UDC 004.491:005.21
Survey Paper

Comparisons of Bitcoin Cryptosystem with Other Common Internet Transaction Systems by AHP Technique

Davor Maček *davor.macek@foi.hr*
UniCredit S.p.A. Zweigniederlassung Wien
Vienna, Austria

Dino Alagić *dalagic@foi.hr*
NTH ICT d.d.
Varaždin, Croatia

Abstract

This paper describes proposed methodology for evaluation of critical systems and prioritization of critical risks and assets identified in highly secured information systems. For different types of information assets or security environments it is necessary to apply different techniques and methods for their prioritization and evaluation. In this article, VECTOR matrix method for prioritization of critical assets and critical risks is explained and integrated into AHP (Analytic Hierarchy Process) technique as a set of fixed criteria for evaluation of defined alternatives. Bitcoin cryptocurrency was compared and evaluated along with other common Internet transaction systems by information security professionals according to defined VECTOR criteria. Also, the newly proposed hybrid AHP model is presented with potential case studies for future research. This article tries to discover security posture of Bitcoin cryptocurrency in the context of information security risks related to the existing most common online payment systems like e-banking, m-banking, and e-commerce.

Keywords: Cryptosystem, Cryptocurrency, Bitcoin, Analytic Hierarchy Process, Multi-criteria Decision Analyses, VECTOR, Information Security Risk, transaction systems

1. Introduction

Note: The views expressed in this article are those of the author and do not necessarily reflect the views of the UniCredit S.p.A. nor Zagrebačka banka d.d.

In regard to computer security it can be said that it represents a combination of confidentiality, integrity and availability of data, information and information systems. It thus, inevitably, involves security risks. According to ISACA BMIS [1], risk management is recognized as a key component of managing IT security risks. In today's globally networked and complex business environment there is an expansion of security threats, vulnerabilities and other related risks. Most of today's cyber-attacks are financial based and so are the cases of hacktivism [2]. The amount of cybercrime, security breaches and incidents is increasing significantly, and so are financial losses [3], [4], [5], [6], [7].

Given that we have recently witnessed the ever increasing Internet fraud with the help of various methods and techniques such as phishing and/or identity theft, the need arises for additional security measures to protect customers when using Internet banking, but also to protect banking systems and electronic commerce systems themselves. Of course, such additional protective measures cause a significant increase of transaction costs. However, in the last few years there an alternative has appeared regarding the use of conventional centralized payment systems, such as Internet banking, mobile banking or e-commerce, in the form of crypto currency or Bitcoin technology.

Bitcoin is used for electronic payments on the Internet and its most important feature is its decentralized nature, meaning that no institution or central authority are authoritative nor do they control the Bitcoin network. Also, to a certain extent Bitcoin allows anonymity to the users which in turn makes it difficult to track the transaction chain [8]. Therefore, specific security issues and security challenges occur, particularly in the context of trust, privacy and integrity of such a complex cryptosystem, as well as the inevitable risks that Bitcoin system carries for its users but also for society as a whole.

The motivation for the research topic linked to the Bitcoin cryptosystem/cryptocurrency developed as the authors of this article, during their professional work in a financial institution and high-tech company, were often faced with various implementations of certain security solutions related to transaction systems such as e-commerce, e-banking and m-banking, along with the advantages, shortcomings and risks that such systems encompass. So the idea was born to explore today's increased usage of Bitcoin technology and its operation modes along with security aspects of the Bitcoin system itself, and also to make comparisons with the existing, most prevalent Internet transaction systems that are being used.

It is a well-known fact that it is very difficult or sometimes even impossible to address all security risks in the environment appropriately and on time, particularly in big corporate environments. However, spotting the most critical ones is absolutely essential. So, it is obvious that some sort of security risk management and risk prioritization is needed.

This paper presents Analytic Hierarchy Process (AHP) technique for multiple criteria decision making (MCDM) process [9], [10], VECTOR matrix method for initial identification and prioritization of high critical security risks, and a proposal of the new AHP model with integration of VECTOR method into AHP technique. VECTOR matrix method is used for static criteria evaluation of alternatives in AHP technique [11], [12].

As already mentioned, the motivation for the topic and future research related to information security risks is connected to the authors' working in a financial institution and being faced with threats, vulnerabilities, and operational IT security risks along with consequential regulatory, compliance and reputation risks, including the need for a quick prioritization of issues, their resolving and reporting. Risk assessment in financial institutions, in particular with regard to information systems security, should be the starting point of any planning and strategy development or the selection of a possible security solution.

The paper is organized as follows: the research problem of security risks prioritization and IT security risks of online transaction systems is presented in section 2. Bitcoin cryptosystem is explained in section 3. Research methodology with the research plan by using AHP technique and VECTOR risk matrix method, and proposed new AHP model for prioritizing critical risks and security solutions evaluation are presented in sections 4, 5 and 6. Conclusions with future research proposals and potential case studies are given in section 7. At the end of the paper, all relevant references are listed.

2. Research Problem: Information Security Risks of Common Online Payment Systems

Todays' state of the art denotes that so many payment systems are available on the Internet which allow us to easily conduct payment transactions in real time from almost any place in the world by using any device with network connection. But, on the Internet, there are also numerous threat agents, threats, and vulnerabilities along with the availability of security exploits, all of which appear on a daily basis. Consequently, to address all these security concerns and related risks becomes very challenging not only for every organization, but also for every individual.

