



Role of Social Networks in E-government: Risks and Security Threats



Rasim Alguliyev

Institute of Information Technology, Baku, AZERBAIJAN

 0000-0003-1223-7411  35770330500  V-7265-2018



Ramiz Aliguliyev

Institute of Information Technology, Baku, AZERBAIJAN

 0000-0001-9795-1694  A-1072-2013

Farhad Yusifov

Institute of Information Technology, Baku, AZERBAIJAN

 0000-0002-9114-9972  G-6787-2017

 farhadyusifov@gmail.com

ARTICLE INFO

Received: 23 August 2018

Accepted: 25 October 2018

Published: 12 November 2018

DOI: <https://doi.org/10.12973/ojcm/3957>

ABSTRACT

Social networks are becoming an important intermediary for interaction between governments, citizens, governmental agencies and business sectors. The popularization of social networks among users allows transforming public administration into open governance form and changing government-citizen relationships. There are various applications of social media to enable communication between users and share personal information. Currently, different attacks on social networks targeting the e-government system pose a great risk for users. In paper the role of social networks and security in e-government is examined. Potential threats targeting the confidentiality and security of each social network user are analyzed and classified. A multi-criteria evaluation method is proposed for analysis of social networks security threats. Potential threats are ranked according to the criteria determined by the Fuzzy TOPSIS method. In the numerical study, the social network security threats are evaluated and ranked according to selected criteria (such as interception of confidential information, reputation loss in government-citizen (G2C) relations and organization of social-political conflicts).

Keywords: e-government, social network, security threat, attack, multi-criteria evaluation, fuzzy TOPSIS

INTRODUCTION

Currently, social networks are very popular in the world. Millions of people use different forms of social networks that allow them to communicate with friends, relatives, and share personal information. However, popularity of social networks creates a great risk for their users (Fire, Goldschmidt, & Elovici, 2014; Kayes & Iamnitshi, 2017; Novak & Li, 2012; Rathore et al., 2017). Rapid increase in the amount of personal information shared by social network users turns them into a desirable target of the malicious users. When uploading multimedia content such as user photos, videos and others, there may be various problems with the privacy and security of user data (Dreßing, et al., 2014; Fire,

Goldschmidt, & Elovici, 2014; Gao, et al., 2011; Kayes & Iamnitchi, 2017). Uploaded multimedia content can carry information transmitted through the virus that begins distributing on the social network site and beyond its boundaries almost immediately after uploading. Interception of sensitive personal information as well as spam, malware, social bots and identity theft can be carried out as a result of malicious attacks (Fire, Goldschmidt, & Elovici, 2014; Rathore, et al., 2017; Zhang & Gupta, 2016). At the same time, the personal information intercepted for malicious purposes may be subject to serious cybercrime such as bank fraud or transaction fraud using user-sensitive information (Rathore, et al., 2017; Zhang & Gupta, 2016). According to researchers, the attacks on social networks have a wide range of applications ranging from the interception of personal data to distribution of malware (Raggio, 2016; Rathore et al., 2017).

An extremely skillful attack can endanger the corporate network and is a serious threat to users. The Internet Security Threat Report (2016) shows that the increase in hackers' use of social networks cannot be denied (Symantec, 2016). According to researchers and experts and analysis of existing statistics of attacks on social networks shows that social networks for hackers are the best way to realizing cybercrime (Fire, Goldschmidt & Elovici, 2014; Kayes & Iamnitchi, 2017; Rathore et al., 2017; Zhang & Gupta, 2016).

Many researchers and companies dealing with security issues offer different solutions to reduce potential threats related to increase of social networks threats (Cao et al., 2016; Fire, Goldschmidt, & Elovici, 2014; Rathore et al., 2017; Zhang & Gupta, 2016). Many studies have investigated security issues in social networks (Fire, Goldschmidt, & Elovici, 2014; Gao et al., 2011; Jin & et al., 2013; Novak & Li, 2012; Rathore et al., 2017; Zhang & Gupta, 2016).

In the research, social networks threats are analyzed and a summary of the various current threats is reviewed. The goal is to assess the potential threats in order to achieve a secure, efficient and secure social networking ecosystem. Identifying, evaluating and preventing threats to the security of social networks allow understanding the basic principles and perspectives of the social network security concept. In the research, the potential threats to social security are evaluated and the perspective research directions are identified.

ROLE AND SECURITY ISSUES OF SOCIAL NETWORKS IN E-GOVERNMENT

In recent years, the rapid development of ICT and the widespread use of social networks enable the transformation of public administration into open governance form and change the government-citizen relationships (Alguliyev & Yusifov, 2018; Dwivedi et al., 2017; Karakiza, 2014; Landsbergen, 2010). In other words, social networks are a bilateral communication tool between government and society that promote government transparency and the development of a democratic society (Banday & Mattoo, 2013; Bergquist et al., 2017; Bertot, Jaeger, & Grimes, 2010; Song & Lee, 2016). Transparency in governance can be achieved by establishing a feedback mechanism on government-citizen (G2C) relationships.

