International Journal of Scientific Research and Management (IJSRM)
||Volume||11||Issue||08||Pages||904-913||2023||
Website: https://ijsrm.net ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v11i08.ec01

Remote execution of physical tasks by putting into contribution DOSN: Case of Money Transfer

Jean-Pierre Lienou[1], Thierry Noulamo[2] and Alain Djimeli-Tsajio[3]

[1] Department of Computer Engineering, University of Bamenda
College of Technology, Bamenda, Cameroon
[2] Department of Computer Engineering, University of Dschang
Fotso Victor University Institute of Technology, Bandjoun, Cameroon
[3] Department of Telecommunication and Network Engineering, University of Dschang,
Fotso Victor University Institute of Technology, Bandjoun, Cameroon

Abstract
Distributed Online Social Networks (DOSN) provide some advantages that are not yet fully exploited. It can help reduce cost especially when it comes to manage remote physical agents to fulfill some tasks under delegation of other agents that are weakly coupled. This paper tackles the problem of structuring and organizing such a network and a case study is applied on international money transfer. Recent studies showed that the difference between the amounts of money transfer between less developed and developed countries is not too high. The money transfer institutions are widespread but at international level, only few companies share the market giving the lion share to Western Union and Moneygram. Building a social network of "gentlemen" can transform two international transfers to two or more national transfers. It can then reduce the charges of international transfers, speed up at time the process of money transfer, include more people that are outside the banking system. A prototype is constructed using three key concepts to solve arisen problems. Firstly, the gentlemen approach uses some kind of godfather relationship used in most djangui unions in Cameroon to welcome new members. The graph database Neo4J was chosen to ease the process of identifying the chain of godfathers in case a "bad guy" joins and abuse members of the network. Secondly, the knapsack problem (KP) in all its varieties is implemented in the case the amount to be transferred from one country to another could not match a one-to-one relationship. Thirdly, a signcryption mechanism is used to solve the cryptographic functionalities that occur during message exchanges on the platform. Due to the fact that such social network has to dealt with trust, reputation, privacy and security, it can be considered as a powerful tool for investigating societal problems such as financing terrorism or deception on the Internet. A game theory can then be applied to detect the conditions making the network not interesting to hackers.

Keywords: *contribution DOSN, Money Transfer*

1. Introduction

For several decades, massive movements of populations have been made from one part of the terrestrial globe to another part in the search for peace, for quality education or to simply leave the difficult economic or climatic conditions. Although perilous, these displacements result in loss of human lives and a percentage of the displaced manage to stabilize somewhere. Living conditions sometimes get worse but also in some cases better. When living conditions get worse, the group of people that stayed behind finances the urgent basic needs of the displaced by sending money into a more or less formal banking or money transfer system. Needless to say, the displaced are outside the formal banking system most of the time. If conditions improve, we see the opposite effect and the displaced person finances certain activities of the members of his family who remain there. In both cases, the companies that share the international transfer costs, sometimes at exorbitant rates, do not participate in solving the problem of poverty. The clear observation nowadays is that

the critical mass of displaced persons or emigrants achieve a sufficient balance to initiate the fall in transfer or transfer fees between the monetary masses which move in both directions in a global manner. It is aberrant that transfers are made in both directions when one can replace two international transfers with two or more national transfers using network technology. To solve this problem, we propose a social network which will be responsible for connecting people with complementary needs so that they can help each other to meet their needs with their own or with people from little doubtful morality. This solution makes it possible to transform an international transfer into national transfers which is much less expensive because for the same amounts, the international transfer can cost up to five times more than a national transfer. It's obvious that each member participating in a transfer has a moral obligation to pay the other side of the transaction.

Once you integrate the technology, it stands to reason those men of no integrity will infest the system with all the possibilities of fraud (payment has a meaning, money laundering, etc.). It is difficult to build such a trusted system online. Several problems arise. How do you track down honest and dishonest members of the group? Identify them, manage their requests, check that each member has fulfilled their obligations, etc.

