IJICTR
International Journal of Information & Communication Technology Research

Volume 15- Number 3 – 2023 (21 -30)

Impact Assessment for Cyber Security Situation Awareness

Sina FarahaniNia
Department of Computer Engineering
Amirkabir University of Technology
Tehran, Iran
sfarahani85@aut.ac.ir

Motahareh Dehghan*
Department of Industrial and Systems Engineering
Tarbiat Modares University
Tehran, Iran
m_dehghan@modares.ac.ir

Babak Sadeghiyan
Department of Computer Engineering
Amirkabir University of Technology
Tehran, Iran
basadegh@aut.ac.ir

Salman Niksefat
APA Research Center
Amirkabir University of Technology
Tehran, Iran
niksefat@aut.ac.ir

Received: 5 May 2023 – Revised: 25 August 2023 - Accepted: 2 September 2023

Abstract— **Cyber security situation awareness is important for the analysis of cyberspace, and detection of ever-changing threats. As computer networks and systems continue to increase in complexity and sophistication, the requirements and on a cybersecurity operator increase as well. In this paper, we propose a simulation system to assess the impacts of attacks on cyber assets and identify critical assets. Our proposed system helps to have better situation awareness. For this purpose, we first generate the business process model of the organization. This business process model not only contains information about the mission activities but also contains features of the process itself and the context in which the system operates. Then, we determine the dependency between the processes and the cyber assets of an enterprise. Finally, we simulate some attacks on cyber assets. We evaluate the impacts of attacks on the cyber assets and asset-dependent processes by comparing the Measure of Effectiveness before and after of attack simulation.**

Keywords: Cyber Security, Situation Awareness, Business Process Model, Simulation; Cyber Attack, Measure of Effectiveness, Impcat Assessment

Article type: Research Article

I. Introduction

In cyberspace, threats have a complex form and include internal and external attackers with different skill levels. Currently, attackers usually employ automated tools to exploit and control target systems remotely. When systems are infiltrated, attackers might use the current infiltrated system to expand their attacks and achieve the next targets [1]. In this case, cyber security situation awareness is important for the analysis of cyberspace, and detection of ever-changing threats. Situation Awareness is a cognitive process that can percept and comprehend the current situation, and project the near future. Then, based on the obtained awareness, any plans, decisions, and acts can be performed.

There are different definitions of situation awareness. One of the most famous of which provided by Mica Endsley in 1995 [2] is the perception of environmental elements and events with respect to time or space, the comprehension of their meaning, and the projection of their future status.

* Corresponding Author
The author has been affiliated with Apa research center of Amirkabir University of Technology as a researcher at the time of this project

[DOI: 10.61186/itrc.15.3.21]

This definition makes a subtle distinction between three levels of situation awareness, i.e., perception (including observation), comprehension, and projection (including prediction). Its lowest level is observation and perception, and the highest level is the projection of the near future, i.e., the projection of the current situation into the future in an attempt to predict the evolution of the tactical situation.

In this paper, we propose a simulation system to assess the impacts of attacks on cyber assets and identify critical assets. Our proposed system helps to have better situation awareness. We first generate the business process model of the organization that contains information about the mission activities, the process features, and the context in which the system operates. Then, we determine the dependency between the processes and the organization's cyber assets. Finally, we simulate attacks on cyber assets and evaluate their impacts on cyber assets and asset-dependent processes. We consider the duration of processes and attacks in our simulation system. Our proposed system helps to identify the critical assets and discover the system's susceptibility to different attack impacts. Assets can be tested against 6 types of cyber-attacks which are Degradation, Modification, Interruption, Interception, Fabrication, and Unauthorized Use. Users can create their customized business process models and apply various attacks on different assets. Hence, no privacy concern is considered for using this simulation system. Attacks are applied alongside the normal execution of the workflow and they affect the system while it is being executed. Finally, the simulator performs the simulation with and without applying attacks on the system and compares the results of each simulation.

In this paper, we review the previous works in section II. Then, we state the details of our proposed system in section III. We evaluate the results of our proposed system in section IV. Finally, we summarize the overall features of our proposed system and state the conclusion of the paper.

II. Previous Works

There are some commercial simulation tools that provide features to perform different kinds of simulation but they are for general purposes and their implementations are private. Hence, we cannot use or modify them to assess the impact of cyber-attacks on cyber assets.

Business processes are an integral part of every organization. They refer to sets of activities, which are performed to achieve an outcome that is of interest to an organization or its customers. Capturing information on such processes, process models are present in all phases of the business process management lifecycle [3].

"Despite the relevance of process models for the documentation, analysis, and improvement of business processes, creating them is a time-consuming and an error- prone task that requires substantial expertise. Modeling business processes is even more challenging in the case of domain-specific processes [4, 5]."

For common business activities, there exist some accessible Business Process Management (BPM) tools that can be used to represent a business process, run a simulation of the process, evaluate and improve them. Examples of such Commercial BPM tools include iGrafx from Corel, and Oracle's BPA [6] [7].