The implementation of the latest technologies, applications in social media (such as blogs, Facebook, Twitter, and Google+) allows governments to take advantage of new communication and interaction tools (Alguliyev, & Yusifov, 2018; Dwivedi et al., 2017; Khan, Swar, & Lee, 2014; Mcnamara, 2011). On the other hand, social media is becoming a platform providing everyone with easy access to the Internet and government is joining it to connect with its citizens in order to increase citizen engagement and commitment

level. Network societies can function simultaneously in several directions: connecting people to reach a certain goal, dissemination of information, flexible mechanisms for regulating the political course, citizen-government relations, and so on. (Karakiza, 2014; Khasawneh & Abu-Shanab, 2013).

Particular attention should be paid to the application of key components of e-government in the most dynamically developing social networks in the field of modern social communications in the context of existing research, as well as identifying potential risks and adverse trends in the content exchange process. Researches show that in the past few years, a number of topical research trends have emerged with application of Web 2.0 technologies in the e-government (Alguliyev & Yusifov, 2018; Alotaibi, Ramachandran, et al., 2016; Chun et al., 2010, Parveche & Sachs, 2010; Rodruguez-Bolivar, 2017; Ubaldi, 2013). Researches on Web 2.0, social media, social networks and their use in the public sector show that issues such as the formation of social media and the role of social networks in public administration have been widely studied (Alguliyev & Yusifov, 2018; Kaur & Saini, 2016; Magro, 2012; Park et al., 2016). Key research areas include the role of social networks building a feedback between e-government and citizen, security issues establishing interactions with public authorities using social networks, transformation of social culture and management forms in the use of social media in e-government.

Social networks have a significant impact on the performance of governments. For example, as a result of the survey, it has been shown that the impact of social media on the political activity of citizens and political participation is increasingly important (Grubmüller, Götsch, & Krieger, 2013; Kamiloglu & Erdogan, 2014; Park et al., 2016; Rainie et al., 2012). Experts note that social media will help governments to become more transparent by providing citizens with better service and access to information, by opening an active channel with them, and ultimately empowering citizens (Bertot, Jaeger & Grimes, 2010; Khasawneh & Abu-Shanab, 2013; Song & Lee, 2016). Also, if governments use such sites effectively, it will enable them to become more effective and active participants in society. In terms of e-participation, social media provides new communication tools to quickly and efficiently deliver any message or news from governments (Aladallah, Cheung, & Lee, 2015; Alguliyev & Yusifov, 2018). Citizens can participate in online discussions with their local and national governments on issues of public interest. This will create a more open, transparent and mutually acceptable relationship between citizens and governments (Alguliyev & Yusifov, 2018; Khasawneh & Abu-Shanab, 2013).

Note that public authorities using social networking analyses pay attention to people as citizens and not as customers and consumers, and expand their activities in public-political areas. Therefore, social media analytics aimed at government purposes requires better judgment for the legal and ethical aspects of various reasons (Grubmüller, Götsch, & Krieger, 2013; Park et al., 2016; Rainie et al., 2012).

First of all, the concept of confidentiality in social media is almost completely changed (Rathore et al., 2017). Participants are less concerned to share personal information about themselves and their friends. It is difficult for the user to distinguish which information is for public or private use. The concept of confidentiality is becoming increasingly incomprehensible and in general, the lack of clear media confidentiality in ICT field and social media accelerates this process. While the problem of confidentiality seems to be less important for social media users, empirical evidence suggests that such concerns are rising when users communicate directly with government agencies (Facebook^{1,2}, 2018;

Rathore et al., 2017; Silic & Back, 2016). As a result, citizens' acceptance of the use of the social media by the governments requires legitimacy. Therefore, it is essential for governments to comply with the existing legal norms to ensure the safety and confidentiality of citizens' information (Grubmüller, Götsch, & Krieger, 2013; Park et al., 2016).

To protect confidentiality, governments should only use publicly available information. This means that with the help of appropriate analytical tools, citizens' information they share in their personal accounts should be collected, but they must limit them to public listed posts. In spite of the numerous advantages of social networks such as functional element of e-government in the Internet, they remain a real threat to public security. In recent years, social networks have become even more popular and, according to statistics, the number of users is expected to grow rapidly every year by 2020 (Rathore et al., 2017). At the same time, the growth dynamics of users has dramatically increased the number of security vulnerabilities that impact users' confidentiality.

Users share a large number of personal information on social networks, and this makes them a target for various types of Internet threats including identity theft, spamming, phishing, online predators, Internet fraud and so on. (Fire, Goldschmidt & Elovici, 2014; Kayes & Iamnitshi, 2017; Novak & Li, 2012; Raggo, 2016; Rathore et al., 2017). Social networks provide extensive opportunities for hackers to identity theft. In such types of attacks, a malicious person, without the user's consent, can intercept his or her personal information, including bank accounts, phone numbers, addresses etc., and use them to commit cybercrime. For example, many social networks, such as Facebook, offer game apps to their users. These applications require personal information such as user credit card information, phone number, email address etc. to complete the registration process. Of course, the risk of personal data theft and phishing attacks is increased when a user provides the phone number and credit card information. In some cases, applications may cause the user to resort distract the user's attention to harmful content and damage their reputation.

