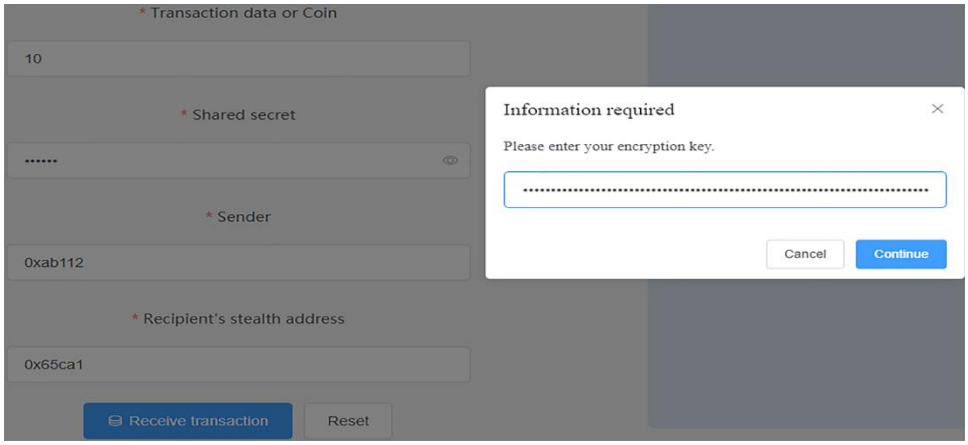

Fig.6. User interface of Symmetric Encryption of Protocol Data.

Fig.7. Storage of Encrypted Data on IPFS/IPNS.

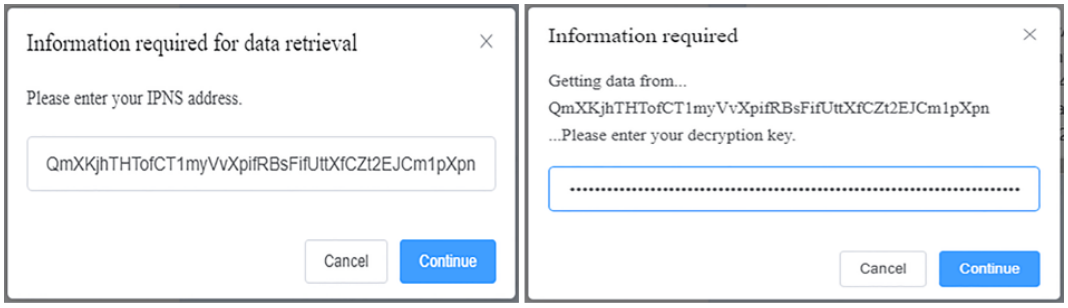

Fig.8. The Data Access (a) Data Recovery (b) Decryption Processes.

5.2. Data Decryption

Whenever required, users can access protocol-related data. We leverage the decentralized nature of IPFS/IPNS to allow users recover protocol-related data as well as transaction data in the event of theft or loss of their devices. This is accomplished by the user entering the IPNS address (see Fig. 8a) which subsequently retrieves data at that location and prompts the user to input the decryption key (see Fig. 8b). Fig. 8 illustrates the data access and decryption processes.

5.3. Experimental Results and Discussion

We conduct extensive experiments on the revamped protocol regarding encryption, data retrieval to simulate data recovery, decryption and throughput. For brevity, we present a snippet of encrypted and decrypted data in Fig. 9.

Fig.9. Encrypted and Decrypted User Data Retrieved from IPFS.

Given that the revamped protocol has inherent communication overhead witnessed during the data upload and download to and from IPFS, in Fig. 10, we show results on throughput as we retrieve diverse data sizes from the decentralized storage hub. This is realized by programmatically (i.e. checking execution time in JavaScript) measuring the time (in *ms*) it takes to store data to and retrieve data from the decentralized storage hub.

