An Intelligent Game Theoretic Model With Machine Learning For Online Cybersecurity Risk Management

Talal Alharbi[1†]
talal@mu.edu.sa
Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Al Majmaah 11952, Saudi Arabia

Abstract
Cyber security and resilience are phrases that describe safeguards of ICTs (information and communication technologies) from cyber-attacks or mitigations of cyber event impacts. The sole purpose of Risk models are detections, analyses, and handling by considering all relevant perceptions of risks. The current research effort has resulted in the development of a new paradigm for safeguarding services offered online which can be utilized by both service providers and users. customers. However, rather of relying on detailed studies, this approach emphasizes task selection and execution that leads to successful risk treatment outcomes. Modelling intelligent CSGs (Cyber Security Games) using MLTs (machine learning techniques) was the focus of this research. By limiting mission risk, CSGs maximize ability of systems to operate unhindered in cyber environments. The suggested framework's main components are the Threat and Risk models. These models are tailored to meet the special characteristics of online services as well as the cyberspace environment. A risk management procedure is included in the framework. Risk scores are computed by combining probabilities of successful attacks with findings of impact models that predict cyber catastrophe consequences. To assess successful attacks, models emulating defense against threats can be used in topologies. CSGs consider widespread interconnectivity of cyber systems which forces defending all multi-step attack paths. In contrast, attackers just need one of the paths to succeed. CSGs are game-theoretic methods for identifying defense measures and reducing risks for systems and probe for maximum cyber risks using game formulations (MiniMax). To detect the impacts, the attacker player creates an attack tree for each state of the game using a modified Extreme Gradient Boosting Decision Tree (that sees numerous compromises ahead). Based on the findings, the proposed model has a high level of security for the web sources used in the experiment.

Keywords:
Cybersecurity, security risks, risk management, online service, threats, risk analysis.

1. Introduction

The medium of Internet has grown in popularity for its information sources and services that are offered online. The usage of Internet has been on the rise and around 48% of the global population as of 2017 [1] and increased by roughly the same percentage in when internet became a major transporter of data using networks. The public nature of these networks and their nodes also evolved interests of cyber criminals towards the internet [2]. Information confidentiality, availability, and integrity must all be guaranteed via safe and stable computer systems and hence "Cyber security" refers to set of security methods applied in cyber spaces for safeguarding user's information and assets against unauthorized accesses or assaults [3]. The primary purpose of cyber defense systems narrows down to ensuring vital data is safe and accessible. Cyber networks are becoming increasingly significant to all including individuals and industries where their data is prone to and assaults from both within and outside networks [4]. A threat is an agent that uses a specific negative penetration approach into networks for studying impacts of the operations in terms of behaviors of the networks or computers. The goals of security risk analyses then become identifying and quantifying dangers for taking apt decisions. Risk analyses require data about organization's assets and their associated probable risks as system's vulnerabilities get exploited by attackers [5]. Threats to organizational assets including their networks, software, physical components and data [6] stem from human activities and natural disasters where threats based on the former may be malevolent. Malevolent human risks include theft of identities, destructions of organizational assets, frauds, unauthorized accesses to networks/services, infections of systems using malicious codes and disclosures of private information [7]. Most studies substantiate rising security and privacy concerns making cyber security's main aim as safeguarding of networks, data and programs from unauthorized accesses. Managing information security risks are comprehensive processes that

Manuscript received June 5, 2022
Manuscript revised June 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.6.49

include identification and analyses of risks to organizational information is exposed, assessing potential business consequences and impacts, and determining steps for eliminating these risks or getting them down to acceptable levels [8]. These demands: detailed analyses of assets; ramifications of security events; probabilities of successful attacks on ICTs and benefits of security systems with their associated financial costs. Information security can be managed using standards and guidelines like ISO 27000 series and NIST (National Institute of Standards and Technology) publications [9] and in addition CSGs can also be employed to maximize cyber security at given investment levels. CSGs are strategies that employ game theories to detect and reduce cyber risks as missions (contexts) [10]. CSGs can assess cost-effective utilizations of defense mechanisms that protect ICTs thus yielding Pareto-optimal security portfolios in terms of quantitative cyber risk assessments and investments. This also demands knowledge on whole ranges of threats and possible attacks [11]. CSGs can also simulate attacker's reactions to defensive measures, since smart attackers can indulge in matching modifications while picking up the most promising assaults for steps taken by defender to improve security of systems. Furthermore, rather of depending on thorough research, the proposed framework emphasizes task selections and executions as a means of achieving effective risk management and treatments. The goal of this study is to model CSGs using MLTs. By limiting mission risks, CSGs maximize system's abilities to continue unhindered in contested cyber environments. The remainder of the research is organized as follows: section 2 examines some of the most recent strategies for detecting cybersecurity risks efficiently. The proposed methodology's approach is presented in section 3. The fourth section summarizes the findings and discusses them. The conclusion and future efforts are discussed in section 5.

