Risks Assessment and Approaches to Creative of the Reliable Software Modules for IoT Devices

Vadym Malinovskyi, Leonid Kupershtein, Vitaliy Lukichov

Information Protection Department
Vinnitsia National Technical University
Vinnitsia city, Ukraine

Abstract — The some especial aspects and of software functional stability in the IoT devices and their risk factors and algorithmic stability were considered in this paper. The main risk factors and their probabilities, including special informational influences in IoT are considered in these paper. Also was considered a basic approaches of the reliable and fault tolerance algorithms and software modules.

Keywords — Internet of Things (IoT), Data stability, Informational influences, Software, Cybersecurity, Realiability analysis, Software quality, Software modules.

I. Introduction

Most users and industrial IoT and BYoD devices are more and more covers all spheres of humans live, from personal everyday use to professionals use and utilization in the industrial area – such of the Industrial Internet of Things (IIoT) and Commercial Internet of Things (CIoT) [1]. Now, in difficult times and hybrid war and world crisis the question of cyber security of xIoT devices is very acute and actual, what we can see at the big number of cyber attacks on IoT sector and computer and network sector in general. The latest trends of cyber threats are shown, that the individual specials types of cyber threats is a very dangerous and make made a software and hardware faults, which cause to economical and time losses [1].   A wide implementation of xIoT technologies of remote monitoring and remote control in industrial area, the consequences of cyber threats can be very significant and commensurate with the weapons use. That’s making very actual to developing and implementation a various approaches and methods of software cyber defence and reliability increasing. Also it’s allow organizing highly efficient, secure and comfortable automated management, monitoring and data processing of IoT information systems.

The goal of research – is a detailing a research of data stability in IoT software and provide and describes of more decision risks assess and approaches to achieve of maximum level of IoT software stability.

II.Related work

A related works provides a description of the main approaches to protection and processing and risk compensation in IoT data systems section is essential to most research authors articles [1] – [2], [4] – [7]. In this works were described a few key parameters, such as probability of failure-free operation, reliability function, and reliable parameter. But in some cases, given the difference in the intensity of cyber threats and non-compatibility of individual events of cyber threads – the some indexes of keys parameters $k(x)_i$ (such as probability of failure-free operation [1]) may be a very small compared to more significant cyber threats and unreliable factors. That it allows neglecting an individual, especially not influencing additive (or multiplicative) components of probabilities of failure-free operation [1]. That’s, allows us to assume, that the some key parameters, such as probability was that the IoT or BYoD object will fail during time t characterizes the opposite property – unreliability [1] and is expressed, if taking to account only is a maximum probabilities, as: $q_{sum}(t)=\sum_{i=0}^{N} p_i(t)1\xrightarrow{p_i \max(t)>>p_i(t)} p_i \max(t)$. Obviously, $q_{sum}(t)$ $q(t)$ can be considered as a maximum failure distribution function factor (or sum of maximum, most important probability), its derivative: $fi\max(t) = -{}^{dpi\max(t)}\!/_{dt}$. It's the density of the maximum distribution functions of uptime or, the density of maximum failures factors. Experimentally, as a results of the simulation in MathCad and MathLab environments, were received the values of maximum failure distribution function factor in the range: 0.7325 … 0.9341 (high risk conditions) – in taking into account the conditions only of most important factors of cyberthreats and their influences; 0.1521 … 0.4243 (low risk conditions) – in taking into account the conditions only smallest factors of cyberthreats. The average range of values of maximum failure distribution function factor is in range 0.4423 …0.6827. The average range of values of the probabilities of failure-free operation, which was receive by simulation is in range 0.52 … 0.74 , that which is ensured in conditions with most important factors of cyber threats and uses reliable approaches in software.

Modern users and industrial IoT devices has a significant problems – it‘s a complex cybersecurity and low reliability for it's functionality, which slows down their implementation in the critical and industrial spheres. With the growing popularity of smart devices IoT services, the intensity of cyber threats and reducing of summery reliability is inversely increasing.

