Avoid Shortcomings of Cashless Transaction System using Blockchain

Abdulaziz Albesher* [1], Kareem Kamal A.Ghany [1,2]

[1]College of Computing and Informatics, Saudi Electronic University, KSA
[2]Faculty of Computers and Information, Beni-suef University, Egypt

***Abstract*—Technology is backbone of every system in today/s era. But as it is known that every coin has two faces. Technology is invented for betterment of society and humanity but it is necessary to ponder on security issues of digital system. Cashless Economy is a debatable issue of current days. This Paper addresses Errors and Loopholes in Cashless Transaction System (CTS), Mathematical Model to Illustrate loopholes, Difference between Cash and Cashless economy, Electronic Pickpocketing types, Security essentials of online shopping and how to avoid it using hash function, Soft Targets of intruders in cashless economy and some illustration for the same. Lastly this paper discusses the future of cashless economy and Online Shopping using blockchain technology.**

Keywords. Blockchain - Hash function - Electronic Pickpocketing - Cloud Computing.

I. Introduction

In the past decade, the usage of internet increased many time. From private sector to government sector nobody is untouched by its magic. In the era of 1990 to 2000 when personal computer was a dream and storage means hard disk of 2GB, it was unimaginable that one day our data can be stored in space and it can be accessed anytime anywhere in the world.

In the last decade starting from 2010 till date these things are having success as common storage from flash memory to memory card and from 2 GB to 32 GB, and device storage up to 256 GB. Cashless Economy is still a new concept for researchers and having bright scope in near future. Its research area is having many open problems which can be solved from potential researchers of next decade.

On the other hand, the importance of cloud computing is increased for organizations in both governmental and private sectors. The Technology that provides highly scalable usage of applications, computational powers, storage, and infrastructures is now leading solution to transform in the Information Technology (IT) sector.

Since its emergence cloud computing concept has been labeled different terms. Some of the familiar names available in the literature for cloud computing include on-demand computing and computing as a service [1] [2]. The different names and understandings of this emerging concept made it difficult to develop a common understanding among the public and private leaders of what cloud computing really means.

The most basic definition of what cloud computing is conducting pre-defined computing services and delivering them over the internet as requested, or when needed. The other element of this basic definition is that these computing services are conducted remotely and away from the request's computers, servers, or mobile devices. The requester could be an individual, a company, or a government. In all these three cases, the computing services are executed and delivered through the internet from the remote location of the service provider based on a pre-defined and agreed upon contract. Examples of could computing services include processing power, storage, or an application, and all are delivered over the internet.

Apart from this basic definition, there exists a disagreement in the literature on what cloud computing is. This disagreement is commonly attributed to the different usages of cloud computing and to the nature of who the requester is? Cloud computing provides several methods to monitor and obtain information technology resources especially if it been used in a large scale. The term "Cloud" emerged based on the schematic clouds that represent the Internet (network diagrams) or various parts of it. webmail is a clear example of cloud computing. To describe webmail mechanism, webmail provider ensures system's accessibility and manages server space; to access an account end-user should enter the targeted web address and submit user information. Usually the housing of all essential software and hardware maintained by the email client i.e., Gmail and Yahoo, to guarantee the support of the email accounts. The aforementioned process is similar to the process of cloud computing. The only difference is that in cloud computing you have variety of information that can be accessed instead of accessing your email only. One of the salient advantages of cloud computing is shifting the process, storage and management of data from the local machine to the cloud. This supports organizations to save costs and create new business opportunities.

An Administrative approach is very clear and transparent in most of the organization around the world where experiments is going on in this field. A common smart device user who itself is a layman in cloud services and environment wants a cloud data which should be synchronized with his or her smart device. Currently, it is common to access data using the Internet with a limited alignment to the server requirement. This requirement consists of data centers that are maintained and monitored constantly by the Internet service provider.

As the resources become more globally interconnected, a new technology revolution is on the edge. Managing and sharing resources became available from anywhere regardless of time and space. Cloud computing facilitate this method by offering large area of storage where resources are accessible as a hub

978-1-7281-1232-9/19/$31.00

is available anywhere and by anyone as a service rather than as a product.

