Българско списание за Инженерно Проектиране

брой №44, ноември 2021г.

ЦЕЛ И ОБХВАТ

„Българско списание за инженерно проектиране” е периодично научно списание с широк научен и научно-приложен профил. Целта му е да предостави академичен форум за обмен на идеи между учените, изследователите, инженерите, потребителите и производителите, работещи в областта на машиностроенето, транспорта, логистиката, енергетиката, технологиите, съвременното компютърно проектиране, а също така и в областта на различни интердисциплинарни научни и научно-приложни проблеми. Издателите приветстват научни публикации с високо качество и значими научни, научно-приложни и творчески приноси.

РЕДАКЦИОННА КОЛЕГИЯ

Председател
Б. Григоров, ТУ-София, България

М.Т.Георгиев	ТУ-София, България	**К.Деметрашвили**	ТУ, Тбилиси, Грузия
Г.Дюкенджиев	ТУ-София, България	**С.Симеонов**	ТУ, Бърно, Чехия
М.Денчев	ТУ-София, България	**В.Николич**	Университет в Ниш, Сърбия
И.Малаков	ТУ-София, България	**А.Янакиев**	Notingham Trent University, UK
П.П.Петров	ТУ-София, България	**Н.Чернев**	University of Auvergne, France
В.Панов	ТУ-София, България	**B.Lepadatescu**	Transilvania University of Brashov, Romania
М.З.Георгиев	ТУ-София, България	**N.Zrnic**	University of Belgrad, Serbia
Н.Л.Николов	ТУ-София, България	**M.Jovanovic**	University of Nish, Serbia
М.Георгиев	МГТУ Станкин, Москва, Россия	**D.Michalopoulos**	University of Patras, Greece
В.Христов	ТУ-София, България	**N.Kubota**	Tokyo Metropolitan University, Japan
Ch.Apostolopoulos	University of Patras, Greece	**С.Емельянов**	Юго-Западный гос. университет, Курск, Россия
Л.Червяков	Юго-Западный гос. университет, Курск, Россия	**В.Спасов**	ВТУ „Т.Каблешков“, София, България
О.Лисовиченко	Национален технически университет, Украйна	**В.Кирилович**	Государственный университет "Житомирская политехника", Украина

Редактор
Р.Митрев, ТУ-София, България

Издател: Машиностроителен факултет, Технически университет-София. ISSN 1313-7530; **Адрес на редакцията:** София, бул.Климент Охридски №8, Технически Университет-София, бл.4, Машиностроителен факултет; **Електронна версия:** bjed.tu-sofia.bg.

Списанието се индексира в Index Copernicus: www.indexcopernicus.com

Всички статии в списанието се рецензират от членове на редакционната колегия и външни специалисти.

Bulgarian journal for
Engineering Design

issue №44, November 2021

AIM AND SCOPE

Bulgarian Journal for Engineering Design is a periodical scientific issue covering wide scientific and application areas of engineering activities. The aim of the journal is to provide an academic forum for exchange of ideas and information between scientists, engineers, manufacturers and customers working in the spheres of mechanical engineering, transport, logistics, power engineering, modern computer – aided design and technology and solving different interdisciplinary scientific and applied problems. The editors welcome articles of substantial quality bearing significant contribution to the engineering knowledge.

