Ilkogretim Online - Elementary Education Online, 2021; Vol 20 (Issue 5): pp. 4622-4637
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.05.510

Security of Information Technology Infrastructure Library (ITIL) Processes in the IoT environment: Design of a Framework

Akram Ghanaee, Ph.D. in Information Technology Management, Faculty of Management and Accounting, Qazvin Islamic Azad University; Akramghanaee@gmail.com
Mohamadreza Sanaei, Assistant Professor, Faculty of Management and Accounting, Qazvin Islamic Azad University; Mohamadrezasanaei@gmail.com
Javad Mehrabi, Assistant Professor, Faculty of Management and Accounting, Qazvin Islamic Azad University; Mehrabijavad@QIAU.AC.IR

Abstract- One of the main pillars of the Information Technology Infrastructure Library (ITIL) is processes, the security of which in the Internet of Things (IoT) is one of the pillars of this research. The security of ITIL processes requires proper management to maximize security levels so that complex paths can be eliminated, performance improved, the structure of ITIL processes optimized, and, finally, goals achieved. In the present research, we propose a framework based on a detailed analysis of relationships, manual and systematic models by studying the security of research achievements in three parts: free, university and organizational.This framework is formed with component analysis, hybrid relationships, possible scenarios in three phases of general, private and release based on security zones and the final simulated model of Security-General-Private-Release (SGPR). Finally, by changing various parameters, its effect on the levels are measured and a calibration test is performed to match the model parameters with the simulation output.

Keywords: **ITIL, IoT, Simulation Model, Security Framework**

I. INTRODUCTION

In IoT, every physical object in the virtual world is acceptable, accessible, and configurable [1-3]. Undoubtedly, objects in IoT are a context for playing an active role in human activities, systems and processes. An intelligent factor consists of a person, intelligent objects, processes and technological ecosystem as key elements of our systematic approach to IoT security [4]. IoT consists of the aggregation of a wide range of data connected to the Internet. As a result, security risks increase with new services [5]. Along with the development of IoT, the number of security attacks is increasing day by day, therefore, a defense mechanism is needed to identify and cope with attacks and threats in IoT [6].

In today's world, processes and process innovations are used to advance and achieve goals [7]. Improving effectiveness is possible through processes, management methods, emphasis on structure and comprehensive changes in the shadow of security [8]. One of the tasks of management is to reduce and minimize attack routes and their complexity in order to reduce the cost of protection to the lowest possible level and thus increase the level of security to the highest possible level, which will be possible by proper analysis of the possibility [9]. It can be said that instead of directly presenting a defense mechanism on each of the parts, first only the data analysis is carried out and the security of the network is evaluated.In this way, important structures and actions around the processes are prioritized and reciprocal actions are taken. Also, the processes that have the most effect on the strategy are identified and their performance is systematically evaluated [7, 10]. Security issues can be examined with tools, models, criteria as well as methods. We also find that increasing security significantly reduces latency, which can often be reduced at a cost [11, 12]. Modeling IoT security is difficult due to the large number of heterogeneous devices and multiple threats, so we try to use the results of the analysis to achieve the capabilities of the proposed framework to find possible attack paths and reduce the effect of attacks [2].Abundant communications and their difficult limitations lead to security challenges [4]. Considering the growth of technology, we should minimize security problems so that we can achieve maximum security growth through rapid development [13]. To identify weaknesses, it should be analyzed and examined, and we should be able to carry out this analysis automatically to achieve optimization of computational and security methods by reducing the instructions [14].

In the topic of IoT and ITIL security, management is vital and in fact acts as a bridge between processes and structure in order to achieve strategy. Since ITIL is a process-based reference model, one of the most important factors contributing to ITIL's success is proper process management [15]. In the first step, the status of processes and vulnerabilities is investigated and information about processes and vulnerabilities is analyzed in the second step. In defining statements, visions and missions, implementing ITIL processes in the third step, called situation analysis, is one of the important tasks of conducting case studies [16].The particular challenges we face in ITIL are about analysis [17]. The first step in determining structure is process design [18]. Focusing on processes before the selection, implementation, execution, support, modification and integration of processes is the consensus of most institutions [17]. Strategies for process improvement are organized in three phases: First: Determining the context, scope, and objectives of the process. Second: Understanding the existing process (workflow modeling) and Third: Designing the desired new process (evaluating and selecting improvements). In fact, the main technique is the solution to improve the modeling of doing the work [19].

The explicit objectives of processes are rarely regulated, evaluated, and methods of continuous improvement [20]. However, the issue of process security can simply indicate the conditions where the discovery of the answer or the correct solution can help to improve the current appropriate situation [21]. Given the most important issues mentioned above, the important issue is to ensure the security of the processes. There are also criteria for ensuring process security, and effective communication is established between the various parts of IoT and ITIL (providing manual models), which can be achieved by providing a framework (a combination of two frameworks).Paying attention to the role of management decisions in ensuring the security of processes and the realism of management programs considering security factors, resources and possible changes that will inevitably have devastating effects if not properly managed and implemented. Therefore, creating security (which is a process itself) is essential in all fields. As processes, nodes, and secure communications show, there were no defects within the system. A case study (situation analysis), taking into consideration the implementation motivations, the implementation benefits, the implementation status and the implementation results, along with focusing on the real issues of the processes, the right understanding of the definition of processes and determining the graph attacks at the security level, show the process of providing and evolving the final framework [2, 22-26].Since any action to improve the status of processes and their security needs to be changed, change management in this area is considered important [15]. Simple frameworks are more useful than complex ones. Meanwhile, the framework is the best practice in attempting to improve IT service management processes [17, 27]. The framework should be also built before it can is used, for a baseline, to evaluate any changes in them, as well as to ensure the continuous improvement of newly implemented processes and values [28].

This research first provides systematic and extensive research on the two factors of ITIL and IoT, and also analyzes two-stage and multiple relationships considering the importance of process security. Based on the analyses, it creates manual models that lay the groundwork for the simulated SPGR model with three security phases of general, private and release. This enables managers to make security decisions without incurring cost, risk and time and based on possible scenarios. The proposed framework is based on manual models and simulated models.

II. RESEARCH BACKGROUND:

In this section, first the background of research on IoT is investigated, then the background of research on ITIL is investigated, and finally, by referring to the background of both factors and analyzing the relationships and components, manual models that are the basis of the SPGR model are formed.

2.1. Background on IoT

It can be said that IoT is a system of physical and virtual objects, each of which is included in the capabilities of the network and are connected to exchange and collect information locally or remotely via the Internet. Because these connections are made via the Internet, they are typically vulnerable to security threats in the IoT environment [29]. In order to counter the many innovations in IoT for security, organizations provided the best security practices, which these settings are based on the law and based on the best security measures and simulated scenarios for security breaches and subsequently programming for countermeasures [30].IoT security requirements are part of the waves of IoT

innovation, and it can be said that the biggest security challenges in IoT are related to the relationships, interoperability and cooperation between the components and processes in IoT. With the development of IoT, security attacks are increasing day by day and consequently the number of identified mechanisms for IoT attacks is also growing [6]. Analysis is used to identify the threat of events and related planning is done according to the level of threat, and thus the structure and important actions are prioritized and reciprocal actions are performed and the appropriate plan is proposed for the security level and the degree of vulnerability of the system will be specified [9, 10, 29].In research on IoT security, communication elements have been used by providing a framework, and by using security risk analysis, sustainable control for IoT can be achieved. In these frameworks, they have used multiple scenarios to show the risks and they will lead to detecting attacks more quickly [6, 31-34]. Types of attacks are divided into active and inactive attacks according to the nature of the behavior.Active attacks include Routing attacks in sensor networks, DoS (denial-of-service), fabrication, lack of cooperation, modification, impersonation and eavesdropping, and inactive attacks include mintor and eavesdropping, traffic analysis and camouflaging adversaries. [35-39] (Types and number of attacks are used in calculating the probability of attack at the levels).