2. Literature Review

This section reviews some of the most modern ways for identifying cyber securities with efficient models in this section. Cruz et al. [12] proposed CockpitCI project's DIDSs (distributed intrusion detection systems) for industrial controls using SCADAs (supervisory control and data acquisitions). The systems were assessed and validated using special hybrid test beds that replicated electrical distribution grid SCADAs. Jarjoui et al. [13] proposed a new methodology for enhancing cyber resilience in identifying realistic organizational drivers and priorities from viewpoints of organizations. The study mitigated identified cybersecurity risks with holistic roadmaps that were multi-dimensional. Gordon and colleagues [14] proposed mechanism for including cost–benefit analysis in NIST's Cybersecurity Frameworks where their analyses assisted in identifying higher tiers for NIST Implementations. Sivanathan et al. [15] proposed SDNs (Software Defined Networks) architecture with MLTs for managing IoTs (Internet of Things) where programmed telemetry flows and robust data-based models monitored network activities. According to Makawana et al [16], MLTs have huge potential in cybersecurity where the study executed bibliometric analyses by categorising cited publications based on their implementation techniques, article types, publishers, and article efficiencies. Fernandezderroyabe et al [17] in their study investigated cyber breaches and their effects on SMEs (small and medium-sized enterprises) by considering functions of cybersecurity in SMEs with their economic relevance. The study also examined economic, financial, and management repercussions due to security breaches in SMEs. El-Sofany et al. [18] proposed a new cybersecurity strategy for safeguarding cloud services from all sorts of DDoS attacks. With an average performance of 95.41 percent, an average accuracy of 96.53 percent, an average sensitivity of 92.31 percent, and an average specificity of 97.39 percent, the studies revealed promising results for stopping DDoS attacks. Mattina et al. [19] suggested MARCS (Mobile Augmented Reality for Cybersecurity) platform for visualizing real time data for enhancing user perceptions and threat responses. Kure et al. [20] suggested an integrated strategy for managing cybersecurity risks where risks were identified and controlled proactively. Their scheme followed existing risk management practices and standards of stakeholders' model, and physical system components with their associated interdependences. Their assault model facilitated determinations of appropriate risk levels and select mitigation strategies accordingly. Hong et al [21] proposed risk managements using audits and controls, system controls and building contingency plans for managing information securities which potentially served for

future applications and empirical research. Meszaros et al. [22] suggested novel technique which addressed security concerns of online services and could be exploited by both service providers and customers. Their procedural outcomes resulted in identifying relevant activities that assisted in mitigating recognized security threats and breaches. If used regularly, the scheme could provide risk scores for online which can be tracked and reported. As a result of the foregoing discussion, it is clear that the current research paradigm places a greater emphasis on task selection and execution that leads to successful risk treatment outcomes rather than comprehensive studies.

3. Methodology

It has been proposed modelling CSGs with MEGBDTs (Modified Extreme Gradient Boosting Decision Trees) were utilized in this study to improve detection rates where CSGs limited mission risks. The suggested framework's main components were Threat and Risk models. The models were tailored to meet special characteristics of online services in cyberspaces. Risk management procedures are also included in the proposed framework. Risk scores are computed by combining probabilities of successful attacks with outcomes of mission impacts that help in predicting consequences of cyber catastrophes. The chances of attack's successes are assessed using threat models applied on system's topologies and defenses. CSGs consider system's interconnections and hence planning defenses involves assessing all possible attack paths while on the other hand attacker may need only a single gap or flaw to exploit. This research work uses theoretic game solutions to identify better defense tactics and reduce maximum cyber risks in its game formulations (MiniMax). To detect the impacts, the attacker player creates an attack tree for each state of the game using a modified Extreme Gradient Boosting Decision Tree (that sees numerous compromises ahead). The procedure of the suggested methodology is depicted in Figure 1.

3.1. Framework Architecture Proposed

Frameworks using technologies are being proposed for mitigating new risks in cyber security as the nature of these threats cannot be foreseen. This work's proposed framework can be extended to handle new threats and solutions. The Framework has self-assessments which can