There are several ways to transfer money, each with its drawbacks and advantages. The advantages often optimize the parameters of readiness to pay, speed while the disadvantages are often security, high transfer fees, fraud, money laundering. Although electronic money is getting off to a good start to replace fiat money, the latter still has a bright future ahead. The system proposed here emphasizes transfer fees and certain aspects of fraud such as money laundering. Most money transfer technologies revolves around telephony systems, SWIFT.

The majority of organizations specializing in the transfer of funds encounter limitations, among which we can cite:

- The first limitation of money transfer is that these financial organizations that offer this kind of service are unfortunately limited in the scope of their network;
- Money transfers are limited based on the maximum amount you can send;
- The main problem with these international transfers lies in their cost, which is still considered expensive by users.

This last argument by applying it to the case of Cameroon, for example, shows that nearly 10% of the sums transferred remain in the transfer fees. The main objective is to reduce this amount and allow the transferred amounts to be more useful for the actions for which they are meant to be. To reduce charges, we propose to build a platform capable of connecting senders and recipients from different sides so that the senders in turn send the money directly to each other without going internationally. The problems generated are trust, compatibility of amounts, deadlines for disbursement of funds. In terms of trust, we offer a social network based on sponsorship that can be easily implemented on a graph database, in this case Neo4j; for the compatibility of the amounts, we use one of the variants of the KP depending on the case, for the deadlines, a careful analysis of the information system and for security, signcryption which minimizes the exchange of data on the network, reduce computational power and no need to use certificates.

The objective of this paper is to present an architecture making it possible to reduce the costs of money transfer through the construction of a social network of average security level but allowing to provide a solution to the problem of money transfer. which is increasingly seen as a deterioration in the terms of trade between countries in the north and those in the south. Such a Framework can be used as a real online transfer tool by taking several precautions to eliminate the unscrupulous from the network, but also as a platform dedicated to understand the behavior of the Internet user in a fraud situation and thus explore avenues. and propose solutions for cyber deception. This transfer situation in the event of unequal amounts results in the combination of other sending possibilities to cover the amount to be sent in the opposite direction to meet up with the larger amount. There are several variations of the KP where we believe the most universal case is the hybrid knapsack algorithm. Section II presents the materials and methods used, section III the implementation and obtained results, section V will be a conclusion and perspectives. A section of appendixes closes the paper

2. Materials and Methods

With the fact that the topic under consideration can be reapplied in many other areas, we have chosen for simplicity to apply to money transfer. In this section we present the state of the art of problems the domain may be facing depending of the community.

The Money Transfer can be resumed by the existence of formal ways and unformal ways. With formal ways, there is a disadvantage of the charges that may be high. Interested parties must be identified. The delay is average depending on the chosen method among the formal ones [1]. The non-formal ones have the charges that are very low, parties may not be formally identified.
Depending on categories in table 1, Category 1 like Swift sends only messages and other banks do the clearing and have mutual compensation. In order to collect the transferred money, you must be formally identified and the transfer may take a few hours to days. The risk is too low unless the parties are under restrictions. In our system, two international demands are transformed to two or more national transfers. The platform just put the parties in relation. It can incorporate a clearing system or not. The version under test does not clear the funds.

Table 1 Characterization of some money transfer systems

	Sample of System	Charges	Clearing	Formal identification	Scope	Expected delay	Taken risk
Category 1	SWIFT	High	NO	YES	Their Network	Medium	Low
Category 2	CHIPS, CHAP, FEDWIRE	High	YES	YES	Their Network	Medium	Low
Category 3	MoneyGram, Western Union, Cooperatives, MFI, etc.	Average	Agreement	Yes	Their Network	Medium	Average
Category 4	Telephone Companies	Low	Agreement	Somehow	Their Network	Low	High
Non-Formal	Coach Courrier	Low	Yes	Somehow	Their Network	Medium	High
	Diaspo Transfer	Very low	No	No	Social Network	Fast or Low	Average

The money Transfer problem can be related to Knapsack Problem as follows. From country A there are N demands to transfer various sum to another country B and from B there are M demands to transfer to country A. Each demand is characterized by some properties such as Amount, fractionality, latest expected date to be sent, etc. Furthermore, in order to transfer, there is a table from which the client can know the charges to be paid as the platform dues. Positioning ourselves on the platform perspective, the charges is perceived as the Profit or value, the amount to be sent as the Weights. The maximum of the amounts from one side is to be used as the amount not to be above and known in the KP as Capacity [7, 8, 9]. After solving for one case, all the demands that were retained are removed from the system and the remaining demands are reused in the algorithm iteratively until the residual demands are left aside waiting for new demands or the owners are informed that it could not be solved at the moment. He is then left with the choice to wait for new demands or to cancel his demand.

