Journal of Intelligent & Fuzzy Systems 37 (2019) 27–34
DOI:10.3233/JIFS-179060
IOS Press

Secure cloud computing model for communication network management

Shuicheng Tian[a], Kai Tang[a,b,*], Pengfei Yang[a], Aifang Jia[a] and Melvin, Hailey[c,*]
[a]*College of Safety Science and Engineering, Xi'an University of Science and Technology, Xi'an, China*
[b]*Department of Electric Power, Xi'an Electric Power College, Xi'an, China*
[c]*The Colorado Community College System, USA*

Abstract. To build a safety behavior evaluation system in network management, the cloud computing model is introduced in this study for parametric study. First, the development model of cloud computing management is expounded, a parametric model of safety behavior coefficient is constructed by using a cloud computing platform. Then, an optimization and update scheme is put forward from the algorithm flow and evaluation model, and an adequate evaluation model is established by effectively evaluating the state of security management. Finally, the parameter data is refined through USES data mining algorithm to ensure the reasonable calculation of the data. In the test of the parameter model, the simulation is carried out by adopting the cloud computing platform. The test results prove that the application of the parameter model can guarantee the reasonable management of safety behavior, the error in the process of safety behavior management can be reduced, and the accuracy of control can be enhanced. The parameter model is worthy of further application and extension.

Keywords: Cloud computing, safety management, safety behavior coefficient, optimization decision

1. Introduction

Computer network multimedia communication technology is developed from the communication network, and the superior computer performance can lay a robust technical foundation computer multimedia image transmission and primary data [1]. Subsequently, the broadband of wired network also provide a technical guarantee for the rapid development of computer multimedia technology. Mobile communication technology has developed rapidly in recent years, and the transmission bandwidth of the mobile network has also increased. [22–24]. Mobile terminals are characterized by convenience, and more people prefer to use and store multimedia services in mobile terminals [2]. As the increasing number of mobile users, the bandwidth of mobile communications will increase rapidly. Because of the significant increase in the channel transmission flow of mobile communication [25], higher requirements are also proposed for the transmission channel bandwidth [3]. To improve security behavior in the process of safety management, it is necessary to have the most significant impact on the demand for mobile channel resources and the overall benefit. Therefore, in the process of parameterization optimization of the safety behavior coefficient, the contradiction between mobile communication and channel resources would be solved. Adoption of cloud computing security calculation and the management pattern can answer the fundamental disagreement but needs to be done in the aspect of safety coefficient of behavior parametric optimization, and this paper would explain the study of this area based on the cloud model. □

In this paper, we propose a cloud computing model for network communication security. The first part is

*Corresponding author. Kai Tang, College of Safety Science and Engineering, Xi'an University of Science and Technology, Xi'an, 710054, China. E-mail: kaitang1@foxmail.com and Melvin, Hailey, The Colorado Community College System, USA. E-mail: hmelvin@student.cccs.edu.

to analyze the characteristics of the current safety management behavior coefficient and to explore the feasibility of an innovative application of the behavior coefficient under the support of computer technology. The second part is the analysis of the central principle and implementation process of a cloud computing model. The third part is to put forward the optimization strategy to improve the accuracy and reliability of behavioral safety factor optimization. The rest of the paper is organized as follows: Section II demonstrates the performance problem of graph Biological simulation algorithm and discusses the motivations of this research. Then the algorithm design is presented in Section III. In Section IV, we will show the optimization strategies for the proposed algorithm. We conclude the paper and describe the future research opportunities in Section V.

2. Related work

Multimedia applications business has spread over the last several years, services in wireless broadband connection are gradually expanding, a lot of multimedia messaging service has been able to reach the application effect of the terminal, but the study is still in progress in the field [4]. Due to the enormous individual difference in the traditional data service application, multimedia can set the transmission speed by referring to its network resource situation. For example, a multi-level video coding system can carry out the original video coding, but different limited levels might have been set. The necessary information of videos in the transmission at the base level will also generate higher video data [5]. Therefore, multi-speed data transmission can be performed in the computer multimedia transmission system, but the transmission speeds could be different, which may result in low transmission quality for images and videos. For the sake of achieving a wireless network resource, ensuring the safety management during transmission, satisfying high requirements of the customers, the optimization of safety behavior would be offered in services when the speed of transmission changes [6]. The security management of computer network resources has been often reported in previous literature. Generally speaking, network resource security management can be divided into static security management and dynamic security management. In a static security management system, the allocation of network resources can be optimized by scheduling basic static networks. But in the process of the actual work, many users are dynamic intervention directly to the network, so it requires changes over time in the process of the network security management. And when it comes to the distribution of the static security management, the dynamic process of network security management has the following advantages: first, the accurate dynamic presentation for security network resources, second, the performance of compared information could be acquired in this allocation method can get more performance. L.X.CAI et al. have defined a large number of video and the number structure of speech for the capacity output of wireless LAN. To meet the various needs of users, J. Xu and other researchers transformed the attenuation model into a restricted Markov channel model [7] in the wireless transmission channel [8]. This model also lays a good foundation for the security management model constructed in this paper for cloud computing data transmission [9, 10].