Recent attacks on Internet banking clients' in Croatia and other European countries which happened in 2014 and 2015, together with growing credit card frauds on the Internet, encouraged us to think about alternative ways of online payments, and to compare their security characteristics with the existing common online transaction systems.

So, some of the questions that came to our minds were the following:

- How much indeed are these online payment systems secure today?
- How do customers access their online accounts or wallets?
- In what way are customers' data secured?
- Is there any type of online transaction monitoring?
- Whether an alternative in the form of cryptocurrency is sufficiently secure to compete with common online banking and e-commerce systems?

This research will try to explain certain information security concerns regarding the current most common online payment systems and an upcoming alternative in the form of Bitcoin cryptocurrency, as well as evaluate/compare these systems against each other to see the ratio [13].

Another discovered issue is the prioritization of information security risks. There are certain approaches for prioritizing information security risks like TARA methodology developed by Intel [14] or MITRE Risk Impact Assessment and Prioritization technique [15] which can be very valuable for business to mitigate critical risks, but none of the systems mentioned are based on solid mathematical foundations like AHP, TOPSIS or some other multi-criteria decision analysis technique. Even well-known and globally acknowledged risk management and risk assessment methods/techniques like ISO/IEC 27005:2011 [16], NIST SP 800-30 [17] or OCTAVE [18] do not consider prioritization of security risks based on some mathematical quantitative model, just qualitative impact levels. Only the FAIR risk assessment methodology [19], based on accurate threat modeling, was found capable to provide certain quantitative model and corresponding results, but its drawback is that it cannot make any comparisons of security solutions that our proposed model should be able to do. But the new ISO risk assessment standard finally recognizes and induces Multi-criteria decision analysis (MDCA) as one of the possible risk assessment techniques [20].

So, the following research questions are formed:

- How can organizations identify and prioritize exposures and vulnerabilities based on a MCDA/MCDM technique to isolate and minimize security risks that will have the greatest impact, and deploy their limited resources in the most effective manner possible?
- Whether some new MCDA/MCDM model can be proposed for prioritizing critical information security risks and the evaluation of security solutions?

Answers to these important questions should also be given with this research.

3. Bitcoin Cryptosystem

Bitcoin is a decentralized *peer-to-peer* payment system and a form of digital currency which appeared as a result of a project of open source software by the beginning of 2009, devised and developed by Satoshi Nakamoto. Bitcoin system has no central repository, server or a central administrator for transaction processing or cash storage. All system payments are recorded in the so-called public book that represents a publicly available file on users' computers as the most important part of the Bitcoin system, i.e. Bitcoin network. Bitcoin financial transactions are recorded in this file without the intervention of any central or authorized authority. Bitcoins are simply records in a block-chain and do not exist outside of it [21].

Bitcoin is the digital money, created and stored electronically. Bitcoins are produced by people all around the world using their computer and/or supercomputers with the help of a software implementing an extremely complex mathematical algorithm. Bitcoin is the first example of a type of currency called cryptocurrency. Production of Bitcoins is called mining wherein individuals and companies are involved in this activity in exchange for transaction fees and newly created Bitcoins [21].

The Bitcoin scheme is designed as a decentralized system where no central monetary authority is involved. Bitcoins can be bought on different platforms, but new money is created and introduced into the system only via mining activity [8].

In addition to mining, Bitcoin can be obtained in exchange for money (buying and selling), products or services. Users can electronically send and receive bitcoins for arbitrary transaction fee by using the so-called Bitcoin wallet software on a personal computer, mobile device or web application. Bitcoin system has been designed so that there can exist or can be produced (mined) a maximum of 21 million Bitcoins (BTCs), and its smallest unit is named Satoshi.

By connecting to the Internet, computers that contain a public record or a Bitcoin transaction file form a network which anyone can access by using the wallet software. Thus, for example, in a transaction in which the agent A wants to send X Bitcoins to the recipient B, the agent A advertises itself in the network as a sender A by using one of the available software applications. Bitcoin servers or nodes can validate transactions, add them to the copy of the public file, and then such updates are advertised to all other nodes.

Maintenance of block-chain is called mining, and those who work for it receive newly created Bitcoins and transaction fees. The so-called miners can be located anywhere in the world where they process transaction payments by checking the validity of each transaction and adding it to the block-chain. Payment of transaction fees is not mandatory, but it can speed up the transaction confirmation. Payers are encouraged to include such transaction fees, because it means that their transactions will probably be added earlier to the block-chain, since miners can choose which transactions will be processed at what time and are more likely to concentrate on those for which they were paid or received some sort of compensation. Network software confirms the transaction when recording the transaction into the block. The next block of transactions confirms the previous transaction additionally, and after 6 confirmations (blocks), the transaction will be confirmed unconditionally.

Bitcoin wallet can be defined as something that stores the digital evidence of ownership of Bitcoin, and provides access to and the use of Bitcoin (purchase, sale). Bitcoin uses public key cryptography where two cryptographic keys are generated, one public and one private key. The public key can be thought of as the account number, and a private key as the ownership credential. Basically, it can be said that the wallet is a collection of those keys.

Bitcoin address is the identifier of a user’s Bitcoin wallet within the network. Bitcoin ownership linked to a specific Bitcoin address can be demonstrated by knowledge of the private key that belongs to this particular address. For the owner it is extremely important to protect the private key against loss or theft. If the private key is lost, the user cannot prove their ownership in any other way. Bitcoins are then lost and cannot be returned. Due to the fact that anyone who knows the private key can take over the ownership of Bitcoin associated with that key, the theft can happen when the private key is discovered or stolen, which poses a high risk for the user [21].