However, security analysis at different levels gives you the advantages and limitations of information systems. This means that security control is ensured by analyzing the system in a dynamic environment by changing security requirements, threats and vulnerabilities [31].

2.2. Background on ITIL

ITIL is for understanding the strategy and represents the institutional measures taken to provide technology services [40], also the structure and processes make a big difference in ensuring success [41]. Meanwhile, because of the study of the structure of processes, it should be known that the structure shows the relationship between the components, while services and processes describe how they change. In fact, the structure identifies the proper behavior required for service management.It also explains the relationship between processes, individuals, technology, and partners [16]. As organizations strive to better manage IT performance, providing an efficient framework is a solution, and the most important thing organizations expect from implementing ITIL is to balance current services with future possible needs [42], which plays a vital role in how ITIL is secured. Security management with a systematic approach in them is to create, implement, operate, monitor, review, maintain and improve security [43].The use of framework to improve performance is one of the important factors in research. Finally, strengthening ITIL process paths will lead to optimal decision making and process effectiveness [44, 45], which can help to take better measures about processes by drawing the relevant processes [22]. The ITIL framework is an important guide for changes in IT organizations. ITIL information processes include: strategy, service catalog management, knowledge management, incident management and request management [28].If there are changes, efforts are needed to improve the process. In fact, it continuously improves processes with fact-based information about performance, results, communication, and changes [46, 47].

III. RESEARCH METHODOLOGY

In this research, in order to provide a security framework for ITIL processes in the IoT environment, at first, extensive and systematic research in the fields of IoT and ITIL were studied. The connections, commonalities and requirements of both factors were identified. Initial information is obtained in three parts: free, university, and organizational, through monitoring and searching in research, universities, and organizations, as well as numerous journals and conferences. Then, the probability of an attack in each of the three phases that could have caused the immune system to malfunction was calculated, the equations were determined, and finally used in the SGPR model.This research is provided in three phases and four areas in research achievements with three parts: free, academic and organizational. Finally, relying on the analyses, manual and systematic models, the final framework is provided.

IV. FACTORS AND COMMONALITIES BETWEEN THE TWO FACTORS ITIL AND IOT

In order to be in line with the objectives of the research and provide a security framework, it is necessary to provide a clear analysis of factors and relationships. It is necessary to analyze and identify processes, their stimuli and factors and relationships that are needed to ensure security [48]. Each of the items mentioned in this section is one of the levels used in the overall Security-General-Private-Release (SGPR) model. According to the security framework provided by McNaughton et al. to support the processes, support management with five factors of incident management, problem management, change management, release management, and configuration management are the main components. Security management and transfer management are also the main factors of the framework [28].Since ITIL is a process-based reference model, one of the most important factors contributing to the success of ITIL is proper process management [17, 43]. The principles of process management include process awareness, process ownership, process measurement and process improvement [15]. In order to provide a security framework, we specify the security system requirements and security levels, and then review and describe the components, mechanisms, and vulnerabilities of the system, provide a model for design and implementation, and finally establish a security framework [20].

Security systems include access control systems, antiviruses and firewalls, which include creating a secure environment through multiple analyses, continuous management for the security of security systems [5]. Five phases are suggested for preparing the IoT security framework: data processing (process creation), security model processing, security virtualization, security analysis, model updating [2]. In this research, the first step of the security decision maker mainly provides the required inputs (system security and information criteria) to build the IoT network. In the second phase, topology and vulnerability information is taken as input, and possible paths in the IoT network are identified. In the third step, the attack graphs and attack paths are specified. In the next step, the analysis and determination of equations and the probability of the occurrence of attacks are determined, and in the fifth step, modeling is carried out.

The issues raised in this section are used to calculate the probability of an attack in each of the areas and phases, which ultimately leads to the modeling of processes in the simulation system. Process modeling provides a precise functional basis that enables us to modify and improve at various stages, adjust and regulate. It can also be said that showing the main workflow model provides the best framework for identifying the main issue [49]. Further investigation reveals the security gap between the IoT and ITIL factors. Implementing ITIL is a complicated process and requires difficult and complex decisions [44]. A) What changes in strategic management processes and settings to improve processing results, behavior, and performance?

B) Does determining the process structure to optimize the results and process of the organization help with better decisions of managers [50-52]? In fact, at this stage the question is: should managers choose a framework or use a combination of frameworks as needed [28]? Preventive change management can turn a failure into a success. It should be noted that change management has a direct effect on security [53]. Meanwhile, in process reengineering, sufficient attention should be paid to subprocesses, as they create process areas and process areas act as a function [19].

V. THE PROCESS OF ACHIEVING THE FINAL FRAMEWORK:

It is important to understand that the integration of processes in any of the components without considering the human in pragmatic relationships may jeopardize ITIL [45]. Therefore, considering taking the right steps in implementing ITIL will definitely play a significant role in stabilizing security. It is important to note that in defining statements and visions and missions, implementing ITIL processes in the third step, called situation analysis, is one of the important tasks of conducting case studies [16]. To conduct the case study, we use the simulation model due to many important cases.The simulation model is usually used effectively and extensively because of its ability to evaluate changes and new processes in an environment by creating scenarios [54]. The security situation is investigated in two parts: vulnerabilities and processes, which are basically the input of the analysis. In investigating the security levels of the mentioned cases, by determining the status of the processes, the attack graphs can also be identified and examined. Using attack graph is one of the effective ways for IoT security issues [2, 23]. In several researches, simulation model has been used to present security models and analyses [2, 13, 51, 55-57].

VI. SECURITY ANALYSIS MODULES

As mentioned in the previous sections, each of the areas and phases are under potential influence of attacks, and these attacks are as graphs. The attack graph is presented as subgraphs and sections in various phases. Also, to provide the security framework of the processes, four security areas can be considered: 1. General attacks and its effect on levels and layers (Area A). 2. Relationships between factors between IoT and ITIL and process security (Layer B). 3. Process content (Area C). 4. Private modules (under the influence of case study in position analysis) (Area D).These effects will be completely presented in the simulation section as well as the level of effects after the changes. We consider the whole set of AP attack paths in the graph. ap∈ has one or more vulnerabilities for a specific purpose from the AP level. Any process that is a subset of processes. p ∈P, Therefore:

∈Agt,P∈AP, Apap∈{Gat ،ITIL ،IOT ،Ps ،Cs ،Pco}

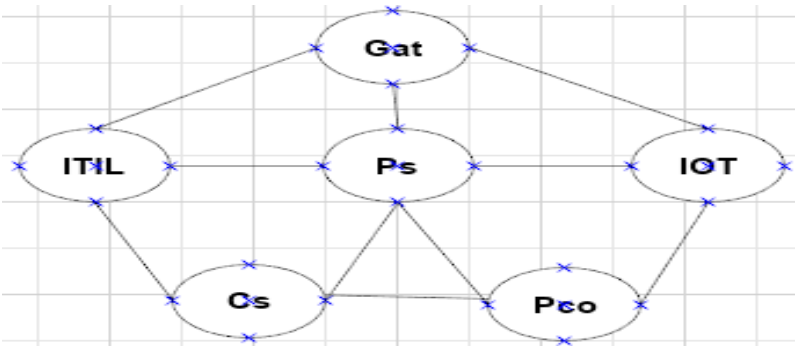


Figure 1: Attack Graph (Atg)

The structure defines how the variables interact if the content includes the meaning and concept of the variables [11]. In ITIL4, four factors of cost, time, risk and results are the most important and determining factors [58], also latencies are factors that affect dynamic and feedback systems. In addition to paying attention to the content of the concept of variables, special attention should be paid to the relationship between variables, i.e. structure. The numbers next to each indicate the number of branches and possible levels for the attack to occur. Table 1 lists the elements and the symbols used.In addition, Figure 2 shows the number of branches and levels in which there is a probability of attack. This probability of attack will affect the flows, levels and parameters. It is also used in equations. It should be noted that the probability of attack in each of the branches is [1 and 0].