In 2008, there were 42.8 million mobile cloud users worldwide, accounting for 1.1 percent of global mobile users. In the next five years, mobile cloud computing would enter a period of rapid development. By 2014, the number of global users reached 998 million, and the annual growth rate was 30-50%.

3. Cloud computing security

3.1. Security management mechanism based on cloud computing

To ensure the security management process, the author thought the problem of the transmission channel in the mobile communication network, and it is necessary to establish a security management model of communication channel resources based on cloud computing mode, which can optimize the safety behavior coefficient in the model [11–13]. Set B for the communication network bandwidth, the allocation of user bandwidth is k and u, while the user's minimum bandwidth is u, the integer parameter is k. For mobile communication networks, different utility functions can be used to measure the satisfaction of users using the network transmission process. By using a sigmoidal calculation function to express the data flow to calculate the satisfaction, the expression is:

$$U(r) = 1 - \exp\left(-\frac{w_2 r^2}{w_1 + r}\right) \tag{1}$$

In the computation expression, $U(r)$ represents the user satisfaction of the mobile communication network and r represents the communication bandwidth of the network transmission. And w_1, w_2 representing the waveform parameter of the adjustment satisfaction, the waveform of the function is shown in Fig. 1. In general, the calculation of the parameters, w_1 w_2 in the expression is based on the mobile multimedia business and the final number of the security management of the quality of service to determine [14–17]. The valid parameter optimization is the influence on the wireless resource management communication, and the parameterization optimization in the process of security management may play a significant role. It can be seen from the computation expression 1 that to enhance the security management in the mobile network transmission process. And it's also need to allocate high communication bandwidth as much as possible. From another point of view, it needs to improve the overall revenue of wireless network transmission, control the safe transmission process [18]. According to the requirements of bandwidth and user data traffic for mobile wireless networks, it is impossible for the system model to allocate the maximum bandwidth of mobile communication network to the users. This paper changes the security behavior parameterization from the security management process of cloud computing security model [19, 20]. To realize the dynamic flow optimization model of wireless network transmission, we need to allocate the number of users in the mobile communication network in Poisson distribution, and the average value is λ. It is assumed that mobile communication users can obey exponential distribution during network transmission and the average value is $1/u$. Based on the security management model of

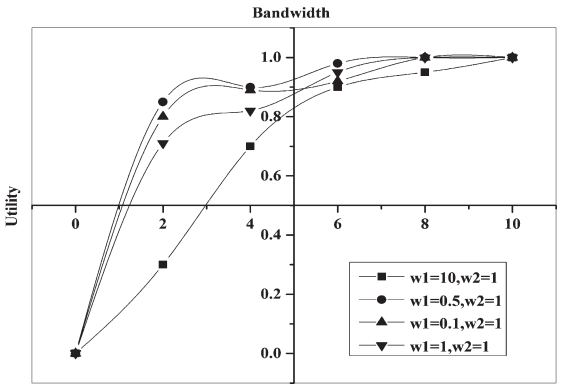

Fig. 1. Utility function of multimedia services.

cloud computing, the distribution of communication resources of the wireless network is increased, and the maximization model of wireless network transmission in the adjustment of security behavior parameters is formed.