Another important issue is that many companies collect information from different sources, third-party resources, including social networks to create a user profile to sell products and disclosure user behavior. Social network users are unable to determine for which purpose the shared data will be used, due to the unauthorized collection of user's data and the unawareness of the users about these technologies. For example, user data can be transmitted to law enforcement for security reasons or may be used by the vendor for marketing purposes. In this regard, social networking profile, collected large volume of personal data, the user behavior data etc. can directly affect the user. (CareerBuilder; Facebook^{1,2}, Dreßing et al., 2014; Khan, Swar, & Lee, 2014; Rathore et al., 2017; Silic & Back, 2016). Note that regardless of how convenient and effective the e-government system is, if it does not provide reliable protection of confidential information it will always face with the resistance of the citizens, and in this case it is very difficult to recover lost trust.

SOCIAL NETWORKS SECURITY THREATS

Social networks are currently very popular and the number of their users is growing rapidly. Social networks such as Facebook, Flickr and Twitter allow billions of users to share personal data and multimedia data with friends, relatives and other online users. User data is used illegally by malicious users and various organizations for the purpose of increasing their profits. There are many security threats in the social network that

threaten users' shared data (Fire, Goldschmidt & Elovici, 2014; Kayes & Iamnitchi, 2017; Novak & Li, 2012; Rathore et al., 2017).

One of the most noticeable potentially harmless options in the social networking context can be the unauthorized use of personal information for advertisement purposes, selection of the potential acquaintances or selection of content that may be of interest. These methods are regarded as a standard mechanism within social networks and everyone is aware that personal information is collected, analyzed and used for various purposes, including commercial use (Sandmark, 2011). The transfer of personal data from various social networks has already been confirmed for a fact (CareerBuilder; Facebook^{1,2}, Rathore et al., 2017). One of the biggest problems for users is that, as a consequence of the social network's fault, multiple user-specific data leakage may be noted within the framework of various projects. One of the causes of serious disturbance is the hacking of user accounts or account loss and the intercept of all personal information. When this situation becomes massive, more serious problems occur. There are many potential threats to users such as technical vulnerabilities, viruses, Trojan horse, phishing and other malicious software, and can be used to intercept the user's confidential information (Raggio, 2016; Silic & Back, 2016). Phishing attack is one of the most widespread attacks by cybercriminals according to experts, and the main target is Internet payments, Internet banking, online games, Internet stocks, Web 2.0 technology used sites and so on (Raggio, 2016; Rathore et al., 2017; Silic & Back, 2016).

In addition to the threat of personal data manipulation, social networks are a tool for mass protests in the context of public security threats. The destructive challenges in social networks are exposed to external interference, causing government-citizen conflicts, protests in a short period of time. For example, in research Nien (2017), the role of social media in establishing a chain of equivalence between activists participating in protest movements is explored. Note that socially trusted social networks are used quite successfully in the e-government segment for the protection of government interests, achieving transparency in government-citizen relations, enhancing effectiveness in decision-making and enhancing e-participation mechanisms.

In literature, threats are classified into 4 categories (multimedia content threats, traditional threats targeting personal information, social-oriented threats, threats to children safety) (Fire, Goldschmidt & Elovici, 2014; Kayes & Iamnitchi, 2017; Rathore et al., 2017).

The first category includes multimedia content threats used to user profiles disclosure. Obviously, content sharing is one of the most important functions of social networks. The most common form of this type of data is multimedia content. However, shared high-quality images, videos are used in a variety of ways, increasing the probability of interception of location information, face recognition, and other data, and creates conditions for illegal use.

The second category includes traditional threats. Vulnerabilities in the social network infrastructure are used to attack users in different ways. Phishing, malicious software for intercepting personal data etc. can be shown as traditional attack methods. This information is used as a very effective tool for malicious acts. Malicious person can commit more serious cybercrimes after intercepting confidential information, bank information etc.

The third category includes social threats. These threats have more coverage and disclosure of social relationships among social network users is a potential threat to them.

Table 1. Social networks security threats

Social networks security threats			
Multimedia content threats	Traditional threats targeting individual information	Social threats	Threats targeting children
Multimedia content exposure	Phishing	Corporate espionage	Cyber-grooming
Disclosure of sensitive information	Malware	Cyber-stalking	Cyber-bullying
Content manipulation	Fake profiles	Impact to social opinion	Cyber-blackmail
Metadata disclosure	Spam	Reputation loss	Cyber-suicide
Links disclosure and redirection	Fake links	Encouraging social confrontation on racial, ethnic and religious grounds	Malicious content addiction
Unauthorized access to videoconferences / messages	Violation of user anonymity	Destructive provocation	Incite to bad habits
Fake tagging and sharing	Profile cloning	Forming fake image / reputation	Internet addiction
Unauthorized disclosure and use of information	Disclosure of relations	Creating target groups	Abuse of trust

Malicious persons may deliberately commit cyber-crime against a certain social group, for example a company employee, by disclosing the relationships between social network users in different ways. For example, people from different social groups can be instigated to commit cybercrime, espionage, share malicious information etc., being motivated by offered gifts, money or due to blackmail.

