Are Tokenization, Moving Target Protection Technology, Biometric Authentication, Machine Learning, Artificial Intelligence, and Quantum Cryptography the saviors on the cybersecurity war?

Luis O. Noguerol
University of Phoenix, USA
luisonoguerol@gmail.com

Information Technology has been going through an unparalleled development as no other industries. Technological advances are invading our lives in an unimaginable ways 25 years ago. Benefits are tangible in every single industry from healthcare and agriculture to engineering, national defense, and personal development.
Iansiti and Richards, (2006), indicated that a number of networks of industries organized to deliver services to the end users. This network of industries is termed "business echosystems." The amount of dissimilar technologies oriented to facilitate common daily tasks are in the raise and the trend is growing. Multiple tasks have been humanized as for example agriculture and construction and other aspects of live have been dramatically shifted from traditional/standards to a new epoch in which the compulsion to be interconnected becomes a necessity. For how long can you be "disconnected" from social media or away from your smart phone? More than 48 hours? Give a try and good luck on this effort.

Justifications to be perpetually interconnected comes in different "packets, colors, and flavors," but without mentioning a particular reason, the reality is that we do have an existential problem with this situation. Of course numerous and unalike benefits from the technological revolution we are experimenting create this dependency but efforts to secure the whole ecosystem is just in a developing stage.

This is the real problem of the 21 Century. No the kind of new technologies and how those are going to improve our lives, this is a fact – no question about it, but how can we minimize the irrational amount of security glitches we face and will be facing for the rest of the century? And no, this is NOT about Physical Security – which of course still the most important – probably. This is about cybersecurity. In other words, the security of the electronic data, considering electronic data as anything processed by an electronic device. Yes, this is a broad definition and being more precise, considering the unexpected amount of new electronic devices is simple unpredictable or even better, an irresponsibility.

As a consequence of the technological revolution and the yottabyte amount of data crossing the different types of communication mediums nowadays; the implications of data breaches from every single point of view; the lack of regulations when it comes to cybersecurity specially in USA; and the potential for those problems to increase, "secondary" industries have been emerging as the *world saviors* and traditional ones are going through a fast transformation in which no adapting means, loss of the business. Of course, the cybersecurity sector is expanding as well in the race for having a "piece of the cake," now and later. No doubts that the business in cybersecurity have a prominent future and is precisely this, what make vendors to repeat in different super sophisticated ways the same type of solutions, elucidations that by the way, are not serving well for the purposed intent with few exceptions to be followed. Of course, leaders always exist and will continue to be in place. Solutions as well, the ones that have been consistently proving their capacities to minimize cybersecurity breaches. Electronic data protection should be understood as ensuring the confidentiality, availability, integrity and authenticity of information. At the same time, none of the technologies can perform all these functions simultaneously. Therefore, adherence to each of these principles requires the use of appropriate solutions

Mathematical algorithms from Euclidean and the Delone triangulation to Rivest–Shamir–Adleman and Porter's algorithm are proving to be of huge help when it comes to cybersecurity. Complexity on the telecommunications channels, disparity of new and emergent technologies, compatibility issues, security breaches on the raise, a substantial amount of devices to protect the electronic data that are signature based, those to mention only few of existing and becoming problems complicate the cybersecurity panorama but as if it was not enough, the protection of the electronic data include human factors and this last component modify the cybersecurity equation. If in addition of the aforementioned factors we link the problem to end users' necessities in which expectations are on the raise when it comes to speed, comfort, convenience, and accessibility just to mention few then the need to protect electronic transactions is pivotal nowadays. In the middle of what appears to be a chaotic situation, the question to be asked is which is the best solution? Of course, this solution does not exist yet and making this assumption can contribute to more security breaches but necessity have the last word over preferences and inactivity and passiveness just obfuscate the problem. Are we attending then to the end of the world? No, no yet.

Some proved solutions have been helping to remediate cybersecurity gaps as for example Moving Target Protection Technology, Biometric Authentication, Machine learning, Artificial Intelligence, Quantum Cryptography, (on the initial stage of development), and Tokenization.

Moving target protection technology

The protection technology of a moving target can also make a significant contribution to cybersecurity in the future. Now this technology is only being tested and is not widely used in practice. The new protection system was first introduced in 2016 by scientists from the University of Pennsylvania. Using the technology of protecting a moving target, developers intend to solve one of the main problems of data protection - to deprive the authors of cyber-attacks of access to the code that is used for encryption. Experts say that having one fact of encryption today is not enough. To protect data, you need to continuously change the system, and then the attacker will not be able to obtain relevant information about its state, which can be used at the next moment in time. As a result, it will be extremely difficult to plan an attack. Biometric authentication.

Among the promising areas of information security, experts also include biometric authentication technologies that allow users to be authenticated by measuring the physiological parameters and characteristics of a person and his behavior. Voice biometrics and face recognition technologies are developing the fastest in this segment. These solutions are already actively used in the field of forensic science and social control and are gradually becoming a standard feature in smartphones. However, analysts believe that the future of biometrics is due to the use of “closed data”, such as heart pulse, drawing of intraocular vessels, the shape of earlobes, and more. In addition, biometric data can be protected by implanted under the skin chips, tablet computers, as well as DNA testing and analysis of human neural connections.

Machine learning

Machine learning are already able to detect and eliminate most of the attacks, the purpose of which is to disable companies' websites, compromise confidential data and steal money.

Artificial Intelligence

In the field of data protection remains the question of guaranteed exclusion of the adoption of wrong decisions by machines. The expert says that artificial intelligence is being introduced everywhere, but security experts have not yet been able to completely solve the problem of protection against “false positives” when using AI, and this is the direction that is crucial for the development of information security in the future.