The decision process based on cloud computing can represent the security management process of mobile multimedia communication resources [21], we assume that the user's network satisfaction to mobile media can be requested, and the request time can be inversely proportional, then the efficiency of the user's service request processing will be higher. The more communication channel resources are allocated to the user, the ratio of the user's request resource satisfaction and the assigned user's wireless channel resources is proportional. The user satisfaction of mobile multimedia communication system is divided into N categories. The definition of the cloud-based communication security management process, for user satisfaction, can be in the mobile communication system to form an event. $k1 \cdot u$ Defines the number of wireless channels that represent user satisfaction and the amount of user satisfaction is n_i. In the new multimedia network, the request multimedia service uses the R to express, the user satisfaction; I, representing the completes how the body business, will release the wireless channel resources represented by D_i. Therefore, we need to adopt a cloud computing method to control the safety behavior factor of the wireless mobile communication network security management process. The random event is represented as $e \in \{R, D_1, D_2, ..., D_N\}$. In such cases, the system usage status of the mobile multimedia network is evaluated as:

$$S = \{s | s = \langle n_1, n_2, ..., n_N, e \rangle\} \tag{2}$$

If a mobile terminal user can intervene in the wireless Internet Service system, the mobile multimedia Internet will accept the user's urgent request. Assuming the above request service process is accepted, the assigned wireless channel will be the price. We give the Izumo calculation model the action set to compute the expression:

$$A(s) = \begin{cases} -1, e \in \{D_1, D_2, ..., D_N\} \\ \{0, 1, ..., N\}, e = R \end{cases} \tag{3}$$

To ensure the controllability of cloud computing security management process, revenue calculation is carried out for the cloud computing model. We can evaluate the benefits of a network transmission process using representations $r(s, a)$. The revenue

structure of this security management process can be divided into two parts; one is the revenue part of the system, the other is the system expenditure part, the calculation expression is:

$$r(s, a) = x(s, a) - \tau(s, a)y(s, a) \tag{4}$$

To evaluate the system state of s in an expression, the selected necessary action is represented by a, then the total income of the entire security management model is:

$$x(s, a) = \begin{cases} -1, e = R, a = 0 \\ U(k, u), e = R, a = i \end{cases} \tag{5}$$

MATLAB system platform for programming related events Simulator, for our earlier proposed in the cloud-based dynamic wireless channel resource optimization and security Process Control model, performance evaluation of the simulation calculation. In the whole simulation process, the service quality evaluation of security process management can be divided into several levels, corresponding to the number of channel transmission, that is, the value of K is 1, 2, 3 respectively. Without extraordinary algorithm requirements, we control the wireless communication transmission security management control channel quantity to 10, the requested service will reach the communication network average rate, the setting value is $\lambda = 7$, but the user in transmits the data the process to set the wireless communication network channel resource The average rate is 5 and 10 respectively. To be able to control the wireless transmission data safely, we need to control the revenue of the whole cloud computing model within the convergence range of cloud computing; we set the discount factor of the calculation model to 0.1.

3.2. Security behavior parameter model based on cloud computing

At the same time, in order to meet the accuracy of the simulation calculation, our test performance simulation cycle is limited to 30 minutes. The design details of the protocol should also be taken into account in the specific application. The basic process structure diagram of the steps above is as follows:

Tables 1 and 2, respectively, are parameter states of different cloud computing functions, each state corresponding to the wireless channel resource allocation management security behavior coefficient parameterization correction process, existing numerical display system primary condition, movement management,

Table 1
Optimal decision table 1

n1/n2	0	1	2	3	4	5	6	7	8	9	10
0	3	3	3	3	3	3	2	2	2	1	0
1	3	3	3	3	2	2	2	1	0	0	0
2	3	3	2	2	2	1	0	0	0	0	0
3	2	2	2	1	0	0	0	0	0	0	0
4	2	1	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0

Table 2
Optimal decision table 2

n1/n2	0	1	2	3	4	5	6	7	8	9	10
0	2	2	2	2	2	2	2	2	2	1	0
1	2	2	2	2	2	2	2	1	0	0	0
2	2	2	2	2	2	1	0	0	0	0	0
3	2	2	2	1	0	0	0	0	0	0	0
4	2	1	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0

and safety management process model deterioration strategy.

For example, in a mobile network transmission process, assuming that the user is using the wireless communication channel resources, the mobile multimedia service reaches the multimedia network request, the system decides for the $A = 3$. And then, the system assigns the third channel to the wireless transmission channel, this kind of security management process is called the behavior parameterization process.