For instance, iGrafx is a general-purpose simulation tool that can be used to test resources against attacks. The drawbacks of using these kinds of software are [8]:

- A license must be purchased
- It is a general-purpose simulation tool
- Resources and attacks have to be defined individually
- All required fields for resources and attacks must be specified
- Attacks are not a separate unit from the resources and processes
- For different simulations, all things have to be re-defined from scratch
- The results are raw and have to be re-processed to produce desired outcomes
- It demands a lot of time to design any simulations

These cons are enough to prove that utilization of these tools is hard. Additionally, there are other approaches for risk assessment such as Probabilistic Risk Analysis [4], Quality Function Deployment [5], Analytic Hierarchy Process [9], Risk- to-Mission Assessment Process [10], Mission Assurance Analysis Protocol [11], and OCTAVE Allegro [12].

Although these approaches are for performing cyber risk assessments, the mission models that are generated and used in them have restricted usage for computing online impact assessments. They assess the cyber risk in an offline process and focus on the potential cyber effects against a wide variety of possible mission instances. Moreover, the specific timing and duration of the attack effect are not specified. Risk assessment models ignore timing and workflow information which makes it impossible to distinguish between attacks that can be recovered quickly and attacks that would take much longer to recover.

OUR PROPOSED IMPACT ASSESSMENT SYSTEM

In this section, we state the details of our proposed system. We include in our proposed system the timeline, workflow, and attack thread for online impact assessment of cyber-attacks and detection of critical assets. We describe different parts of the system in the following as it is crucial for a better understanding of our approach.

[DOI: 10.61186/itrc.15.3.21]

- ICT Resource: It is an operating cyber unit with a response speed, such as a server or a switch. The simulator, by using its response speed, can calculate the time taken by the resource to complete a given task [11].
- Workflow: It is a group of processes with different jobs, joined together to achieve a final goal by performing assigned tasks. A workflow starts from a start point, has multiple processes along the way, and is terminated at one or multiple endpoints [12].
- Timeline: As mentioned above, any resource has a response speed and consequently a response time. In addition, every process uses multiple resources to reach its goal and as a result, the system must keep track of time to do the simulation in a time series way. With the help of a timeline, the simulator can apply attacks on resources and generate attack reports.
- Transactions: Transactions are the smallest units of executions. They have execution time, data quality, execution history, and fields related to different cyber-attacks. Transactions are injected into the workflow and executed by resources [13].
- Cyber-Attacks: All cyber-attacks can be divided into 6 categories: Degradation, Modification, Interruption, Interception, Fabrication, and Unauthorized Use. They have a start time, duration, impact value, and target resource.

  Duration can be constant or distribution function like uniform, normal or exponential distribution. All attacks
  change the Boolean field of their own in affected transactions [14].

Attacks are briefly described as follows:

– Degradation: It is a type of attack which causes a decrease in resource performance and data quality. It affects accessibility and data accuracy.

– Modification: It is a type of attack which causes a decrease in data quality. It directly affects data accuracy and confidentiality.

– Interruption: It is a type of attack which causes a resource to deny any requests for some time. It affects accessibility.

– Interception: No target resources nor data are affected by this attack. It only affects data confidentiality.

– Fabrication: It is a type of attack which causes misinformation to enter the system, so data quality is decreased. It affects data accuracy and privacy. The difference between fabrication and modification is in the way data is manipulated. In fabrication, the original request is ignored and a brand-new request takes place but in modification, the original request is manipulated.

– Unauthorized Use: It is a type of attack which causes a decrease in data quality. If a user who doesn't have enough permission to do some actions, gains the power to do so, he may cause harm to the existing data or inject false information.

- Business Process Modeling Notation (BPMN): It is an open standard to diagram a business process. It is like a flowchart and uses standardized graphics to represent the participants, choices and flow of the process. It consists of resources, processes, and their connections. An example of a BPMN for a system with three servers and a database is illustrated in the Fig. 1. The workflow of this model consists of 5 processes, two of which are run in parallel.

After defining the different parts of our proposed system, we explain its implementation details. The goal of the proposed system is to facilitate and accelerate the procedure of defining business process models, applying attacks, and evaluating the impacts of attacks. Here we make use of a graphical BPMN modeler and graphical user interface in the system to make it easier for the user to interact with the simulation tool. Implementing the simulation system is divided into two parts:

1) BPMN Modeler
2) Simulator Engine

BPMN Modeler: Our proposed system provides graphical features that users can easily create their business process models. It should have options to create workflows with capabilities to define resources response speed, type of connections (series and parallel), and load balancing. With the help of bpmn-js[15], a library based on Reactjs providing a clean web application to design and create BPMN models, and some customization, a modeler tool is developed to fulfill all the requested needs.

Simulator Engine: This is the part responsible for fetching data from a user, processing input data, executing the simulation process, and generating reports. These three steps are handled in a layered architecture. The GUI is responsible for getting data from a user, the BPMN processor is responsible for processing input data and the Executing Engine (heart of the system) is for simulations and reports. Different steps of a simulation process are demonstrated in the Fig. 2.