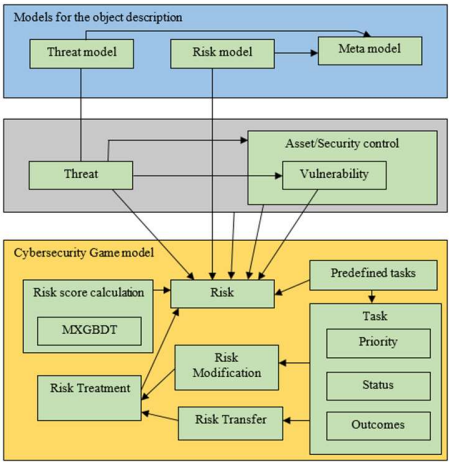

Figure 1: Methodology's overall Procedure

be used by organizations to identify threats and weaknesses on their own and without help from outside organizations. The generic nature of the proposed work is targeted towards most online users as the dynamic nature of internet data when recorded for specific periods of time can help in revealing future actions or states. Moreover, customizations of this framework's contents to suit online business makes it dynamic and enables assessment of severity levels when malicious content are detected, thus preparing systems for deployment of countermeasures. This also guarantees that mitigations related to high-risk scenarios are accomplished on schedule allowing Framework's usage in several ways like reflecting maturity of organizational risk management systems. The proposed Framework is zero-trust based implying it does not presume the presence of trusted environments and does not consider account trust levels. This method assists in discovery of neglected or concealed hazards like those posed by business partners, contractors, subcontractors, and others. This proposed framework based on risk managements can assist online users in terms of enhanced security encompassing consumers and service providers. The proposed software tools can aid in automating process execution and are built around Threat models which include Risk models and Meta models. Figure 1 depicts the entire Framework. Threat identifications and descriptions, assets, vulnerabilities, threats, and environmental components are all used in the framework. Pertinent risks are identified. Specific environments having assets and security restrictions may have weaknesses that could be exploited by adversaries. Risk descriptions contain information on threats, environments, assets, vulnerabilities, risk scores, and therapies for mitigating them. Tasks need to be fulfilled for risk adjustments or transfers. The priorities, status, and results of activities are further defined. A set of predefined tasks is included in the Framework. They were recognized as frequent tasks that can aid in the implementation of

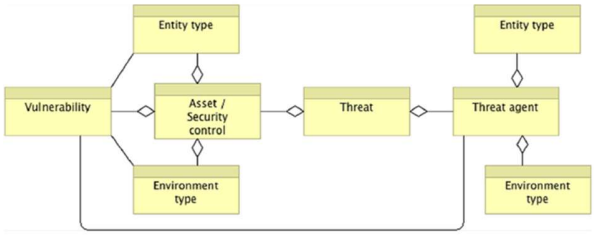

Figure 2: Threat Model

security measures to counter threat categories defined by the threat models.

3.2. Threat Models

The basic aim of Danger models is visibly conceiving all threat scenarios relevant to online service environments that makes it easy to identify. Threats can be identified, classified, and described using the Threat model. The approach is based on the perspectives of both providers and consumers. Threats that affect the environment are not included since they appear to pose a risk to neither the provider nor the user of an online service. The approach also ignores any hazards that may have an indirect influence. Because environmental risks aren't really specific to internet services, they aren't explored in depth.

3.2.1 Structure of Threat Models

The proposed Threat models are depicted using assets and threat agents based on entity types and environmental characteristics (refer to Figure 2). An asset's vulnerabilities or security controls that could be exploited by threat agents are also considered in this study.

3.2.2 Assets and Security Controls

The model considers a security control that protects a specific asset to be an asset. The BMIS model1 inspired the definition of the following five asset kinds for classification:

- Human: This category includes humans who are involved in operations, as well as those who provide and consume online services.
- Governance: This refers to both business and information technology governance.
- Processes and activities: These imply process and activate in provisioning and consumptions of online services.
- Technologies: Technological resources and concepts employed in provisioning and consumptions of internet services.
- Information: Data assets that are processed or stored using technologies in online services.

Specific vulnerabilities can be found in the first four classes. Information assets lack vulnerabilities of their own; flaws may only be controlled in the security systems that protect them. Assets can be found in one of three sorts of environments:

- The environment in which the provider operates.
- The surroundings of the consumer.
- Third-party or sub-contractor environments which encompasses products or service environments of third parties and sub-contractors used for delivering online services to consumers.

3.2.3 Threat Agents

Threat agents are persons or entities with a purpose or have the ability to compromise security of provided online services. The Threat models identify two types of threat agents:

- Human: Threats can stem from many people who compromise online systems for engaging in unintended, purposeful, or inactive behaviors.
- Technological: Threats arise from malware activities, malfunctions or failures, accidents, and other incidents.

From the perspectives of online services, Threat models accommodate encounter four environments of threat agents:

- The environment in which the provider operates.
- The surroundings of the consumer.
- The environment of third parties.
- Surroundings - entities in this environment class have no connection to either the supplier or the consumer; this environment can also be referred to as cyberspace. Only human threat agents can harm assets defined as human and governance.

3.2.4 Vulnerabilities

Threat models distinctly outline common vulnerabilities for asset types that can be exploited by threat agents (refer to Table 3 [22]). Vulnerability type's IDs are used to map threat categories and vulnerabilities.

3.2.5 Threat Classification

Table 4 [22] defines threat types as mixtures of assets and threat agents where examining root causes related to the two

are important for Threat models to portray proper combinations of threat agents working on assets:

- Humans are threat agents who can jeopardize all kinds of assets including governances, processes/activities, technologies, and data.
- Technological threat agents may provide a threat to processes, activities, technology, and data.

Except informational assets, which do not include vulnerabilities, all threat types can exploit flaws in their relevant asset categories. Hence, threats, vulnerabilities, and responsibilities are all documented.