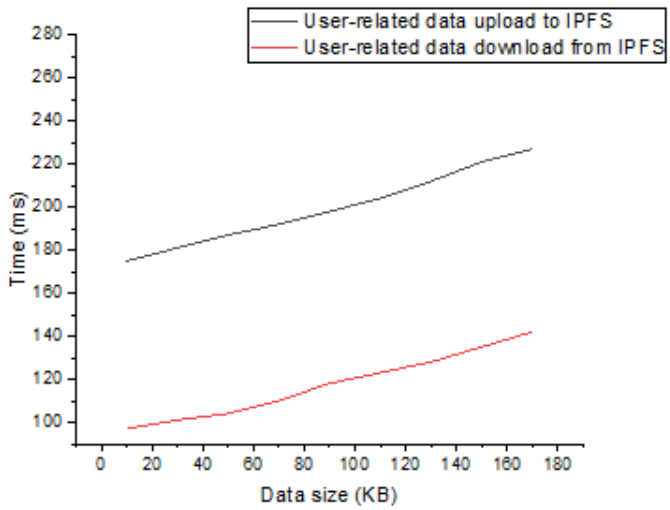

Fig.10. Experimental Result on Throughput.

Notice from Fig. 10 it takes protocol users less than *250ms* and *150ms* to store and retrieve data respectively from IPFS hence attesting to usability.

It is therefore not difficult to see from the experimental results that the revamped protocol satisfies the aforementioned fundamental security requirements. To this end, it becomes imperative for cryptographic researchers and practitioners alike to design cryptographic protocols that meet basic security requirements aside other desirable security guarantees in response to societal dynamics.

6. Security and Protocol Analysis

This section provides a concise security analysis of our proposed solution by expatiating on how our solution adequately satisfies fundamental security principles.

6.1. Data Availability

This security principle seeks to ensure that data is continuously and readily available for access during normal and catastrophic events. Unlike the original DkSAP-IoT protocol, our solution stores the protocol-related data not in the mobile or IoT device but on IPFS which provides a decentralized storage platform as proof of existence making it highly-performant and reliably persistent. Invariably, the proposed solution is robust and resilient to such attacks as DoS and DDoS which can potentially compromise data availability.

6.2. Confidentiality and Privacy

In order to keep information secret consequently avoiding intentional or accidental disclosure to unauthorized entities, our solution uses symmetric encryption, specifically AES-256. This is performed after the completion of the original DkSAP-IoT protocol so that all required protocol-related data are symmetrically encrypted. This way, data privacy and content confidentiality are guaranteed. Moreover, the stealth address utilized makes transactions unlinkable consequently strengthening privacy.

6.3. Data Integrity

Our solution utilizes IPFS/IPNS to store user data and computes SHA-256 hash of content received owing to its content-based addressing scheme. With pre-image resistance, second-pre-image resistance and collision resistance characterized by the underlying cryptographic hash function, it is computationally infeasible for an attacker to change the data stored on the decentralized storage platform and get the same hash. Ultimately, this provides strong guarantee of data integrity.

6.4. Security

We assume users store the AES key securely in our protocol. With this assumption, AES is computationally secure as for key size of 128, 192 or 256 bits, such attacks like brute-force and biclique are computationally infeasible and ineffective. For instance, [49] details that a brute-force attack on AES-128 would mean cycling through $2^{128} = 3.402*10^{38}$ possible key permutations to discover a valid key to decrypt the ciphertext into plaintext. At decryption rate of $10^{13} / s$, an attacker with such computing power would require about $5.3*10^{17}$ years to find the decryption key. Table 1 shows a similar security analysis. Meanwhile, it is also worthwhile to state that AES appears to be a resistant primitive in both the classical and post-quantum era [50].

Table 1. Security Analysis of AES-256.

Key size (bits)	Key pool	Decryption time at a rate of 10^9/s	Decryption time at a rate of 10^{12}/s
256	$2^{256} = 1.16*10^{77}$	2^{255}ns = $1.84*10^{60}$	2^{255}ns = $1.84*10^{57}$

6.5. Feasibility in Resource-constrained Devices

To ascertain the feasibility of the proposed solution in mobile and IoT devices, we perform an evaluation of the solution. We take cue from a variety of recent research works as evident from Table 2.

Table 2. Feasibility of our Proposed Solution in Mobile and IoT Devices.