The KP concerns the selection from a set of n given items, each having weight and value, a subset of items with weight sum not greater than capacity and whose profit is the maximum. The KP can be classified broadly in two categories. The 0/1 which is solved mainly using branch and bound or dynamic programming and the fractionable, solved using greedy methods. For the Knapsack Problem 0/1 there are so many specialized cases that have been recently under investigations. Some sub cases are: Subset Sum Problem (SSP), the Strongly Correlated 0-l KP (SCKP), the Inverse Strongly Correlated 0-1 KP and the BKP (BSSP and BSCKP) [2].

The security in a wireless mobile environment that is inherent to social network members environment coupled with equipment having less memory, battery and not powerful computational means directed us to use signcryption. One of the methods that can provide confidentiality of messages, authentication of messages and their senders, forward secrecy and public verifiability is signcryption. In the context of social network, the multi-authority [12] multi-message and multi-receiver scheme [4] properties are desired.

2.1. Data Collection and Materials used

Many charges have been investigated and the average ones are from RIA. The current applicable charges are in table 2.

International Journal of Scientific Research and Management (IJSRM)
||Volume||11||Issue||08||Pages||904-913||2023||
Website: https://ijsrm.net ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v11i08.ec01

Max Bound	WAEMU		Other African Countries		International		
Amount	Charges HT	Total	Charges HT	Total	Charges HT	Total	Server charges
15000	939	969	822	852	3645	3675	920
25000	1023	1073	910	960	5265	5315	1330
50000	1929	2029	1761	1861	6075	6175	1545
60000	2738	2858	2373	2493	6885	7005	1750
100000	4960	5160	3518	3718	9315	9515	2380
120000	5262	5502	4415	4655	10935	11175	2795
150000	6155	6455	5208	5508	13365	13665	3415
180000	6885	7245	6201	6561	15795	16155	4040
210000	8977	9397	7459	7879	19035	19455	4865
240000	9564	10044	8952	9432	23895	24375	6095
270000	9581	10121	9375	9915	26325	26865	6715
300000	11543	12143	9774	10374	31995	32595	8150
400000	13677	14477	11593	12393	36045	36845	9210
600000	17266	18466	14776	15976	41715	42915	10730

Table 2 Sending intervals of money and their charges in average in RIA, Cameroon April 2022

In Table 2, the Max bound represents the maximum of the interval and charges HT shows the charges without tax and Total includes the 0.02% taxes from the financial law applicable since 2021 financial year. From this table 1, we are to use the column International since the target for the system is on the international transfers. For national transfers, much more lower prices existed and the best ones can be found with telecommunication companies and some banks or micro finance institutions.

2.2 Modeling our solution as a Knapsack Problem

The KP as in literature can be broadly classified depending on the exactitude of the solution, the objectives, the choices and so on. We can identify the Bounded Knapsack Problem (BKP), the Unbounded KP (UKP) which can be solved using Dynamic Programming or Branch & bound Algorithms with their variants. Many other exotic variants exist such as the Quadratic, the Multiple Choice and the Multi objectives KP which are solved using Lagrangian relaxation or Pisinger algorithm.

The initial system can be perceived as on Figure 1.