3.3. Cybersecurity Game Model for Controlling Risk

The major aims of Risk models are detection, assessments, and treatments of risks where perceptions of all related risks are considered. CSGs are algorithmic games in which models are used to define the system, threat environment, and defensive capabilities. It generates results by running algorithms on certain models. CSGs can automate many expert-level skills like attack route identifications and eliminate the need for manual defenders. When components of systems or defense strategies or threats change, defenders can be updated on relevant models that are affected by these adjustments and CSGs can be restarted to analyze new conditions or identified vulnerabilities. CSG's attacker models take advantage of network architectures, access relationships, and information on component types which are effective substitutions for threat, vulnerability and components (T, V, C) of the model. For Example, "Risk = Threat (T) Vulnerability (V) Consequence (C)", is frequently used in risk formulations and criticized by Cox, with something that controls any T &V interdependencies. CSGs describe individual incidental risks as the product of cyber event's likelihood (i.e., PCI) and predicted losses suffered due to incidents (i.e., LCI). CSGs describe risks totally called TSRs (total system risks) which is the sum of all incidental risks associated in a collection of occurrences created by attackers.

$$Risk = \sum_{CI=1}^{N} P_{CI} L_{CI} \quad (1)$$

$$Risk = Max_{CI,N}(P_{CI} L_{CI}) \quad (2)$$

CSG's optimization of contexts are derived from CMIAs (Cyber Mission Impact Assessments) which describe cyber hazards associated with systems executing certain tasks like use-case scenarios or mission threads. CSGs sift through processes looking for prospective cyber events, attack pathways, implications, and deployment of defense mechanisms. CSGs are two person games with zero-sum outcomes where both attackers and defenders are assigned the same value in gains or losses. The "game" in CSGs is simply a defensive player designing and configuring defenses in systems while the attacker assumes that there are no known vulnerabilities in the system and considers it complex to compromise components that would have the most impact. System risk scores, the system metrics in CSGs, can be computed using Equations (1) or (2) based on risk preferences of the defender. To determine impacts, attacking player generates attack trees for each state of the game using MEGBDTs to view compromises ahead. Attack tree's leaf nodes depict the risk scores or probabilities and effects as per Equation (1). MiniMax determines how defensive strategies can effectively reduce risk scores. Since, using defenses' costs money, the game ends if one of two conditions are achieved. When defenders have spent money allotted to them, game determines optimal assortments of defense techniques. Attacker models are also a part of the proposed CSGs. The models are detailed in subsequent sections.

3.3.1 Incident Impact Modeling

CSGs use CMIAs (LCIs from Equation (1) to calculate consequences (losses) or impacts after cyber incidents, CMIAs are tools for collecting mission information in executable simulation forms and replicate activities including missions, IT, durations, dependencies, IT resources, time constraints, and control processes. Model levels of ICTs are developed by identifying activities and processes associated with components of ICTs. This included hardware, software, and data. Processes in ICTs are collection of procedures that support mission tasks and rely on resources of ICTs. Task-related dependencies in ICTs can be traced (usually from network diagrams). Each ICT resource in paths must act for completion of the mission. The repercussions are that each activity of ICTs would have if it was affected by given cyber effects.

3.3.2 Creating a Model of The Assailant

CSGs features are pre-programmed for assault models that games can employ. Assault models compute likelihood of successful attacks based on topological constraints imposed by systems on attackers. In assault models, the following characteristics influence the likelihood of successful attacks:

- Attacker's efforts to compromise components by getting directly connected within same networks or other connected network crossing networks boundaries.
- Attackers use components similar to previously compromised components.
- Attackers have control or use vulnerable components that can be exploited to gain entry into networks.

- Attacks on servers compromise its related network services.
- Attackers use roles of users who have accesses to all resources within networks and thus gain access and influence other network components.

Chain rules compute chances of successful travel around the network compromising components. Attacker models can span various networks, trusts, and segmentation barriers where the models capture key security features of segmentations, diversifications, and least privileges.

$$P(A_1, A_2, A_3, \ldots\ldots, A_n) = P(A_1|A_2, A_3, \ldots\ldots, A_n) \quad (3)$$

$$P(A_2|A_3, \ldots\ldots, A_n)\ddot{P}(A_{n-1}, |A_n)P(A_n) \quad (4)$$

3.3.3 Risk Evaluation

To evaluate risk, CSGs need to use attack models on topologies of systems and estimate impacts that can occur given the restrictions of topologies. As a result, there is a need for topological models which displays interconnected ICT resources including firewall rules, connections, users, roles, defined accesses, and constraints. Topological models allow automated computations of attack trees. The attack tree models are computed using MXGBDTs (Modified Extreme Gradient Boosting Decision Trees) in this work and depicted in Figure 3 which displays complexities that can occur even while studying simple four-host systems. CMIAs compute all the mission's impacts shown in the figure (bottom left). When numerous components are affected, consequences might be very severe. Even though the model in the diagram only has two subnets, it shows a trust connection from S1 to S4, from S1 to S4. Attacker models then compute the likelihood of each attack step's success yielding attack trees. As can be seen, attack trees have two right branches involving compromising of host S2, despite the fact that it has no implications but might be a useful steppingstone for other nodes.