Reference	Criteria	Results	
[51]	Performance of AES-256-bit encryption in mobile device	Time (ms)	2.151
		Memory (KB)	0.431
		CPU (%)	0.013
	Performance of AES-256-bit decryption in mobile device	Time (ms)	0.69
		Memory (KB)	0.431
		CPU (%)	0.014
[28]	Computations involved in DkSAP-IoT	Update of the shared secret with hash function results in about three orders of magnitude faster computation. Reduced transaction size and overall cost less than 50% of DKSAP.	

Carefully analyzing the revamped solution from security and protocol perspectives reveal some key findings as follows:

- Based on the compelling evidence from Table 2, we assert that our proposed solution is mobile and IoT-friendly.
- Even amid adversarial attacks, the user can always recover protocol-related data from the decentralized storage hub.
- The user can always be rest assured that protocol-related data have not been tampered with.
- Blockchain-based transaction is privacy-preserving and so is protocol-related data owing to the confidentiality integrated into the revamped protocol.

7. Conclusion and Future Work

Data confidentiality, integrity and available are undoubtedly fundamental security principles required in information systems and the design of security protocols. This work presents a modified implementation of Dual-Key Stealth Address Protocol for IoT (DkSAP-IoT) that guarantees confidentiality, integrity and availability of protocol-related data unlike the original protocol. We realize such fundamental security requirements via encryption and decentralised storage paradigm. Security and protocol analysis of the proposed solution indicate that the solution not only allows transaction recipients to anonymously receive their transactions but also guarantees data security and satisfies the renowned CIA triad. The code is publicly made available on GitHub thus paving way for the development of privacy-centric and data security-minded DkSAP-IoT protocols for transaction recipients. This research will be useful in the development of privacy-preserving protocols based on blockchain systems consequently affording users the opportunity to enjoy anonymous payments while guaranteeing confidentiality, integrity and availability of protocol-related data. Our future task would be to develop a fully-fledged mobile application for the solution presented.

Acknowledgment

This work was supported by the Key Research on Cyberspace Security Data Analysis, Sichuan Provincial Department of Education [grant number 17zd1119]; National Natural Science Foundation of China (Youth), Image Source Forensics Security Research [grant number 61702429].

References

[1] Nakamoto, S., *Bitcoin: A Peer-to-Peer Electronic Cash System. Whitepaper (2008)*. 2009.
[2] Wood, G.J.E.p.y.p., *Ethereum: A secure decentralised generalised transaction ledger.* 2014. 151: p. 1-32.
[3] Cachin, C. *Architecture of the hyperledger blockchain fabric*. in *Workshop on distributed cryptocurrencies and consensus ledgers*. 2016.
[4] Sultan, K., U. Ruhi, and R.J.a.p.a. Lakhani, *Conceptualizing Blockchains: Characteristics & Applications.* 2018.
[5] Zheng, Z., et al. *An overview of blockchain technology: Architecture, consensus, and future trends*. in *2017 IEEE International Congress on Big Data (BigData Congress)*. 2017. IEEE.
[6] Joshi, A.P., M. Han, and Y.J.M.F.o.C. Wang, *A survey on security and privacy issues of blockchain technology.* 2018. **1**(2): p. 121-147.
[7] Islam, M.R., et al. *A Review on Blockchain Security Issues and Challenges*. in *2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC)*. 2021. IEEE.
[8] Harshini Poojaa, K. and S. Ganesh Kumar, *Scalability Challenges and Solutions in Blockchain Technology*, in *Inventive Computation and Information Technologies*. 2022, Springer. p. 595-606.
[9] Möser, M., et al., *An empirical analysis of traceability in the monero blockchain.* 2018. 2018(3): p. 143-163.
[10] Meiklejohn, S., et al. *A fistful of bitcoins: characterizing payments among men with no names*. in *Proceedings of the 2013 conference on Internet measurement conference*. 2013.
[11] Motamed, A.P. and B.J.A.N.S. Bahrak, *Quantitative analysis of cryptocurrencies transaction graph.* 2019. 4(1): p. 1-21.
[12] Gaihre, A., Y. Luo, and H. Liu. *Do bitcoin users really care about anonymity? an analysis of the bitcoin transaction graph*. in *2018 IEEE International Conference on Big Data (Big Data)*. 2018. IEEE.
[13] Goldfeder, S., et al., *When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies.* 2018. 2018(4): p. 179-199.
[14] Yuen, T.H., et al., *Efficient linkable and/or threshold ring signature without random oracles.* 2013. 56(4): p. 407-421.
[15] Malina, L., et al. *Lightweight Ring Signatures for Decentralized Privacy-preserving Transactions*. in *Proceedings of the 15th International Joint Conference on e-Business and Telecommunications, Porto, Portugal*. 2018.
[16] Liu, J.K., et al., *Linkable ring signature with unconditional anonymity.* 2013. 26(1): p. 157-165.
[17] Yang, X., et al. *Lightweight anonymous authentication for ad hoc group: A ring signature approach*. in *International Conference on Provable Security*. 2015. Springer.
[18] Wang, L., et al., *Cryptographic primitives in blockchains.* 2019. 127: p. 43-58.
[19] Miers, I., et al. *Zerocoin: Anonymous distributed e-cash from bitcoin*. in *2013 IEEE Symposium on Security and Privacy*. 2013. IEEE.
[20] Danezis, G., et al. *Pinocchio coin: building zerocoin from a succinct pairing-based proof system*. in *Proceedings of the First ACM workshop on Language support for privacy-enhancing technologies*. 2013.
[21] Mizel, P., F. Raetz, and G.J.A.F. Schmuck, Zug, Switzerland, Tech. Rep, *Asure: First scalable blockchain network for decentralized social security systems.* 2018.