The trends of 2022 are indicate that the main problems of functionality in modern IoT are:

- Complex cybersecurity of IoT devices and combined with them devices;
- Different reliability risks of IoT devices and their modules;
- Software and hardware core components reliability and low fault free interferences each for each, at of operating functionality witch implements of the IoT platphorm total functionality and also functionality of complex data infrastructures with this IoT devices.

II. Methodology

The methodology in a research paper is the section involves the evaluation of the most significant ones. Also risks assessments are include only the main influence factors of most intensive cyber threats.

Risk assessment when working with information in the Internet of Things is carried out in accordance with the criterion of a comprehensive assessment using the likelihood of the occurrence of a threat:

$$P(\lambda i)\max = \sum_{i=1}^{m} p_{\max i} \cdot k_i \cdot k_m = P_i\,(\lambda) \cdot K_{CMS}\,, \qquad (1)$$

where p_i – unit probabilities of the occurrence of a cyber threat for each of the main informational factors of threats; $p_{\max i}$ – maximum unit probabilities of the compatible occurrence of a cyber threat for each of the main informational factors of threats. $\mathrm{k_i}$ – correction coefficients for each threat factor; $\mathrm{K_S}$ – complex correction coefficients for all threat factors; k_m – coefficient of risk level for each cyber thread or unreliabalence in each of units; K_{CMS} – complex risk factors coefficient .

It's a takes into account only the most important and most influence factors.

It's should be noted that for a comprehensive assessment of the cyber threats it will be fair 0 < $P(\lambda i)\max$ <1, and the higher the set of factors with the corresponding probabilities $\mathrm{r_i}$, the greater the total probability will approach 1.

Accordingly, the conditions (1) of stable work (and implements a basic conditions, as shown in paper [1]) with the absence of risks are ensured by the evaluation of the indicator (stability coefficient):

$$R' \xrightarrow{t_i \to t_{i\min}} {}^{1}\!/_{P_{\max}(\lambda_i)} \to 1 \,. \qquad (2)$$

The higher the indicator R' ($R' \epsilon$ 0 …1) – the better the conditions for the stability of the software in IoT information systems [1].

The most important data in IoT (financial, economical or important technical data, such as shown at the fig.1) and their sub parameters must be protected first and by main priority.

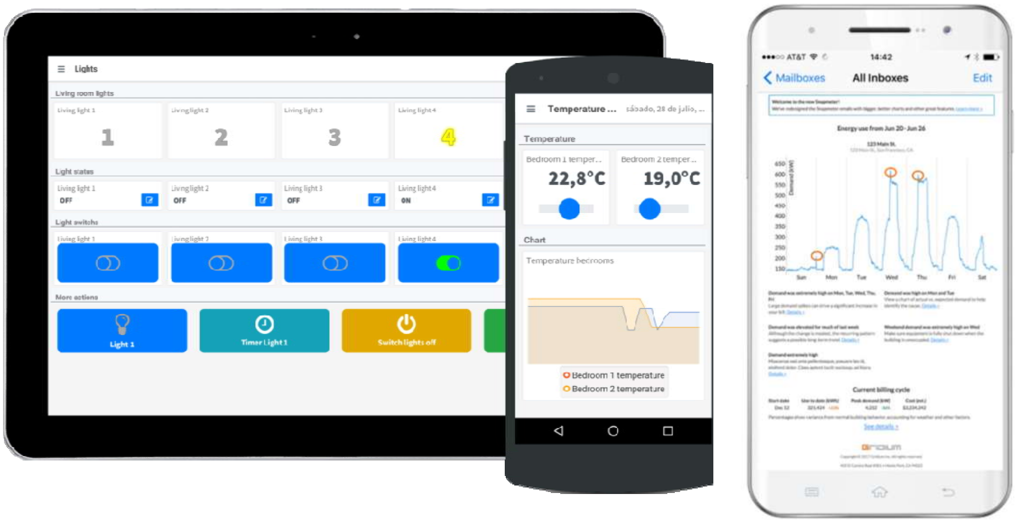

Figure 1. – Example Illustration : Protection the most important and critical sensitive data parameters in IoT devices

Fig. 1 is represents the main field of potentional risk of most important data modification and importance of it's security and protections in data procession IoT software and also is each of it's unit.