Bitcoin is just an example of one among hundreds cryptocurrencies today available. The reason for its selection in this research is that it was the first cryptocurrency to ever appear, and it is still the world's most dominant cryptocurrency according to transaction volumes in m$ [22]. Also, there were certain factors considered for selection of cryptocurrency [23], [24]. But, as with any new emerging technology, digital currencies also bring certain security risks [25].

3.1. Transactions

Integrity component of Bitcoin security refers to prevention of unauthorized transactions from the wallet of an individual. Bitcoin transactions denote a constant transfer of ownership of Bitcoins to a new address that is presented as a one-way hash function resulted from public key computations. The corresponding private key acts as a protection feature for the owner, and a valid message for the payment from a certain address must contain the associated public key and the digital signature which actually proves the possession of the associated private key. The risk of theft of the private key can be reduced by generating keys offline on an uncompromised computer and storing that key to an external protected/encrypted disk.

The traditional model of banking confidentiality is achieved by restricting access to the information on the parties involved in the execution of transactions, such as the payer, recipient of the payment and a trusted third party. The necessity of public disclosure of all transactions excludes this method, but confidentiality can still be preserved in a way that the public keys of Bitcoin users are kept anonymous. The Bitcoin community can see that a user sent a certain amount to another, but cannot see the information that uniquely connects a transaction with anyone, the person who performs the transaction nor the person who accepts it. Using Bitcoin is basically considered to be anonymous, but yet completed transactions may eventually be connected with individuals if the owner of the key is somehow disclosed.

Today's trade on the Internet relies almost exclusively on financial institutions that serve as trusted third parties for electronic payments processing. But on the other hand, there is a proposal of an electronic system based on cryptography, not on trust, allowing any two parties to perform mutual transactions directly, without the need for a trusted third party. Thus, Bitcoin was proposed as a solution to the problem of double spending by using *peer-to-peer* distributed servers with a time stamp to create a computer proof of the chronological order of transactions. The assumption is that the system is safe as long as honest nodes together control more processing power than any organized group of attackers with their computer nodes.

In the Bitcoin cryptosystem, a transaction is a set of data confirmed with a digital signature and sent to the Bitcoin network in order to form blocks. The transaction contains references to previously executed transactions and connects a certain number of Bitcoins with one or more public keys (Bitcoin addresses). The transaction is not encrypted. The block-chain browser is an area where all transactions are combined in the form of a block-chain, and can be found and checked there. This is necessary to determine the technical parameters of a transaction and check the payment details. Electronic Bitcoin is defined as a chain of digital signatures. One owner transmits its own Bitcoin to the next (buyer) in a way that digitally signs both the hash of the previous transaction and the public key of the next owner, and then adds them to the end of the Bitcoin chain. Bitcoin recipients can verify the signatures to verify the chain of ownership [26].

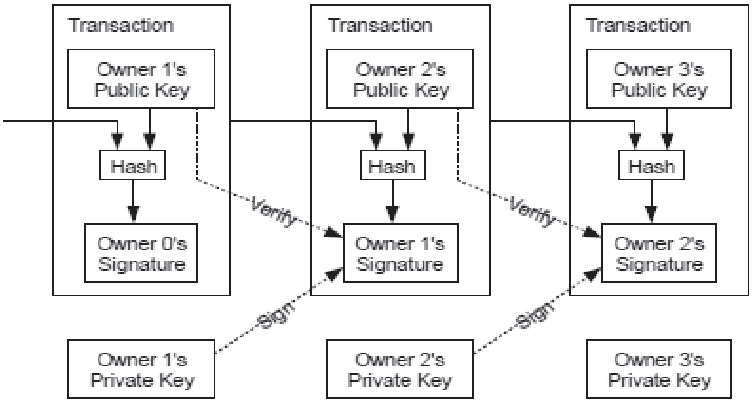


Figure 1. Signing of transactions with the hash [26]

The issue of potentially double spending during the same transaction is dealt with through the timestamp server. So, the timestamp server makes a hash of a block of items which are timely labeled and then the hash is publicly announced. Timestamp proves that the data had been there at a specific time in order to even be able to enter into the hash function. Each timestamp contains the preceding timestamp in its own hash, thus creating a chain, wherein each additional timestamp reinforces (i.e., increases) the previous one.

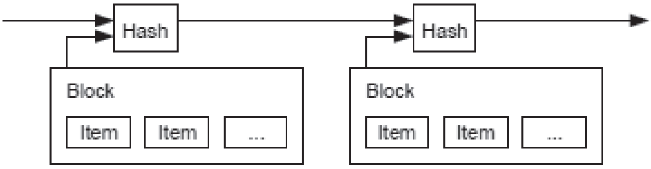


Figure 2. Adding blocks of items in the hash [26]

It is important to emphasize that the probability of a hacker (or some malicious group) with a slower processor reaching the CPU power of honest nodes in the network decreases exponentially by adding new hash blocks in the chain.

3.2. Proof of Work of Bitcoin Network

The proof-of-work involves scanning for a value that, when hashed, such as with SHA-256, begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For the Bitcoin timestamp network, the increment of a nonce was implemented in the block until a value was found that gives the block's hash the required zero bits. Once the CPU effort has been expended to satisfy the proof-of-work, the block cannot be changed without redoing the previous actions. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.