The fourth category includes threats targeting children and teenagers. Obviously, children and teenagers face many threats on social networks. However, there are a number of threats that specifically target young people and teenagers in the social network. These threats include children's cyber-bullying, cyber-stalking, cyber-blackmail, cyber-grooming, abuse of trust and so on. For example, in some cases cyber threats to children can have disastrous consequences, and in practice, there are facts about children committing suicides to end their lives. Social network threats can be categorized as shown in [Table 1](#).

In literature, various categories of social networks security threats are classified (Fire, Goldschmidt & Elovici, 2014; Rathore et al., 2017). The types of threats and their impact on users are analyzed and classified by organizations and research institutions dealing with security issues (Kayes & Iamnitchi, 2017; Novak & Li, 2012).

Thus, expanding the capabilities of e-government in social networks has a significant impact on socio-communication processes and the development of e-democracy in the country. Besides, increased access to information resources and sources increases the number of threats and risks. Note that information interaction is an essential component of e-government, information security is a preventive measure aimed at struggle cyber-terrorism and interception of personal information. Failure to maintain the confidentiality of personal data, regardless of whether the e-government system is effective, transparent and comfortable will result in the loss of citizens' trust in the system and the failure of the e-government project in general. In this regard, the evaluation of potential social network security threats allows the development of more effective management methods.

EVALUATION OF SOCIAL NETWORKS SECURITY THREATS BASED ON FUZZY TOPSIS METHOD

Nowadays, multi-criteria decision-making (MCDM) methods are widely practiced in almost all fields of science. In literature, MCDM methods can be used in various fields, such as personnel selection, selection of equipment in production, projects selection, etc. Literature analysis shows that MCDM methods have been applied in various fields (Afshari et al., 2017; Khorami & Ehsani, 2015; Tuan, 2017). Over time, MCDM models have found its application in solution of various complex issues of decision-making. AHP, TOPSIS, VIKOR, PROMETHEE, ELECTRE, SAW, MOORA, MULTIMOORA and other methods were used to solve decision-making problems (Alguliev et al., 2016; Karabasevica, 2015; Khorami & Ehsani, 2015; Mardani et al., 2015). There are research studies on the comparison and review of MCDM methods (Khorami & Ehsani, 2015; Mardani et al., 2015; Stanujkic et al., 2013; Turskis & Zavadskas, 2011; Zavadskas et al., 2014).

Literature analysis shows that there are numerous research studies on the application of fuzzy MCDM methods. Fuzzy MCDM are widely used to rank the solution alternatives characterized by fuzzy values based on multiple criteria (Alguliyev et al., 2016; Capaldo & Zollo, 2001; Dursun & Karsak, 2010; Kelemenis & Askounis, 2010; Rouyendegh & Erkan, 2013; Tuan 2017).

A model for evaluating the social networks security threats based on the fuzzy TOPSIS (Technique for Order Preferences by the Similarity to Ideal Solution) method is proposed in this paper. The TOPSIS method allows calculating an integral index for alternatives taking into account many criteria and provides ranking of alternatives for the procedure of selection the options with the decision maker. The Fuzzy TOPSIS method was used to select and rank the alternatives and make group decisions in a number of application issues (Alguliyev et al., 2016; Capaldo & Zollo, 2001; Chang, Yeh, & Chang, 2013; Dursun & Karsak, 2010; Kelemenis & Askounis, 2010; Rouyendegh & Erkan, 2013; Tuan, 2017). Note that the most commonly used AHP (Analytical Hierarchy Processes) method for multi-criteria ranking of alternatives has a number of deficiencies. This includes difficulty of calculation, contradiction of expert estimates due to large number of experts etc. (Alguliyev et al., 2016).

Let's review the evaluation of social network security threats based on fuzzy TOPSIS method.

Let's say that n number of alternative sets A_i , $i = 1, 2, \dots, n$ must be evaluated by a group of K decision makers E_k ($k = 1, 2, \dots, K$) based on m number of criteria C_j , $j = 1, 2, \dots, m$. Criteria are not inter-dependent, are equally important and can be evaluated.

Evaluation is carried out by each decision maker E_k in order to determine decision matrix $S^k = \|s_{ij}^k\|$, $i = 1, 2, \dots, n$; $j = 1, 2, \dots, m$; $k = 1, 2, \dots, K$.

TOPSIS method consists of following stages (Chang, Yeh, & Chang, 2013; Alguliyev et al., 2016).

Step 1: Construct a decision matrix for the ranking.