Based on the Fig. 2, the user must take four steps to get the desired results. They are:

1) Designing the business process model (workflow)

[DOI: 10.61186/itrc.15.3.21]

2) Inputting the model into the system (the system starts to process the model as soon as it is fed with data)
3) Inputting attack data
4) Inputting attack priorities (the system performs the simulation, and generates reports)

When it comes to designing BPMN models, there are so many things to offer. But the proposed system only uses the parts that are needed for our purposes. These parts and their configurations are explained as follows:

Resources: Business process models can have as many resources as required, but the response speed for each resource must be set separately.

Resource Pools: Resources must be in one and only one resource pool as illustrated in the Fig. 3. All resources in a resource pool must be of one type. If a resource pool has multiple resources, load balancing is automatically applied by the system. The default load-balancing algorithm is Round-Robin but other algorithms can be used, too. It is worth mentioning that resources have no connections with other parts of the workflow. They are controlled by their pools and the pools are keeping the connections.

Processes: One and only one pool must be created for processes to make them distinguishable from resources. Each process can use a resource directly by connecting to its resource pool or indirectly by connecting to a resource pool that uses another resource pool as a dependency.

Connections: As stated before, connections are vital for simulation models. Processes must be connected to each other as well as resources. To make a difference between inter-process connections and other ones, two types of connections are used in the modeler tool. The former type of connection is used to connect two processes and the latter one is used to connect a process to a resource pool or

a resource pool to another one. Please notice the connections shown in the Fig. 1.

Gateways: Gateways can model a parallel or conditional workflow, i.e., a workflow can be paralleled into multiple paths or conditionally based on time and data quality. We have Parallel, Exclusive and Inclusive gateways as demonstrated in the Fig. 4.

- Parallel: It makes a one-path workflow into multiple paths and tries to execute them simultaneously. At last, it merges the results of all paths and continues in its one-path way.

- Exclusive: It starts checking conditions from the very first path and if a path meets the requirements, it continues that one and ignores other paths. To be more precise, it does not make a multi-path workflow; it just checks for one path and continues in a one-path manner.

- Inclusive: It starts checking conditions from the very first path but unlike the exclusive gateway, it does not stop if a path meets its requirements, it moves on to other paths and checks them, too. Finally, it executes all paths that have met its requirements in parallel. We can say it is a mix of parallel and exclusive gateways.

Start and End gateways are also used to demonstrate the start and endpoint of the workflow. A model must have one and only one start point and at least one endpoint. After processing the BPMN file and creating corresponding objects for the simulator, the system asks the user for attack information. In this part, a user can define attacks without any count or resource limitations. An attack is defined by a type, its target resource (which is dynamically extracted from the previous section), a start time, an impact value (if applicable), a duration type, and duration information based on duration type. Finally, a user must provide attack priorities (Highest, High, Medium, Low, Lowest, and Not Important) for the simulator. The engine has different parts and objects to handle the simulation process. These parts are as follows:

Start point: All models have one start point where the simulation starts to execute.

Event generator: This part is responsible for generating enough transactions for the simulation process. First, one transaction will enter the simulation zone, and then the calculated execution time is used to determine the total number of transactions needed to perform the simulation. It is calculated by adding the furthest start time among all attacks and its duration and dividing by one transaction execution time.

$$Total\ number\ of\ transactions = \frac{The\ longest\ attack\ (the\ biggest\ starttime\ +\ duration)}{Execution\ time}$$

• Executor: Executors are containers that keep the states of their transactions in the model. They start from the start point and continue in the workflow. The executors' handover the transactions to processes to be executed. It is mandatory that each executor has only one transaction in hand and they do not have any role in the execution parts of the transactions.

• Resource: Process executions are performed in these parts. They acquire a transaction and lock them until the execution time needed for that resource is passed. If a resource has a dependency, the transaction is first handed over to their dependency and then back to the original resource. While the transaction is locked in a dependency resource, the execution time for the original resource is not stopped and is taken into account for the final results. Transaction propagation is not limited to the number of resource layers.

[DOI: 10.61186/itrc.15.3.21]

