Open Access Library Journal
2024, Volume 11, e11787
ISSN Online: 2333-9721
ISSN Print: 2333-9705

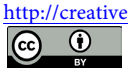
Development of a Conceptual Model for Ensuring Cyber-Resilience of Software Systems

Shafagat Mahmudova

Department of Scientific-Theoretical Problems of Software Engineering and Intelligent Software Systems, Institute of Information Technology, Baku, Azerbaijan
Email: shafagat@gmail.com

How to cite this paper: Mahmudova, S. (2024) Development of a Conceptual Model for Ensuring Cyber-Resilience of Software Systems. *Open Access Library Journal*, **11**: e11787.
https://doi.org/10.4236/oalib.1111787

Received: June 6, 2024
Accepted: July 7, 2024
Published: July 10, 2024



Abstract

Cyber-resilience of software systems is the ability to prevent, resist, and recover from adverse incidents using IT resources. Infrastructure can be extended through cyber-resilience. In this case, the problems can be solved in a short time. In this study, some methods of ensuring the cyber-resistance of the software system are explored. The role, type, and characteristics of cyber-resilience for the software system are also examined in the work. Ways to implement Cyber-resilience measures for cyber security and information technology are analyzed. The paper also outlines the ways to enhance cyber-resilience through smart threat operations. Cyber security possibilities and the ways to solve the problems encountered are highlighted. A new model is developed to ensure the cyber-resilience of the software system used.

Subject Areas

Cyber-Resilience

Keywords

Cyber-Resilience, Software System, Cyber-Security, Information Technology, Model

1. Introduction

Cyber-resilience refers to the ability to prevent, resist and recover from bad events using IT resources. It is actually the capacity to face challenges.

The concept of software sustainability is applied to technology. Resilient software is robust and able to "recover" from unexpected problems and incidents.

The research conducted by the Cyber Resilience and Intelligence Division (CRID) is essential to analyze multimodal data flows to prevent attacks on the

current and future infrastructure of the country, and to help ensure systems remain functioning in the face of attacks. CRID is also actively engaged in efforts such as increasing the number and diversity of employees with the skills necessary to solve the growing cyber-physical problems in the economy and national security infrastructure, ensuring the security of systems, and preventing fraud and waste [1].

The Internet of t Things (IoT), including computing capabilities, artificial intelligence (AI), digital home security systems, health, connected devices, national defense systems, smart factory equipment and advanced communication networks such as 5 G, 6 G, refer to cyber explosion. Numerous cyber vulnerabilities must be identified and addressed in the country's most critical economic and national security infrastructures. In addition, obviously, there are not enough employees with the necessary skills, training and experience to solve these problems.

Sophisticated nation-state cyber actors exploit these vulnerabilities to steal valuable information, threaten national security, and disrupt and destroy systems critical to livelihoods and survival. It is important to characterize the intent, behavior and personality of the adversaries so that a smart approach to protecting the nation can be provided. Mishandling in financial systems and national defense is one of the important issues to increase the resilience of command and control networks.

1) Cybersecurity typically refers to resistance to cyber-attacks. Creation and arrangement of cyber controls restricting the extent and mitigating the impact of attacks is the basic strategy of the organization. In successful cases, the companies will be able to prevent most attacks, or continue to function with minimal delays and damages.

NIST Cyber Security Framework is robust cyber resistance frameworks. However, several other good practices created daily in this field fail to be beneficial in the fight against cybercrime. Moreover, some leading organizations with good practices struggle to meet their own aspirations across all affected areas of the enterprise [2].

2) Nowadays, cyber attacks are targeting all sectors with growing sophistication, frequency and severity. All of these emphasize their unavoidability and the impossibility of totally defending the integrity of critical computer systems. To this end, cyber-resilience offers a good substitution for current cyber security paradigm. Cyber-resilience is defined as the opportunity to endure, recover from and adapt to failures caused by cyber-risks. [3] attempts to ensure a broader organizational consideration of cyber-resilience and the pressures related to its application. The article applies Weick's (1995) sense making framework to study four foundational pressures of cyber-resilience, which are a definitional tension, an environmental tension, an internal tension, and a regulatory tension. Moreover, the authors explain how these tensions are embedded in cyber-resilience practices at three stages, as the preparatory, response and adaptive stages. For their study, they use qualitative data from a sample of 58 cyber security profes-

sionals to reveal these tensions and how they reverberate across cyber-resilience practices.