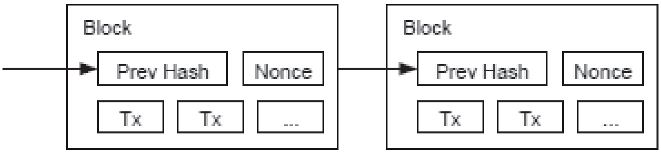


Figure 3. Hash chaining [26]

The proof-of-work also solves the issue of determining representation in the majority of decision making. If the majority were based on one-IP-address-one-vote, it could be crashed by anyone able to allocate many IPs. The proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing (malicious) chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all the blocks after it and then catch up with and surpass the work of the honest nodes [26], [27].

To compensate for the increasing CPU speed and varying interest (especially that of malicious ones) in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they are being generated too fast, the difficulty increases.

Bitcoin network operates according to the following, strictly defined steps:

1) New transactions are advertised to all network nodes
2) Each network node collects new transactions into a block
3) Each node works to find a weight of proof about the work for its block
4) When a node finds the evidence of the work, it advertises its block to all other nodes
5) Other nodes accept the new block only if in the block all previous transactions are valid and if they have not been previously spent
6) Nodes confirm their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before much time has elapsed [26].

4. Common Online Transaction Systems

This section will in short present the most common Internet transaction systems available today.

4.1. E-banking

E-banking is one of the oldest Internet payment transaction systems which employs WWW (World Wide Web) Internet service. There are various types of user authentication and authorization of transactions depending on application security mechanisms of each bank. For the purposes of this research, retail e-banking application security mechanisms of the biggest Croatian banks were evaluated. The reason for choosing the retail e-banking application for evaluation in the research, instead of business e-banking application was due to the fact that there are much more e-banking retail users than the business ones. Also, all other evaluated systems include much more privately customers than business/companies. In addition, e-banking authentication and authorization mechanisms can differ significantly between retail and business customers.

4.2. M-banking

Mobile banking is quite different from the common e-banking regarding the method used to access the services, software, user interface, which is fully customized for mobile phone (or tablet) screens, as well as security policies associated with mobile devices. Mobile banking uses a WAP (Wireless Application Protocol) Internet service accessing it by a mobile phone (GSM) network, when Wi-Fi network is not accessible. For the purpose of this research, similar to the case of e-banking, retail m-banking application security mechanisms of Croatian banks were evaluated.

4.3. E-commerce (Payment Service Providers)

Today, there are indeed plenty of various payment service providers (payment gateways, acquirers and/or processors) on the Internet. Those companies provide direct payment services to their customers without any bank functioning as a mediator. But, for the payments, these systems still use credit or debit cards issued by the bank to their customers. The list of some of the most popular online payment solutions can be found on the *Search Engine Journal* website [28]. Since all these e-commerce payment systems differ concerning their security policies and mechanisms, it was decided to select the world's most widely used payment acquirer according to the number of customers and the number of processed transactions per year for the purpose of evaluation. PayPal payment system is currently by far the most popular alternative to credit cards and cash in Croatia.

POS (**P**oint-**O**f-**S**ale) systems for card acceptance in traditional merchant store were intentionally left out of this research due to the fact that many of these systems still use dial-up communication, and thus cannot be categorized as online systems. Also, those systems have specially dedicated hardware, POS appliance for card acceptance, so it would be very difficult to compare it with other existing online transaction payment systems.

5. Related Work and Research Methodology

This section will in short describe the related (previous) work, then the research methodology for AHP as MCDA technique and VECTOR Matrix risk assessment method along with the reasons for their selection in solving this kind of specific multi-criteria decision making problem.

5.1. Related Work

There is a previous work related to the integration of VECTOR matrix into AHP technique [29]. That work just tried to explain the criticality of certain business and security requirements (i.e. PCI DSS) regarding card payment standards, and not the security posture of the payment systems or environments itself. But the work itself served as a good basis to make a hybrid model for this research of comparisons of the most common online payment systems according to VECTOR criteria incorporated into AHP technique.

5.2. Research Methodology

5.2.1. Analytic Hierarchy Process (AHP)

The Analytic Hierarchy Process (AHP) is a structured technique for organizing, analyzing and making complex decisions, based on mathematics and psychology. It is recognized as a leading theory in multi-criteria decision making field [9].

The AHP is a multi-criteria decision-making (MCDM) approach that was introduced by Thomas L. Saaty in the 1970s and has been extensively studied and refined since that time. The AHP is a decision support technique which can be used to solve complex decision problems. It uses a multi-level hierarchical structure of objectives, criteria, subcriteria and alternatives. Important data are derived by using a set of pairwise comparisons. These comparisons are used to obtain the weights of importance of the decision criteria and the relative performance measures of the alternatives in terms of each individual decision criterion.

To make a decision in an organized way in order to generate priorities, we need to decompose the decision into the following four steps [10]:

1. Define the problem and determine the kind of knowledge sought.
2. Structure the decision hierarchy from the top with the goal of the decision, then the objectives from a broad perspective, through the intermediate levels (criteria on which subsequent elements depend) to the lowest level (which usually represents a set of the alternatives).
3. Construct a set of pairwise comparison matrices. Each element in an upper level is used to compare the elements in the level immediately below with respect to it.
4. Use the priorities obtained from the comparisons to weigh the priorities in the level immediately below. Do this for every element. Then add its weighed values and obtain its overall or global priority for each element in the level below. Continue this process of weighting and adding until the final priorities of the alternatives in the most bottom level are obtained.