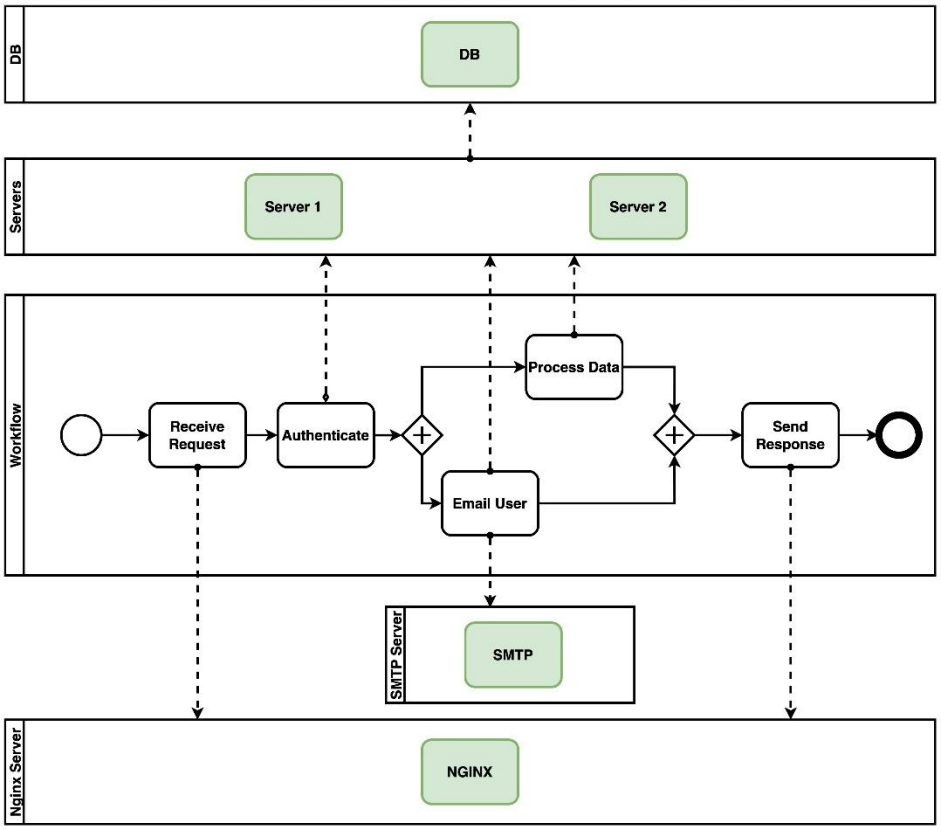

Figure 1. An Example of a BPMN Model

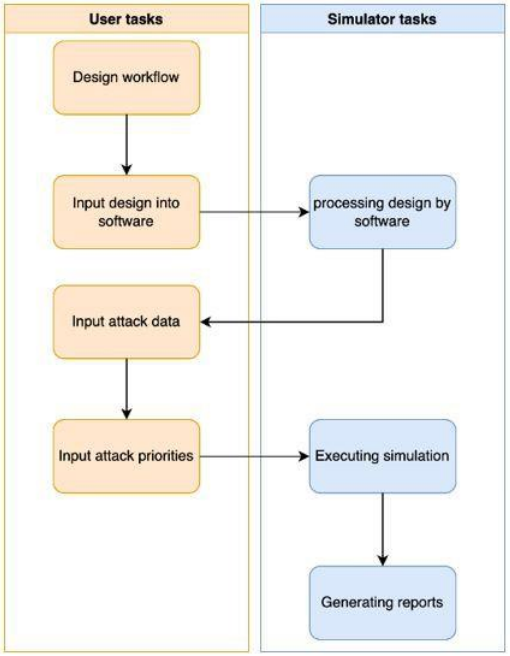

Figure 2. Steps of a Simulation Process

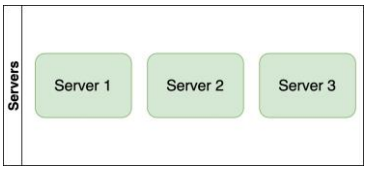

Figure 3. A Resource Pool with Three Assets

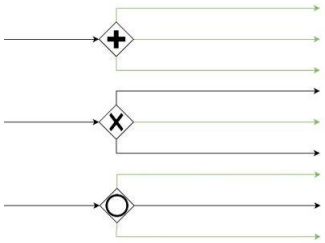

Figure 4. Parallel, Exclusive and Inclusive Gateways, Respectively (Green Arrows Are Executed)

[DOI: 10.61186/itrc.15.3.21]

Resource Pool: This part is responsible for load balancing and choosing an appropriate resource for any arrived transactions.

• Gateways: A transaction is taken apart into multiple sub- transactions in gateways. As noted in the BPMN model part, three types of gateways are possible.

• Attack: Based on attack type, transactions are modified in this part. When a resource is under attack, it hands over transactions to attack managers and they change attack fields based on their programmed behavior. The only attribute that is not changed is execution time which is applied to resource response time and consequently on transactions execution time. It is important to apply effects in parallel with the execution of the model so the real-time attack impacts can be simulated. In this way, the results are genuine and can represent a miniature image of real-world attack events.

• Clock: This part is the most important and complex unit in the system. The simulator uses parallel threads to handle transactions and those threads are using the same resource sets. It is crucial to keep resources, attacks, and transactions in sync to keep track of time and its validity. The clock is doing this job by syncing resources with a negligible delay and this delay can be ignored in the final results so it seems that resources are actually in sync.

• Resource Reporter: When a transaction enters a resource pool, an instance of a resource report is created and then it records all the events happening between entry and exit of the transaction. In the end, the final report is generated based on these instances of reports.