EDITORIAL BOARD

Chairman
B.Grigorov, TU-Sofia, Bulgaria

M.T.Georgiev	TU-Sofia, Bulgaria	**K.Demetrashvili**	TU, Tbilisi, Georgia
G.Diukendzhiev	TU-Sofia, Bulgaria	**S.Simeonov**	TU, Brno, Czech Republic
M.Denchev	TU-Sofia, Bulgaria	**V.Nikolich**	Nish university, Serbia
I.Malakov	TU-Sofia, Bulgaria	**A.Ianakiev**	Notingham Trent University, UK
P.P.Petrov	TU-Sofia, Bulgaria	**N.Chernev**	University of Auvergne, France
V.Panov	TU-Sofia, Bulgaria	**B.Lepadatescu**	Transilvania University of Brashov, Romania
M.Z.Georgiev	TU-Sofia, Bulgaria	**N.Zrnic**	University of Belgrad, Serbia
N.L.Nikolov	TU-Sofia, Bulgaria	**M.Jovanovic**	University of Nish, Serbia
M.Georgiev	MGTU Stankin, Moscow, Russia	**D.Michalopoulos**	University of Patras, Greece
V.Hristov	TU-Sofia, Bulgaria	**N.Kubota**	Tokyo Metropolitan University, Japan
Ch. Apostolopoulos	University of Patras, Greece	**S.Emelianov**	South West State University, Kursk, Russia
L.Cherviakov	South West State University, Kursk, Russia	**V.Spassov**	VTU „T.Kableshkov“, Sofia, Bulgaria
O.Lisovychenko	National technical university, Ukraine	**V.Kirilovich**	Zhytomyr Polytechnic State University, Ukraine

Editor
R.Mitrev, TU-Sofia, Bulgaria

Publisher: Mechanical Engineering Faculty, Technical University-Sofia. ISSN 1313-7530; **Publisher Address:** Bulgaria, Sofia, Kliment Ohridski blvd. №8, Technical University-Sofia, Mechanical engineering faculty; **Electronic version:** bjed.tu-sofia.bg.
The journal is indexed in Index Copernicus: www.indexcopernicus.com
All papers are reviewed by the members of Editorial Board and by external specialists.

Българско списание за инженерно проектиране, брой 44, ноември 2021г.
Bulgarian Journal for Engineering Design, issue 44, November 2021

Съдържание/Contents:

USING WEB BASED CALCULATOR OF EMOTIONAL MODELS FOR IDENTIFICATION OF COMPROMISED INTERNET OF THINGS DEVICES

Aleksandar HRISTOV, Rumen TRIFONOV
Faculty of Computer Systems and Technologies, Technical University of Sofia
e-mail: ahristov@tu-sofia.bg

Abstract: The purpose of present paper is to propose an intelligent system for identification of compromised Internet of Things (IoT) devices due to cyberattack, using Web based calculator of Emotional Models (EM). Monitoring is being made and the state is identified through time-synchronized series of indexes for usage of memory, network port and processor. Using system monitor time-synchronized indexes of non-compromised IoT devices are saved as well as indexes of compromised IoT devices due to some well-known cyberattacks in Internet of Things are saved. The parameters of the proposed system are being specified in order to distinguish (filter) the two states of the IoT devices (non-compromised or compromised) by these indexes. A web based calculator of EM is presented, its usefulness is discussed and tasks for the future development are defined.

Keywords: Information Security, Artificial Intelligence Systems, Emotional Models, IoT devices, Web Technologies

1. INTRODUCTION

Nowadays interest in the Internet of Things (IoT), the Industrial Internet of Things (IIoT) and in particular the information security [3] of IoT devices is a growing. The review of the literature showed that the problem with information security of IoT devices is still poorly developed and there are no available systems for detecting compromised IoT devices as a result of cyberattack.

The concept of IoT was first proposed by MIT in 1999. The early IoT was a network based on the RFID technology and devices. It combined objects with the Internet based on the agreed communication protocols to implement intelligent identification and management of objects and realize interconnection and information sharing. IoT is an Internet where all things are interconnected: Information Technology (IT) that includes devices in the data center, in the cloud, bring your own devices (BYODs), and thousands of sensors and actuators connected in the field; Operational Technology (OT) that includes industrial control systems (ICSs), supervisory control and data acquisition (SCADA) systems, and all the devices that connect to these systems; Consumer Technology (CT) that includes connected devices in the home, wearable technology, smart cars, and more. By converging IT and OT, operations managers use IT tools to sift through the reams of operational data and make real-time decisions. IT teams can also use this data to do innovative things such as improving the supply chain and reducing downtime. New device types and the increasing number of devices per person all add up to a significant portion of connected devices in the age of IoT. IoT security includes devices and applications from IT, OT, and CT. Security includes physically securing the outside and inside perimeters of places, such as data centers, where data is stored, but not only. Securing IoT devices is challenging due to the sheer number of them, the fact that they are found in non-traditional locations, and that many of them cannot be upgraded. IoT devices are increasingly being compromised and used in a wide variety of attacks because they often lack critical device protections such as strong passwords, up-to-date operating systems, and segmented networks.