Table 1. Introduction of the used elements and symbols

Elements	Symbol	Symbol	Symbol (free, university, organizational)
General attacks	Gat	Inactive attacks	Iat
Active attacks	Aat	IOT Security	IOTs
Security system	Ss	Security management	Sm
Security phases	Sph	Total security	Ts
ITILSecurity	ITILs	Process content	Pco
Process management	Pm	Case study attack rates	Cs)r (
Support management	Spm	IOT content	IOTc
Transfer management	Tm	ITIL content	ITILc
Case study	Cs	Process security	Ps
Free research	Fre	Rate of each of the items used (*)	(*)r
University research	Ure	Case study time	Cst
Organizational research	Ore	Research time	Ret
Research	Re	Total research	Tre
Release cost	Rec	Attack graph	Atg
Total process	Tp	Processes	P

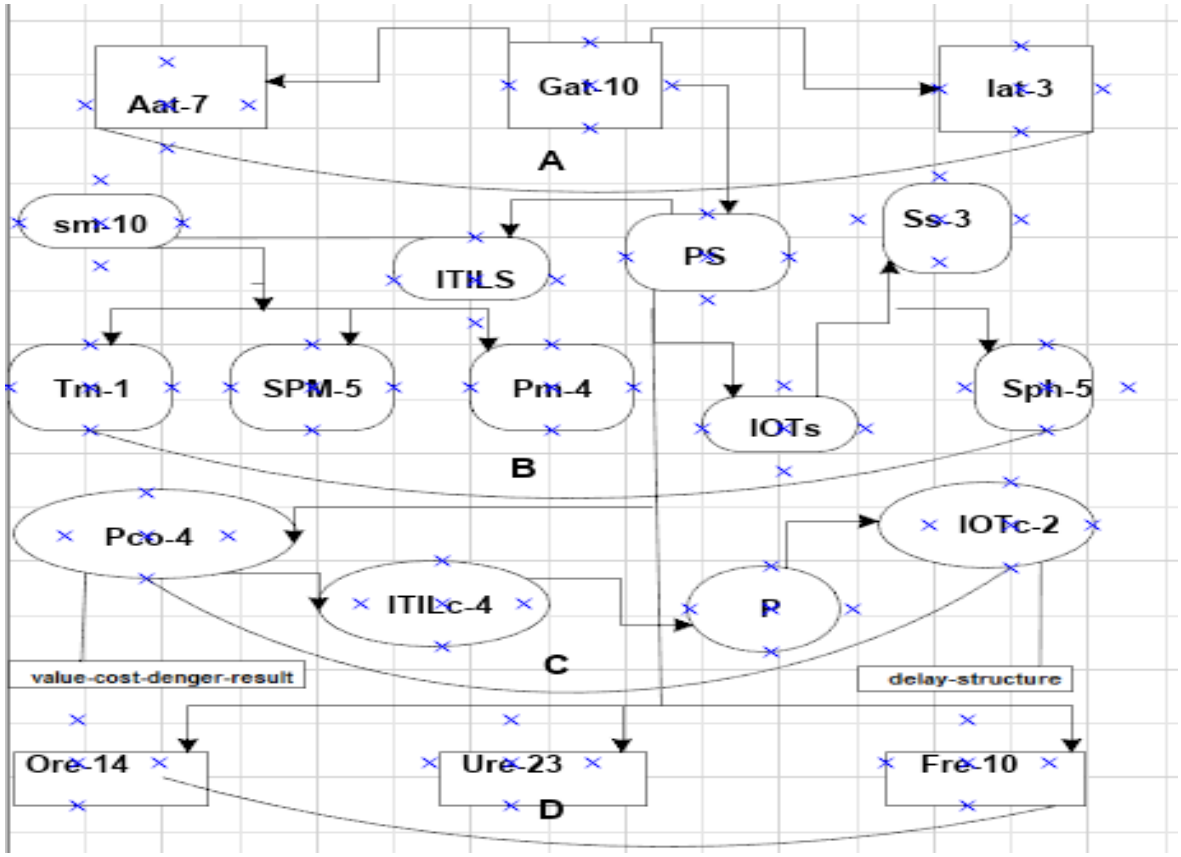


Figure 2. Manual model of how the items affecting the modules are related

6.1. General security module:

The general security module including the structure, attacks, and, as shown in Figure 2, are specified in the processes section and in Area C.

In general, any process that is a subset of processes. p ∈P and AP is the attack path specified in the attack graph,therefore:

$$ap \in AP, AP \in Atg,\ P_{IOTs} \in \{Re,(Ss,Sph),IOTsr\}$$

$$1.\ IOTs = (Re) \cap (Ss, Sph) \cap (IOTsr)$$

$$ap \in AP, AP \in Atg,\ P_{ITILs} \in \{P,(Tm,Spm,Pm),ITILsr\}$$

$$2.\ ITILs = (\cap P)(Tm, Spm, Pm) \cap (ITILsr)$$

$$ap \in Ap, AP \in Atg, P_{Cs} \in \{Pco,(Cst,(Fre,Ure,Ore),Csc,Csr)\}$$

$$3.\ Cs=(Pco) \cap (Cst) \cap (Fre,Ure,Ore) \cap (Csr) \cap (Csc)$$

$$ap \in AP, AP \in Atg, P_{Pco} \in \{Ps, (ITILc,IOTc), Pcor\}$$

$$4.\ Pco=(Ps) \cap (IOTc,ITILc) \cap (Pcor)$$

$$ap \in AP, AP \in Atg, P_{Ps} \in \{Gat,(IOTs,ITILs), Psr\}$$

$$5.\ Ps=(Gat) \cap (IOTs,ITILs) \cap (Psr)$$

$$ap \in AP, AP \in Atg, P_{Gat} \in \{(Aat,Iat),Gatr\}$$

6. Gat=(Aat,Iat)∩(Gatr)

ap∈AP, AP∈ Atg, P_{Ts}∈{Cs, IOTs, ITILs,Jo,Co,Ret}

7. Ts =(Cs)∩ (IOTs)∩ (ITILs) ∩(Jo, Co)∩(Ret)

Each of the above relations shows the attack paths leading to the given level. Each level is in the security area and the relevant phase, which ultimately needs to be identified to provide the ultimate security.

6.2. Private security module:

In this module, we investigate and study in situation analysis (case study) in three parts:

1. Free part: includes personal system (security of equipment, security of roles and security of processes), topic selection (approval of beneficiaries), research design (definition of project, approval of beneficiaries), problem statement, research objectives, importance and necessity of research and article (research achievements). The number of levels at which an attack is likely to occur is considered to be 10.