Step 2: Choose of linguistic variables for the alternatives with the respect to criteria.

Step 3: Calculation of aggregate fuzzy rating for alternatives.

Step 4: Normalize the aggregate fuzzy decision matrix.

Step 5: Construct normalized fuzzy decision matrix.

Table 2. Linguistic variables for threat evaluation

Linguistic variables	TFNs
Very high	(8, 9, 10)
High	(6, 7, 8)
Medium	(4, 5, 6)
Weak	(2, 3, 4)
Very weak	(1, 1, 2)

Table 3. Individual fuzzy decision matrix of E_1

Alternatives	Criteria		
	C_1	C_2	C_3
A_1	(6, 7, 8)	(4, 5, 6)	(1, 1, 2)
A_2	(4, 5, 6)	(8, 9, 10)	(4, 5, 6)
A_3	(4, 5, 6)	(6, 7, 8)	(2, 3, 4)
A_4	(2, 3, 4)	(1, 1, 2)	(6, 7, 8)
A_5	(4, 5, 6)	(2, 3, 4)	(1, 1, 2)

Step 6: Determine of fuzzy positive ideal solution and fuzzy negative ideal solution.

Step 7: Calculate the distance of each alternative from the fuzzy positive ideal solution and fuzzy negative ideal solution.

Step 8: Calculation of CI_i closeness index of each alternative. The closeness index CI_i for each A_i is calculated as following:

$$CI_i = \frac{D_i^-}{D_i^- + D_i^+}, i = 1, 2, \dots, n$$

Step 9: Ranking the alternatives. Alternatives A_i are ranked in descending order based on CI_i value and select the alternatives with highest CI_i value.

NUMERICAL EXPERIMENT

Let's assume that malicious attacks targeting the e-government system are committed against social network users. Social network security threats are likely to be: A_1 - phishing; A_2 - fake user profiles; A_3 - unauthorized access to user messages; A_4 - sensitive information disclosure; A_5 - cyber-stalking.

The criteria used to evaluate the threats include: C_1 - interception of confidential information; C_2 - reputation loss in government-citizen (G2C) relations; C_3 - organize of social-political conflicts.

Let's assume that in this case, five alternative sets A_i ($i = 1, 2, \dots, 5$) are evaluated by a group consisting of five decision makers (experts) E_k , in relation to three criteria C_j ($j = 1, 2, \dots, m$).

The appropriate linguistic variables are represented to evaluate alternatives to each criterion. Decision makers use the TFN linguistic variables provided in **Table 2** to evaluate alternatives in relation to criteria.

According to Step 1 and Step 2, decision matrixes based on evaluation of decision makers (experts) in accordance with 5 alternatives are shown in **Table 3-7**.

Table 4. Individual fuzzy decision matrix of E_2

Alternatives	Criteria		
	C_1	C_2	C_3
A_1	(4, 5, 6)	(2, 3, 4)	(4, 5, 6)
A_2	(2, 3, 4)	(6, 7, 8)	(2, 3, 4)
A_3	(8, 9, 10)	(4, 5, 6)	(2, 3, 2)
A_4	(1, 1, 2)	(2, 3, 4)	(4, 5, 6)
A_5	(6, 7, 8)	(2, 3, 4)	(8, 9, 10)

Table 5. Individual fuzzy decision matrix of E_3

Alternatives	Criteria		
	C_1	C_2	C_3
A_1	(8, 9, 10)	(4, 5, 6)	(2, 3, 4)
A_2	(6, 7, 8)	(1, 1, 2)	(4, 5, 6)
A_3	(2, 3, 4)	(6, 7, 8)	(4, 5, 6)
A_4	(4, 5, 6)	(8, 9, 10)	(1, 1, 2)
A_5	(2, 3, 4)	(4, 5, 6)	(6, 7, 8)

Table 6. Individual fuzzy decision matrix of E_4

Alternatives	Criteria		
	C_1	C_2	C_3
A_1	(4, 5, 6)	(1, 1, 2)	(4, 5, 6)
A_2	(6, 7, 8)	(2, 3, 4)	(6, 7, 8)
A_3	(8, 9, 10)	(6, 7, 8)	(4, 5, 6)
A_4	(1, 1, 2)	(8, 9, 10)	(2, 3, 4)
A_5	(2, 3, 4)	(4, 5, 6)	(2, 3, 4)

Table 7. Individual fuzzy decision matrix of E_5

Alternatives	Criteria		
	C_1	C_2	C_3
A_1	(6, 7, 8)	(1, 1, 2)	(6, 7, 8)
A_2	(2, 3, 4)	(6, 7, 8)	(4, 5, 6)
A_3	(8, 9, 10)	(4, 5, 6)	(1, 1, 2)
A_4	(1, 1, 2)	(2, 3, 4)	(6, 7, 8)
A_5	(6, 7, 8)	(4, 5, 6)	(8, 9, 10)