3.3.4 Decision Tree with Modified Extreme Gradient Boosting (MXGBDT)

XGBoosts (Extreme Gradient Boosts) are repressors and classifiers based on GBDTs (Gradient Boosting Decision Trees) [23]. The regression tree's central nodes indicate attribute test values, and leaf nodes with scores represent judgements. Since XGBoost utilizes additive learning techniques that utilize 2nd order approximations, loss function derivatives of first and second orders are pertinent to fit the models. Initially, additive boosting tree's 2nd order approximations are derived for clarity where m implies data's count while n represents features count and zi represents sigmoid function's raw prediction inputs, while probabilistic forecasts are denoted by (y_i)^= σ(z_i), where σ(.) represents sigmoid functions. Discrepancies in notations of (y_i)^ should be noted as in analysis it is denoted as z. yi denotes true labels, α and γ are loss function's parameters [24]. Gradient/hessian' expressions are reported in merged formats that are independent of yi values, since they can simplify program implementations and aid vectorizations of other related. In practice, the additive learning target is as follows:

$$\mathcal{L}^{(t)} = \sum_{i=1}^{n} l\left(y_i, z_i^{(t-1)} + f_t(x_i)\right) + \Omega(f_t) \quad (5)$$

Where, t indicates the iteration in training. The notations in the equation have been replaced. When 2nd order Taylor expansions are applied to equation (5), it results in:

$$\mathcal{L}^{(t)} \approx \sum_{i=1}^{n}[l\left(y_i, z_i^{(t-1)} + g_i f_t(x_i)\right) + \frac{1}{2}h_i(f_t(x_i))^2 + \Omega(f_t) \quad (6)$$

$$\propto \sum_{i=1}^{n}[g_i f_t(x_i) + \frac{1}{2}h_i(f_t(x_i))^2] + \Omega(f_t) \quad (7)$$

The last statement is derived from the fact l(y_i,z_i^((t-1))) te word may be omitted from learning goals as it has nothing to do with the model's fitting in the iteration.

XGBoost compulsorily requires hand derived derivatives as cannot differentiate automatically. Resulting expressions could be used in a variety of of MLTs. Both loss functions have sigmoid activations, and the following sigmoid basic characteristic will be used consistently throughout the derivatives:

$$\frac{\partial \hat{y}}{\partial z} = \frac{\partial \sigma(z)}{\partial z} \quad (8)$$

$$= \sigma(z)(1 - \sigma(z)) \quad (9)$$

$$= \hat{y}(1 - \hat{y}) \quad (10)$$

- Attrition factor based XGBDT

In addition to the regularized aim, the extra strategies are utilized to prevent overfitting. Attrition reduces the weight by a factor w_j^* for the stages of boosting tree 's attrition factor like learning rates during optimizations, thus minimizing effects of particulars tree while leaving room for subsequent trees to enhance the model. The fixed structures q(x), calculate optimal weights for j leaves w_j^* j by:

$$w_j^* = -\frac{\sum_{i\epsilon I_j} g_i}{\sum_{i\epsilon I_j} h_i + \lambda} \quad (11)$$

Where $\in$ represents factors of approximations which intuitively imply the points are roughly selective. Data

points weighed by hi represents weighs and thus Equation (6) can be rewritten as

$$\sum_{i=1}^{n} \frac{1}{2} h_i (f_t(x_i) - g_i/h_i)^2 + \Omega(f_t) \quad (12)$$

Defining $I_j = \{i|q(x_i) = j\}$ as instances of set of leaves j, Equation (14) can be rewritten by expandin Ω as:

$$\mathcal{L}^{(t)} = \sum_{i=1}^{n} [g_i f_t(x_i) + \frac{1}{2} h_i f_t^2(x_i)] + \Omega(f_t) \quad (13)$$

$$\mathcal{L}^{(t)} = \sum_{i=1}^{n} [g_i f_t(x_i) + \frac{1}{2} h_i f_t^2(x_i)] + \frac{1}{2} \lambda \sum_{j=1}^{T} w_j^2 \quad (14)$$

which results in weighted squared losses with labels gi/hi and weights hi. Finding candidate splits for large values satisfying criteria are non-trivial.

Only internet-based assault phases are included in final attack trees of Figure 3. This is due to the fact that rational attackers would always choose most efficient techniques to compromise system components. Since, threats are identified in the context of MiniMax, and insider accounts compromises are less likely to succeed than internet-based assaults, they have been removed from trees. Nonetheless, this small example creates a broader attack tree than the image (only some of the tree pathways are shown). Many key instances can be missed when only one step ahead of the adversary is viewed. The number of attack steps to investigate in CSGs are parameters that can be customized. Unless systems are made up of exceptionally complex defensive limits, it will suffice most systems.