Assuming that the number of users in the system is $n = 3$, independent users take up the number of wireless multimedia channels for K2, which proves that the 4 wireless multimedia channel is occupied, the equivalent of wireless channel multimedia request process, the number of optimized strategies for the $a = 2$, in the distribution of wireless channels. To go U-ease, mobile multimedia requests are sufficient. Assuming that the bandwidth of the system is used, the more practical benefits go back to setting the optimal security behavior decision $A = 3$, but it is not set to $a = 1$ or set to $a = 2$. At the same time, in another aspect, the optimization of the safety behavior parameters will also have a conservative effect on the decision. As can be seen from Tables 1 and 2, the cloud computing decision model also has a significant change when optimizing the parameter w1 of security behavior. Add the set w1 value of 0.1, then mobile wireless transmission of the request service atmosphere for Mulberry and wireless channel (K1, K2, K3), $w1 = 0, b = 1, \lambda = 7, u = 10, n3 = 0$ then set the effectiveness of the atmosphere for 0.774, 0.942, 0.987.

4. Experimental design and analysis

4.1. The experimental environment of the parametric model

To further verify the parameterized model of cloud computing security management mentioned above, we reassess the performance of the mobile multimedia channel optimization model and compare the total network efficiency gain and the congestion rate of the multimedia optimization model. As long as the model has enough wireless channel essential resources, carries on the greedy algorithm comparison and the mobile wireless client's allocation bandwidth, then the system algorithm can achieve the maximum gain, and then the security management scope is controllable. Figure 2 shows the security management model of the channel transmission of mobile wireless multimedia, and the contrast difference of network efficiency gain by greedy allocation algorithm. As can be seen from the graph, the service request of mobile multimedia increases the standard rate (λ), the efficiency of the cloud computing model will increase correspondingly. If the request of the mobile multimedia integrated service reaches the upper limit of the communication network, the greedy algorithm will form the maximum allocated wireless channel bandwidth of the mobile communication network. Therefore, there is a particular risk, assuming that the next mobile wireless communication network, channel communication resources are insufficient, the greedy allocation algorithm can only refuse a mobile multimedia request service.

4.2. Parametric model of resource allocation testing

The security model of mobile multimedia channel resource optimization is presented in this paper when mobile multimedia requests reach the limit of the communication network; the algorithm is more conservative when it considers the channel resources allocated by mobile multimedia. □

As can be seen in Fig. 3, as the basic request of mobile multimedia service reaches a specific probability increment value (λ), greedy allocation algorithm will increase the congestion rate of the request of mobile multimedia service correspondingly. The congestion rate of the multimedia service request in optimizing the security management process is relatively slow. In this way, mobile multimedia shows that the optimal management model of the mobile multimedia channel is stronger than the greedy algorithm from the congestion rate. □

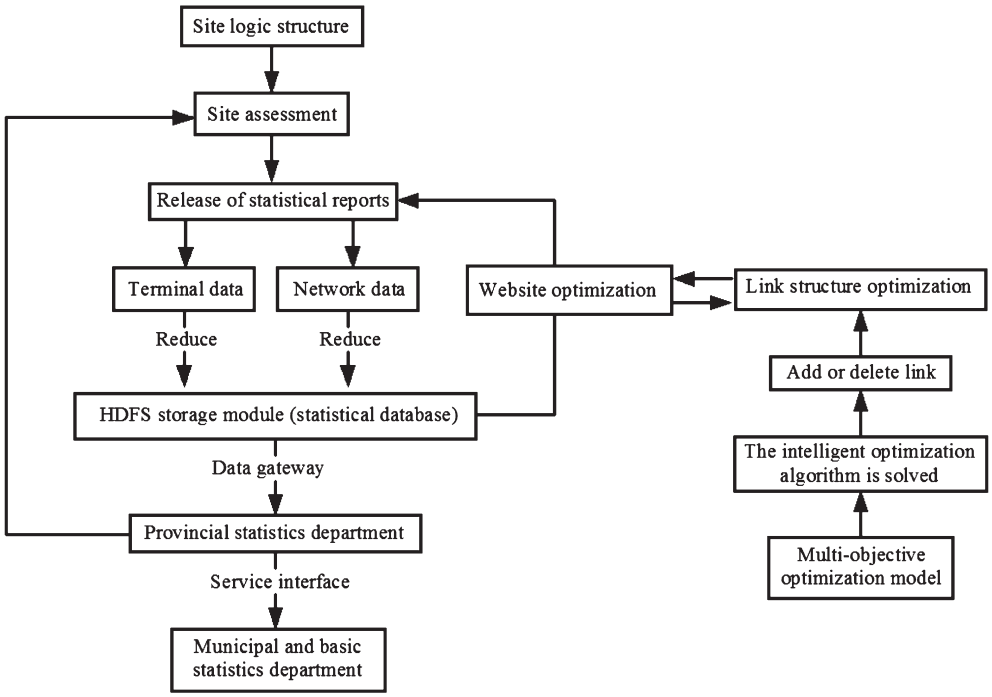

Fig. 2. Structure diagram of security behavior parameter model.