2. University part: University system (security of equipment, security of roles and security of processes, topic selection (selection of student and approval of the supervisor), research design (project definition, application request, approval of the application, approval of the supervisor, approval of the jury And consultant approval), problem statement, research objectives, research importance and necessity, proposal approval (approval of application, approval of the jury, approval of the postgraduate council and approval of the research council), defense (professors, referees and students), dissertation and article (research achievements). The number of levels at which an attack is likely to occur is considered to be 23.

3. Organizational part: organizational system (security of equipment, security of roles and security of processes), topic selection (organizational selection and organizational approval), research design (presentation to design and plan, plan in research working group, priority of research plan, planning and development council and announcing the invitation in the time interval), problem statement, research objectives, importance and necessity of research and article (research achievements). The number of levels at which an attack is likely to occur is considered to be 14.

In the above three parts, the probability of an attack in each of the stages will be calculated in general.

6.3. Release security module:

In each part of the case study, including free, university and organizational, a conference is selected according to the compatibility of personal, university or organizational policies. Depending on the type of decision making, research achievements may be presented in journals, conferences, or executive systems. The maximum level review for the journal is considered to be 24 levels in which an attack may occur. From adapting the beneficiary criteria to the journal to the article being in the queue for publishing (depends on the journal and can be easily changed in the variable change section). Investigating the maximum levels in the conference in presenting the research achievements from adapting the conference to the beneficiary criteria to the publication of the article is considered to be 8 levels.Also, publishing the article in the executive systems, because the relevant organization is responsible for publishing these achievements, therefore, security approval is provided based on specific organizational policies and it is not necessary to provide security levels in the publication stage in this section. It should be noted that each of the processes and subprocesses with operators can be defined as a regular relation and can form an algebraic relation. In the SGPR model, if we consider PSGPR as a set of processes, then aligned processes, process sequences, process changeability, neutral member in processes, participation, cycle operator, and process option are true.

VII. SIMULATION STEPS:

The steps for simulation of dynamic systems for case study are done in four parts:

- Determining equations
- Determining the probability of occurrence of each level (accumulations) and flow rates
- Specifying levels and flow rates
- Providing dynamic system modeling

7.1. Equations

If system dynamics are used to simulate a system, identifying the nature of rate equations is crucial. Since the level or storage equations necessarily strengthen the laws of survival, they can be deduced directly from the storage (levels) and flow diagrams [11]. The method of calculating the flow rates affecting the levels (accumulations) based on Table 1 and Figure 2 and also according to their effects in the SGPR model is as follows:

1. (Gat)r=Aat*Iat
2. (ITIL)sr=Pm*Spm*Tm*P*Gatr/Tp
3. (IOT)sr=Sph*Ss*Re*Gatr/TRE
4. (Ps)r=IOTs*ITILs*Gat
5. (Pco)r=ITILc*IOTc*Ps
6. (Cs)r=Fre*Ure*Ore*Cst*Csc*Pco
7. (Ts)r=IOTs*ITILs*Jo*Co*Ret*Rec*Cs

7.2. Determining the probabilities of occurrence of each level and flow rate:

The SGPR model is supposed to determine the degree of effect of attack probability on levels and flows, and then some values of the effect of attack probability are changed using the Anylogic cloud and the relevant analysis will be carried out.

According to Table 1 and Figure 2, the descriptions of the journal and conference levels, as well as the branches associated with them and the probability of an attack occurring in each of them, are:

1. P(Ts)=10p(Gat)+18p(Lat)+10p(ITILs)+8p(IOTs)+6p(Pco)+47p(Cs)=1

2. P(Gat)=3p(Iat)+7p(Aat)=1

P(Iat)=3/10 P(Aat)=7/10

3.P(Ps)=10P(ITILs)+8P(IOTs)=1

P(ITILs)=10/18 P(IOTs)=8/18

4. P(ITILs)=P(Sm)=p(Tm)+5p(Spm)+4p(Pm)=1

P(Tm)=1/10 P(Spm)=5/10 P(Pm)=4/10

5. P(IOTs)=5p(Sph)+3p(Ss)=1

P(Sph)=5/8 P(Ss)=3/8

6. P(Pco)=2p(IOTc)+4p(ITILc)=1

P(IOTc)=2/6 P(ITILc)=4/6

7. P(Cs)=10p(Fre)+23(Ure)+14(Ore)=1

P(Fre)=10/47 P(Ure)=23/47 P(Ore)=14/47

8. P(Co)=1/8 Co=0.125 P(Jo)=1/24 Jo=0.041

Also, the probability of attack in each subsection, including the free, university and organizational parts, was calculated according to the descriptions of the research procedure and the probability of attack in each of them. This calculation for the probability of occurrence by calculating the attack in each of the cases announced in the subsections was calculated according to the descriptions related to the private part and the probability of the occurrence of an attack in each of them with details in subsections and subsections can only be ignored and was estimated to be almost zero. Therefore, it was considered in general and due to the fact that research is conducted in dynamic systems and has less involvement with details.so we just address the possibility of an attack in general. According to the above explanations, the value of probability of attack on each of the levels and parameters was given in the table. Description of the table below: The time of publication of the case study is 6 months and the case study is 24 months. The cost of the case study is $ 1,500 and the cost of publication of research achievements is $ 600. Also, the number of researches is 10,000 and the number of processes is 20,000, which can be changed in the parameters change section.

Table 2. Parameters and values considered in the SGPR model

Ss=0.37	Tm=0.1	Spm=0.5
Pm=0.4	Sph=0.625	Fre=0.297
Ure=0.489	Ore=0.21	Aat=0.7
Iat=0.3	Jo=0.041	Co=0.125
Ret=6	Tp=20000	Cst=24
Csc=1500	Rec=600	ITILc=0.66
IOTc=0.33	TRE=10000	

The values in the above table are adjusted taking into consideration the probability of attacks and are used in the values of parameters, equations and flow rates in the SGPR model.

7.3. Determining levels, flow rates and parameters:

Effective values are titles that are denoted by the word "rate" and are used as effective flows in the model. Levels are things that are affected by flows, although in some cases flows may be affected by levels. Parameters are also factors that affect the flow rate and are obtained by calculating the probability of an attack.