3.3.5 Calculating the Risk Score

The information required to generate the risk score using the attack tree generated by investigating pathways contains the equation (1). Each branch of the tree represents a different sort of assailant. If the attacker chooses that path, each leaf node in the tree represents the EVs (expected values) of losses while defending. EVs are sum of effects (losses) caused by compromises and likelihood of completing all processes required to accomplish compromises. Chain rules are applied to likelihood of completing branch's steps, providing likelihood stages completions. They are awarded to game defences for minimizing risks. Equation (2) can be used by defenders who need to concentrate on tree's worst risk cases as defences may lower total risks but oversee tree's worst-case risks (refer Equation (2)). A different defensive portfolio may be necessary to best guard against each risk equation.

3.3.6 Modeling Defender Approaches

CSGs require models of defense that can be used in order to analyze defender choices. Some of the defenses are aimed at lowering the chances of an incident succeeding. One of two methods is commonly used to do this. Protecting the

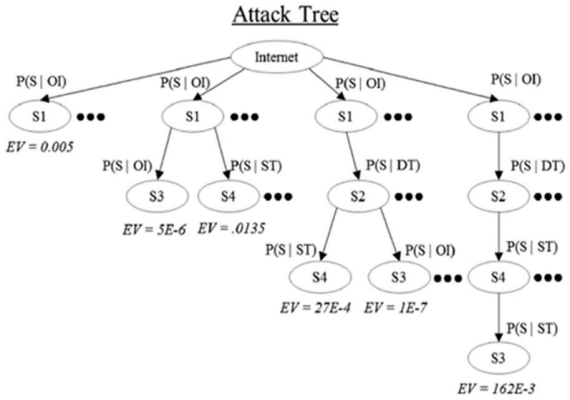

Figure 3. Topological Attack Graph Calculation for Risk Scoring Using MEGBDTs

cyber resources themselves is one option, while changing access is another. Each security approach necessitates an evaluation of how well it is projected to function in preventing certain cyber incident impacts. Redundant process paths with redundant servers are introduced as incidents affecting initial servers have zero effects. CSGs, on the other hand, will finally find the attacker scenario that compromises both servers since it searches many attacker steps ahead. However, according to the threat model, the chances of an adversary compromising both are fewer than the possibilities resulting in reduced mission risks. CSGs can also simulate defenses that are applicable throughout the entire assault lifecycle. Employee background checks, for example, may lower the likelihood of attackers gaining insider accesses, whereas response procedures can restore compromised components to their operational states in mission-compatible timeframes. The contents of new process iterations are dependent on prior iterations. As a result, only necessary changes that reflect changes in reality are required in subsequent iterations. This method substantially simplifies executing actions of recurrent iterations as only prior variables need to be updated. Hence, all Risk management process iterations can be compared and corresponding reports on factors created.

4. Results and Discussion

This section provides a condensed explanation of a system evaluation completed for a customer. A more extensive explanation of the concept is given in [25,26], which is implemented in JAVA. The following effect outcomes of cyber events were covered in this work: "Lost Customer CardRecord, "Merchant Loss of Customer Records," "Lost Purchase," "An Illegal Purchase," and "Multiple Illegal Purchases" are all examples of illegal purchases [26]. Ab example for assessments of losses in this work, consider the loss of a single customer record versus the loss of all

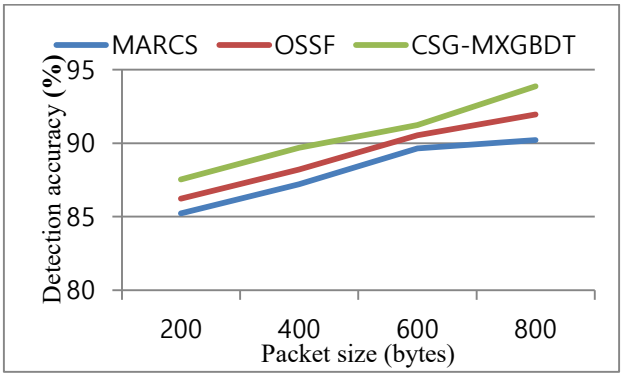

Figure 4. Detection Accuracy of the Proposed CSG-MXGBDT

customer data. The topology model is also straightforward to construct, requiring only a network diagram, knowledge about user access characteristics, and access rules.

Interacting with cyber security experts to capture their expectations on which event impacts a defense protects against is now required when modelling defensive techniques.

Based on Figure 4, it is identified that the proposed CSG-MXGBDT method has high detection accuracy as 93.87% for the packet size is 800 bytes than the existing MARCS and OSSF based techniques. Thus, the result explains that the proposed CSG-MXGBDT method is greater to the existing algorithms in terms of better detecting results with high accuracy rate.

Figure 5 shows the throughputs of the proposed CSG-MXGBDTs are better in terms of performance than existing methods. The proposed CSG-MXGBDTz produce higher throughputs. It concludes that the proposed method produces higher throughput when compared to the existing methods.

From Figure 6, it is identified that the proposed CSG-MXGBDT model has high risk reduction rate compared to the existing OSSF and MARCS methods. In this, the risk score is calculated with the help of MXGBDT. Finally, the proposed model has high performance results with the help of MLTs.