Throughout in the history of information system management significant evolution have been achieved to reduce users' needs of complicated computer software and hardware. This continues development begin since timesharing functions proposed in 1960s, network computers in 1990s and commercial grid computing reaching to the era of cloud computing. In 2010 more focus was projected to this technology and how it can contribute in increasing the capabilities of a system. In addition, understanding how it helps in cutting costs and improve the use of the available resources and infrastructure. Most of the current cloud service providers requiring a subscription fees to provide the services in real time over the Internet. The software providers are realizing that simply by engaging into cloud environment, more benefits can be obtained in short time and with best business applications facilities. Moreover, it radically boost the infrastructure and different resources at very reduced cost [3], [4]. User-side desires of software, hardware and its complexity is significantly decreased when using cloud services. Cloud services modified the perspective of information technology delivery model. From the statistic shown that massive developments and implementations of cloud computing services market is likely to accomplish between Rs 150 lac crore and Rs 250 lac crore respectively in 2014 and 2015 [5]. Even though the use of cloud computing introduces several advantages, many issues and risks should be overcome which mainly related to the process of management and implementation. In addition, cloud computing technology still suffer from lack guidelines, legislations and standards. According to a survey released in 2015 by Bhagawat et. al. [6], 74% of IT executives and CIO's (Chief Information Officer) stated that security and privacy are the most vital threshold that affects the acceptance of cloud services [7].

The blockchain is defined as a data structure which is decentralized with maintained internal consistency through reached consensus by users on the network at the current state [8]. It opened up a new horizon of possibilities for trustless transactions and exchange of information. If the Internet democratized, the blockchain has applied the peer-to-peer exchange of value.
Figure (1) shows a simple version of a blockchain. The transaction data part of a block holds a single or multiple new transaction. Each new transaction is hashed and then paired with a block, this process will be repeated several times until ending with a single hash remains.

The rest of the paper is organized as follows, section II discusses the related work, section III describes the proposed approach and its phases, section IV presents the experimental results, and finally conclusion and future work are provided in section V.

II. Related Work

In this section we conclude the nearest research to our idea, although there are many other researches but we will present the follows:

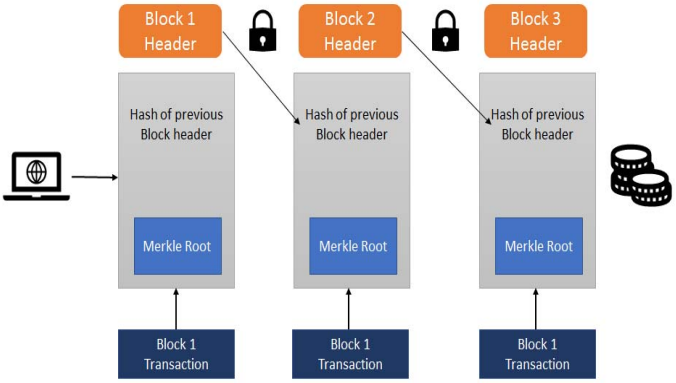

Fig. 1. Simple Version of Blockchain

Yin et. al [9] concentrate on quantum attack in the blockchain, and propose a novel transaction authentication scheme, which is suitable for blockchain.

Dorri et al. [10] proposed an approach for security architecture based on blockchain. The privacy of the users is ensured by using changeable public keys. The security of their architecture is largely inherited from the strong security properties of the underlying blockchain technology.

Kammüller in [11] used a notion of Kripke semantics as formal foundation that then allows to express attack goals using branching time temporal logic CTL. The use of the mechanized Isabelle framework is illustrated on the example of a privacy attack to an IoT healthcare system.

Augot et. al presented in [12] an identity management scheme built into the Bitcoin blockchain, allowing for identities that are as indelible as the blockchain itself. Moreover, also a decentralized Bitcoin is used to facilitate a shared control between users and identity providers, allowing users to directly manage their own identities, fluidly coordinating identities from different providers, even as identity providers can revoke identities and impose controls.

In [13] Meshkov et. al proposed an alternative difficulty adjustment algorithm in order to reduce the incentive to perform a coin-hopping attack, and also decrease inter-block delays.