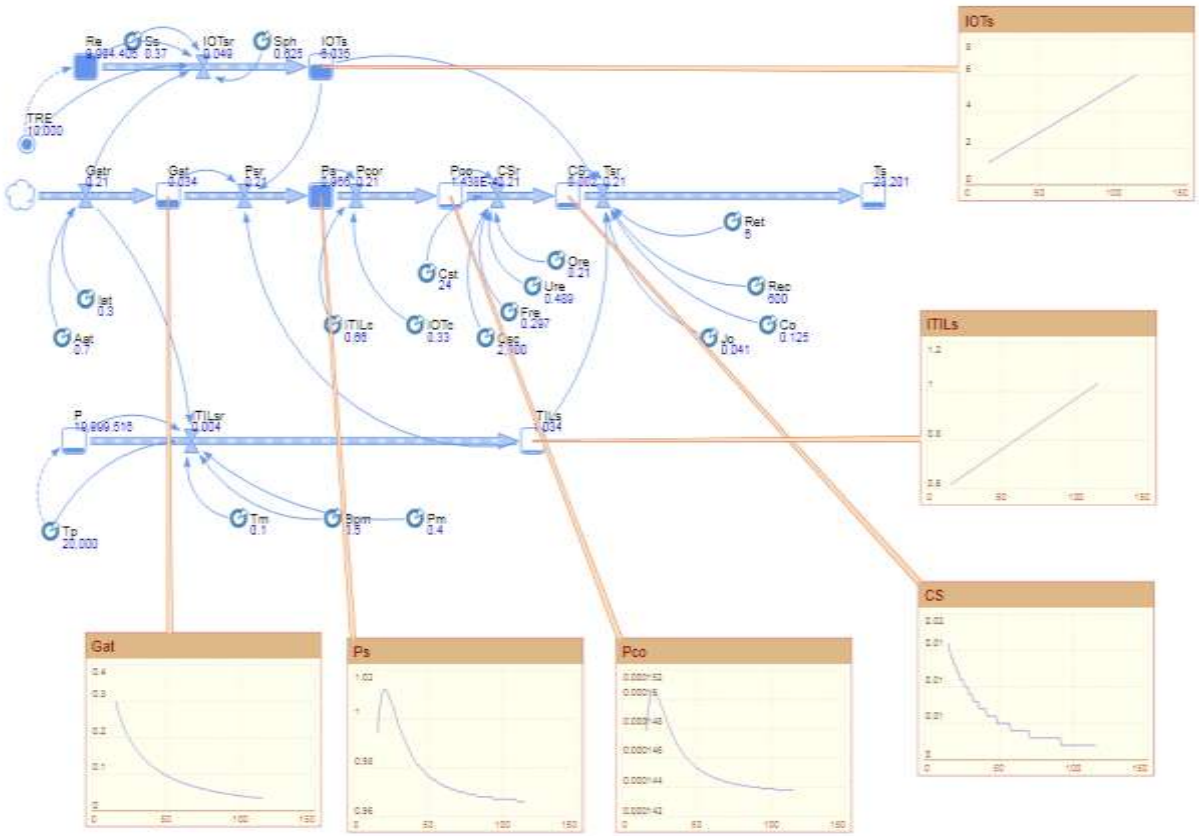
Levels, flows and parameters in the general SGPR model are identified and distinguished by the following names:

1. Levels (accumulations) with names: Re, IOTs, Gat, Ps, Pco, Cs, Ts, P and ITILs.
2. Flows with names: IOTsr, Gat, Psr, Pcor, Csr, Tsr, ITILsr.
3. Parameters with names: TRE, Ss, Sph, Aat, Iat, ITILc, IOTc, Cst, Fre, Ure, Ore, Jo, Co, Ret, Tp, Pm, Spm, Tm, Rec, Cst.

Each level may be affected by flows and each flow may be affected by levels. Meanwhile, flows and levels may also be affected by parameters.

7.4. Modeling of dynamic systems

The steps considered for the security model are the probability of attacks occurring in general, private, release and security evaluation modules, respectively. The overall model name is SGPR. In the general security phase, the effect of general attacks and the effect of various factors and parameters on Ps, IOTs, ITILs and Pco are investigated. In the private security phase, the status of the case study was examined and the probability of attacks in each of the subsections was investigated with related factors that the probability of attacks details was estimated to be almost zero. Therefore, in general, the calculation and its effect in the private security phase, including general attacks, time and cost on the case study are measured and investigated. In the release security phase, the probability of attacks at the journal and conference levels with the time and cost of release as well as general attacks are investigated.



شکل شماره 3 اجرای مدل ابتدایی شبیهسازی

Figure 3. Implementation of the primary simulation model

First, we define the factors, parameters, levels and flows in the primary model (Figure 3). Using the equations and relations obtained in the previous sections, we adjust the model. By bypassing the loop in the primary simulation system, we realize the need for the loop due to the inconsistency with the initial assumption as seen in Cs (case study), as the security of the processes increases, the security in them decreases, therefore, we use a balancing feedback loop. Number of unweighted negative links in Cs (case study). By reducing Gat (general attacks) the security of the processes increases so we need an amplifier loop. We use an amplifier loop.We put the amplifier loop in Psr (process security rate) and then run the model. Then we add the time palette with the factors that we specify. Then we run the model. Figure 4 shows the execution of the model after adding the loops. In fact, in the simulation test, one can answer questions such as what if?

As shown in Figure 4, IOTs increase over time, and also ITILs increase over time, although to a lesser extent. In the case of Gat, which our goal is to reduce its value, it decreases and approaches zero. In the case of attacks in Pco, the value is very low and remains almost constant during execution. Ps increases, then continues a steady path, and Cs remains at about the same calculated value and increases slightly. Overall, the increase in IoTs and ITILs gives us an acceptable and expected range, and ultimately increases total security.

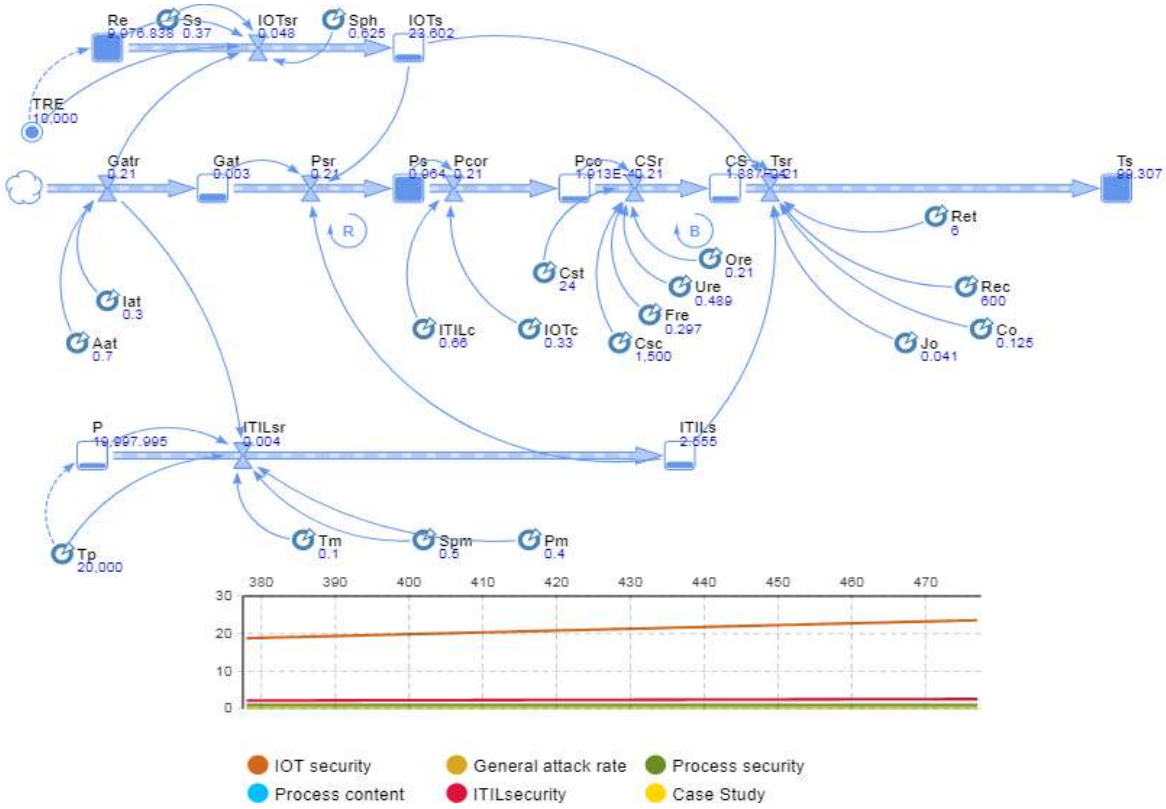


Figure 4. Execution of the SGPR model

7.4.1. Parameter change test:

In this step, we will test how the parameters change that how it affects various levels, this is possible using the Anylogic Cloud. We specify inputs and outputs for the time palette. We run the simulation model in this environment, it must be exactly what we received after the execution. Then in this environment in various steps by changing the range of parameters, its effect on other levels can be observed.