5. Conclusion

In this research, a cyber security game based on MLTs was proposed for Online Services Security. Its major purpose is to make internet security risk management easier for both providers and customers. The Framework proposed consists of the following components: Threat, risk, and risk management models The approach of the Framework starts with the identification of relevant danger circumstances based on defined threat scenarios. The process continues

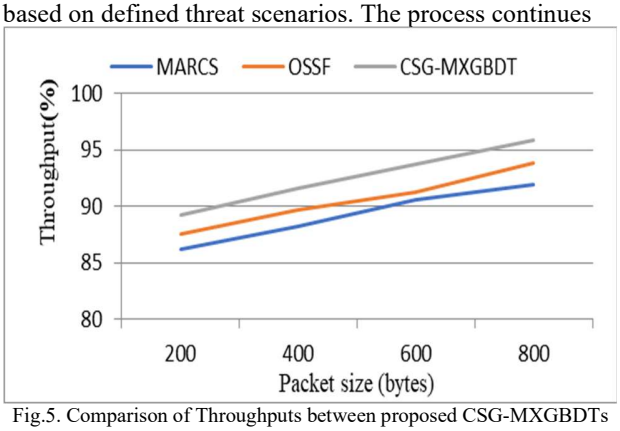

Fig.5. Comparison of Throughputs between proposed CSG-MXGBDTs and Existing Methods

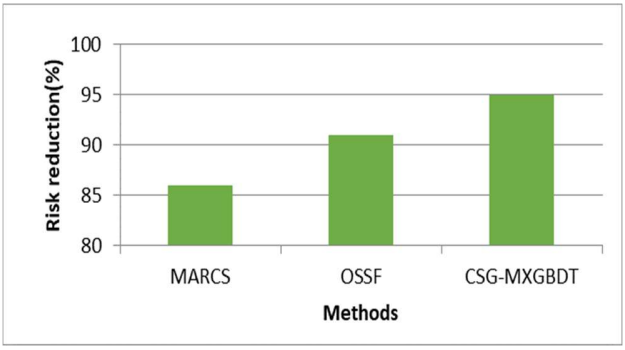

Figure 6. Risk reduction comparison between the proposed and existing methods

with the identification of specific threats and the connection of those risks to potentially impacted assets (such as online service components). Individual hazards are then recognized and addressed based on the specified task set. This technique allows for more effective risk management of complicated online services by concentrating on the most likely causes of unfavorable events and the responsibilities that contribute to risk treatment. CSGs use quantitative approaches to estimate the cyber risk of a mission system. Many data collecting procedures that occur during traditional risk assessments are formalized in CSGs into computer-readable artefacts that characterize the system (i.e., a system topology model and impact model). CSGs algorithmically encapsulate expert-level skills that employ these computable objects to provide a consistent, complete, and repeatable cyber risk assessment using MXGBDTs. Additionally, because CSGs explicitly capture computational artefacts, risk assessments may be rapidly revised if the system or missions change. A defender only needs to update the required CSGs and restart them to update the assessment. At the moment, it is unrealistic to expect CSGs to generate risk scores that are matched to reality. We explain how CSG-MXGBDT can be used to anticipate which defense techniques are most successful

and where they should be utilized in this study. When paired with a decision goal, CSG-MXGBDT may be used to determine if a set of defense measures accomplishes a decision objective (e.g., reduce risk by 70%) or a cost threshold (e.g., how much money to spend) (i.e., how much money to spend). The proposed Framework, as well as all of its components, were validated and tested in a real-world large-scale organizational scenario. All of the Framework's goals were met when it was first established. This effort will also focus on a budget-based framework with deep learning architecture.

Acknowledgment

The author would like to thank the Deanship of Scientific Research at Majmaah University for supporting this work.

References

[1] Sikkandar, Mohamed Yacin. "Design a Contactless Authentication System Using Hand Gestures Technique in COVID-19 Panic Situation." Annals of the Romanian Society for Cell Biology (2021): 2149-2159.

[2] Behera, Santosh K., Pradeep Kumar, Debi P. Dogra, and Partha P. Roy. "A Robust Biometric Authentication System for Handheld Electronic Devices by Intelligently Combining 3D Finger Motions and Cerebral Responses." IEEE Transactions on Consumer Electronics 67, no. 1 (2021): 58-67.

[3] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., &Xu, M. (2020). A survey on machine learning techniques for cyber security in the last decade. IEEE Access, 8, 222310-222354.

[4] Manshaei, M. H., Zhu, Q., Alpcan, T., Bacşar, T., &Hubaux, J. P. (2013). Game theory meets network security and privacy. ACM Computing Surveys (CSUR), 45(3), 1-39.

[5] Barreno, M., Nelson, B., Joseph, A. D., &Tygar, J. D. (2010). The security of machine learning. Machine Learning, 81(2), 121-148.