[22] Sasson, E.B., et al. *Zerocash: Decentralized anonymous payments from bitcoin*. in *2014 IEEE Symposium on Security and Privacy*. 2014. IEEE.[23] Andrychowicz, M., et al. *Secure multiparty computations on bitcoin*. in *2014 IEEE Symposium on Security and Privacy*. 2014. IEEE.
[24] Cramer, R., I.B. Damgård, and J.B. Nielsen, *Secure multiparty computation*. 2015: Cambridge University Press.
[25] ByteCoin. *Untraceable transactions which can contain a secure message are inevitable*. 2011, Bitcoin Development & Technical Discussion Forum.
[26] Courtois, N.T. and R. Mercer. *Stealth Address and Key Management Techniques in Blockchain Systems*. in *ICISSP*. 2017.
[27] Al-Fawa'reh, M. and M.J.I.J. Al-Fayoumi, *Detecting stealth-based attacks in large campus networks.* 2020. 9(4).
[28] Fan, X. *Faster dual-key stealth address for blockchain-based internet of things systems*. in *International Conference on Blockchain*. 2018. Springer.
[29] Todd, P. *Stealth Addresses*. 2014, Available online: http://www.mailarchive.com/bitcoindevelopment@lists.sourceforge.net/msg03613.html, Accessed: June 8, 2020.
[30] Hasan, H.R. and K.J.I.A. Salah, *Combating Deepfake Videos Using Blockchain and Smart Contracts.* 2019. 7: p. 41596-41606.
[31] Hasan, H.R. and K.J.I.A. Salah, *Proof of delivery of digital assets using blockchain and smart contracts.* 2018. 6: p. 65439-65448.
[32] Nguyen, D.C., et al., *Blockchain for secure ehrs sharing of mobile cloud based e-health systems.* 2019. 7: p. 66792-66806.
[33] Cao, S., et al., *Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain.* 2019. 485: p. 427-440.
[34] Wang, Y., et al., *Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain.* 2019. 7: p. 136704-136719.
[35] Verizon, *Verizon: 2019 Data Breach Investigations Report.* Computer Fraud & Security, 2019. 2019(6): p. 4.
[36] Symantec, *Internet Security Threat Report.* 2019, Available online: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf, p. 1-61.
[37] Yu, G.J.I.C.e.A., *Blockchain Stealth Address Schemes.* 2020. 2020: p. 548.
[38] Williamson, Z.J., *The aztec protocol.* Available online: https://github.com/AztecProtocol/AZTEC , 2018.
[39] Bernabe, J.B., et al., *Privacy-preserving solutions for Blockchain: review and challenges.* 2019. 7: p. 164908-164940.
[40] Nieles, M., K. Dempsey, and V. Pillitteri, *An introduction to information security*. 2017, National Institute of Standards and Technology.
[41] Benet, J., *Ipfs-content addressed, versioned, p2p file system*, arXiv preprint arXiv:1407.3561 2014.
[42] IPNS. *Inter-Planetary Name System*. 2019; Available from: https://docs.ipfs.io/guides/concepts/ipns/.
[43] Zhong, P., et al. *Privacy-Protected Blockchain System*. in *2019 20th IEEE International Conference on Mobile Data Management (MDM)*. 2019. IEEE.
[44] Yadav, V. and R. Mathew. *Analysis and Review of Cloud Based Encryption Methods*. in *International conference on Computer Networks, Big data and IoT*. 2019. Springer.
[45] Miao, F., et al., *A (t, m, n)-group oriented secret sharing scheme.* 2016. 25(1): p. 174-178.
[46] Courtois, N.T. *Anonymous Crypto Currency-Stealth Address,Ring Signatures, Monero. Comparison to Zero.Cash*. 2017, Available from: http://www.nicolascourtois.com/bitcoin/paycoin_privacy_monero_6g_Paris28032017.pdf.
[47] Vuejs. *Vue.js: The Progressive JavaScript Framework*. 2021; Available from: https://github.com/vuejs/vue.
[48] *Crypto-js: JavaScript library of crypto standards*. 2017; Available from: https://github.com/brix/crypto-js.
[49] Stallings, W., *Cryptography and network security: principles and practice*. 2017: Pearson Upper Saddle River.
[50] Bonnetain, X., M. Naya-Plasencia, and A.J.I.T.o.S.C. Schrottenloher, *Quantum security analysis of AES.* 2019: p. 55-93.
[51] Rachmat, N. *Performance Analysis of 256-bit AES Encryption Algorithm on Android Smartphone*. in *Journal of Physics: Conference Series*. 2019. IOP Publishing.