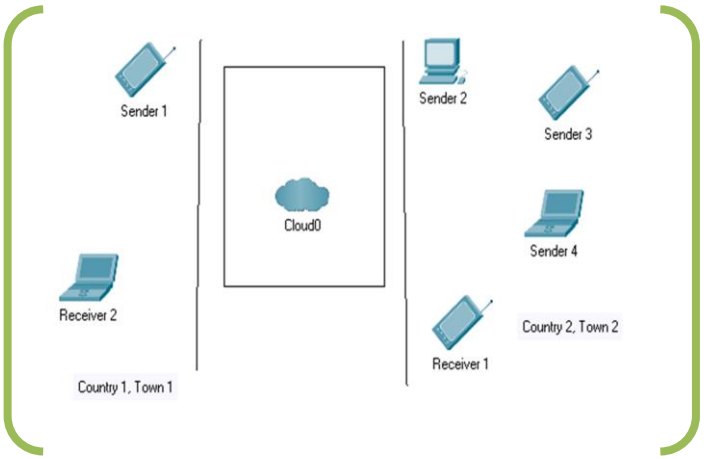

Figure 1 Initial situation for clients ready to fill a demand on the platform

From table 2, the objective is to charge at the level of the server an arbitrary amount base on the amount of RIA. We have chosen ¼ of the charges to represent values or in other words our profits, the weights are represented by the total charges + taxes. The capacity is modeled as the current amount in the interval. To make it simple, the taxes are not recomputed and the weights are divided by 1000. So, the vector used to determine the values is (15, 25, 50, 60, 100, 120, 150, 180, 210, 240, 370, 300, 400, 600). The capacity is the amount to be sent divided by 1000 and is the ceil value in the above vector.

2.3. Modeling the security

To avoid phishing, we use the concept of Godfather and to secure communications, the lightweight signcryption mechanism is implemented.

Signcryption consists of 3 essential functions: KeyGen, SigEnc and VerDec. Let us suppose that 2 people A and B wish to communicate: - KeyGen allows to generate a pair of keys (SDKA, VEKA) and (SDKB, VEKB) where VEKA, VEKB are public and SDKA, SDKB are private - SigEnc (SDKA, VEKB) for sign encrypt the message - VerDec (VEKA, SDKB) to de-sign the message. Multiple implementations can be as per the algorithms in [5, 11].

The implementation used is the one in [4].

2.4 The signcryption and unsigncryption processes

Hyper Elliptic Curve Cryptography is a special case of elliptic curve where the genus g ≥ 2,

HECC used can be defined over Fq (finite field) and defined by

$y^2 + h(x)y = f(x) \bmod q$ (1)

Where h(x) ∈ F[x] is a polynomial where the degree of h(x) ≤ g and f (x) ∈ F[x] is a polynomial known as monic polynomial and the degree of f (x) ≤ 2g + 1. The ultimate objective is to form a jacobian group JC (Fq), and select a divisor D (which is generator of JC group). The mumford representation of D is

$$D = \big(a(x), b(x)\big) = \left(\sum_{i=0}^{g} a_i x^i, \sum_{i=0}^{g-1} b_i x^i\right) \in J_c(F_q)$$

Unsigncryption

The signcryption routine Signcryption *(k,da, m,Pb, Pa*) is used to compute signcrypted text, after obtaining *Pb* (the receiver public key).

Signcryption *(k,da, m,Pb, Pa)*

- Select a random scalar *k* where *(k* ∈ 1,2,3,*n* - 1*)*
- *(K*1*) = h(φ(kD))*
- *(K*2*) = h(φ(kPb))*
- *C = EK*2*(m)*
- Compute *r = hK*1*(m||bind inf o)*

– Compute $s = (r+Kda) \bmod n$
– Compute $R = rD$

Therefore, the Signcrypted transmitted text is (c, R, s).

Unsigncryption

At Receiver end for converting Signcrypted text into plan text Unsigncryption (k,Pb,Pa,db,h, c,R, s) function is used to reverse the signcryption just after receiving the signcrypted text.

Unsigncryption (Pb,Pa, db,h,c, R,s)

– Compute $(K1,K2)$
– $(K1) = H(\varphi(s(Pa + R)))$
– $(K2) = H(\varphi(s(db(Pa + R)))$
– Compute $m = DK2(c)$
– Compute $r = hK1(m||bind\ inf\ o)$
– Check $rD =? R$, if true accept the message, else reject

For each member of the social network supposed to send money, he must be in a path from founder members to its position in the database graph. The maximum amount a person can send is the total amount the chain can be used from the godfathers. The concurrency problem should be avoided. Once the money has been paid on both sides, the godfathers' money is released and ready to be reused. The exchanged messages on the platform is done with a signcryption mechanism. The reason for choosing such mechanism is that the signcryption's cost is lower than the classical signature and encryption. Most of the time the parameters to assess a signcryption implementation model is the use of certificates [3] the number of receivers [10] and also the used concepts and its complexity [11].