All described parts are necessary for the system to perform the simulations. First, the executors and

Transactions are created and executed in thread pools. The number of concurrent threads is adjustable according to the power of the machine. Threads keep the number of simultaneous transactions in the model and forbid overloading the engine. All transactions start from the start point. They can face three possibilities throughout the model. These possibilities are:

1) Process: If an executor is in place of a process, it hands over the transaction to the process and then the process executes and creates demanding reports. Process execution is mainly the execution of its direct or indirect resources. A pseudo-code to perform this action is demonstrated as follows:

2) Gateway: If an executor is in place of a gateway, the path is decided according to the gateway behavior. As mentioned before, a parallel gateway divides the current path into multiple paths and a dummy transaction is created for each of the sub- paths. Finally, dummy trans- actions are merged with the main one. An exclusive gateway finds the first path that matches its requirements and continues. Inclusive gateways choose sub-paths based on the provided conditions and continue as parallel gateway.

3) Endpoint: If an executor is in place of an endpoint, the execution process is done.

These three possibilities are enough to perform an attack-less simulation with the model. To apply attack effects, when a transaction is locked in a resource that is under attack, it is handed over to the attack manager to inject attack effects into the transaction. If the resource is under multiple attacks, they are applied linearly. Each transaction has a boolean field corresponding to a specific type of attack, a quality field with a default value of 1, and an execution time field. All attacks set their field to true when applying their effect on the transactions. Degradation, Modification, Fabrication, and

Unauthorized Use, change the quality of transactions to a number between 0 and 1. Degradation and Interruption affect the execution time of the transactions. Explanations for time- related attacks are given below:

• Degradation: When a resource is under degradation attack, its response time gets longer according to the attack value. As transactions are locked in a resource, they have to wait until the response time is passed. When the response time gets longer, they have to wait longer to be released and consequently their execution time grows.

• Interruption: When a resource is under interruption attack, it becomes unavailable to transactions. This is implemented in resource pools where resources are getting picked to serve transactions. If there is an alternate resource in the resource pool, only the switch time is considered in execution time. But, if there are no other available resources, transactions are held and so a resource becomes available. This waiting time is mirrored in transactions' execution times.

Finally, after simulating with and without attacks, the system has two sets of transactions and resource reports to calculate the final results. The system calculates three variables for each attack type. These variables are:

1) Request ratio: It is the number of total affected transactions divided by all transactions. It shows the spread of the attack in the simulation process.

2) Quality ratio: It demonstrates the final average quality of transactions.

3) Time ratio: it shows the difference between normal and manipulated execution time. It ranges from

[DOI: 10.61186/itrc.15.3.21]

1 to infinity such that the bigger the number, the longer it takes to finish execution under attack compared to normal time.

After getting the above values, each attack's Measure of Effectiveness (MoE) for the model is calculated as follows:

$$MoE_{attack} = w_{requestRatio} \times requestRatio + w_{qualityRatio} \times qualityRatio + w + timeRatio \times timeRatio \quad (1)$$

The weights are given in Table 1. Finally, with the help of individual MoE for attacks and provided weights by the user (attack priority section), the final MoE is calculated as follows:

$$MoE_{total} = \Sigma_i \text{ in attacks } w_i \times MoE_i \quad (2)$$

MoE indicates the impact of attacks on the given business process model. This value does not have a meaning per se but it is helpful for comparisons between different business process models and different attack schemes. For example, if the user uses one business process model for two

simulations with different sets of attacks, he can conclude that the model with the bigger MoE is more impacted by the attack set.

A. A Case Study

For more clarity, we explain this process in the form of an example. Consider the model illustrated in the Fig. 1 as our input model.

It consists of four resource pools (database, servers, SMTP servers, and nginx). Each asset has a response speed, and the servers' pool has two assets. In the process pool, a request is received by the nginx servers and then an authentication is performed by the servers. After authentication, two tasks are fired simultaneously, processing data using the servers and emailing the user using the SMTP servers. Finally, the response is ready to be sent back to the user by the nginx servers. Reminding that each time the servers perform a task, the database is called for information and data.

Now, the next step is to define attacks. Fig. 5 demonstrates the panel to do so.

In this example, an Interruption is applied to the database with a duration following normal distribution which starts after 10 minutes. Server1 is under Degradation after 4 minutes and the nginx server is intercepted after 1 minute with a duration of uniform distribution between 20 and 30 minutes. Next, based on the Fig. 6, the priorities must be set. Based on the Fig., Interruption has the highest priority which has a coefficient of 5, Degradation is next up with a coefficient of 4, and Interception comes last with a coefficient of 3. These coefficients are used to calculate the final MoE, which is shown in the Fig. 7.

These three MoEs in the Fig. 7 are explained more to clarify the meaning of the numbers.

• Interruption: The number 1.071 indicates that in general, it takes twice the time for the database to perform its tasks and it is blocked for almost one complete cycle of a normal process.

• Interception: The number 0.433 indicates that about 43.3% of the requests are intercepted through the nginx servers.