III. METHODOLOGY

The main problem appeared when using cashless transaction systems is that inter-connectivity has suffered many fundamental problems when it comes to the trust of the transactions. So blockchain will act as not only a central trusted authority in a massively distributed network, But also as a multiple sources of trust that must all agree, based on an algorithm that this transaction can be trusted as valid. It should use completely new level of privacy, security, and trust to the online world [14], [15].

The main idea of our approach is to generate a new hash value for each transaction to keep them from being linked to a common owner, also this helps us to detect any changes made to original transactions as shown in figure (2).

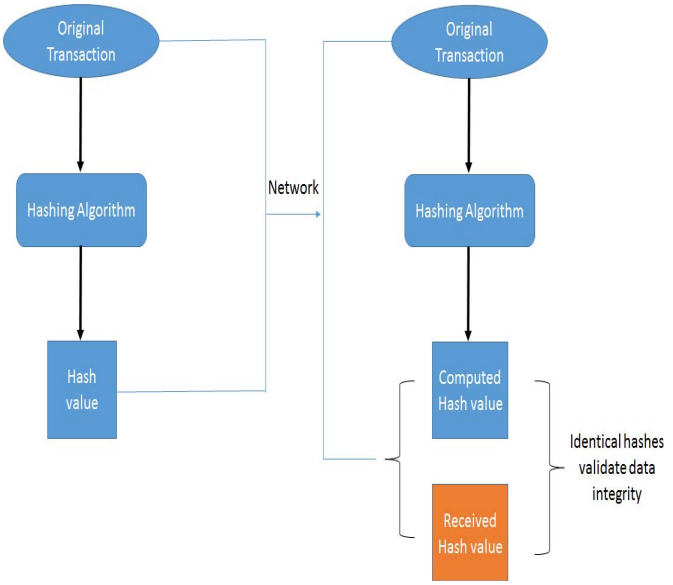

Fig. 2. Overall model for the proposed hashing approach

The following algorithm describe the idea of calculating the differentiation:

Algorithm 1 Using Arithmetic and Geometric Progression

1: Determine the first term of transaction.
2: Determine the common difference/ Common Ratio.
3: Determine the n^{th} term using Equation 1 and Equation 2.
4: Total =$\sum$ **n**.
5: Claculate h', where h' is the hash value.
6: Find the difference between surcharge using AP and GP, where AP is the arithmetic progression and GP is the geometric progression.
7: Calculate the Differentiation.

IV. Experimental Results and Discussion

Let a Transaction is done **n** times using Debit/Credit Card and we consider Service tax deduction is uniform 1% in each transaction.
Let the first transaction is done of 1000 SAR by the card excluding tax of 1-2%, and each successive transaction deducts tax of this 1000 SAR ranging from 1-2.5%.
Arithmetic Progression Tells us if a is first term **d** is common difference **n** is last term so equation for finding n^{th} term is as follows:

$$An = a + (n-1)d, \tag{1}$$

$$Sn = n/2[2a + (n-1)d] \tag{2}$$

From the above example N^{th} Transaction if a =1000 d=10 (uniform % of tax)

50th Transaction of 1000 SAR will be 1000+490 i.e 1000 SAR give tax 490 SAR after 50 transactions.

So as seen if Cash rotates 50 times, it is still 1000 SAR, but if cashless rotates 50 times including the surcharge and debit/credit card tax it becomes 1490 for service provider and extra burden on card user is 490.

An example of the results is shown in Table I.

TABLE I. Comparison of Cash and Cashless Transaction

Service Provider	Tax/Surcharge	Cash Amount In SAR	Cashless Amount
Paytm	2%-3.5%	100	102 - 103.5
FreeCharge	1%-2%	100	101 - 102
JioMoney	1%-2.5%	100	101 - 102.5
E-Wallet	2%-3.5%	100	102 - 103.5
Online Shopping	1%-2.5%	100	101 - 102.5
Daily Needs Company	1%-2.5%	100	101 - 102.5

To ease the challenges of cashless transactions, it has been identified the following Security Features that online user must be aware of:
1. First and foremost, beware of Hidden Pickpocketing as discussed above in Section III.
2. Currently, Online Shopping theft investigators are completely dependent on Service Providers for evidence acquiring. However, the person who works for the service provider, and collects data on behalf of investigators, is not an official forensics investigator and totally to rely on him is not favorable and is not possible to guarantee his integrity in a legal system.
3. An honest employee of a CSP (Cashless Service Provider) must not scheme with a malevolent user to hide important proofs or to add invalid evidence for proving that the malicious user is benign.
4. On the other hand, an honest investigator must not make a deal with an attacker. Even if a valid evidence is provided by CSPs to investigators, some crucial evidence can be removed by a dishonest investigator before presenting it to the court or some false proofs can be provided to the court to outline an honest cloud user. In conventional storage systems, only the doubtful investigator can plot or scheme.
5. It is critical to store the volatile Data in permanent databases so that even if a virtual machine is terminated by an innocent user, we can still gather the evidence.