3. Implementation of the new Algorithm

The partial ER model with pertinent fields corresponds to the one in Figure 2. Here the ApproximationPercentage indicates up to which amount it could be approximated. Fractionnable indicates the maximum number of fractions that could be acceptable. From Figure 1, the KP obtained can be perceived as a hybrid one since the Fractionnable parameter can transform it as an Unbounded if the value is -1 to a 0/1 if its value is 1 that means not fractionable, or a certain number that gives the maximum number with which the number of fractions can be up to. According to us, no variant of KP takes into account such number of cases.

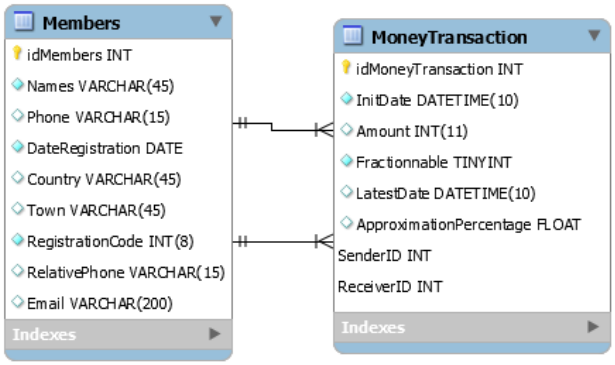

Figure 2 ER model of the used fields

The algorithms used and their variants

First of all, a test is done to identify the type of knapsack to be applied.

3.1 0/1 Algorithm of Knapsack Problem

KNAPSACK (n, W)

1. for w = 0, W
2. do V [0,w] ← 0
3. for i=0, n

4. do V [i, 0] ← 0
5. for w = 0, W
6. do if ($w_i \leq w$ & v_i + V [i-1, w - w_i]> V [i -1,W])
7. then V [i, W] ← v_i + V [i - 1, w - w_i]
8. else V [i, W] ← V [i - 1, w]

The algorithm for the fractional knapsack is presented in pseudocode 2

3.2 Fractional Algorithm of Knapsack Problem

Fractional Knapsack (Array v, Array w, int W)

1. for i= 1 to size (v)
2. do p [i] = v [i] / w [i]
3. Sort-Descending (p)
4. i ← 1
5. while (W>0)
6. do amount = min (W, w [i])
7. solution [i] = amount
8. W= W-amount
9. i ← i+1
10. return solution

Profit	0	50	52	64	94	200	252					
Weights	0	0.96	1.33	2.66	3.16	4	4.53					
Profit	Weight	Item i	0	1	2	3	4	5	6	7	8	9	10
50	0.96	1	0	50	50	50	50	50	50	50	50	50	50
52	1.33	2	0	50	52	102	102	102	102	102	102	102	102
64	2.66	3	0	50	52	102	114	116	166	166	166	166	166
94	3.16	4	0	50	52	102	114	144	166	196	208	210	260
200	4	5	0	50	52	102	200	250	252	302	314	344	366
252	4.53	6	0	50	52	102	200	252	302	304	354	452	502

Figure 3 A snapshot of sample of application with dynamic programming

3.3. Hybrid Algorithm of Knapsack Problem

This algorithm is applied when the situation is not a 0/1 and also not a fractionable up to infinity.

Hybrid Knapsack (Array v, Array w, Array f, int W)

1. for i= 1 to size (v)
2. do p [i] = v [i] / w [i]
3. Sort-Descending_with (p, f)
4. i ← 1
5. while (W>0)
6. do amount = min_spec (W, w [i], f[i])
7. solution [i] = amount
8. W= W-amount
9. i ← i+1
10. return solution

The function min_spec() takes into account the number of fractions acceptable before being used in the computation of the minimum value.