• Degradation: It might seem that the number 0.059 is wrong but it is showing the expected number. The servers pool has two assets, so the requests are divided equally for both assets and in this way, only a small number of requests get affected.

In the Fig. 7, the number 6.893 is the total MoE of the simulation. It is calculated based on the attacks' priorities and MoEs.

$$MoE_{total} = \Sigma_i \text{ in attacks } w_i \times MoE_i = 1.071 \times 5 + 0.059 \times 4 + 0.433 \times 3 = 6.89$$

As mentioned earlier, total MoE does not mean anything unless compared to other total MoEs.

All these details and implementations are designed to demonstrate an important capability of the system, i.e., Critical Assets Analysis (CAA). With this feature, the user can give a business process model to the system and the system automatically assigns different attack schemes and performs multiple simulations to find the most vulnerable assets in the model.

For this purpose, after processing the input model, a fixed start time, duration, and value are generated randomly. The number of transactions for each simulation is considered fixed. We also use constant values to make sure that all simulations have the same environment and the results are comparable to each other. After generating initial values, 6 attack objects are created and injected into the engine but only one of them is used during each simulation. Then the system loops through all assets and for each iteration, it applies all the attacks separately, i.e., 6 simulations are performed for each asset. Fig. 8 illuminates this concept. The CAA result for the above example is given in the Fig. 9. In the example, the database is the most impacted asset among all. Server1 and server2 have close results, even in detailed MoEs, and that is because they are the same and this result is expected. One point in this example which stands out is the impact of Interruption on servers. The interruption has no impact on servers because they have an alternative when they are offline. So no blocking occurs and the system works normally. In CAA, many results can be extracted by analyzing the resultant table. This feature gives enough reliable information about the model that organizations and experts can act according to its results.

III. EVALUATION

We evaluate our proposed system by considering the following factors:

- Stability of the results

[DOI: 10.61186/itrc.15.3.21]

- Validity of the results when using distribution functions

Our proposed system is stable if for one model and attack set, the order of MoE for different attacks barely changes. In some cases where the values of multiple MoE are close to each other, the order may change due to hardware limitations and the probabilistic approach of the system. Hardware limitations happen when the simulator is about to apply or lift an attack. In such cases, based on the speed of the system, the attack effect is applied or lifted gradually. This happens because attack effects must be set for all resources in a series manner and this lets some transactions to slip away from being affected in every run. This problem can be ignored in multiple runs of the same system as it does not have a big impact but on different systems. As is illuminated in the Fig. 10, the faster the hardware can set the effect on resources, the faster to reach the maximum request ratio. For example the purple system is the fastest and the green one is the slowest of all. The margin of being safe for MoE is not a fixed value and it changes for different simulations. In our tests, it did not exceed 0.8 and in this simulation, the most vulnerable asset had a MoE of 5.8 while it was 2.8 higher than the second asset.

The system may use different distribution functions that their parameters can be given by the user and the calculations are all inside the system. To validate the results of probabilistic simulations, the system performs the simulation multiple times and computes the average of all results to ensure that they are valid and not biased based on one accidental low or high value. With this technique, results become more stable as it is the goal of the previous part. To correlate the model with KPI, we can perform the simulation with different designs, attacks, configurations, and parameters. The minimum of MoEs can be obtained with respect to the corresponding

graphs. Moreover, It should be noted that the formula of MoE is not our concern. We can change the formula, and consider the nonlinear effects of an attack.