In [4], a specific approach for identifying compromised devices as a result of a cyberattack is proposed. It is based on monitoring the usage of memory, network interface card (NIC) and processor to determine the state (compromised / non-compromised) of IoT devices. The decisive rule (a function dividing the space of two disjoint sets) of the algorithm finds the correspondence of the state from a time series of values as an input. A peculiarity of the approach is the pre-treatment, i.e. using training samples of time series (usage of memory, network interface card and processor), three cluster areas are determined as well as the center of each cluster. The first cluster corresponds to a non-compromised state, while the second and third clusters correspond to states after SQL Injection. For the second cluster filtering by a predefined field of the table is being done and for the third cluster the values are inserted into a table after their transformation. An advantage of the approach above is that it distinguishes these two specific compromised states and a disadvantage is that it cannot identify all sorts of other compromised states of the IoT device.

Different approaches are known in the literature [10, 12, 13] for identification of the IoT devices especially in IoT sensor swarms [8 and its references] – some behavioral files are stored and periodically the device must generate the same files that are to be equal to the etalon ones. Mostly cryptography hashing or public key authentication are used. NIST's NICE [11] includes all the processes necessary to assure that existing and new IT systems meet the organization's cybersecurity and risk requirements. In the NICE Protect and Defend work category it is discussed how to conduct assessments of threats and vulnerabilities; determining deviations from acceptable configurations or policies; assessing the level of risk; and developing or recommending appropriate mitigation countermeasures.

The purpose of present paper is to propose an intelligent system for identification of compromised Internet of Things (IoT) devices due to cyberattack, using Web based calculator of Emotional Models (EM).

2. EMOTIONAL MODEL BASED METHOD FOR IDENTIFYING COMPROMISED IOT DEVICES

As it has already been mentioned above, present work is privy to Web-based approach of processing of the information for the IoT device based on the emotional model [6,7,14,15] is proposed and Web application developed in [6] is used.

Emotional model concept, containing P number of emotions and Q number of feelings, is shown on Fig. 1. It is based on the relations between emotional inputs, feelings and mood, given in the Eq. (1), Eq. (2) and Eq. (3) [6].

Emotions (i=1…P) are described as specific perceptual information $u^E_i(t)\in[0,1]$ and each feeling (j=1…Q) is updated at every one moment as the summation of emotions. The i-th emotional input to j-th feeling $u^E_{i,j}(t)$ is calculated as:

$$u^E_{i,j}(t)=d_{i,j}u^E_i(t),\ d_{i,j}\in[0,1],$$
$$\text{for each j } \sum_{i=1}^{P}d_{i,j}=1 \qquad (1)$$

$d_{i,j}$ is the degree of contribution from the i-th emotional input to j-th feeling.

The j-th feeling $u^F_j(t)$ is updated by emotion's inputs and constraints from the mood $u^M(t)$:

$$u^F_j(t)=ku^F_j(t-1)+(1-k)\sum_{i=1}^{P}u^E_{i,j}(t),$$
$$k=\frac{\gamma^F}{1+u^M(t-1)} \qquad (2)$$

γ^F is the discount rate of the feelings $(0<\gamma^F<1)$.

Mood as a relatively long-term state is updated by a change in feelings. The mood is updated by the sum of feelings:

$$u^M(t)=\gamma^M u^M(t-1)+\frac{1-\gamma^M}{Q}\sum_{j=1}^{Q}u^F_j(t) \qquad (3)$$

γ^M is the mood discount rate $(0<\gamma^M<1)$.