3) Performance of manufacturing is increased through the integration, automation and digitalization of related networked systems. Therefore, networks become potential targets of attackers to compromise companies due to the vulnerability of these systems. Thus, the study highlights the functional structure of cyber resiliency in cyber-physical production systems. It uses Axiomatic Design as a design methodology for the concept design of a cyber-resiliency module. Design parameters are disintegrated and design guidelines for readiness for cyber attacks are ensured based on functional necessities. These guidelines are applied to a cyber-physical demonstrator which implements the Industrial Internet of Things with a digital twin. Accordingly, physical/virtual solutions for the system are found. This approach based on an axiomatic design ensures the study of solution-neutral functional requirements which provide functional cyber resiliency solutions. Offered guidelines have practical value in the planning phase of manufacturing system networks to raise their longstanding resiliency. The authors guarantee the solution-neutral design of cyber resiliency in manufacturing companies [4].

4) Natural disasters and cyber intrusions repetitively threaten the electric grid operation. The introduction of Internet of Things (IoTs) based on distributed energy resources (DERs) offers prospects for flexible services to empower efficient, reliable and resilient operation. Moreover, IoT based DERs have cyber vulnerabilities and entails cyber-power resiliency analysis of the IoT-integrated distribution system. The article highlights the development of metrics to monitor resiliency of cyber-power distribution system, while maintaining consumers' privacy. In this case, resiliency involves the system's capacity to ensure energy to the critical load even during bad incidents. The IoTTrustability Score (ITS) of offered cyber-power Distribution System Resiliency (DSR) metric involves the effects of IoTs using a neural network with federated learning. Resiliency related ITS and other factors are integrated into a single metric using Fuzzy Multiple-Criteria Decision Making (F-MCDM) to compute Primary level Node Resiliency (PNR). In conclusion, DSR is computed through PNR aggregation of all key nodes and characteristics of distribution level network topology and vulnerabilities exploiting game-theoretic Data Envelopment Analysis (DEA) based optimization. The proposed metrics is beneficial for first, monitoring the distribution system resiliency taking into account a holistic cyber-power model; second, enabling data privacy by not applying the raw user data; and third, enabling better decision-making to select the best possible mitigation strategies. Offered ITS, PNR, and DSR metrics are confirmed satisfactory for the IoTs-integrated IEEE 123 node distribution system [5].

5) The study offers a new algorithm to software using artificial immune systems applying the Bayesian method. The system refers to an adaptive computing system and uses models, principles, mechanisms, and functions to solve problems in theoretical immunology. The article applies it different fields of science.

It also explores the system's valuable importance and the methods for malware detection. The article analyzes some related works in the field of artificial immune system and identifies the challenges. The possibility of occurrence of any event under certain conditions is precisely calculated by the Bayesian method. Therefore, the Bayesian method is applied to software using artificial immune systems. Fast software performance can be achieved by applying this method. To this end, the article develops a new algorithm and performs trials and achieves good performance [6].

6) The article reviews software security and studies the methods for the analysis of software security and identifies the problems of software protection. It explores the risks for software projects, their management, determination and categories. The process of software development involves the construction of its agreed structure. The article describes the standard-based ontology of cyber security and reviews the main concepts related to cyber security problem and their relationships. It also studies basic structure, concept, etc. of intelligent software system to ensure cyber security [7].

2. Development of a Model for Ensuring Cyber-Resilience

Figure 1 presents the model designed for ensuring cyber-resilience of software.