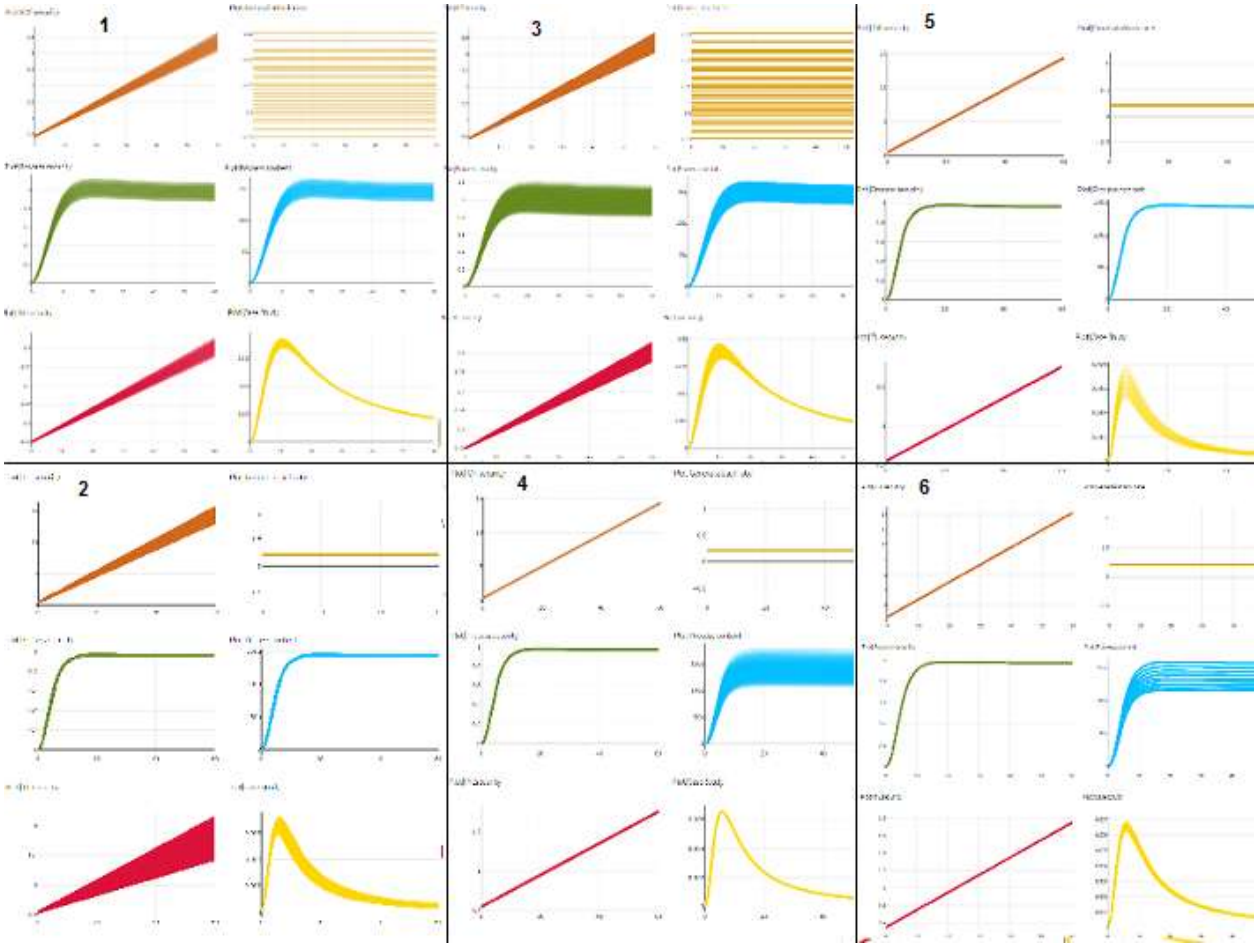


Figure 5. Changing the range of parameters in 6 steps

- Changing the range of parameters in the general phase: Changing the range of parameters in the general phase is done in three steps. First we change the range of the two parameters Aat and Iat ¬ (Figure 5, Part 1). Changing the range of these two parameters affects all levels, and by changing the value of active and inactive attacks, the change and effect on other levels becomes obvious (these changes are made in Area A). In the next step, we test the change in the parameters of IOTs and ITILs. This change of parameters affects IOTs, ITILs and Cs and causes changes in their diagrams (Figure 5, Part 2).Other levels remain almost unchanged (these changes take place in Area B). Then we change the range of Gatr and Pcor parameters in this phase (Figure 5, Part 3). This effect of changes occurs at all levels (these changes occur in security areas A and C).
- Changing the range of parameters in the private phase: In this phase, we change the range of the five parameters Csc, Cst, Fre, Ure and Ore (these changes are done in Areas C and D). The effect of the changes in Pco is clearly visible, and the rest of the change diagram remains almost unchanged at levels (Figure 5, Part 4).
- Changing the range of parameters in the release phase: In this phase, we change the range of the four parameters Rec, Ret, Jo and Co (these changes are done in Areas C and D). The effect of these changes in Cs is clearly visible and the rest of the levels remain almost unchanged (Figure 5, Part 5).
- Changing the range of time and cost parameters: In this step, due to the importance of these two parameters, both are investigated separately (these changes occur in Area C). We investigate the effect of changing the four parameters Cst, Csc, Ret, Rec on other levels. This effect of changes in Pco is visible and almost all other levels remain unchanged (Figure 5, Part 6).

7.4.2. Calibration test

Then, a calibration test was performed to confirm the matching of the parameters with the output values and the fit with the data. The calibration test was performed in four stages: general, private, release, and time and cost (Figure 6). A database is created before calibration and the results are stored in it after each simulation. This software optimization uses analysis tools and uses several objective functions such as

maximization and minimization and scatter search to find the best scenario.Five parameters of the general phase Ss, Sph, Tm, Pm and Spm, three parameters of the private phase Fre, Ure and Ore and two parameters of the release phase Jo and Ret, Rec, Cst and Csc were calibrated in the time and cost section in four stages. After the calibration test, the best option in the test is displayed that we can replace.