Below it is proposed a universal method for identifying various compromised states of IoT devices. This method uses indexes of the mood obtained from the EM for the usage of memory, network interface card (NIC) and processor in percentages, of the IoT device.

Keeping in mind well known facts for 3D computer and its performance, in order to identify compromised IoT devices through EM the number of the emotions has been chosen 3: first emotion is the usage of memory; second emotion is the usage of NIC and third emotion is the usage of processor. Thus, the proposed approach requires the collection of data for usage of memory, NIC and processor. This data become the initial values of the feelings and the mood for the new operation.

The approach proposed in the present paper requires the collection of data for usage of memory, NIC and processor, which become the initial values of the feelings and the mood for the non-compromised state of IoT device. The emotional pattern used in this observation is the same for different states (compromised or non-compromised). But when more data is gathered for usage of data for usage of memory, NIC and processor, EM can be changed and developed by changing the observed emotions and feelings, as well as the settings of the model itself. A separate XML document with emotional data is created for each of these states (compromised or non-compromised) and is analyzed by passing through the emotional model calculations. By analogy with [6,7,14,15] the number of the feelings has also been chosen 3- F1, F2 and F3. This way an additional priority can be assigned to each feeling when "training" the model. For example, usage of memory, NIC and processor. In this paper values of the parameters (γ^F and γ^M and the degree of contribution $d_{i,j}$) have been chosen arbitrarily.

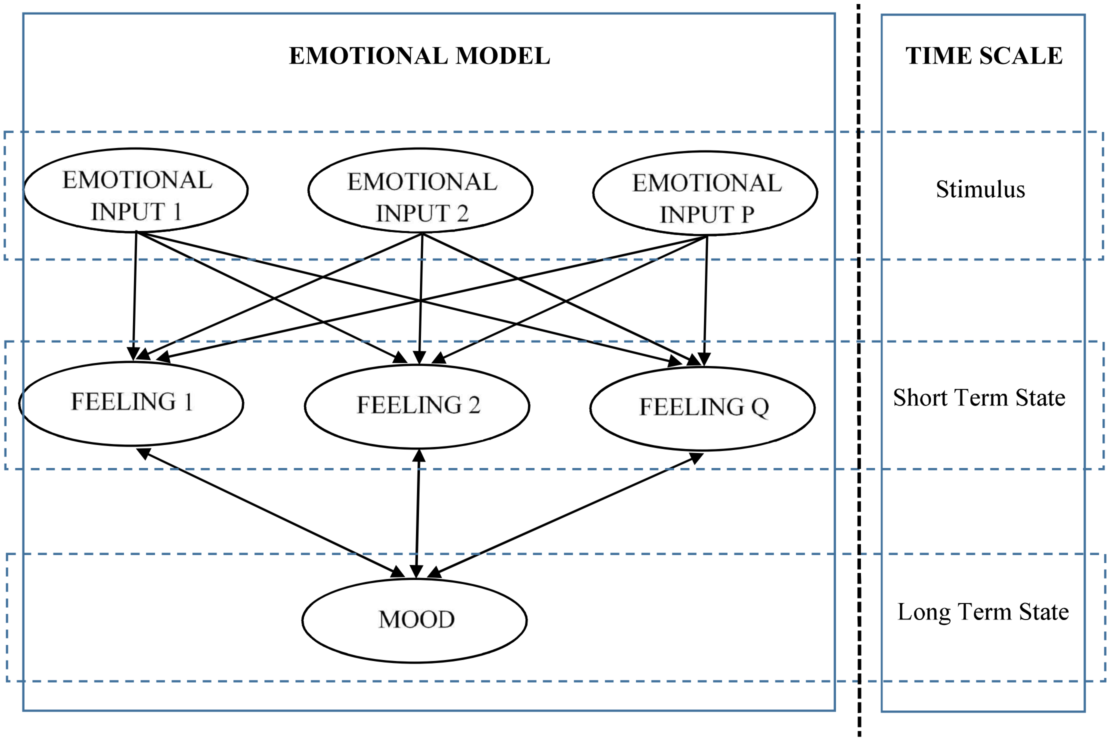


fig.1 Emotional model concept.