The principles of reliable functionality for operating units in IoT software are privides by some separate approaches in software development and implementations methods in IoT. First of all, must be provided a high level of cyber security and hardware reliability by different ways and tools. Second, must be released reliable and reservation data algorithms (data graphs) in critical software, compatible with high reliable and stable hardware support (reliable realizable hardware architecture and components).

Third, must be granted a traditional and famous data model of strong separate parameters and separate access levels and rights of user data with complex security methods are widely used to protect access to resources. A number of modern attacks and modern hacking software can use many methods to explore and hack user data and software modules (or their units) and get access to it's in IoT devices. That needs to gain unauthorized access to internal software, which can then be modified or downloaded. Especially in current times, the hierarchy and evolution of methods and software systems of both a technical nature and social engineering for obtaining closed data and information for the purpose and further use of them for fraudulent and cybercriminal purposes and committing crimes of an economic nature has significantly increased.

To best protect data and increase its stability and functionality it is important to understand what makes this data and data software units reliable, how it content can be identified by a unique identifier and reproduce and verify at another point (mechanism of checksums/Hash functions) with complex protection mechanisms. A special feature is also the authorization data and ensuring the reliable implementation of complex authorization models (such as Triple AAA model, provided by Cisco Inc.). In particular it create the reliable accounts and reduce a parts of risks, when accessing the software part and as one of the components of the security policy information systems as a whole. Creating a reliable checksum (hash function) mechanisms on different stages of computing processes for each software modules, and also reliable strong passwords are an integral part of the security measures of modern data systems. Trusted identifiers and data must meet the requirements listed in order of importance:

1. Have unchanging unique content and functionality;

2. The value of identifiers does not change as at the point of creation information data, as well as at intermediate points and to the final points of their reception/processing;

3. Work fault tolerance algorithms should not take a lot of resources and not have extremes of work functions (peaks during work in tracking mode);

4. Methods of conversion and comparison of keys of data identifiers should not be complex and take up a lot of computing resources.

5. Uses an mechanisms of automated controls of check checksum and hash function of software modules by all its lifecycle and working process. Also it's may take places for the working files and functional data of this software modules.

6. Identifiers must not be readily accessible to functional testing modules and must be protected from other leaks and access. Hash functions and checksums should be relatively complex as well data and generated on the basis of the received data, may contain numbers, symbols and their mixture in the upper and lower registers.

The popularity of using trusted data and the checksum/Hash function mechanism to verify data integrity is due to the fact that such verification is simple to implement in digital hardware, easy to analyze, and well suited for detecting common errors and vulnerabilities, weak cryptoresistance caused by the presence of noise in data channels, and information systems.

Given such a large number of potentially possible cyber threats and information risks for IoT and mobile personal devices, it is necessary to use comprehensive IoT approaches and mechanisms at all levels. It is also relevant to develop new progressive approaches and world-leading practices, such as demarcation of networks, IoT segments, ZeroTrust area, data protection systems for IoT. Basic model was shown in paper [1]. The use of a comprehensive method of checking and neutralizing cyber threats is also relevant. In general, the structural mechanism and complex approach to data protection in the Internet of Things and its component should include the parallel use of information protection mechanisms:

$$F_{Actual}(IoT\ Security) \rightarrow F_{Max}(t_i, x_i \in n; y_i \in m; z_i \in k; t_i \rightarrow t_{imin}, p_i \rightarrow p_{max}) + \Delta F(F_i(t_i, x_i \in n; y_i \in m; z_i \in k; t_i, p_i) +$$