5.2.2. VECTOR Matrix Method

VECTOR matrix is a free, open source and pretty simple qualitative self-assessment risk method, developed to help business systems in defining the priorities of critical assets and risks, including information security risks. This method allows users to easily quantify and visually represent all possible aspects of risk to the business system. VECTOR method for qualitative risk assessment is based on the following formula [12]:

RISK = V+E+C+T+O+R

VECTOR is the acronym derived from the following English words:

V = Vulnerability,
E = Ease of Execution,
C = Consequence,
T = Threat,
O = Operational-Importance,
R = Resiliency.

The reason to have chosen the AHP technique for evaluation of alternatives with a fixed VECTOR criteria and not some other MCDA method was that other MCDA methods (i.e. ELECTRE, PROMETHEE) did not fit well for this kind of multi-criteria decision making problem. TOPSIS method could fit to a certain extent, but there are significantly less application examples of TOPSIS method in information security and risk problems than relating to the AHP method [30], [31], [32], [33]. Also, it is compulsory to point out that other MCDA methods have not shown enough flexibility or even feasibility to incorporate necessary fixed VECTOR criteria within themselves. One of the very important and influential instigators for selection of the AHP as a MCDA technique came from the paper [34] where information security risk management methods were compared by using certain AHP criteria.

There were some approaches to use other MCDA techniques for risk analysis, but none were found to be enough relevant in the area of information security. There were found certain relevant articles in the area of information security risk management and usage of some multi criteria decision analysis technique such as TOPSIS or PROMETHEE, but they were always in joint mixture models with the AHP technique [35], [36]. On the other hand, VECTOR matrix method was selected due to its simplicity and proven speed for the ranking of critical assets or security risks [12], [36].

So, the AHP technique was used for this kind of complex multi-criteria decision making issue, while the VECTOR matrix was used for criteria selection in this AHP model. The proposed hybrid AHP model strives to solve the issue of multi-criteria decision making under conditions of uncertainty, i.e. the risks, which online transaction systems carry inherent in themselves.

The following research hypothesis was created: the proposed AHP model with fixed VECTOR criteria is applicable for evaluation of critical online payment systems.

6. The AHP Model for Evaluation of Online Transaction Systems

The main goal of this research is to evaluate the applicability of the proposed AHP model with an integrated fixed VECTOR criteria for the ranking of alternatives. In this case, study alternatives to be evaluated and ranked are different online (Internet) transaction (payment) systems. More specifically, the objective is to evaluate security characteristics of Bitcoin cryptosystem in comparison to other widely used online transaction systems.

A small group of information security experts with broad experience and knowledge of online banking transaction systems were used to test functionality and applicability of the defined hybrid AHP model. To ensure the relevance of the experts' judgments, only individuals who were or still are engaged on e-banking, m-banking and e-commerce systems in the bank were selected to test the applicability of the proposed model.

Criteria for ranking alternatives in every AHP model are defined depending on the appointed problem, i.e. the alternatives and the goal. Certain research related to this type of hybrid model have already been done [29] for the case of prioritizing certain critical risks and security requirements. However this new research now attempts to observe the applicability of the AHP model when evaluation of some security systems or business solutions is needed. The previous research has served as a groundwork for the construction of a hybrid AHP model with fixed VECTOR criteria for evaluation of online payment systems.

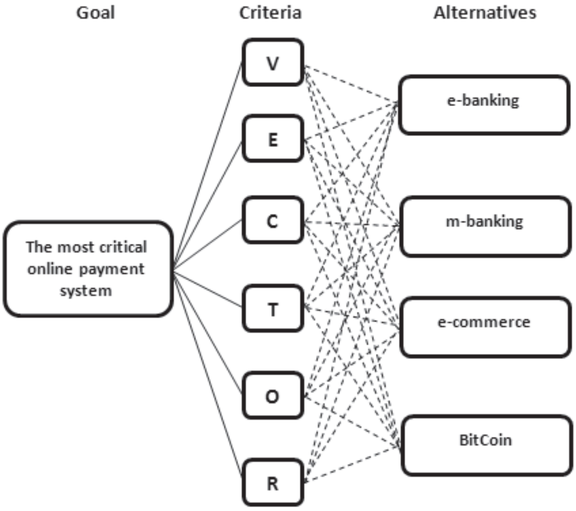


Figure 4. The AHP model with VECTOR criteria for evaluation of online transaction systems

During the evaluation process for VECTOR criteria the following important aspects for each criterion are considered:

Vulnerability criterion; the following common web and application vulnerabilities are considered:

- OWASP TOP10 [37]
- OWASP Mobile TOP 10 [38]
- Man-in-the-Middle and Man-in-the-Browser attacks

Ease of Execution criterion: the authentication and authorization means and its implementation (e.g., two-factor authentication and transaction authorization rules) are considered.

Consequence: possible ramifications for entire social and economic system in case of exploitation, e.g. reputation or regulatory risks, lawsuits or financial losses are considered.

Threat: the most common Internet threats conducted by threat agents [39], such as specially crafted financial malware (e.g., Zeus bot, Carbanak, Dyre, Dridex, CryptoLocker, etc. [40], [41]), DDoS (Distributed Denial of Service) attacks, spoofing, phishing, pharming, SSL/TLS attacks and so on, are considered.

Operational-Importance: overall economic and social context in case of exploitation and/or service unavailability is discussed, similarly to the consequence criterion.

Resiliency: the possibility of recovery of each evaluated system in case of failure is looked at, especially in case of the DDoS attacks – for this particular criterion more weight means less resistance of the system itself.