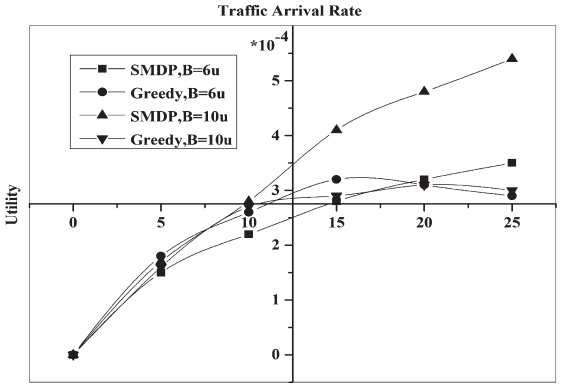

Fig. 3. The system gain of cloud computing model.

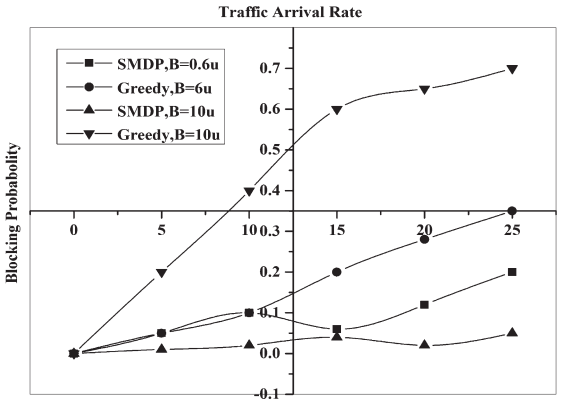

Fig. 4. Congestion rate of mobile multimedia wireless transmission.

In Fig. 4, the optimization process of the security behavior parameter is further analyzed in the process of wireless network security management, and the request of mobile multimedia service reaches the mobile communication network.

4.3. Performance testing of parametric models

In this paper, a security resource management model for the mobile communication network is proposed to take different probability values. Assuming that the multiple body service request compliance rate is low, it will have more mobile channel resources to stay. In such a case, the probability value will increase correspondingly when the mobile communication network receives the new service request. Assuming the service request compliance rate of the mobile communication network is 3, the requested probability of allocating mobile communication channel resources reaches 97%. When the users of mobile multimedia service increase, the resources of mobile communication channel will be occupied, many wireless multimedia requests will occupy the channel resources in the future, the security management process of cloud computing is significantly challenged. □

Because the current optimization process of the mobile multimedia communication channel is designed for the security management process, the