Table 8. Creating normalized aggregate fuzzy decision matrix

Alternatives	Criteria		
	C_1	C_2	C_3
A_1	(0.636, 0.750, 0.864)	(0.333, 0.417, 0.556)	(0.412, 0.500, 0.647)
A_2	(0.455, 0.568, 0.682)	(0.639, 0.750, 0.889)	(0.588, 0.735, 0.882)
A_3	(0.773, 0.886, 1.000)	(0.722, 0.861, 1.000)	(0.353, 0.441, 0.588)
A_4	(0.205, 0.250, 0.364)	(0.583, 0.694, 0.833)	(0.559, 0.676, 0.824)
A_5	(0.455, 0.568, 0.682)	(0.417, 0.528, 0.667)	(0.735, 0.853, 1.000)

According to step 4, the normalized aggregate fuzzy decision matrix for benefit criterion is shown in **Table 8**.

According to step 6, fuzzy positive ideal solution A^+ and fuzzy negative ideal solution A^- are determined according to the normalized values.

$$A^+ = \{ 1.000, 1.000, 1.000 \}, A^- = \{ 0.205, 0.333, 0.353 \}$$

According to Step 8 and 9, A_1 alternatives are ranked by descending order based on CI_i closeness index values.

As described in **Table 9**, social networks security threats are ranked in accordance with A_3, A_2, A_5, A_1 and A_4 sequence. As the result shows in this case, according to the criteria selected, unauthorized access to user messages is the greatest threat to the social network security.

Table 9. Ranking of threats

Alternatives	CI_i	Rank
A_1	0,430	4
A_2	0,544	2
A_3	0,598	1
A_4	0,380	5
A_5	0,504	3

CONCLUSION

Nowadays, social networks are very popular among users and the number of users is growing rapidly. Such popularity of social networks allows transforming public administration into open governance form. From this point of view, social networks create a bilateral communication environment between government and citizen that promotes government transparency and the development of a democratic society. Note that transparency in the governance can be achieved through the creation of a feedback mechanism on government-citizen relations.

However, the popularity of social networks creates great risks for their users. Rapid increase in the amount of personal information shared by social network users turns them into a desirable target of the malicious people. At the moment, various attacks targeting the e-government system are carried out against social networks and these are considered a major threat to users. The paper explores the role of social networks in e-government and security issues. Potential social networks security threats are analyzed and classified. The attacks on social networks are classified into 4 categories (multimedia content threats, personal information security threats, socially directed threats, threats targeting children).

The paper recommends a multi-criteria evaluation method to analyze social security threats. Potential threats are categorized according to the criteria determined by the fuzzy TOPSIS method. The numerical experiment assumes that social network users will be exposed to a variety of malicious attacks (phishing; fake user profiles; unauthorized access to user messages; sensitive information disclosure; cyber-stalking). Based on the proposed approach, the threats are evaluated and ranked based on criteria such as interception of confidential information, reputation loss in government-citizen (G2C) relations and organization of social-political conflicts. The calculation process of the proposed method is not complicated and the results of a numerical experiment are shown. In future studies, empirical research will be preferred using hybrid methods to evaluate threats in order to form a safe and secure social network eco-environment.

ACKNOWLEDGEMENT

This work was supported by the Science Development Foundation under the President of the Republic of Azerbaijan - Grant № EIF-KETPL-2-2015-1(25)-56/05/1

REFERENCES

- Afshari, A. R., Nikolić, M., & Akbari, Z. (2017), Personnel selection using group fuzzy AHP and SAW methods. *Journal of engineering management and competitiveness*, 7(1), 3-10.
- Aladallah, M., Cheung, Y., & Lee, V. (2015) Enabling Citizen Participation in Gov 2.0: An Empowerment Perspective. *Electronic Journal of e-Government*, 13(2).