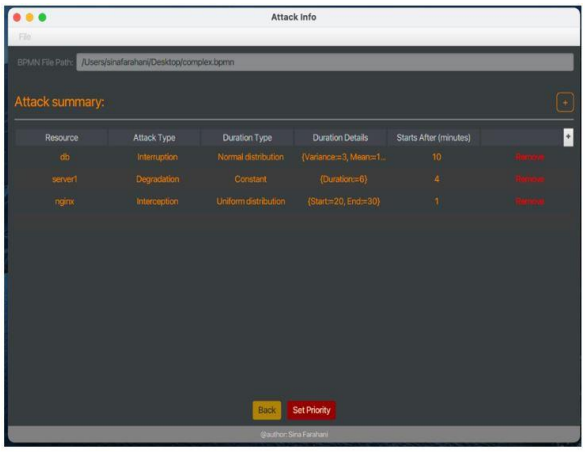

Figure 5. System Attack Definer

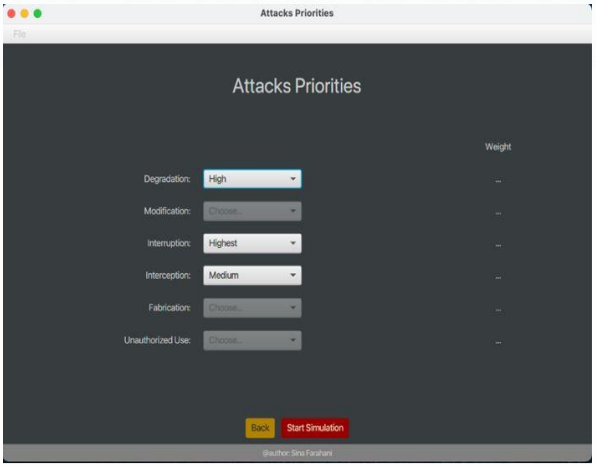

Figure 6. Attack Priorities Panel

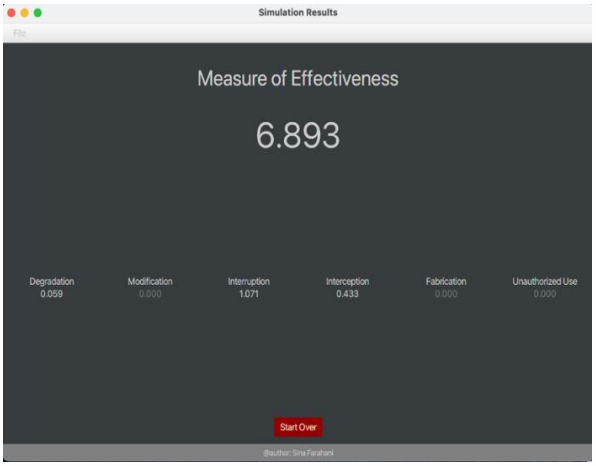

Figure 7. Simulation Result Panel

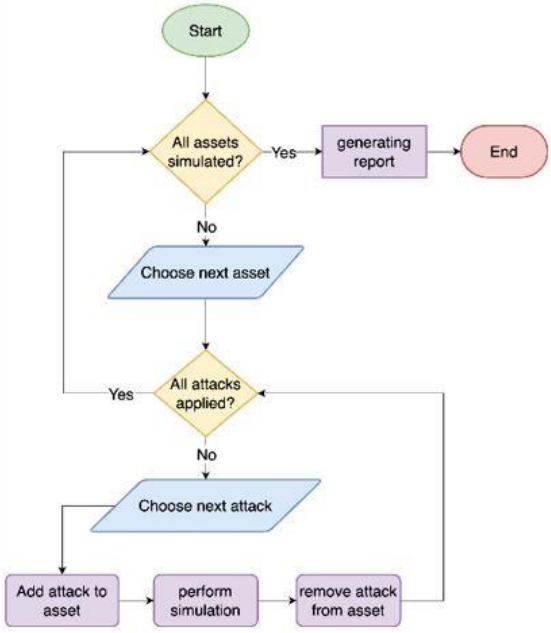

Figure 8. CAA Process Steps

[DOI: 10.61186/itrc.15.3.21]

TABLE I. RATIO WEIGHTS FOR ATTACK TYPES

	Request Ratio	Quality Ratio	Time Ratio
Degradation	1	1	1
Modification	1	1	0
Interception	1	0	0
Interruption	0	0	1
Fabrication	1	1	0
Unauthorized Use	1	1	0

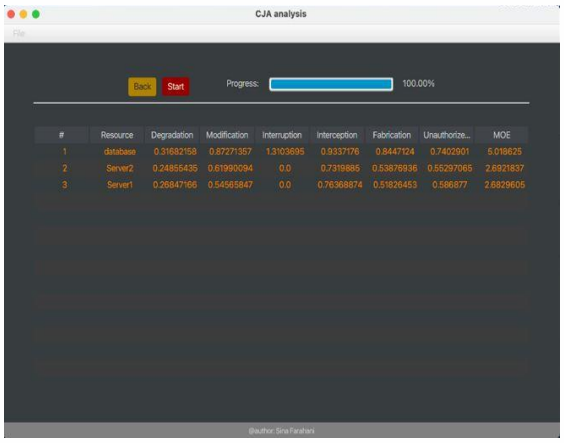

Figure 9. Example of CAA Results

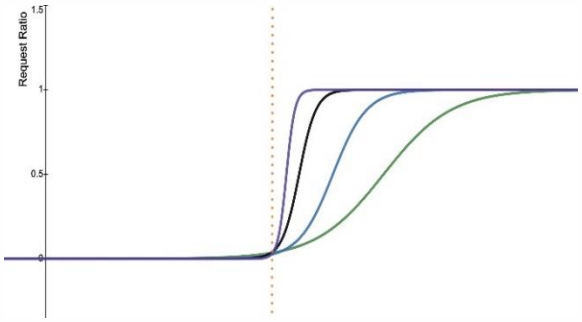

Figure 10. The effect of hardware limitations

IV. CONCLUSION

In this paper, we proposed a simulation system to assess the impacts of attacks on cyber assets and identify critical assets. Our proposed system helps to have better situation awareness. For this purpose, we first generate the business process model of the organization. Then, we determine the dependency between the processes and the cyber assets of organizations. Finally, we simulate attacks on cyber assets and evaluate their impacts on cyber assets and asset-dependent processes. We consider the duration of processes and attacks in our simulation system. Our proposed system is suitable for identifying the critical assets and discovering the system's susceptibility to different attack impacts. As discussed in the evaluation section, our proposed system generates reliable results which leads to the same results on every run.