$$+ F_{ZeroTrustZonePolicies}(t_i, x_i \in n; y_i \in m; z_i \in k; t_i \rightarrow t_{imin}, p_i \rightarrow p_{max}) \tag{3}$$

where, F_{Actual} *(IoT DataSecurity)*, F_{Max} *(IoT DataSecurity)* – actual, max and additional (from minimal risk factors components) designation of a complex conditional function of maximum IoT information protection and reliability indexes with a minimum number of threats in IoT systems; $F_{ZeroTrustZonePolicies}$ $(t_i,, x_i \in n; y_i \in m; z_i \in k ; t_i \rightarrow t_{imin})$ – the use security functions by providing of access rights delimitation policies and information security policies based on the concept of zero trust in IoT zones*;* $t_i,$ – conditional time intervals; $x_i \in n ; y_i \in m ; z_i \in k$ – corresponding information parameters and their belonging to sets; $t_i \rightarrow t_{imin}$ – criteria for performing functions in the shortest possible time.

In general, it is possible to achieve the maximum level of protection (minimal risks factors) in the Internet of Things devices only with the use of an integrated complex approaches, with consideration only max influence factors in data flow model, the use of the above-mentioned individual complex components and integrated approach for information protection function in IoT, under conditions:

$$F_{Actual}(IoT\ DataSecurity) \rightarrow F_{Max}(IoT\ DataSecurity) + F_{\Delta}(IoT\ DataSecurity) \tag{4}$$

It is extremely difficult to ensure full functional security and secure data transmission and processing for personal IoT with mobile personal devices of users as part of it, taking into account the different functional orientation and the use of individual multi-structured components in the complex and multi-component information system of modern IoT, as well as taking into account the specifics of the use of publicly available Internet channels – as one of the main sources of cyber threats.

Ensuring stability and reliability of functionality, the concept of data integrity, availability and confidentiality (CPA) in modern IoT is one of the priority tasks on future. New models and methods should be based on a complex combination of functionality, data virtualization technologies, the use of modern IDS/IPS with mixed additional functionality. Also, in order to increase the level of security, additional conditions for checking and controlling third-party information flows with reliable improved encryption with offset and in combination with computing parallelism should be created process with demarcation of access rights at different levels of computing and virtual computing environments (shells) for different processes.

Approaches to Creative of Reliable and Fault Tolerance Algorithms must provides by strong reliable parallel processing or alternative logical condition paths processing if software irrational or failure condition are occurs. Fault tolerance end point (point of entry) in cycle must include a alternative way of processing in software algorithm path (algorithm path) or provide a start a spare software resources. Also may be involved a special additional software modules to provide a alternative ways to similar functions of data processing. That's provides a high level of functional stability of software. If the hardware fault is occur, and hardware architecture having a strong serial data processing model, that are not prevent to general software failure. That, for strong reliable stabile and reliable data processing model in IoT software must be granted a parallel or reservation hardware architecture or fault tolerance or recovery methods [3].

III. Results

Since informational threats in microprocessor tracts in data systems, including microprocessor devices of the Internet of Things (IoT) are quite often complex and have a complex nature and stages of implementation, then solutions aimed at protecting the computing process and the algorithms of the microprograms of the control microcontroller must also has a comprehensive approaches. This approaches of increasing the data security and reliability must realization by transmission and processing data flows in MC microprograms with more reserve and stability principles in IoT software.

To ensure the closure of potentially dangerous critical places of the IoT controller architecture, individual and complex approaches are used to organize the necessary state of security:

1. Control of the integrity and reliability of the memory content in software (including a strong control a sensitive and potentially malicious content), which is provided by checking and correcting errors of the Error Correction Code and checking parity. It also provides additional protection against attacks aimed at preventing code bugs from infecting systems;

2. Control of external and internal data flows and key-parameters of software platform in IoT. For example, a temperature sensor continuously measures the temperature of the environment surrounding the microcontroller, which also may be threated;