The best options in the general phase (Part 1 of Figure 6):

Ss=0.4Tm=0.1Spm=0.1Pm=0.42Sph=0.52

The best options in the private phase (Part 2 of Figure 6):

Fre=0.35 Ure=0.5 Ore=0.23

The best options in the release phase (Part 3 of Figure 6):

Jo=0.043Co=0.15

After performing the test in this step, we calibrated two time parameters along with the above two items:

Ret=6.2Cst=26

The best options in time and cost (Part 4 of Figure 6):

Ret=6.2Cst=30Csc=2002Rec=602

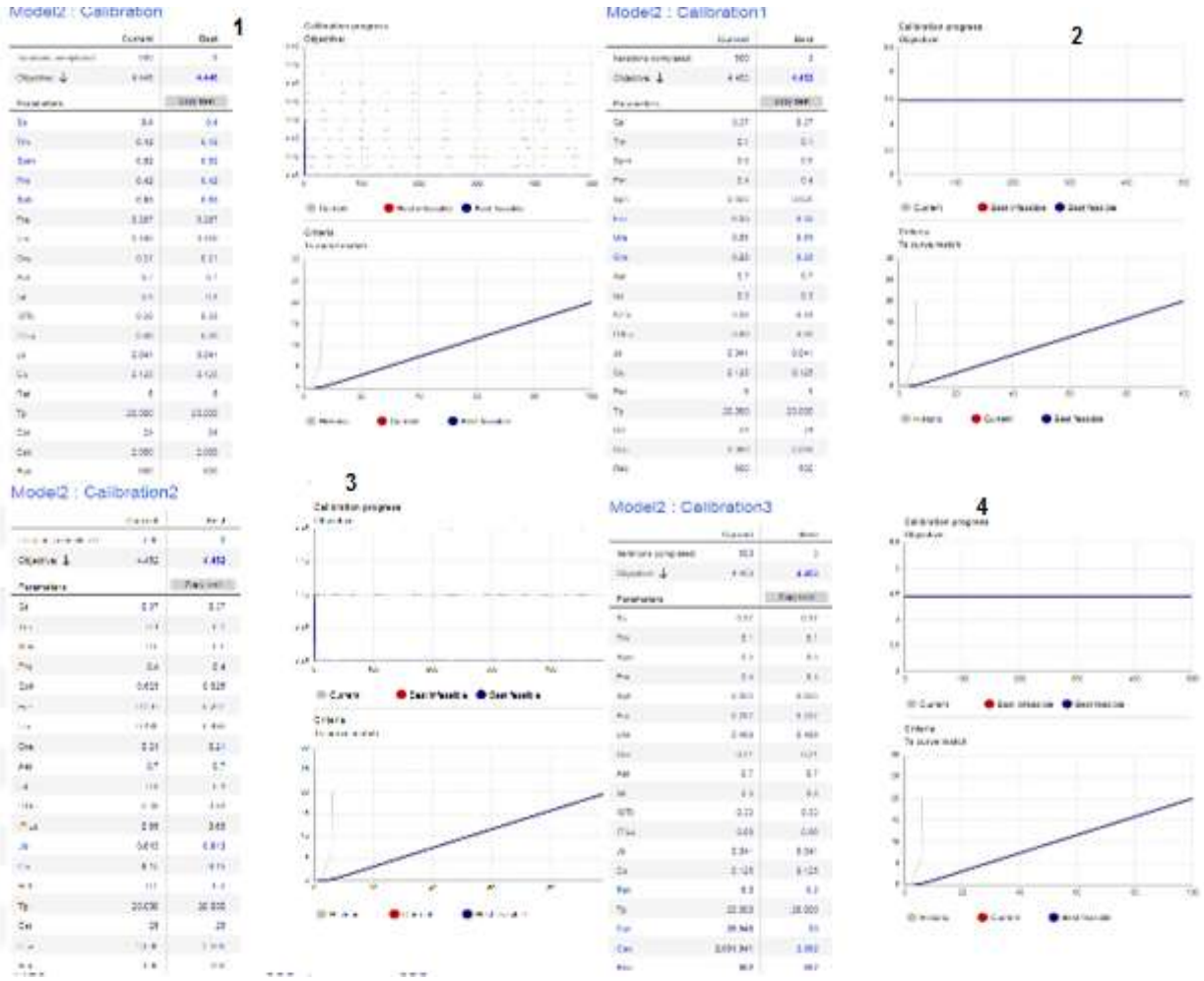


Figure 6. Calibration test in 4 stages

VIII. CONCLUSION AND FUTURE WORKS

The present research evolved in three stages. The first stage was to investigate and analyze the foundations of the two factors IoT and ITIL and combine related research to find a manual model based

on which we can make subsequent relations. It also detects attacks that may affect the two factors. The second step is the evolution of manual models and the presentation of relations for the SGPR model processes with operators, communications, and links. Finally, three phases and four security areas were proposed for security. The third stage was to determine the equations, the probability of attack on the surfaces and flow rates, to create the simulation model and calibration.It was determined how the security areas affect each other and also how the parameters affect the levels and flow rates in the three security phases of general, private and release were identified and distinguished. Also, how to change the range of different parameters in various phases on different types of levels and how it affects the levels and areas were determined.

Recommendations from the present study for security:

- Paying attention to the probability of general attacks at all levels, flows, factors, communications.
- Prioritizingthe addressing of public attacks in the form of different categorizations and classifications, considering the security challenges related to IoT that may occur if security is improved by insecurity and security analysis around it.
- Pay attention to the security systems and the proposed phases according to what was presented in detail.
- Having holistic view in creating strategy security at different levels and avoiding meticulous view.
- Optimal investment in time and cost based on the best option to increase the content of the processes and improve the case study.
- Programs that provide security and program management should be aware of the functional aspects of the various programs, which include probabilities and limitations.
- Considering process security as a cycle, not a step.
- Providing an updated version according to possible changes in agents, factors, relations and finally manual and systematic models.
- In case of combining IoT and ITIL factors, one should pay attention to the commonalities of both factors and pay attention to the commonalities according to the proposed cases. Also one should pay attention to the existing security gaps between IoT and ITIL factors and the processes that are supposed to be secured.
- Lack of investment in creating unnecessary levels due to the small number of attack events at the mentioned levels (approximately equal to zero).

Researcher's recommendations:

1. Changing the security approach in case of need to change according to the existing conditions without following the existing instructions.
2. Experimental implementation of various security cases and subsequent identification of cases, factors, agents and relations that disrupt security.
3. Correct and accurate implementation of security cases after testing security frameworks.
4. Laying the groundwork for security in case of interference and the presence of factors such as IoT and ITIL.

- Recommendations for future researchers:
- Separating case studies in each specific case and investigating the details with a different perspective other than a strategic one.
- Investigating various human and inhuman roles in presenting research achievements and using appropriate simulations to help us in conducting research.
- More detailed and in-depth study of economic and time issues in providing security and presenting research achievements.
- Conducting research on the matching of security programs in case studies with existing security programs and policies.

REFERENCES

1. Roman, R., J. Zhou, and J. Lopez, *On the features and challenges of security and privacy in distributed internet of things.* Computer Networks, 2013. **57**(10): p. 2266-2279.
2. Ge, M., et al., *A framework for automating security analysis of the internet of things.* Journal of Network and Computer Applications, 2017. **83**: p. 12-27.
3. Sicari, S., et al., *Security, privacy and trust in Internet of Things: The road ahead.* Computer Networks, 2015. **76**: p. 146-164.