This system helps the security experts to assess the impacts of cyber-attacks on the cyber assets, and identify the critical assets of their organizations by spending less money and time. Moreover, based on the results of the simulation, they can select appropriate and timely countermeasures.

The simulation is for an enterprise, and we do not consider the services over global networks.

Moreover, our proposed system can model the centralized system. However, it can be used for modeling the distributed systems with some modifications in simultaneous requests. Our proposed system considers a one-to-one relationship between attacks and resources to analyze the critical assets. Moreover, a certain duration and a specified start time are determined by the system. Then based on these values the attacks are performed on cyber assets. For future work, it would be worthwhile to consider multiple attacks, different duration, and start times.

Since our proposed system works sequentially, for future work, it would be worthwhile to modify the system for collaborative networked situations. We should handle the loops, and multiple connections between assets.

Moreover, the design of a system to assess the impact of attacks on cloud-based environments is of interest.

REFERENCES

[1] K. K. R. Choo, "The Cyber Threat Landscape: Challenges and Future Research Directions", Computers & security, vol. 30, no. 8, pp. 719-731, 2011.

[2] M. R. Endsley , Toward a Theory of Situation Awareness in Dynamic Systems, Human Factors, vol. 37, no.1, pp. 32–64, 1995b.

[3] D. Sola, et al., On the Use of Knowledge Graph Completion Methods for Activity Recommendation in Business Process Modeling, In International Conference on Business Process Management, pp. 5-17. Springer, Cham, 2021.

[4] S. Emilio, I. A. Amantea, and G. Fornero, Risk-aware Business Process Modeling: a Comparison of Discrete Event and Agent-based Approaches, In 2019 Winter Simulation Conference (WSC), pp. 3152-3159. IEEE, 2019.

[5] B. Tim, and R. Cooke, Probabilistic Risk Analysis: Foundations and Methods, Cambridge University Press, 2001.

[6] L. Manuel, and J. Marklund, Business Process Modeling, Simulation and Design, Chapman and Hall/CRC, 2018.

[7] P. Pille, et al., Privacy-enhanced BPMN: Enabling Data Privacy Analysis in Business Processes Models, Software and Systems Modeling, vol. 18, no. 6, pp. 3235-3264, 2019.

[8] B. L. James, Quality Function Deployment: a Practitioner's Approach CRC Press, 2021.

[9] T, Hsin-Yi, and Y. Huang, An Analytic Hierarchy Process-based Risk Assessment Method for Wireless Networks, IEEE Transactions on Reliability, vol. 60, no. 4. pp. 801-816, 2011.

[10] J. Watters, et al., The Risk-to-Mission Assessment Process (RiskMAP): A Sensitivity Analysis and an Extension to Treat

[DOI: 10.61186/itrc.15.3.21]

Confidentiality Issues, MITRE CORP MCLEAN VA Report, 2009 Jul 1.

[11] C. J. Alberts, and A. J. Dorofee, Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments, CARNEGIE- MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST Report, 2005 Sep 1.

[12] R. A. CARALLI, et al., Improving the Information Security Risk Assessment Process,Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst Report, 2007.

[13] A. Blyth, and G. Kovacich, Information Assurance: Security in the Information, Cambridge: Springer, 2006.

[14] A. Ravi, Managing Business Process Flows: Principles of Operations Management, 2/E. Pearson Education India, 2008.

[15] bpmn-js: https://bpmn.io/toolkit/bpmn-js/

Sina FarahaniNia received his B.Sc. in Computer Engineering from Amirkabir University of Technology, Tehran in 2021, and now he is pursing M.Sc. degree in Computer Science in the University of Tehran. His research interests include Distributed Systems, Edge Computing, Security and Privacy and Related Applications.

Motahareh Dehghan is an Assistant Professor in the Department of Industrial and Systems Engineering at the Tarbiat Modares University. She received her Ph.D. degree in Information Security from Amirkabir University of Technology. Her research interests span the area of Information Security, Cyber Security Situational Awareness and Emerging Technologies

Babak Sadeghiyan is an Associate Professor in the Department of Computer Engineering of Amirkabir University of Technology, Tehran, Iran. He received his Ph.D. in Computer Science from University College, University of New South Wales, Australia in 1993. His research interests includes all aspects of Information Security. He has pioneered many original research in the area, and the author of more than 200 conference and journal papers and 5 books. His recent research works are focused on Cybersecurity Situational Awareness. He is a member of Computer Society of Iran, and a founding member of Iranian Society of Cryptology. He has been the head of APA Research Center of Amirkabir University of Technology since 2012.

Salman Niksefat is an Assistant Professor in APA Research Center of Amirkabir University of Technology, Tehran, Iran. He received his Ph.D. degree in Information Security from Amirkabir University of Technology in 2013. His research interests includes Privacy in Computing, Secure Multiparty Computation, Network Security and Intrusion Detection Systems**.**

[DOI: 10.61186/itrc.15.3.21]