4. Results

A CQL query is launched to have all the current transfers. The maximum in terms of weights on both directions is the capacity for the knapsack algorithm. Once selected, we use only the queries that satisfy the other criteria such as deadline, amount, fractionality.

4.1 Architecture of the System

The solution proposed in this work is to build a social network that makes it possible to put money transfer actors together at minimal cost and with an acceptable level of security. The choice of a social network results from the fact that additional functionalities are planned such as the monitoring of projects with actors such as notaries and also social networks are widely used nowadays between various communities.

4.2 System representation

Initial state of a sample case study is represented in Fig 4. In order not to present the multitude of cases that may exist, we present in figure 3 the initial case.

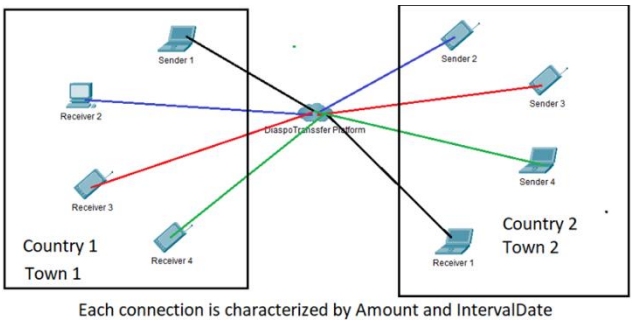

Fig. 4 Initial sample case study after deployment

Initially in this scenario, we have 2 countries and each having one town from which members have submitted their demand to transfer money on our platform. For simplicity, we have 4 members which are senders. One from Country 1 and 3 from country 2. The number of receivers is then the opposite.

Each connection is characterized by the Sender, the Receiver, the Amount to be sent, a dateline the senders will not send the money if there is no compatible case found by then and also specify if the transaction can be fractioned to compensate and get near to the amount to be transferred.
The minimal information needed for such a transaction is represented on fig 2 on the ER diagram.
The RelativePhone can be used for other technical reasons that are not going to be discussed in this paper. The approximationpercentage property let transfer not the total amount but an amount that is near it if the KP fails to propose an exact solution. The role of other attributes can be guessed from their respective labels. A new member is created using the interface form in Fig 5.

Figure 5 Registration form

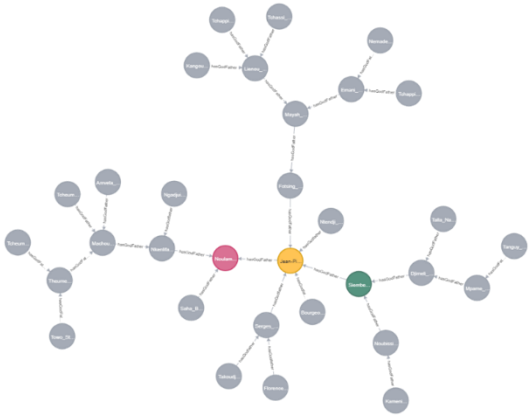

Figure 5 Result of CQL query on Godfathers relationship

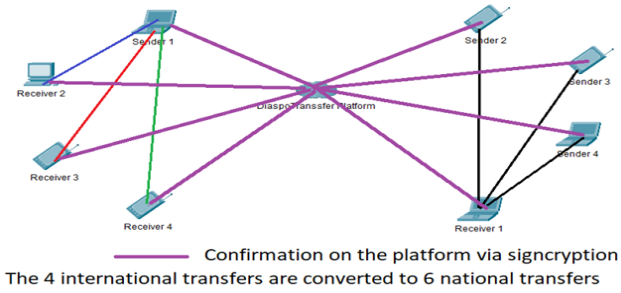

Figure 4 Reconfiguration of transfer statuses after partners confirmed they have paid or received

5. Conclusion

In this paper, we have proposed the use of DOSN to lower the fees needed to control remote tasks monitored by weakly coupled agents. The application is done on a traditional money transfer system. A Matchmaking website is developed and some members (Money Senders) are assumed to be members of the DOSN while money receivers may or not be members. In a nutshell, two or more international money transfers are combined to balance and transformed to local money transfers. The charges are then composed of two parts. The classical local charge (e.g., telecommunication operators or MFI) and a fraction to pay to the platform for matching the demands. The management of the members is guided with a sort of godfather relationship found in Bamileke associations in West Cameroon. Some details are explained in [6].