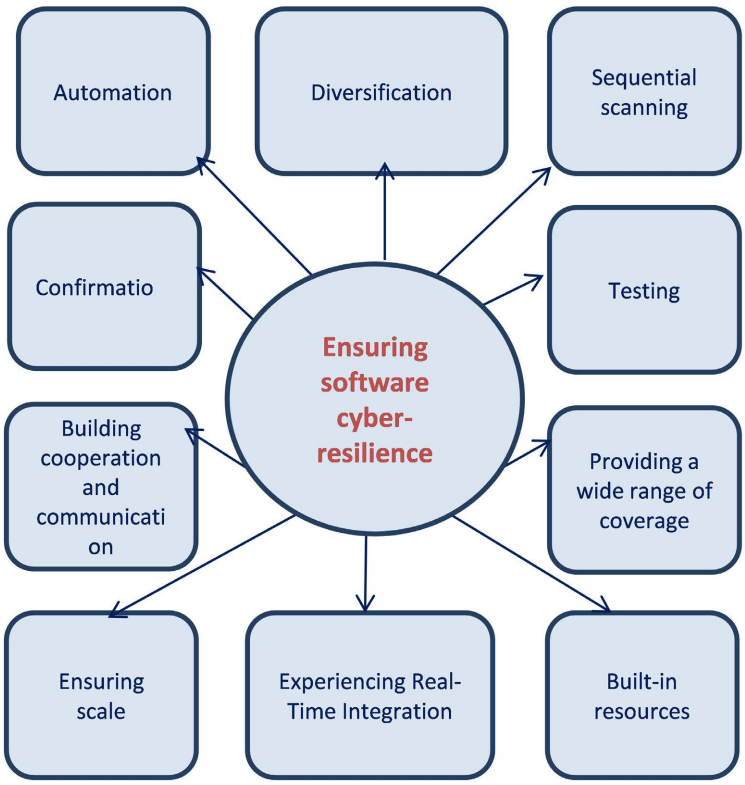


Figure 1. A model for ensuring software cyber-resilience.

1) Since the manual work is prone to errors, it is necessary to automate the process.

2) From a resilience point of view, it is possible to diversify the infrastructure by using multiple providers. Consequently, if one provider experiences downtime, it can turn to another, minimizing the impact and scope of the problem. Therefore, fewer users will be affected by the incident. Infrastructure can be extended by leveraging cyber resilience. In this case, the problems can be solved in a short time [8].

3) Potential errors in software are easier to detect when routine scans are started. This will allow assessing the sustainability of the technology in various aspects, from safety to power. The scans themselves will detect problems before they affect users in real time.

4) To test the code and systems, it is necessary to ensure that any changes made are automatically approved. Hence, making these changes will not interfere with the system or adversely affect the environment in which it resides.

5) Test, trial. This is the wide-ranging and best approach to evaluating the software functionality and ensuring that it can withstand any problems that may arise. Skilled testers must conduct multiple evaluations, from load testing to performance testing. This will help you see how the program will behave and respond to many different types of conditions and understand if there is a need to make adjustments.

6) Resilience strategies cannot be limited to just one situation. It should have a broad scope that includes the environment in which the systems and software run. This likely includes cloud-based environments, hybrid and other possible situations, as well as hybrid and other possible situations.

7) Creation of backup methods. Accordingly, backup methods can be resorted to ensure proper coverage if faced with any downtime in the systems. Instead of going completely offline and disrupting operations, systems can turn to a backup provider.

8) Integration of sustainability mechanisms into existing systems in the enterprise. It should be clear how to get real-time feedback from various support systems, so that when a problem occurs, it can't be ignored, notification will be activated immediately and problems will be resolved quickly and efficiently.

9) As intelligent software systems increase, durability is tested more frequently. Since scalability is a common goal for many organizations, their systems should be built with scalability from the start. It is necessary to consider the long-term perspective. Thus, software systems will be more sustainable when going through this process.

10) Unquestionably, there are skills that increase resilience. Keeping everyone informed and aware of the effort will ensure that all employees contributing to the project are in the circle. This coordination will provide effective functioning as a unit and help everyone understand the project's goals and future challenges.

11) Consumers suffer when they experience outages and other problems with their systems. Therefore, it's so important to build software systems considering this. Resilience means having a powerful product with features and aspects that can withstand shocks. When prioritizing this, it will be possible to create not

only a better intelligent software system, but also gain a reputation as a quality organization.

Figure 2 illustrates the cyber-resilience measures for information technology [9].