Information about the criteria and alternatives are synthesized to determine the relative ranking of alternatives. It is important to put emphasis on the relative and not absolute ranking, because it is about the relationship between criteria and consequently, the alternatives. VECTOR criteria represent qualitative types of criteria that will be used for comparisons based on informed judgments to provide weights and priorities. The relative importance of criteria is obtained by using judgments to determine ranking of the criteria itself. By using pairwise comparisons, the relative importance of each criterion in respect to others can be expressed. So, for that purpose, Saaty's original scale was used [10]. Based on this scale, the relationship matrix among different criteria was given.

Thus, according to the proposed AHP methodology for evaluation of alternatives, the following steps were done:

- The relative importance of VECTOR criteria was done with the help of expert judgments – VECTOR matrix table of pairwise comparisons was obtained.

  Consistency Ratios (CR) for every information security expert judgment and for each comparison were calculated and almost all were in the acceptable range ($CR < 0.1$).Consequently, the opinions of experts were consistent regarding judgments of the VECTOR criteria and the comparisons of alternatives in terms of each observed criteria, which means that the transitivity property is achieved [42]. It is also important to notice that geometric means were calculated for judgments received from each information security examinee.

	V	E	C	T	O	R
V	1	0,2287	0,1859	3,8981	0,3017	0,2971
E	4,3734	1	0,2532	4,8559	0,3615	0,3413
C	5,3783	3,9487	1	6,7595	2,1689	3,1777
T	0,256	0,2059	0,1479	1	0,2109	0,2805
O	3,3145	2,7663	0,4611	4,7429	1	1,8882
R	3,3659	2,9302	0,3147	3,5652	0,5296	1

Table 1. VECTOR matrix pairwise comparisons

- The main Eigenvector was calculated – derived from VECTOR criteria pairwise matrix. In order to calculate the eigenvector, the matrix (Table 1) was first necessary to square. Further, it is necessary to sum up the rows, and in the end it is needed to make a normalization of the matrix. The result is the required eigenvector of VECTOR matrix criteria.

Criteria	Eigenvector values
Vulnerability	0,0595
Ease of Execution	0,1292
Consequence	0,3759
Threat	0,0323
Operational-Importance	0,2231
Resiliency	0,1800

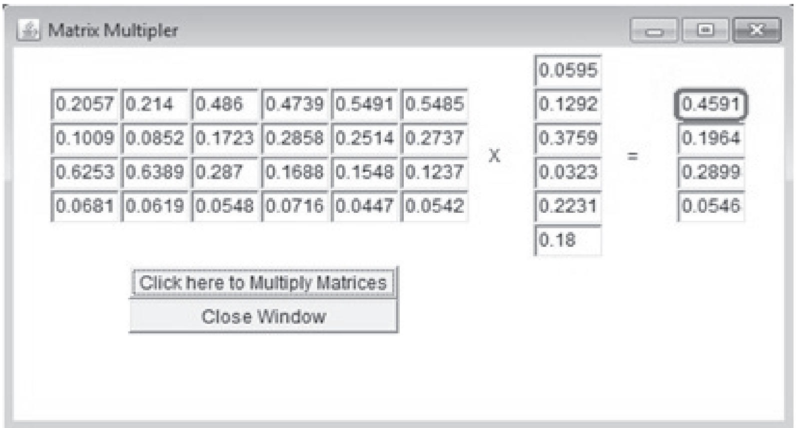
- Table 2. Eigenvector weights for VECTOR matrix criteria

- Eigenvectors for each proposed alternative (online transaction system) are derived regarding each observed VECTOR criterion, according to the same procedure as for obtaining the eigenvector of the VECTOR matrix criteria. When setting the ratios among the alternatives, it was essential to provide the following question: which alternative has the highest risk in relation to the observed VECTOR criterion?

Alternatives\Criteria	V	E	C	T	O	R
e-banking	0,2057	0,214	0,486	0,4739	0,5491	0,5485
m-banking	0,1009	0,0852	0,1723	0,2858	0,2514	0,2737
e-commerce	0,6253	0,6389	0,287	0,1688	0,1548	0,1237
Bitcoin	0,0681	0,0619	0,0548	0,0716	0,0447	0,0542

Table 3. Eigenvectors of alternatives

- The obtained eigenvectors in the ranking of alternatives (Table 3) are needed to multiply with the eigenvector resulted from VECTOR matrix criteria comparisons (Table 2).



$$\begin{bmatrix} 0.2057 & 0.214 & 0.486 & 0.4739 & 0.5491 & 0.5485 \\ 0.1009 & 0.0852 & 0.1723 & 0.2858 & 0.2514 & 0.2737 \\ 0.6253 & 0.6389 & 0.287 & 0.1688 & 0.1548 & 0.1237 \\ 0.0681 & 0.0619 & 0.0548 & 0.0716 & 0.0447 & 0.0542 \end{bmatrix} X \begin{bmatrix} 0.0595 \\ 0.1292 \\ 0.3759 \\ 0.0323 \\ 0.2231 \\ 0.18 \end{bmatrix} = \begin{bmatrix} 0.4591 \\ 0.1964 \\ 0.2899 \\ 0.0546 \end{bmatrix}$$

Figure 5. Obtaining the most critical online payment system

It can be seen from the Figure 5 that the final right-hand column, which was a result of multiplication of eigenvector matrices, has the highest value of 0.4591 in the first row, which actually depicts the e-banking alternative.

The reason for such results probably lies in the fact that all examinees came from the banking industry which faced many online frauds in the last three years.