Note that full factorial experiment for training this EM with specific data for the usage of memory, NIC and processor with 10 levels for each factor leads to $10^{(3x3+2)} = 10^{11}$ combinations

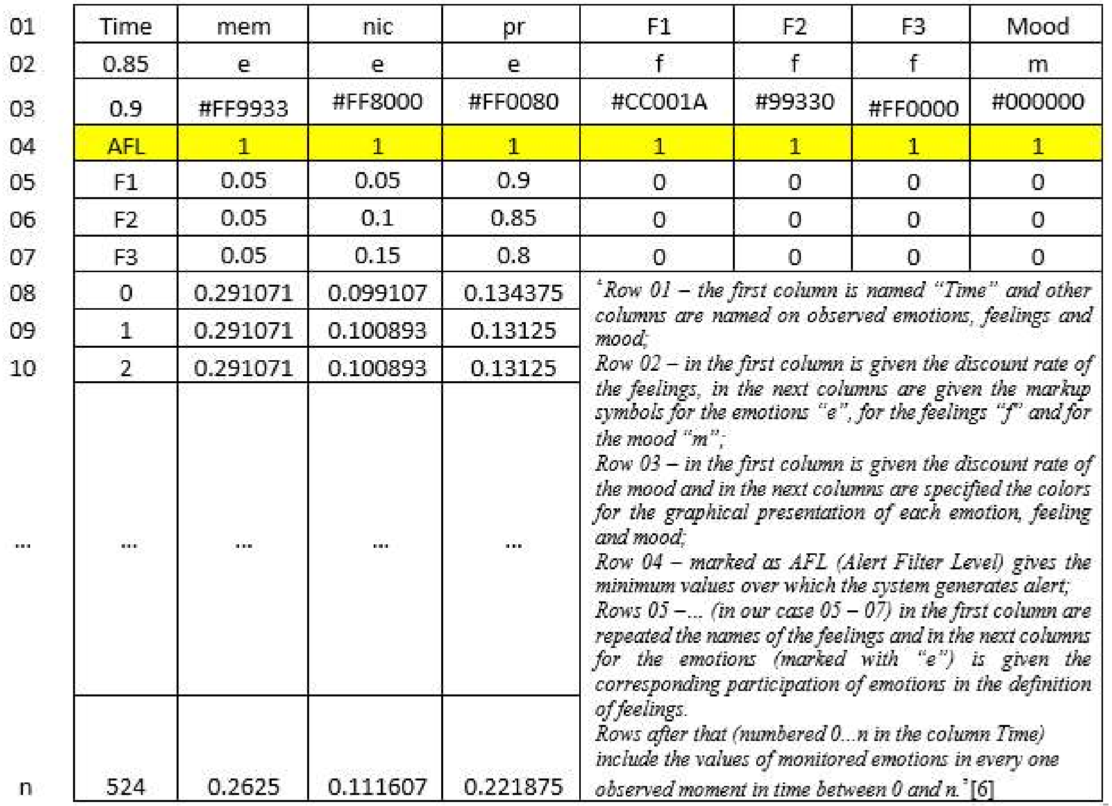
3. WEB BASED CALCULATOR OF EMOTIONAL MODELS

New emotional model for identifying compromised IoT devices is created and calculated by using the Web-application [6] - Web based calculator of Emotional Models. This Web calculator [9] is built by using contemporary Web technologies: HTML5, JavaScript, Canvas and eXtensible Markup Language (XML). The input of emotional model calculator is a XML document with predefined structure. This XML file describes both: emotional model and emotional data. The file was created with MS Excel and saved as XML Spreadsheet 2003. The content of the XML file is shown in Table 1. Its structure and the contents of the cells, row per row are presented in the bottom right corner of the table with italic letters. HTML5 Web calculator of emotional models reads data and according to the emotional model rules calculates the values of the feelings and mood as described in Eq. (1), Eq. (2) and Eq. (3) and visualizes result.