4. Sfar, A.R., et al., *A roadmap for security challenges in the Internet of Things.* Digital Communications and Networks, 2018. **4**(2): p. 118-137.
5. Hong, S. and e. al, *An analysis of security systems for electronic information for establishing secure internet of things environments: Focusing on research trends in the security field in South Korea.* Future Generation Computer Systems, 2018. **82**: p. 769-782.
6. Rathore, S. and J.H. Park, *Semi-supervised learning based distributed attack detection framework for IoT.* Applied Soft Computing, 2018. **72**: p. 79-8.9
7. Han, K.H., Kang, J. G., & Song, M., *Two-stage process analysis using the process-based performance measurement framework and business process simulation.* Expert Systems with Applications,, 2009. **36(3), 7080-7086**.
8. French, w. and c. Bell, *Organization development : behavioral science interventions for organization improvement*1923: Englewood Cliffs, N.J. : Prentice Hall, c1995., Saffarpublishing.
9. Yiğit, B., et al., *Cost-aware securing of IoT systems using attack graphs.* Ad Hoc Networks, 2019. **86** : p. 23-35.
10. Roy, A., D.S. Kim, and K.S. Trivedi, *Attack countermeasure trees (ACT): towards unifying the constructs of attack and defense trees.* Security and communication networks, 2012. **5**(8): p. 929-943.
11. pidd, M., *Computer simulation in management science and industrial engineering*, ed. 42016: Wiley; sharif.
12. White, G., V. Nallur, and S. Clarke, *Quality of service approaches in IoT: A systematic mapping.* Journal of Systems and Software, 2017. **132**: p. 186-203.
13. Stergiou, C., et al., *Secure integration of IoT and cloud computing.* Future Generation Computer Systems, 2018. **78**: p. 964-975.
14. Lee, Y., J. Jeong, and Y. Son, *Design and implementation of the secure compiler and virtual machine for developing secure IoT services.* Future GenerationComputer Systems, 2017. **76**: p. 350-357.
15. Orta, E. and M. Ruiz, *Met4ITIL: A process management and simulation-based method for implementing ITIL.* Computer Standards & Interfaces, 2019. **61**: p. 1-19.
16. CANNON.D, *ITIL SERVICE STRATEGY*2011, UNIVERSITY TEHRAN Publishers.
17. Pollard, C. and A. Cater-Steel, *Justifications, strategies, and critical success factors in successful ITIL implementations in US and Australian companies: an exploratory study.* Information systems management, 2009. **26**(2): p. 164-175.
18. Bon, J.v., *ITIL V3 - A Pocket Guide (Best Practice) Kindle Edition*2007: Van Haren Publishing.
19. Alec, S. and P. McDermott, *Workflow Modeling: Tools for Process Improvement and Applications Development*2009: Artech House.
20. Iden, J., *Investigating process management in firms with quality systems: a multi-case study.* Business Process Management Journal,, 2012. **18(1), 104-121**.
21. Khaki, G., *Research methodology with dissertational approach*2005: Baztab publishing.
.22. Irani, Z., et al., *Technology adoption model and a road map to successful implementation of ITIL.* Journal of Enterprise Information Management, 2013.
23. Saini, V., Q. Duan, and V. Paruchuri, *Threat modeling using attack trees.* Journal of Computing Sciences in Colleges, 2008. **23**(4): p.131-124 .
24. Bayona, S., Y. Baca, and G. Vela. *IT service management using ITIL v3: A case study*. in *2017 12th Iberian Conference on Information Systems and Technologies (CISTI)*. 2017. IEEE.
25. Sheyner, O., et al. *Automated generation and analysis of attack graphs*. in *Proceedings 2002 IEEE Symposium on Security and Privacy*. 2002. IEEE.
26. Ingols, K., et al. *Modeling modern network attacks and countermeasures using attack graphs*. in *2009 Annual Computer Security Applications Conference*. 2009. IEEE.
27. Cumings.S . , *ReCreating Strategy*2002: Yadvareh Publishers.
28. McNaughton, B., P. Ray, and L. Lewis, *Designing an evaluation framework for IT service management.* Information & Management, 2010. **47**(4): p. 219-225.
29. Das, A.K., S. Zeadally, and D. He, *Taxonomy and analysis of security protocols for Internet of Things.* Future Generation Computer Systems, 2018. **89**: p. 110-125.
30. Mohsin, M., et al., *IoTChecker: A data-driven framework for security analytics of Internet of Things configurations.* Computers&Security, 2017. **70**: p. 199-223.
31. Mavropoulos, O., et al., *Apparatus: A framework for security analysis in internet of things systems.* Ad Hoc Networks, 2019. **92**: p. 101743.
32. Huang, X., et al., *SecIoT: a security framework for the Internet of Things*.Security and communication networks, 2016. **9**(16): p. 3083-3094.

33. Hossain, M., et al., *An Internet of Things-based health prescription assistant and its security system design.* Future Generation Computer Systems, 2018. **82**: p. 422-439.
34. Sun, P., etal., *Modeling and clustering attacker activities in IoT through machine learning techniques.* Information Sciences, 2019. **479**: p. 456-471.
35. Padmavathi, D.G. and M. Shanmugapriya, *A survey of attacks, security mechanisms and challenges in wireless sensornetworks.* arXiv preprint arXiv:0909.0576, 2009.
36. Mitrokotsa, A., M.R. Rieback, and A.S. Tanenbaum, *Classification of RFID attacks.* Gen, 2010. **15693**: p. 14443.
37. Douceur, J.R. *The sybil attack*. in *International workshop on peer-to-peer systems*. 2002 .Springer.
38. Muhammad, M.F., W. Anjum, and K.S. Mazhar, *A Critical Analysis on the Security Concerns of Internet of Things (IoT).* International Journal of Computer Applications (0975 8887), 2015. **111**(7.(
39. Thakur, B.S. and S. Chaudhary, *Content sniffing attack detection in client and server side: A survey.* International Journal of Advanced Computer Research, 2013. **3**(2): p. 7.
40. Shrestha, A., et al., *Development and evaluation of a software-mediated process assessment method for IT service management*.Information & Management, 2020. **57**(4): p. 103213.
41. Castillo, F., *Managing Information Technology*. illustrated ed2016: Springer.
42. Peak, D., C.S. Guynes, and V. Kroon, *Information technology alignment planning—A case study.* Information & Management :(5)42 .2005 ,p. 635-649.
43. Haufe, K., et al., *A process framework for information security management.* 2016.
44. Orta, E., Ruiz, M., Hurtado, N., & Gawn, D., *Decision-making in IT service management: a simulation based approach.* . Decision Support Systems, 2014. **66, 36-51**.
45. Mohamed, M.S., et al., *The re-structuring of the information technology infrastructure library (ITIL) implementation using knowledge management framework.* VINE, 2008. **38**(3): p. 315-333.
46. Davenport, T.H. and M.C. Beers, *Managing information about processes.* Journal of Management Information Systems, 1995. **12**(1): p. 57-80.
47. Harrington, H.J., *Business process improvement: The breakthrough strategy for total quality, productivity, and competitiveness*1991: McGraw Hill Professional.
48. Rezaaian, A., *Fundamentals Organization and management*2015: Samt.
49. ZARANDI.MH., E.A., *Enterprise modeling: principles & applications*2012: Amirkabir university of Tehran.
50. Kellner, M.I., R.J. Madachy, and D.M. Raffo, *Software process simulation modeling: why? what? how?* Journal of Systems and Software, 1999. **46**(2-3): p. 91-105.
51. Krebs, R., Momm, C., & Kounev, S, *Metrics and techniques for quantifying performance isolation in cloud environments.* . Science of Computer Programming, 2014. **90**.134-116 ,
52. Edgington, T.M., Raghu, T. S., & Vinze, A. S, *Using process mining to identify coordination patterns in IT service management.* Decision Support Systems, 2010. **49(2), 175-186**.
53. Jeffrey Hiatt and T. Creasey, *Change Management: The People Side of Change* 2013: Prosci Learning Center Publications.
54. Fiedler, F.E., *A contingency model of leadership effectiveness.* New York: Academic Press, 1964.
55. Jiang, H., et al., *A secure and scalable storage system for aggregate data in IoT.* Future Generation Computer Systems, 2015. **49**: p. 133-141.
56. Wang, K.-H., et al., *A secure authentication scheme for Internet of Things.* Pervasive and Mobile Computing, 2017. **42**: p. 15-26.
57. Anderson, J. and L. Rainie, *The internet of things will thrive by 2025, PewResearch Internet Project*, 2014.
58. Axelos, *ITIL4 foundation*2019: Axelos.