The relationships among members are easily found using a graph database Neo4J with the queries done in the Cypher Language. The profit of the platform is being optimized using a peculiar Knapsack Problem algorithm adapted for the properties of money transfer. The number of cases is not high as the ones in the literature and therefore a solution using an exact method was used. The modified algorithm presented and tested on a very simple case. According to us, this is a new KP having a kind of hybrid situation not found in KP in the literature. A data structure is proposed and the adaptation of the KP to take into account the hybrid process of 0/1 and partially fractionable with an upper bound in the fractionality is implemented.
The system should be usable in an environment with less computational power. Therefore, the coded security system is a signcryption algorithm based on Hyper Elliptic Curve cryptosystem which is recognized as a very low processing resource since it requires a lightweight encryption and authentication algorithm [4]. Merging the multi-authority data access control scheme feature is to be done in next version of the system. The next step should also include different currencies including digital money such as Bitcoins and others to see how the system will become more secure and flexible and take into account people from countries that have switched to the use of digital currency officially as Central African Republic since few weeks.

References

1. Auvolat, A., Frey, D., Raynal, M., Taïani, F., Money, F. T., & Taani, F. (2020). Money Transfer Made Simple. https://hal.archives-ouvertes.fr/hal-02861511v1

2. Caccetta, L., & Kulanoot, A. (2001). 1 ALGORITHMS FOR SOME HARD KNAPSACK PROBLEMS.
3. Cao, L., & Ge, W. (2018). Analysis of certificateless signcryption schemes and construction of a secure and efficient pairing-free one based on ECC. KSII Transactions on Internet and Information Systems, 12(9). https://doi.org/10.3837/tiis.2018.09.022
4. Ch, S. A., uddin, N., Sher, M., Ghani, A., Naqvi, H., & Irshad, A. (2015). An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography. Multimedia Tools and Applications, 74(5), 1711–1723. https://doi.org/10.1007/s11042-014-2283-9
5. Daniel, R. M., Rajsingh, E. B., & Silas, S. (2021). A forward secure signcryption scheme with ciphertext authentication for e-payment systems using conic curve cryptography. Journal of King Saud University - Computer and Information Sciences, 33(1). https://doi.org/10.1016/j.jksuci.2018.02.004
6. Guidi, B., Conti, M., Passarella, A., & Ricci, L. (2018). Managing social contents in Decentralized Online Social Networks: A survey. Online Social Networks and Media, 7, 12–29. https://doi.org/10.1016/j.osnem.2018.07.001
7. Howgrave-Graham, N., & Joux, A. (n.d.). New Generic Algorithms for Hard Knapsacks.
8. Kellerer, H., Pferschy, U., & Pisinger, D. (2004a). Knapsack Problems. In Knapsack Problems. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-24777-7
9. Kellerer, H., Pferschy, U., & Pisinger, D. (2004b). Knapsack Problems. In Knapsack Problems. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-24777-7
10. Singh, T., & Ali, R. (2018). An Identity based Multi-receiver Generalized Signcryption Scheme. Asian Journal of Applied Sciences, 6(4). https://doi.org/10.24203/ajas.v6i4.5421
11. ur Rahman, A., Ullah, I., Naeem, M., Anwar, R., Noor-ul-Amin, Khattak, H., & Ullah, S. (2018). A lightweight multi-message and multi-receiver heterogeneous hybrid signcryption scheme based on hyper elliptic curve. International Journal of Advanced Computer Science and Applications, 9(5). https://doi.org/10.14569/IJACSA.2018.090520
12. Xu, Q., Tan, C., Fan, Z., Zhu, W., Xiao, Y., & Cheng, F. (2018). Secure multi-authority data access control scheme in cloud storage system based on attribute-based signcryption. IEEE Access, 6, 34051–34074. https://doi.org/10.1109/ACCESS.2018.2844829