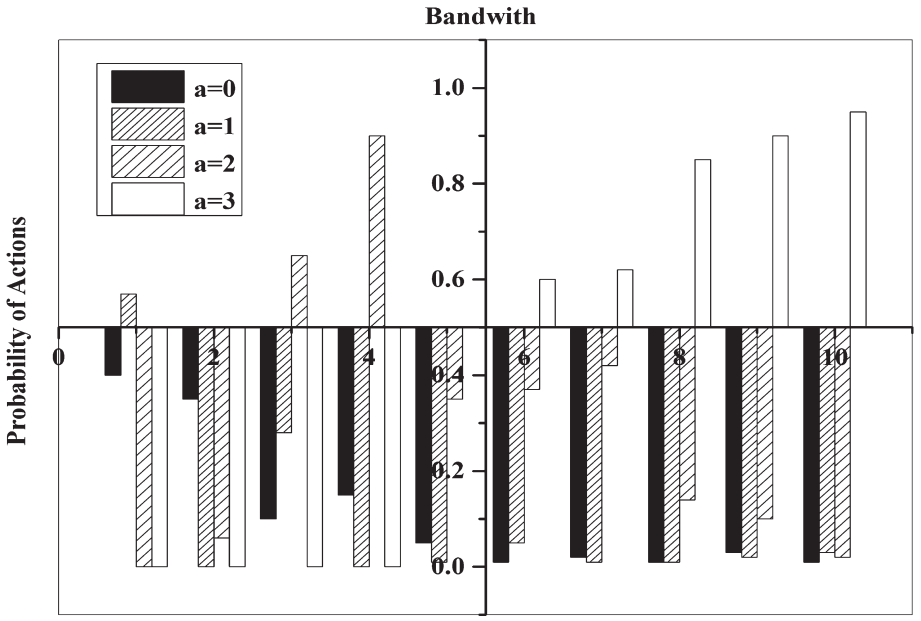

Fig. 5. Security behavior parameter adjustment results of multimedia wireless transmission of data.

whole cloud computing security management model needs to consider the long-term benefit of the system. For the new mobile wireless multimedia service allocation, security considerations need to be more cautious. Therefore, in Fig. 5, we can see that after the Mobile multimedia request service reaches the upper limit, the cloud computing model adopts the decision $A = 3$, and the probability of adopting the decision $A = 1$ and $a = 2$ increases correspondingly. As can be seen from Fig. 5, the cloud computing model of the mobile multimedia communication network can describe the total bandwidth relationship of the system according to the decision of security behavior. As can be seen from the graph, as the number of mobile wireless communication increases, the cloud computing model allocates more bandwidth and increases the probability value. Mobile multimedia network communication bandwidth increases from 1 to 10, and cloud computing model mobile wireless how the business uses $A = 3$ decision, the security behavior coefficient parameterization process is probability 0 to probability 97%.

5. Conclusion

Cloud computing is widely used in wireless network and multimedia information transmission, more optimization parameterized process of safe behavior coefficient is required to solve the problem of channel resource security management and optimization of the mobile communication network. In this paper, a cloud computing model was constructed based on the issues of safety and allocation management for SMDP mobile communications channel resource in cloud computing, with which security behavior parameters were adjusted for optimizing mobile communication channel. Based on available space of communication channel in cloud computing model, the efficiency gain of the entire network has been considered, at the same time, the most significant efforts should be made to optimize the overhead of communication resources effectively. To promote the maximization profit in the long term, the optimization for security behaviors of mobile multimedia services should be adopted. Meanwhile, in order to allocate wireless network meets the requirements of mobile multimedia different quality in different levels, a further derivation was taken on cloud computing model for new multimedia channel resources. And the safety index (constructively) was acquired, and parameterization results of the adopting rate of wireless services for media were obtained probability safety coefficient. Finally, in the conversion test of the parameter model, the adjustment of safety behavior parameters could meet the requirements of the experiment, and satisfactory results were achieved in the simulation test. With the increase of mobile wireless communication, the cloud computing model will allocate more bandwidth and increase the probability value, thus ensuring the accuracy of the safety behavior coefficient. The comprehensive test proved that the model of safety behavior coefficient in cloud computing has strong applicability and convenience. However, in this study, there is no test on the adjustment range of ratio, which should be supplemented and perfected in the future research.

References

[1] J. Baek, Q.H. Vu, J.K. Liu, A secure cloud computing based framework for big data information management of smart grid, *IEEE Transactions on Cloud Computing* **3**(2) (2015), 233–244.

[2] C. Chang, J. Choi and P. Kim, Ontology-based access control model for security policy reasoning in cloud computing, *Journal of Supercomputing* **67**(3) (2014), 711–722.

[3] C. Lin, S.U. Wen-Bo and K. Meng, Cloud computing security: architecture, mechanism, and modeling, *Chinese Journal of Computers* **36**(9) (2013), 1765–1784.

[4] U. Gupta, Survey on security issues in file management in cloud computing environment, *International Journal of Computer Applications*, 2015, 120.

[5] G.T.R. Lin, C.C. Lin and C.J. Chou, Fuzzy Modeling for Information Security Management Issues in Cloud Computing, *International Journal of Fuzzy Systems* **16**(4) (2014), 529–540.

[6] E. Weippl, E. Weippl and E. Weippl, Migration goals and risk management in cloud computing: A review of state of the art and survey results on practitioners, *International Journal of Secure Software Engineering* **7**(3) (2016), 44–73.