4. EXPERIMENTAL RESULTS

In order to conduct the experimental results with existing similar implementations of systems for identifying various compromised states of IoT devices, the initial data for usage of memory, NIC and processor (in percentages) of the IoT device from [4] is used below. The graphical data from [4] is preprocessed in manner described in [1] to transform these data in numerical form as .xml files. These values (from the corresponding .csv file from [8]) for usage of processor, memory and network interface card (NIC) are imported into the EM (.xml file from [8]) through the Copy-Paste functionality of MS Excel.

Table 1. Emotional model for state identification of IoT devices



01	Time	mem	nic	pr	F1	F2	F3	Mood
02	0.85	e	e	e	f	f	f	m
03	0.9	#FF9933	#FF8000	#FF0080	#CC001A	#99330	#FF0000	#000000
04	AFL	1	1	1	1	1	1	1
05	F1	0.05	0.05	0.9	0	0	0	0
06	F2	0.05	0.1	0.85	0	0	0	0
07	F3	0.05	0.15	0.8	0	0	0	0
08	0	0.291071	0.099107	0.134375	*'Row 01 – the first column is named "Time" and other columns are named on observed emotions, feelings and mood;* *Row 02 – in the first column is given the discount rate of the feelings, in the next columns are given the markup symbols for the emotions "e", for the feelings "f" and for the mood "m";* *Row 03 – in the first column is given the discount rate of the mood and in the next columns are specified the colors for the graphical presentation of each emotion, feeling and mood;* *Row 04 – marked as AFL (Alert Filter Level) gives the minimum values over which the system generates alert;* *Rows 05 –... (in our case 05 – 07) in the first column are repeated the names of the feelings and in the next columns for the emotions (marked with "e") is given the corresponding participation of emotions in the definition of feelings.* *Rows after that (numbered 0...n in the column Time) include the values of monitored emotions in every one observed moment in time between 0 and n.'*[6]			
09	1	0.291071	0.100893	0.13125				
10	2	0.291071	0.100893	0.13125				
...	...	...	...	...				
n	524	0.2625	0.111607	0.221875				

Note that the initial values for the emotions i.e. usage of memory, NIC and processor (columns mem, nic and pr from Table 1) correspond to Time n=0 and the final values correspond to Time n=524. Next 3 columns contain the feelings and last one contains the mood.

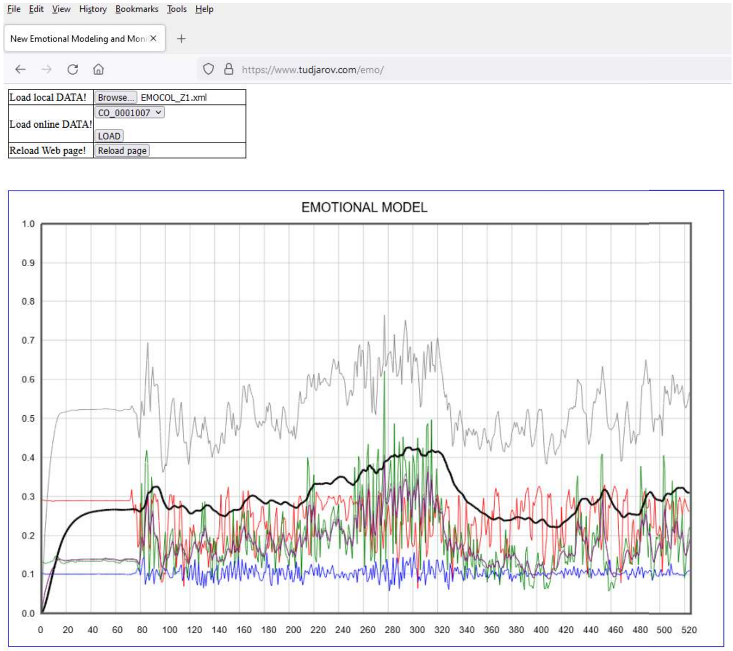
Due to the limited size of the current paper in [10] are given the .xml files for the usage of memory, network interface card (NIC) and processor of the IoT device, in the case when the device is non-compromised (EMOCOL_Z1.xml) and in the case when it is compromised (EMOCOL_Z2.xml). Web based calculator of Emotional Models has been used to calculate the moods for these two states of the IoT device. Corresponding screenshots are shown in fig. 2 and fig. 3.