- Alguliyev, R. M., & Yusifov, F. F. (2018) The Role and Impact of Social Media in E-Government, Book Chapter in L. Alcaide-Muñoz & F. J. Alcaraz-Quiles (Eds.) *Optimizing E-Participation Initiatives Through Social Media* (pp. 28-53), The Advances in Wireless Technologies and Telecommunication book series, USA, IGI Global.
- Alguliyev, R. M., Aliguliyev, R. M., & Mahmudova, R. M. (2016). A Fuzzy TOPSIS+Worst-Case Model for Personnel Evaluation Using Information Culture Criteria. *International Journal of Operations Research and Information Systems*, 7(4), 38-66. <https://doi.org/10.4018/IJORIS.2016100102>
- Alotaibi, R. M., Ramachandran, M., et al. (2016). Factors Affecting Citizens' use of Social Media to Communicate with the Government: A Proposed Model. *The Electronic Journal of e-Government*, 14(1), 60-72.
- Banday, M. T., & Mattoo, M. M. (2013). Social Media in e-Governance. *Scientific Research Journal*, 47-56.
- Bergquist, M., et al. (2017). From e-government to e-governance: social media and public authorities legitimacy work. In *Proceedings of the 25th European Conference on Information Systems (ECIS)*, Guimarrés, Portugal, June 5-10, 858-872.
- Bertot, J. C., Jaeger, P. T., & Grimes, J. M. (2010). Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Government Information Quarterly*, 27(3), 264–271. <https://doi.org/10.1016/j.giq.2010.03.001>
- Cao, J., Li, Q., Ji, Y., et al. (2016). Detection of forwarding-based malicious urls in online social networks. *Int. J. Parallel Program*, 44(1), 163–180. <https://doi.org/10.1007/s10766-014-0330-9>
- Capaldo, G., & Zollo, G. (2001). Applying fuzzy logic to personnel assessment: A case study, *Omega*, 29(6), 585-597. [https://doi.org/10.1016/S0305-0483\(01\)00047-0](https://doi.org/10.1016/S0305-0483(01)00047-0)
- CareerBuilder. (n.d.). Number of Employers Using Social Media to Screen Candidates Has Increased 500 Percent over the Last Decade. Retrieved on 15 April 2018 from www.careerbuilder.com
- Chang, Y.-H., Yeh, C.-H., & Chang, Y.-W. (2013). A new method selection approach for fuzzy group multicriteria decision making. *Applied Soft Computing*, 13(4), 2179–2187. <https://doi.org/10.1016/j.asoc.2012.12.009>
- Chun, S., Shulman, S., et al., (2010). Government 2.0: Making connections between citizens, data and government. *Information Polity*, 15, 1–9. <https://doi.org/10.3233/IP-2010-0205>
- Dreßing, H, Bailer, J., Anders, A., et al. (2014). Cyberstalking in a large sample of social network users: prevalence, characteristics, and impact upon victims. *Cyberpsychol, Behav. Soc. Netw.*, 17(2), 61–67. <https://doi.org/10.1089/cyber.2012.0231>
- Dursun, M., & Karsak, E. E. (2010). A fuzzy MCDM approach for personnel selection. *Expert Systems with Applications*, 37, 4324-4330. <https://doi.org/10.1016/j.eswa.2009.11.067>
- Dwivedi, Y.K. & et al., (2017) Exploring the Role of Social Media in e-Government: an Analysis of Emerging Literature. *ICEGOV 2017*, 97-106. <https://doi.org/10.1145/3047273.3047374>
- Facebook¹ suspends 200 apps over data misuse investigation (2018). Retrieved on 15 April 2018 from <https://www.reuters.com>
- Facebook² temporarily blocks new apps from joining its platform (2018). Retrieved on 15 April 2018 from www.theverge.com

- Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online social networks: threats and solutions. *IEEE Commun. Surv. Tut.*, 16(4), 2019-2036. <https://doi.org/10.1109/COMST.2014.2321628>
- Gao, H., Hu, J., Huang, T., et al. (2011). Security issues in online social networks. *IEEE Internet Comput.*, 15(4), 56–63. <https://doi.org/10.1109/MIC.2011.50>
- Grubmüller, V., Götsch, K., & Krieger, B. (2013). Social media analytics for future oriented policy making. *European Journal Futures Research*, 1(20), 1-9. <https://doi.org/10.1007/s40309-013-0020-7>
- Jin, L., Chen, Y., Wang, T., et al. (2013). Understanding user behavior in online social networks: a survey. *IEEE Commun. Mag.*, 51(9), 144–150. <https://doi.org/10.1109/MCOM.2013.6588663>
- Kamiloglu, F., & Erdogan, E. (2014). Effects of Social Media on Civil and Political Participation and a Field of Survey over on Facebook. *Online Journal of Communication and Media Technologies*, 4(3), 47-77.
- Karabasevica, D., Stanujkic, D., & Urosevic, S. (2015). The MCDM model for personnel selection based on SWARA and ARAS methods. *Management*, 77, 43-52.
- Karakiza, M. (2014). The impact of Social Media in the Public Sector. *Proceedings of the International Conference on Strategic Innovative Marketing*, 384-392.
- Kaur, R., & Saini, D. (2016). Social Networking and e-Government: The Role & Its Impact. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, 5(3), 811-819.
- Kayes, I., & Iamnitshi, A. (2017). Privacy and security in online social networks: A survey. *Online Social Networks and Media*, 3-4, 1–21. <https://doi.org/10.1016/j.osnem.2017.09.001>
- Kelemenis, A., & Askounis, D. (2010). A new TOPSIS-based multi-criteria approach to personnel selection. *Expert Systems with Applications*, 37, 4999–5008. <https://doi.org/10.1016/j.eswa.2009.12.013>
- Khan, G. F., Swar, B., & Lee, S. K. (2014) Social Media Risks and Benefits: A Public Sector Perspective. *Social Science Computer Review*, 32(5), 606-627. <https://doi.org/10.1177/0894439314524701>
- Khasawneh, R. T., & Abu-Shanab, E. A. (2013). E-Government and Social Media Sites: The Role and Impact. *World Journal of Computer Application and Technology*, 1(1), 10–17.
- Khorami, M., & Ehsani, R. (2015). Application of Multi Criteria Decision Making approaches for personnel selection problem: A survey. *International journal of engineering research and applications*, 5(5), 14-29.
- Landsbergen, D. (2010). Government as part of the revolution: using social media to achieve public goals. *Electron J e-Govern*, 8(2), 135–147.
- Magro, M. J. (2012). A Review of Social Media Use in E-Government. *Adm. Sci.*, 2, 148-161. Retrieved on 15 April 2018 from www.mdpi.com/journal/admsci <https://doi.org/10.3390/admsci2020148>
- Mardani, A., Jusoh, A., et al. (2015). Multiple criteria decision-making techniques and their applications – a review of the literature from 2000 to 2014. *Economic Research – Ekonomiska Istrazivanja*, 28(1), 516-571. <https://doi.org/10.1080/1331677X.2015.1075139>
- Mcnamara, J. (2011). *Social Media Strategy and Governance: Gaps, Risks and Opportunities*. Sydney, Australia: University of Technology Sydney.