[7] L. Tot, G. Grubor and T. Marta, Introducing the information security management system in cloud computing environment, *Acta Polytechnica Hungarica* **12**(3) (2015), 147–166.

[8] T. Li, The establishment of information management security under cloud computing environment, *Applied Mechanics & Materials* **713–715** (2015), 2405–2408.

[9] W. Zhang, K. Thurow and R. Stoll, A context-aware mhealth system for online physiological monitoring in remote healthcare, *International Journal of Computers Communications & Control* **11**(1) (2016), 142–156.

[10] Weiping Zhang, Akbar Maleki, Marc A. Rosen and Jingqing Liu, Optimization with a simulated annealing algorithm of a hybrid system for renewable energy including battery and hydrogen storage, *Energy* **163** (2018), 191–207.

[11] M. Moravík, M. Schmid and N. Burch, DeepStack: Expert-level artificial intelligence in heads-up no-limit poker, *Science* **356**(6337) (2017), 508.

[12] E.O. Daniel, Artificial Intelligence and Big Data, *IEEE Intelligent Systems* **28**(2) (2013), 96–99.

[13] J. McCarthy, Generality in artificial intelligence, *Resonance* **19**(3) (2014), 283–296.

[14] M. Imran, C. Castillo and L. Ji, AIDR: artificial intelligence for disaster response, *International Conference on World Wide Web. ACM*, 2014, pp. 159–162.

[15] E. Hovy, R. Navigli and S.P. Ponzetto, Collaboratively built semi-structured content and artificial intelligence: The story so far, *Artificial Intelligence* **194** (2013), 2–27.

[16] R.V. Yampolskiy, Artificial Intelligence Safety Engineering: Why Machine Ethics Is a Wrong Approach. Philosophy and Theory of Artificial Intelligence. Springer Berlin Heidelberg, 2013: 389–396.

[17] M. Moravík, M. Schmid and N. Burch, DeepStack: Expert-level artificial intelligence in heads-up no-limit poker, *Science* **356**(6337) (2017), 508.

[18] D.C. Parkes, M.P. Wellman, Economic reasoning and artificial intelligence, *Science* **349**(6245) (2015), 267.

[19] E.S. Rigas, S.D. Ramchurn and N. Bassiliades, Managing electric vehicles in the smart grid using artificial intelligence: A survey, *IEEE Transactions on Intelligent Transportation Systems* **16**(4) (2015), 1619–1635.

[20] P. Glauner, A. Boechat and L. Dolberg, The challenge of non-technical loss detection using artificial intelligence: A survey, *International Journal of Computational Intelligence Systems* **10**(1) (2017), 760–775.

[21] K. Karthikeyan, R. Sunder, K. Shankar, S.K. Lakshmanaprabu, V. Vijayakumar, Mohamed Elhoseny and Gunasekaran Manogaran, Energy consumption analysis of Virtual Machine migration in cloud using hybrid swarm optimization (ABC-BA). The Journal of Supercomputing, 2018. https://doi.org/10.1007/s11227-018-2583-3.

[22] Mohamed Elhoseny, K. Shankar, S.K. Lakshmanaprabu, Andino Maseleno and N. Arunkumar, Hybrid optimization with cryptography encryption for medical image security in Internet of Things. Neural Computing and Applications. 2018. https://doi.org/10.1007/s00521-018-3801-x.

[23] K. Shankar, Mohamed Elhoseny, E. Dhiravida chelvi and S.K. Lakshmanaprabu, Wanqing Wu. An Efficient Optimal Key Based Chaos Function for Medical Image Security. IEEE Access. 2018. https://doi.org/10.1109/ACCESS.2018.2874026.

[24] I.S. Farahat, A.S. Tolba, M. Elhoseny and W. Eladrosy, Data Security and Challenges in Smart Cities. In: Hassanien A., Elhoseny M., Ahmed S., Singh A. (eds) Security in Smart Cities: Models, Applications, and Challenges. Lecture Notes in Intelligent Transportation and Infrastructure. Springer, Cham, 2019. https://doi.org/10.1007/978-3-030-01560-2_6.

[25] M. Elhoseny, A.E. Hassanien, Expand mobile WSN coverage in harsh environments. In: Dynamic Wireless Sensor Networks. Studies in Systems, *Decision and Control, Springer, Cham*, **165** (2019), 29–52. https://doi.org/10.1007/978-3-319-92807-4_2.