Quantum Cryptography

Technologies will continue to grow rapidly in the future. The specialist is sure that this direction will significantly improve the methods for protecting data transfer. However, to implement these developments, it may take at least 15 years.

Out of all of those, Tokenization is shedding light as an integral part of the solution at least, for now. The modern digital economy is based on tokenization, which is used by billions of people every day. Rouse, M. (n.d.) states tokenization is the process of replacing sensitive data with unique identification symbols that retain all the essential information about the data without compromising its security. In other words, tokenization is the process of replacing valuables (such as money, stocks, credit card numbers, medical records) by tokens that reflect these values, which makes trading easier and safer. This may seem distant, but tokenization has a profound impact on our lives and can transform entire industries. Payment of goods through the Internet would be much riskier if it were not for tokenization. The confidential information of the credit card becomes a digital token, which is useless for hackers, but is used by banks to complete a payment. Companies make digital substitutes for stocks and other securities instead of paper means, because they are safer and more efficient.

Tokenization basically lies in the substitution of real confidential data with other values, or tokens. An unthinkable solution few years ago, not because the lack of algorithms to accomplish the tasks but because the obsolescence of existing technologies at this point. As a result of the implementation of digital tokens, trading companies may no longer need to store user billing information, and attackers who will have access to information on the cards of companies’ clients will not be able to use it. Tokenization is especially actively used in e-commerce. At present, the technology is supported by the VISA and MasterCard payment systems, however, with the development of contactless payments and financial technologies, the use of tokenization may spread to the entire trading market in the near future. Although people already use tokens on a daily basis (most do not know), the true potential of tokenization is revealed only now due to the influence of the blockchain.

Murray (2018) defines a blockchain is a database that is shared across a network of computers. Once a record has been added to the chain it is very difficult to change. To ensure all the copies of the database are the same, the network makes constant checks. Blockchains have been used to underpin cyber-currencies like bitcoin, but many other possible uses are emerging. Blockchain allows you to securely and effectively tokenize a wide range of real assets and businesses, providing new benefits and applications for a wide variety of industries, such as art or health.

In fact, the tokenization with the blockchain allowed us to create a completely new tool for trade and fundraising: security token. Fundraising through the placement of security tokens (STO) is usually cheaper than traditional methods, such as venture capital or the initial public offering (IPO). At the same time, the regulatory requirements are met, the issue rate is increased and the opportunity is given to focus on a wider range of potential investors. Investors can increase the liquidity level of assets faster than under venture capital, trade in secondary markets 24 hours a day and make transactions faster, and small investors can participate in large institutional transactions. Despite the difficulties, assets with a capital of around $ 500 million have already been based on chips in 2018, and this figure will grow rapidly in the coming years. Below are some of the industries that are positively attuned to tokenization.

Payments

Every year, around the world, payment transactions of almost $ 110 billion are processed, including payment systems such as Visa, which report payments of approximately $ 2 billion each year. Two major problems dramatically increase the cost of payments to consumers around the world: incredibly high rates for micropayments ($ 5 - $ 10) and high costs associated with currency conversion for international payments. Remittances are estimated at $ 585 billion, while estimates of global micropayments vary greatly due to differences in definitions.

Rates in various payment processing sectors vary from 2.9% + $ 0.30-0.10 per transaction, plus $ 99 per month. With these rates, most micropayments less than $ 1 are more expensive than the cost of the transaction itself. Currency conversion, KYC / AML and international banking intermediaries increase the cost of remittances up to 6-10%. International payments cost 1 to 3% for travelers and an additional 1-3% for sellers, and this is above other card processing fees.

Some international payments or money transfers also run the risk of getting lost or stuck somewhere in the counterpart bank during the transfer process. The tokenization of blockchains significantly reduces all these costs and prevents losses, so many companies that work with blockchains have begun to provide services in these areas. BitPay, one of the oldest payment systems in the world, in 2018 helped companies earn more than 1 billion dollars. More than 4,500 online merchants accept cryptocurrency payments through the CoinGate payment processor, which has already processed more than 300,000 payments in more than 50 cryptocurrencies. Ho Wah Genting Group, one of Malaysia's largest travel and entertainment conglomerates, in the fourth quarter of 2018, based on the everiToken platform, issued a stable $

500 million currency, offering a more economical way to pay for services of travel and entertainment in a large network of companies.

Pros and Cons of Tokenization

As every technology, tokenization still has problems. There are still some examples of its use, which means that the market remains unverified. As a result, institutional actors are reluctant to participate in large tokenization projects, and as a result, the market lacks liquidity. This institutional alienation is also due in part to the continuing regulatory uncertainty with the presence of unanswered questions. It is not always clear when exactly the liquidation of fixed assets occurs. As mentioned before, the lack of standardization of protocols and technologies leads to problems of compatibility and implementation. The storage of digital assets is also not completely verified and, therefore, is partially risky.

Conclusions

This paper defined and provided the functions of echo systems, tokenization, and blockchain as related to security of information in cyber network. Infact, tokenization, moving target protection technology, biometric authentication, machine learning, artificial intelligence, and quantum cryptography are not the savior of the world; but they are helping to keep the balance between what the “bad” people can do and the limitations they face when trying to compromise the electronic data. This represent a huge challenge for those companies trying to get “their pieces of the cake,” if they keep following traditional approaches for cybersecurity issues.

References

Marco, I. & Richards, G. L. (2006). The Information Technology Ecosystem: Structure, Health, and Performance,” *Antitrust Bulletin* 51, no. 1. Retrieved from https://journals.sagepub.com/doi/abs/10.1177/0003603X0605100104

Murray, M. (2018). Blockchain explained. Retrieved from http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html

Rouse, M. (n.d.). Tokenization. Retreived from https://searchsecurity.techtarget.com/definition/tokenization