V. Conclusion and Future Works

One possible solution to the proposed problem is that CSPs should provide a continuous sync to consumers. Using this information end users can save the synchronized data to any cloud storage for example Big basket, Flipkart, Snap deal and so on. Although, if the opponent is the owner of a VM, this procedure will not work. Secondly, to overcome this issue, CSPs by themselves can mix the organization mechanism with every VM and saving the data within their own organization. CSPs can constantly observe all the running VMs and store the temporary data in a determined storage. The temporary data can be in many forms such as network logs, operating system logs, and registry logs. When a VM is in active state, CSPs can follow which data belongs to which VM. Hence, while saving the data, CSPs can take care of isolating the data per VM.

Lastly its user own wish to use weather cash or cashless system but end user must aware of pros and cons of cashless system and potential security methods. So we presented an initial idea to secure such transaction using hash function. Thus, research area of cashless economy is having many open problems which can be solved from potential researchers of next decade.

REFERENCES

[1] K. Al Ajmi, "Is Cloud Computing Appropriate for Government?", Head in the clouds nature, USA, 2007.

[2] S. Lindsey and C. S. Raghavendra, "PEGASIS: Power-Efficient Gathering in Sensor Information Systems" Proc. International Conference of Comm. (ICC '01), 2001.

[3] S. London, "INSIDE TRACK: The high-tech rebels", Financial Times, 2002.

[4] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud forensics: An overview", in proceedings of the 7th International Conference on Digital Forensics, 2011.

[5] AWS, Amazon web services", ¡http://aws.amazon.com¿, [Last Accessed: 2018].

[6] V. Bhagawat, and A. Kumar, "Survey on data security issues in cloud environment", International Journal of Innovative Research in Advanced Engineering, Vol. 2, No. 1, pp. 31-35, 2015.

[7] R. Marty, "Cloud application logging for forensics", In proceedings of the 2011 ACM Symposium on Applied Computing, ACM, pp. 178-184, 2011.

[8] V. Kundra, "Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud" Statement at hearing of House Committee on Oversight and Government Reform, Subcommittee on Government Management, Organizations, and Procurement, Washington D.C., 2010.

[9] W. Yin, Q. Wen, W. Li, H. Zhang and Z. Jin, "An Anti-Quantum Transaction Authentication Approach in Blockchain", IEEE Access, vol. 6, pp. 5393-5401, 2018.

[10] A. Dorri, M. Steger, S. S. Kanhere and R. Jurdak, "BlockChain: A Distributed Solution to Automotive Security and Privacy", IEEE Communications Magazine, pp. 119-125, 2017.

[11] F. Kammüller, "A Proof Calculus for Attack Trees in Isabelle", DPM/CBT 2017, LNCS 10436, pp. 3-18, Norway, 2017.

[12] D. Augot, H. Chabanne, T. Chenevier, W. George, and L. Lambert, "A User-Centric System for Verified Identities on the Bitcoin Blockchain", DPM/CBT 2017, LNCS 10436, pp. 390-407, Norway, 2017.

[13] D. Meshkov, A. Chepurnoy, and M. Jansen, "Short Paper: Revisiting Difficulty Control for Blockchain Systems", DPM/CBT 2017, LNCS 10436, pp. 429-436, Norway, 2017.

[14] H.M. Sabri, H.A. Hefny, and N. Elkhameesy, " Using Iris Recognition to Secure Medical Images on the Cloud ", 3rd World Conference on Complex Systems, (WCCS15), IEEE, Morocco, 2015.

[15] V. Dhillon, D. Metcalf, and M. Hooper, " Blockchain Enabled Applications ", Apress, USA, 2017.