All those matrix calculations were done by using Web Java applet called Matrix Multiplier [43]. Only for matrix normalization purposes Microsoft Excel was used.

7. Conclusions and Future Research

From the Figure 5 ratios it can be seen as the e-banking is perceived as the most critical online business system (45,91 %), then the second is e-commerce (28,99 %) that is followed by m-banking (19,4 %), and Bitcoin cryptocurrency transaction system is perceived as the least critical with just 5,46 % of concern. It's also important to say that obtained results where e-banking is perceived as the most critical for information security professionals and also for business users lies in the fact that e-banking is still dominant online payment systems where many e-banking frauds occurred in the last couple of years. The new vector (or target) of online fraud activities is expected to be connected with mobile devices, e.g. fake m-banking apps on stores, fake SMS apps (used for obtaining transaction codes), mobile CryptoLocker, etc. So in that context, there is a possibility that repeated research would produce different ratios between online payment systems.

Due to the deluge of security threats and vulnerabilities, and often the lack of time and resources to combat them efficiently in the business environment, prioritizing risks and addressing the most critical ones seems essential. This paper presented a new model for prioritizing critical risks as well as the evaluation of the security (business) solutions, wherein the model is based on the VECTOR matrix method that is integrated into the AHP technique.

This AHP model is just a suggestion as to how to solve certain issues in IT security problem domain when multi-criteria decision-making issue appears related to time constraints and uncertainty. To prove the validity of the proposed model and raise its credibility and trustworthiness along with the appointed hypothesis, the model should to be tested on more case studies. This means that the feasibility and applicability of the proposed AHP model must be confirmed.

Since the VECTOR method for prioritization of critical IT assets or risks, following its definition, has limitations within the AHP model, so is the applicability of the hybrid AHP model also limited to certain areas of information security. To find out what are all those areas of information security in which the presented AHP model is actually applicable additional research is required. The proposed case studies (but not exclusive ones) are, as follows:

- Selection of the solution for online banking transaction monitoring
- Ranking of biometric solutions for digitalization of handwritten signature
- Selection of certain high critical security systems, e.g. firewall, intrusion detection/prevention system, proxies, load balancers, SIEM, VPNs, etc.
- Selection of certain cloud based solution
- Comparisons of security strengths of the most significant cryptocurrency systems
- Ethereum and smart contracts.

To further verify the validity and the results of the proposed hybrid AHP model, it is necessary to evaluate the alternatives by AHP technique according to common criteria that are otherwise relevant for online transaction systems, such as authentication, authorization, confidentiality, integrity and non-repudiation, together with availability as an additional criterion to completely cover the likewise necessary C-I-A security triad. Consequently, the received results would be compared with the results where VECTOR criteria are used for the ranking of alternatives to assess the accuracy of the proposed AHP model. The expected contributions are: The hybrid AHP model with VECTOR criteria for ranking of alternatives would be applicable to certain multi-criteria decision making problems related with information security risks and IT solutions.

Social and, even largely, economical contributions of the new AHP model for prioritizing security risks include possibilities of faster detection and solving of critical risks along with saving business costs. It is believed that the model of AHP technique with the integrated VECTOR matrix for criteria evaluation has a potential in dealing with risks as well as in evaluating certain security solutions. A strongpoint for this assertion would be that the AHP technique is more formal and precise then some other methods for risk prioritization, because the AHP technique has resulted from a proven mathematical model. However, future research are to discover its real feasibility and applicability.

References

[1] R. M. von Roessing, *The Business Model for Information Security*. 2010.

[2] Trustwave, "State of Risk Report State of Risk Report," 2015.

[3] pwc, "The Global State of Information Security Survey," *pwc*, 2016. [Online]. Available: http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html. [Accessed: 01-Jan-2016].

[4] R. Sailors, "7 Top Cyber Risks for 2015," *Protecting Tomorrow*, 2015. [Online]. Available: https://lp3-securit.com/wp-content/uploads/2015/02/PT_7-Cyber-Risks-for-2015.pdf. [Accessed: 01-Jan-2015].

[5] Ponemon Institute, "2015 Cost of Data BreachSstudy: Global Analysis," no. May, pp. 1–30, 2015.

[6] E. P. Information, "OSINT DASHBOARD," 2016.

[7] Trustwave, "2015 Trustwave Global Security Report," *Trust. Glob. Secur. Rep.*, 2015.

[8] Europe Central Bank, *Virtual Currency Schemes*. 2012.

[9] I. Engineering, E. Triantaphyllou, and S. H. Mann, "Using the Analytic Hierarchy Process for Decision Making in Engineering Applications : Some Challenges," *Int. J. Ind. Eng. Theory, Appl. Pract.*, vol. 2, no. 1, pp. 35–44, 1995.

[10] T. L. Saaty, "Decision making with the analytic hierarchy process," *Int. J. Serv. Sci.*, vol. 1, no. 1, p. 83, 2008.

[11] A. Hakemi, S. R. Jeong, I. Ghani, and M. G. Sanaei, "Enhancement of VECTOR method by adapting OCTAVE for risk analysis in legacy system migration," *KSII Trans. Internet Inf. Syst.*, vol. 8, no. 6, pp. 2118–2138, 2014.

[12] D. Maček, I. Magdalenić, and N. Ivković, "Information Security Risk Assessment in Financial Institutions Using VECTOR Matrix and OCTAVE Methods," 2011.

[13] R. Grinberg, "Bitcoin: An Innovative Alternative Digital Currency," *Hast. Sci. Technol. Law J.*, vol. 4, no. 1, pp. 159–208, 2015.