Final values for the mood from calculator of Emotional Models (n=524 in the column Time) for both states of IoT device are shown in table. 2. The first row of the table shows the mood of non-compromised IoT device, and in the second row shows the mood of compromised device. Also, a third row is added to the table, in which the difference in percentages between the mood for compromised and non-compromised state of the IoT device is given.

The experimental results and more precisely the indexes for the mood (Table 2) show that the difference between the compromised and a non-compromised IoT device is Δ = 12.4%. This corresponds to the results and conclusions from [1, 4], which is also a verification of the obtained results.

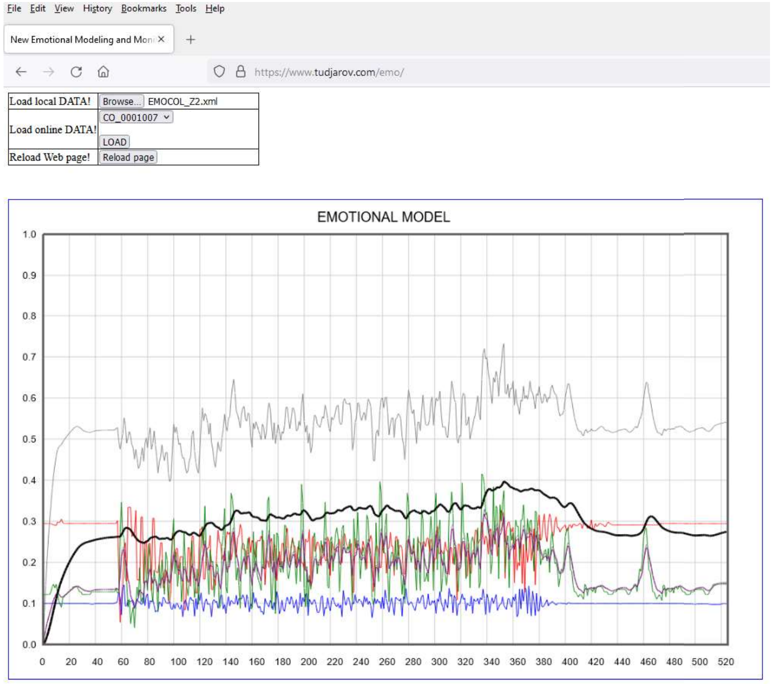
table. 2. Results for memory usage

	E
Non-compromised	0.310
Compromised	0.274
Δ	12.4 %



Load local DATA!	Browse... EMOCOL_Z1.xml
Load online DATA!	CO_0001007 LOAD
Reload Web page!	Reload page

fig.2 A screenshot from the calculator of Emotional Models for the non-compromised IoT device.



Load local DATA!	Browse... EMOCOL_Z2.xml
Load online DATA!	CO_0001007 LOAD
Reload Web page!	Reload page

fig.3 A screenshot from the calculator of Emotional Models for the compromised IoT device.

5. CONCLUSION

An intelligent system for identification of compromised IoT devices due to cyberattack, using web based calculator of EM has been proposed. The results obtained in the present paper are expected to find application in engineering practice, and education process. The proposed approach and web calculator of EM can be relatively easily used in other areas of information security. The work provides an initial solution to such a problem as identification of compromised IoT devices and can be further developed or can be used to give an idea and/or provoke other researchers in their future work.