[6] Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2015, November). An investigation on cyber security threats and security models. In 2015 IEEE 2nd international conference on cyber security and cloud computing (pp. 307-311). IEEE.

[7] Kumar, V. (2005). Parallel and distributed computing for cybersecurity. IEEE Distributed Systems Online, 6(10).

[8] Martínez Torres, J., Iglesias Comesaña, C., &García-Nieto, P. J. (2019). Machine learning techniques applied to cybersecurity. International Journal of Machine Learning and Cybernetics, 10(10), 2823-2836.

[9] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., & Li, J. (2020). Performance comparison and current challenges of using machine learning techniques in cybersecurity. Energies, 13(10), 2509.

[10] Yavanoglu, O., &Aydos, M. (2017, December). A review on cyber security datasets for machine learning algorithms. In 2017 IEEE international conference on big data (big data) (pp. 2186-2193). IEEE.

[11] Ford, V., &Siraj, A. (2014, October). Applications of machine learning in cyber security. In Proceedings of the 27th International Conference on Computer Applications in Industry and Engineering (Vol. 118). Kota Kinabalu, Malaysia: IEEE Xplore.

[12] Soni, S., &Bhushan, B. (2019, July). Use of Machine Learning algorithms for designing efficient cyber security solutions. In 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT) (Vol. 1, pp. 1496-1501). IEEE.

[13] Rosenberg, I., Shabtai, A., Elovici, Y., &Rokach, L. (2021). Adversarial machine learning attacks and defense methods in the cyber security domain. ACM Computing Surveys (CSUR), 54(5), 1-36.

[14] Cruz, T., Rosa, L., Proença, J., Maglaras, L., Aubigny, M., Lev, L., ...&Simões, P. (2016). A cybersecurity detection framework for supervisory control and data acquisition systems. IEEE Transactions on Industrial Informatics, 12(6), 2236-2246.

[15] Jarjoui, S., &Murimi, R. (2021). A Framework for Enterprise Cybersecurity Risk Management. In Advances in Cybersecurity Management (pp. 139-161). Springer, Cham.

[16] Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. Journal of Cybersecurity, 6(1), tyaa005.

[17] Sivanathan, A., Gharakheili, H. H., &Sivaraman, V. (2020). Managing IoT cyber-security using programmable telemetry and machine learning. IEEE Transactions on Network and Service Management, 17(1), 60-74.

[18] Makawana, P. R., &Jhaveri, R. H. (2018). A bibliometric analysis of recent research on machine learning for cyber security. Intelligent communication and computational technologies, 213-226.

[19] Fernandez de Arroyabe, I., & Fernandez de Arroyabe, J. C. (2021). The severity and effects of Cyber-breaches in SMEs: a machine learning approach. Enterprise Information Systems, 1-27.

[20] El-Sofany, H. F. (2020). A New Cybersecurity Approach for Protecting Cloud Services against DDoS Attacks. International Journal of Intelligent Engineering and Systems, 13(2), 205-215.

[21] Mattina, B., Yeung, F., Hsu, A., Savoy, D., Tront, J., & Raymond, D. (2017, April). MARCS: mobile augmented reality for cybersecurity. In Proceedings of the 12th Annual Conference on Cyber and Information Security Research (pp. 1-4).

[22] Kure, H. I., Islam, S., &Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. Applied Sciences, 8(6), 898.

[23] Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2003). An integrated system theory of information security

management. Information Management & Computer Security.
[24] Meszaros, J., &Buchalcevova, A. (2017). Introducing OSSF: A framework for online service cybersecurity risk management. computers& security, 65, 300-313.
[25] Chen, T., He, T., Benesty, M., Khotilovich, V., Tang, Y., Cho, H., & Chen, K. (2015). Xgboost: extreme gradient boosting. R package version 0.4-2, 1(4), 1-4.
[26] Sheridan, R. P., Wang, W. M., Liaw, A., Ma, J., & Gifford, E. M. (2016). Extreme gradient boosting as a method for quantitative structure–activity relationships. Journal of chemical information and modeling, 56(12), 2353-2360.
[27] Turner, A. J., &Musman, S. (2018). Applying the cybersecurity game to a point-of-sale system. In Disciplinary Convergence in Systems Engineering Research (pp. 129-144). Springer, Cham.
[28] Musman, S., & Turner, A. (2018). A game theoretic approach to cyber security risk management. The Journal of DefenseModeling and Simulation, 15(2), 127-146.

TALAL ALHARBI received the master's degree in network security and system administration from the Rochester Institute of Technology (RIT), Rochester, NY, USA, and the Ph.D. degree in security of software defined networks from The University of Queensland (UQ), Brisbane, QLD, Australia. He is currently an Assistant Professor and the Vice Dean for Academic Affairs with the College of Computer and Information Sciences, Majmaah University, Al Majmaah, Saudi Arabia. Prior to this, he was the Vice Dean for Systems and E-Services with the IT Deanship. His research interests include computer networks, networks security, software defined networks, cyber security, and blockchain technology. He received two advanced certificates from RIT focused on network planning and design and information assurance.