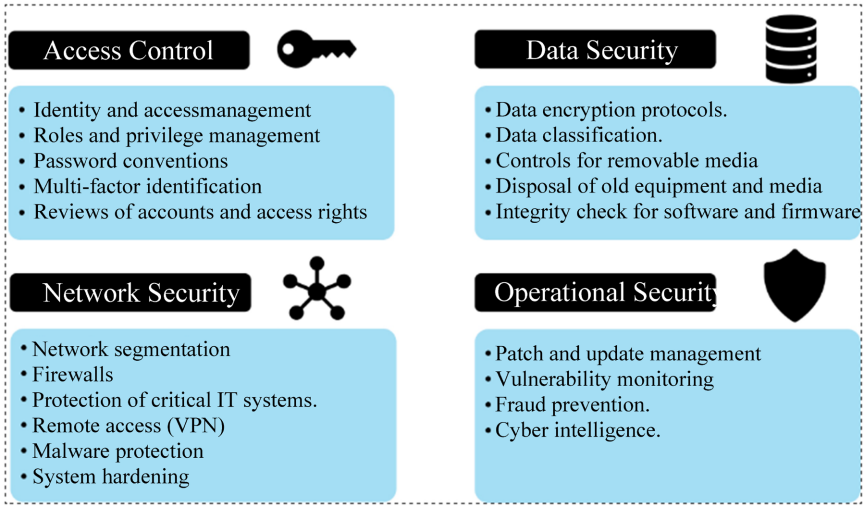


Figure 2. Cyber-resiliency measures for information technologies.

There are four dimensions ensuring the veracity of the information system of an organization, which the concept of cyber resilience counts on. They are as follows:

- We will say that such a process is without memory.
- Access control. Access to a specific information technology network of an organization is regulated and controlled by several strategies. For example, credentials, mainly user names, and passwords are used to access the network. Moreover, the roles and what information users may access are dependent on close supervision to guarantee that rights are removed if a user quits the company or is appointed to different position. Selection of passwords is realized with severer agreements. They should be more compound and contain specific symbols to avoid password attacks. Two-factor authentication is acceptable for highly vulnerable information or if the user accesses the system from a new location.
- Data security. The integrity of the information stored by an organization is regulated by numerous strategies. To avoid breaches data encryption and transmission should be applied. Furthermore, business data should be grouped by its importance level and vulnerability and stored consequently. Vital strategic information should be stored in systems only accessible through internal networks and via extremely protected links. Transferrable data, such as UBS storage drives, laptops and portable devices, should be limited since they characterize security hazards. Moreover, old IT devices should be correctly thrown away. Any storage device intended to be disposed of should be wiped or physically destroyed. The integrity of their software and hardware should

also be confirmed systemically.

- Network security. The integrity of an organizational information technology network is protected through specific strategies. The administrative network is disconnected from the network supporting operations when an it network is segmented. Cyber resilience can advance through network redundancy. Firewalls are the standards to monitor all the incoming and outgoing traffic between a network and the outside, which comprises the use of virtual private networks (VPN) for outside access. Physical protection ranging from locked access for servers and network hubs is also required for IT systems, nonetheless, it should also imply protection from risks such as floods and power outages. Malware attacks the IT network as a propagation tool within the organization's IT infrastructure, thus it must be protected from them. Moreover, cables and switch boxes, etc. of the network must be reinforced against physical damage.
- Operational security. Daily IT operations are also ensured by some strategies. To keep each network component up to date, software upgrades and patches should be ensured. Hackers continuously examine IT networks, so the network should be continually checked for weaknesses. Hackers are motivated to reach the finance of organizations since they are accessible online. Therefore, organization's IT department should adapt to intelligence in the sector, *i.e.*, they have to be aware of new risks and bad incidents occurred in other companies [10].

3. Ways to Increase Cyber-Resilience through Smart Threat Operations

Cyber-security includes a number of technologies, processes, methods to protect computer equipment, data, programs, services, networks from unwanted or unauthorized access, changes and destruction, including unplanned events and natural disasters [11].

Assets in cyberspace, resources of value to an individual, organization or state, can be tangible or intangible. Tangible assets include enterprises, buildings, equipment, vehicles, property of raw materials, etc. Intangible assets include services or service provision, ownership of patents or important information, redundancy, expertise, reputation of employees.

Several issues required to be addressed in cyber-security issues are as follows: [12].

- to determine the protection of objects;
- to determine the source of the dangers;
- to take measures for counter-threats;
- to monitor the vulnerability of all assets;
- to detect systems similar to the cyber-systems of military and government agencies;
- and so forth.

The evolution and expansion of the Internet are facilitated in the virtual

world, which has led to good consequences. Fields like big data, artificial intelligence and machine learning have brought about a big change in the virtual environment.

Semantic Web technologies can also be applied in the field of cyber-security to analyze the types of input data [13].

Security operations are often based on the wrong approach.

For example, the most sensitive assets in hospitals are operations performed in surgical departments. Attackers can steal data and money.