- Nien, W. L. (2017). What is the Role of Social Media in Establishing a Chain of Equivalence between Activists Participating in Protest Movements? *Online Journal of Communication and Media Technologies*, 7(3), 182-2015.
- Novak, E., & Li, Q. (2012) A Survey of Security and Privacy in Online Social Networks, College of William and Mary Computer Science. *Technical Report*, 1–32.
- Park, M. J., Kang, D., Rho, J. J., & Lee, D. H. (2016). Policy Role of Social Media in Developing Public Trust: Twitter communication with government leaders. *Public Management Review*, 18(9), 1265–1288. <https://doi.org/10.1080/14719037.2015.1066418>
- Parvcek, P., & Sachs, M. (2010). Open Government–Information Flow in Web 2.0. *Eur. J. ePractice*, 9, 57–68.
- Rago, M. (2016). *Anatomy of a Social Media Attack*. Retrieved on 14 May 2018 from www.darkreading.com/analytics/anatomy-of-a-social-media-attack/a/d-id/1326680
- Rainie, L., et al. (2012). *Social media and political engagement, pew internet & American life project*. Pew Research Center: Washington DC. Retrieved on 14 May 2018 from <http://pewinternet.org>
- Rathore, Sh., Sharma, P. K., Loia, V., et al. (2017). Social network security: Issues, challenges, threats, and solutions. *Information Sciences*, 421, 43–69. <https://doi.org/10.1016/j.ins.2017.08.063>
- Rodríguez-Bolívar, M. P. (2017). Governance Models for the Delivery of Public services Through the Web 2.0 technologies: A political view in large Spanish Municipalities. *Social Science Computer Review*, 35(2), 203–225. <https://doi.org/10.1177/0894439315609919>
- Rouyendegh, B. D., & Erkan, T. E. (2013). An application of the fuzzy ELECTRE method for academic staff selection, *Human Factors and Ergonomics in Manufacturing and Service Industries*, 23(2), 107-115. <https://doi.org/10.1002/hfm.20301>
- Sandsmark, F. (2011). From Social Media to Social Commerce. *Proceeding of Microsoft Global High Tech Summit*.
- Silic, M., & Back, A. (2016). The dark side of social networking sites: Understanding phishing risks. *Computers in Human Behavior*, 60, 35-43, <http://dx.doi.org/10.1016/j.chb.2016.02.050>
- Song, C., & Lee, J. (2016). Citizens' Use of Social Media in Government, Perceived Transparency, and Trust in Government. *Public Performance & Management Review*, 39(2), 430–453. <https://doi.org/10.1080/15309576.2015.1108798>
- Stanujkic, D., Djordjevic, B., & Djordjevic, M. (2013). Comparative analysis of some prominent MCDM methods: A case of ranking Serbian banks. *Serbian journal of management*, 8(2), 213-241. <https://doi.org/10.5937/sjm8-3774>
- Symantec (n.d.) Internet Security Threat Report. Retrieved on 14 May 2018 from www.symantec.com
- Tuan, N. A. (2017). Personnel Evaluation and Selection using a Generalized Fuzzy Multi-Criteria Decision Making. *International Journal of Soft Computing*, 12(4), 263-269.
- Turskis, Z., & Zavadskas, E. K. (2011). Multiple criteria decision making (MCDM) methods in economics: an overview. *Technological and economic development of economy*, (2), 397-427.
- Ubaldi, B. (2013). Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives. *OECD Working Papers on Public Governance*, 22, 15-35.

Zavadskas, E. K., Turskis, Z., & Kildienė, S. (2014). State of art surveys of overviews on MCDM/MADM methods. *Technological and Economic Development of Economy*, 20(1), 165-179. <https://doi.org/10.3846/20294913.2014.892037>

Zhang, Z., & Gupta, B. B. (2016) Social media security and trustworthiness: Overview and new Direction. *Future Generation Computer Systems*. Elsevier, <https://doi.org/10.1016/j.future.2016.10.007>