As a further work we plan to study the applicability of proposed approach in the cybersecurity of Internet of Things and more accurately identifying of compromised IoT devices after cyberattack trough:

-Finding the optimal coefficients $d_{i,j}$ and γ^F and γ^M (such to maximize the difference in moods for compromised and a non-compromised IoT device, Δ).

-Improvement of parameters of emotional model based on its implementation in practice and analysis of its application.

-Improvement of the contents of emotional data based on their classification and definition of their values by the use of the classification.

-Development and implementation of a monitoring system for devices in IoT network keeping in mind that if this would be an intrusive monitoring, it will kill the worst-case execution time.;

-Development of hardware and software implementation of the system for detection of compromised IoT devices as a result of the cyberattack on FPGA;

-Verification and validation by comparing the results with the results of known models which solve similar problem.

ACKNOWLEDGMENTS

The results published in the paper have been achieved under the project № 212ПД00001-09, funded by Scientific and research sector of Technical University- Sofia.

The author would like to thank the Technical University-Sofia for the financial support.

References

1. Hristov, A. Intelligent system for identification of compromised Internet of Things devices after cyberattack, Bulgarian Journal for Engineering Design, issue 43, January 2021, ISSN 1313-7530 , pp. 17-22 (in Bulgarian).

2. Hristov, V., REMOTE CONTRL OF DEVICES TROUGH SSH TUNNEL, Bulgarian Journal for Engineering Design, issue 38, January 2019, ISSN 1313-7530, pp.21-26

3. Trifonov, R., et. al. Network and Information Security, Avangard Prima, 2013, ISSN 978-619-160-183-7 (in Bulgarian).

4. Sukhoparov M., Lebedev I. Identification the Information Security Status for the Internet of Things Devices in Information and Telecommunication Systems. Systems of Control, Communication and Security, 2020, no. 3, pp. 252-268 (in Russian).

5. Tan L., Jiang J. Digital Signal Processing 2nd Edition, Academic Press, ISBN: 9780124158931, 2013

6. Tudjarov B., Panov V. Web Based Approach for Discovering and Prevention of Customs Violations by Application of Emotional Model, Proceedings of the 25th World Multi-Conference on Systemics, Cybernetics and Informatics: (WMSCI 2021), Orlando, Florida, USA, ISBN: 978-1-950492-54-1 (Collection), ISBN: 978-1-950492-55-8 (Volume I), 77-82 pp.

7. Tudjarov B., N. Kazakov, V. Panov, V. Penchev "Development of the Products - Monitoring and Forecasting based on Emotional Model", University in Tuzla, Faculty of Economics in Tuzla - International Conference Proceedings "How to Manage in Time of Crisis", November 26-28, Bosnia and Herzegovina, 2009, pp.377-385.

8. Zendara O., et. al. Swarm intelligence-based algorithms within IoT-based systems: A review

9. https://www.tudjarov.com/emo/ - Accessed July 23rd 2021

10. https://github.com/sashkinaaa/EmotionalModel - Accessed July 23rd 2021.

11. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf - Accessed July 23rd 2021

12. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6308658/ - Accessed July 23rd 2021

13. https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot - Accessed July 23rd 2021

14. B. Tudjarov, N. Kubota, Sh. Aomura, Z. Anisic "Open Innovation and Web based Monitoring by the use of Emotional Model", 4th International Conference on Mass Customization and Personalization in Central Europe (MCP - CE 2010) Proceedings, September 22-24, Novi Sad, Serbia, 2010, pp.182-187

15. N. Kubota, S. Wakisaka "An Emotional Model Based on Location-Dependent Memory for Partner Robots", The Robotics and Mechatronics Conference 2008 (ROBOMEC'08), Nagano, Japan, June 5-7, 2008, Journal of Robotics and Mechatronics Vol.21, No.3, 2009, pp. 317-323.