Assets must be the core of an effective cyber defense strategy, because in an increasingly digital world, not everything can be correspondingly protected.

Security information and event management (SIEM) can provide real-time detection of known attacks.

Active defense companies use both SIEM and anomaly detection systems to provide more comprehensive threat detection.

While threat modeling, risk analysis, and vulnerability analysis should focus on the asset's value to the company and potential security vulnerabilities, profile of the possible attackers is also vital. Modeling the most likely attackers and how they operate can help identify new vulnerabilities and direct resources to strengthen vulnerable points.

A key part of cyber-resilience is the ability to foresee the attacks before they happen. Threat modeling is a crucial part of this approach. However, to stop real-time attacks, a company must also be prepared with cyber security capabilities as specified below:

Cyber-security measures at the application protection level;

Use of security mechanisms;

Viewing ontology as a basis for the development of an intellectual system;

Verification of application and data accuracy;

Using data, safe scenarios to prevent attacks;

Providing standard proposals for protecting servers from unauthorized access;

Adjusting servers and operating systems;

Checking security measures and other system disturbances;

and so forth.

4. Conclusions

Several issues presented below need to be addressed in cyber security issues:

To determine the protection of objects;

To determine the source of the dangers;

To take counter-threats measures;

To monitor the vulnerabilities of all assets;

To detect systems similar to the cyber systems of military and government agencies;

and so forth.

materials, etcmaterials, etc.

information, redundancy, expertise, reputation of.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] Sergei, P. (2022) Cyber Resilicence. Taylor & Francis.

[2] Phil (2016) Cyber Resilience: Part Two Resistance. https://blog.blackswansecurity.com/2016/02/cyber-resilience-part-two-resistance/

[3] Dupont, B., Shearing, C., Bernier, M. and Leukfeldt, R. (2023) The Tensions of Cyber-Resilience: From Sensemaking to Practice. *Computers & Security*, **132**, Article ID: 103372. https://doi.org/10.1016/j.cose.2023.103372

[4] Aruväli, T., De Marchi, M., Rauch, E. and Matt, D. (2023) Design Decomposition for Cyber Resiliency in Cyber-Physical Production Systems. *Proceedings of the* 15*th International Conference on Axiomatic Design*, Eindhoven, 16 December 2023, 3-14.

[5] Sarker, P.S., Sadanandan, S.K. and Srivastava, A.K. (2023) Resiliency Metrics for Monitoring and Analysis of Cyber-Power Distribution System with IoTs. *IEEE Internet of Things Journal*, **10**, 7469-7479. https://doi.org/10.1109/jiot.2022.3183180

[6] Mahmudova, S. (2021) Developing an Algorithm for the Application of Bayesian Method to Software Using Artificial Immune Systems. *Soft Computing*, **25**, 11837-11843. https://doi.org/10.1007/s00500-021-05972-2

[7] Mahmudova, S. (2022) Development of an Intelligent Software System to Ensure Cyber Security through Ontology. *Proceedings of the NATO ARW Cybersecurity of Industrail Control Systems*, **62**, 27-30.

[8] Cyber-Resiliency Measures for Information Technologies. https://porteconomicsmanagement.org/pemp/contents/part2/digital-transformation/cyber-resiliency-measures/

[9] Jean-Paul, R., Theo, N. and Athanasios, P. Cyber-Resiliency Measures for Information Technologies. Chapter 2.4, The Digital Transformation of Ports. pp. 9-15. Tokyo. https://porteconomicsmanagement.org/pemp/contents/part2/digital-transformation/cyber-resiliency-measures/

[10] Jean-Paul, R. (2021) The Concept of Cyber-Resilience. https://porteconomicsmanagement.org/the-concept-of-cyber-resilience-new/

[11] Bakhtizin, V.B. and Glukhova, L.A. (2010) Technology of Software Development, BSUIR. https://libeldoc.bsuir.by/handle/123456789/754

[12] Borodakii, U.V., Dobrodeev, A.U. and Butusov, I.V. (2014) Cybersecurity as the Main Factor of National and International Security of the KSHI Century. *Issues of cybersecurity UT Cybersecurity*, **1**, 5-12.

[13] Georgescu, T.M. and Smeureanu, I. (2017) Using Ontologies in Cybersecurity Field. *Informatica Economica*, **21**, 5-15. https://doi.org/10.12948/issn14531305/21.3.2017.01