[14] M. Rosenquist, "Prioritizing Information Security Risks with Threat Agent Risk Assessment," *Intel Information Technology*, 2009. [Online]. Available: http://www.intel.com/Assets/en_US/PDF/whitepaper/wp_IT_Security_RiskAssessment.pdf. [Accessed: 01-Jan-2015].

[15] MITRE, "Risk Impact Assessment and Prioritization," *MITRE*, 2015. [Online]. Available: http://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-impact-assessment-and-prioritization. [Accessed: 01-Jan-2015].

[16] *Information technology. Security techniques. Information security risk management*. BSI, 2011.

[17] NIST, "NIST Special Publication," *Risk Manag. Guid. Inf. ...*, no. September, p. 95, 2012.

[18] R. a R. a. C. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process," *Young*, no. May, pp. 1–113, 2007.

[19] C. Carlson, A. Hutton, and A. Gilliam, *Technical Guide FAIR – ISO / IEC 27005 Cookbook*. 2010.

[20] International Organization for Standardization, "ISO/IEC 31010:2009 Risk management - Risk assessment techniques," *Risk Manag.*, vol. 31010, p. 92, 2009.

[21] Bitcoin, "Bitcoinwiki," *Bitcoin*, 2016. [Online]. Available: https://en.bitcoin.it/wiki/Bitcoin. [Accessed: 01-Jan-2016].

[22] Coinmarketcap, "Currencies," *Coinmarketcap*, 2016. [Online]. Available: http://coinmarketcap.com/currencies. [Accessed: 01-Jan-2016].

[23] A. Al Shehhi, M. Oudah, and Z. Aung, "Investigating factors behind choosing a cryptocurrency," *2014 IEEE Int. Conf. Ind. Eng. Eng. Manag.*, pp. 1443–1447, 2014.

[24] A. Hayes, "What factors give cryptocurrencies their value : An empirical analysis," no. December, 2015.

[25] P. Tasca, "Digital Currencies: Principles, Trends, Opportunities, and Risks," p. 110, 2015.

[26] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Consulted*, pp. 1–9, 2008.

[27] M. D. Sleiman, A. P. Lauf, and R. Yampolskiy, "Bitcoin Message: Data Insertion on a Proof-of-Work Cryptocurrency System," *2015 Int. Conf. Cyberworlds*, pp. 332–336, 2015.

[28] Search Engine Journal, "The 10 Most Popular Online Payment Solutions," *Search Engine Journal*, 2015. [Online]. Available: http://www.searchenginejournal.com/the-10-most-popular-online-payment-solutions/. [Accessed: 01-Jan-2015].

[29] D. Maček, I. Magdalenić, and N. Ivković, "Risk Assessment of the Bank's Noncompliance with Payment Card Industry Data Security Standard," pp. 305–311, 2012.

[30] I. Linkov, F. K. Satterstrom, J. Steevens, E. Ferguson, and R. C. Pleus, "Multi-criteria decision analysis and environmental risk assessment for nanomaterials," *J. Nanoparticle Res.*, vol. 9, no. 4, pp. 543–554, 2007.

[31] I. Linkov, F. K. Satterstrom, G. Kiker, C. Batchelor, T. Bridges, and E. Ferguson, "From comparative risk assessment to multi-criteria decision analysis and adaptive management: Recent developments and applications," *Environ. Int.*, vol. 32, no. 8, pp. 1072–1093, 2006.

[32] N. Xu and D. M. Zhao, "The Research of Information Security Risk Assessment Method Based on AHP Method," *Adv. Mater. Res.*, vol. 187, no. 4, pp. 575–580, 2011.

[33] M. Lee, "Information Security Risk Analysis Methods and Research Trends : AHP and Fuzzy Comprehensive Method," *Int. J. Comput. Sci. Inf. Technol.*, vol. 6, no. February, pp. 29–45, 2014.

[34] S. Smojver, "Selection of information security risk management method

using analytic hierarchy process (ahp)," *Cent. Eur. Conf. Inf. ...*, 2011.

[35] M. A. Mohyeddin, "FAHP-TOPSIS Risks Ranking Models in ISMS," pp. 879–882, 2014.

[36] J. Lv and Y. Wang, "A Ranking Method for Information Security Risk Management Based on AHP and PROMETHEE," *Manag. Serv. Sci. (MASS), ...*, no. 60803123, pp. 1–4, 2010.

[37] Owasp, "OWASP Top 10 - 2013," *OWASP Top 10*, p. 22, 2013.

[38] OWASP, "Mobile Top 10 2016-Top 10," *OWASP*, 2016. [Online]. Available: https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10. [Accessed: 01-Jan-2016].

[39] Symantec, "Internet Security Threat Report," vol. 20, no. April, p. 119, 2015.

[40] C. Labs and K. Down, "Top 8 Financial Malware," 2015.

[41] N. Etaher, G. R. S. Weir, and M. Alazab, "From ZeuS to Zitmo : Trends in Banking Malware 1," pp. 1386–1391, 2015.

[42] J. A. Alonso and M. T. Lamata, "Consistency in the analytic hierarchy process: a new approach," *Int. J. Uncertainty, Fuzziness Knowledge-Based Syst.*, vol. 14, no. 4, pp. 445–459, 2006.

[43] Joe Mcdonald, "Matrix Multiplying Calculator," *joemath*, 2010. [Online]. Available: http://www.joemath.com/applets/multmat/. [Accessed: 01-Jan-2016].