3. Approaches, which involving the use of isolation and control of the integrity software modules by Hesh-functions and Checksum mechanisms (MD4, MD5 or SHA 256/SHA 512, CRC8, CRC16, CRC32 or others Hesh-functions algorithms). It's can also be used by cyclic redundancy code engineering or implementation of the fault tolerance algorithms with reserve alternative branches;

4. Hardware-based approaches that use a cyclic redundancy check calculate, i.e. a checksum is calculated that detects errors in data transmission or storage. Not only does this ensure code integrity is checked, but it also means that the signature can be calculated at runtime;

5. Monitoring KPI parameters of software life indexes (health indexes) and resource monitoring is another method with a high degree of protection. To determine the cause of the reset and thereby ensure reset only through authenticated access to the 'Cybertheat indicate flags' status management system.

In the results of work were received the dependencies in probabilities of failure-free operation and parameter of failure distribution function factor in some especially conditions.

Experimentally, as a results of work were received the values of the density of the maximum distribution functions and probabilities of failure-free operation. Maximum failure distribution function factor are in the range: 0.7325 … 0.9341 (high risk conditions) – in conditions with only of most important factors of cyberthreats and their influences and that range of values are in range in 0.1521 … 0.4243 (low risk conditions) – in conditions with smallest factors of cyberthreats influence. The average range of values is in range 0.4423 …0.6827. Also was received the average range of values of the probabilities of failure-free operation, which was receive by simulation is in range 0.52 … 0.74 , that which is ensured in conditions with most important factors of cyber threats and uses reliable approaches in software.

IV. Conclusion

In the conclusion, providing of the maximum stability in IoT software may be reached by providing maximum cyber security and reliability of each software modules component in program environment in IoT. New models, such reliable and fault tolerance algorithms may increase a summary stability of IoT software and data processing model. Also, may take place a providing another perspective methods of stability increasing of IoT software complexly with hardware stability architecture and hardware methods. The given results in paper can to take into account an some most important factors of cyber heats and failures, and summery assessments of risk in IoT more precision.

References

[1] Malinovskyi Vadym, Kupershtein Leonid, Lukichov Vitaliy "Cybersecurity and Data Stability Analysis of IoT Devices"*2022 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkiv 2022, pp. 474-478, [online] Available: https://easychair.org/smart-slide/slide/lRtj

[2] V.V.Sklyar, V.V.Yatskiv, N.G.Yatskiv,"Dependability and SecurityInternet of Things: Practicum", *Ministry of Education and Science of Ukraine, National Aerospace UniversityKhAI, Ternopil National Economic University*, 2019.

[3] K. Nelson, R. Davis, D. Lutz, and W. Smith, "Optical generation of tunable ultrasonic waves," Journal of Applied Physics, vol. 53, no. 2, Feb., pp. 1144-1149, 2002

[4] C. Canella, J. Van Bulck, M. Schwarz, M. Lipp, B. von Berg, P. Ortner, F. Piessens, D. Evtyushkin, and D. Gruss, "A systematic evaluation of transient execution attacks and defenses," *arXiv preprint arXiv:1811.05441*, 2018, [online] Available:https://doi.org/10.48550/arXiv.1811.05441.

[5] O. Voitovych, Y. Baryshev, E. Kolibabchuk and L. Kupershtein, "Investigation of simple Denial-of-Service attacks", *2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T)*, 2016, pp. 145-148, [online] Available:https://doi.org/10.1109/INFOCOM-MST.2016.7905362.

[6] O. Voitovych, L. Kupershtein, O. Shulyatitska and V. Malyushytskyy, "The authentication method in wireless sensor network based on trust model",*2017 IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON)*, 2017, pp. 993-997, [online] Available: https://doi.org/10.1109/UKRCON.2017.810039.

[7] O. Voitovych, L. Kupershtein, V. Lukichov and I. Mikityuk, "Multilayer Access for Database Protection"*2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, 2018, pp. 474-478, [online] Available:https://doi.org/10.1109/INFOCOMMST.2018.8632152.