Authors' Profiles

Justice Odoom obtained his BSc and MSE degrees in Computer Science from Data Link University, Tema, Ghana and Southwest University of Science and Technology, Mianyang, China, in 2015 and 2020 respectively. He is currently pursuing his Doctoral degree with the School of Computer Science and Technology, Southwest University of Science and Technology, China and is a certified Elsevier and Publons academy peer reviewer. His research interests include information security, blockchain technology, ring signatures and privacy-preservation in the sharing of Electronic Health Records (EHRs). He is a member of IEEE and IEEE Computer Society.

Huang Xiaofang received the Ph.D. degree from the Beijing University of Posts and Telecommunications in 2010. She is currently a professor with the school of computer science and technology, Southwest University of Science and Technology, Mianyang, China. Her main research interests include information security, cloud computing, and blockchain technology. She got the information security leading talent award of the district level in 2015.

Samuel A. Danso obtained his first degree in Computer Science in Ghana and Master's degree in Telecom Technology at SMU-India in the year 2012. He is a full-time lecturer, Ghana Communication Technology University-Ghana and obtained the PhD degree from Southwest University of Science and Technology Mianyang-China in the year 2022. His area of research interests includes terahertz active imaging and security on-line and data communications.

Richlove S. Soglo obtained his BSc in Information Technology from Ghana Technology University College, Accra, Ghana in 2018 and holds MSE in Computer Science and Technology from Southwest University of Science and Technology, China. His research interests include blockchain technology, supply chain management and Internet of Things (IoT).

Benedicta N. E. Nyarko obtained her BSc. Information and Communication Technology from Data Link University, Tema-Ghana and MEng. Information and Communication Engineering, from Southwest University of Science and Technology, Mianyang-China. She is currently a Doctoral Candidate in Control Science and Engineering at Southwest University of Science and Technology, Mianyang-China. Her Research Include, Machine Learning, and Pattern Recognition.

How to cite this paper: Justice Odoom, Huang Xiaofang, Samuel Akwasi Danso, Richlove Samuel Soglo, Benedicta Nana Esi Nyarko, "Revamped Dual-key Stealth Address Protocol for IoT Using Encryption and Decentralized Storage", International Journal of Computer Network and Information Security(IJCNIS), Vol.15, No.1, pp.14-25, 2023. DOI:10.5815/ijcnis.2023.01.02