Journal of Theoretical and Applied Information Technology
15th May 2024. Vol.102. No 9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

RISK ASSESSMENT THREAT MODELLING USING AN INTEGRATED FRAMEWORK TO ENHANCE SECURITY

P. SUBHASH[1], MOHAMMED QAYYUM[2], K. MEHERNADH[3], K. JEEVAN SAHIT[4], C. LIKHITHA VARSHA[5], M. NEVAN HARDEEP[6]

[1]Associate Professor, Department of CSE-(CyS, DS) and AI&DS, VNR VJIET, Hyderabad, Telangana, 500090, India

[2]Lecturer, Department of Computer Science Engineering, King Khalid University, Abha 61421, Saudi Arabia

[3-6]Student, Department of CSE-(CyS, DS) and AI&DS, VNR VJIET, Hyderabad, Telangana 500090, India

E-mail: [1]subhash.parimalla@gmail.com, [2]mgiwm@kku.edu.sa, [3]karumurimehernadh02@gmail.com, [4]jeevansahit025@gmail.com, [5]likhithavarsha555@gmail.com, [6]nonu.babulu@gmail.com

ABSTRACT

Today, in the digital world, the security of systems is crucial because, with continuous information exchange and huge quantities of data being processed, the protection of operation processes and data assets becomes paramount. Threat modeling is an important part of cybersecurity management methodology that looks for any possible threats or weaknesses that can break the system or endanger the environment. This paper is an attempt to analyze all the models of threat modeling by taking STRIDE, PASTA, DREAD, TREK, VAST and Attack Trees as references. An integrated model is suggested that combines the benefits of existing approaches, which includes the adoption of a comprehensive frame to deal with cyber threats. This methodology emphasizes iterative refinement and rigorous testing to ensure the effectiveness of threat mitigation strategies. By incorporating user-friendly web portals and the integration of new technologies, this framework enhances usability and addresses emerging threats. Overcoming the key issues in cybersecurity through integrated threat modeling is provided by combining approaches like STRIDE (security threat rating indicating, systemwide generic method), and PASTA (risk-focused, even in its extensive nature), DREAD, TREK, VAST and Attack Trees. This is due to the fact that the six methodologies and the ones that from Attack Trees offer a solution that is adaptable to various organizational contexts. An addition a unique triad is provided - asset-centric, attack-centric, and software-centric - to expand the protection coverage against the different kinds of threats and vulnerabilities. Proposed model Risk assessment threat modelling using an integrated framework to enhance security of action comprises the iterative revision and the exhaustive verification to guarantee the efficiency of prevention power. With the help of easy-to-use web portals and the integrated new technologies that make it all usable and design flexible, and timely as it faces new threats. Conducted on the basis of comparison; this analysis highlights the exclusive advantages of the design in the exact localization and mitigation of threats, achieving an accuracy of 94.2%. The integrated threat modeling framework that is presented in this essay represents a robust and dynamic approach toward cybersecurity, and it aims to improve the security and resilience of the system in the context of the continually changing threats in the cybersecurity world.

Keywords: *Threat Modelling, Integrated Framework, Iterative Refinement, Rigorous Testing, Web-portal*

1. INTRODUCTION

This As it is today, making the systems, computers, and data safe from hackers and such threats is a matter of great importance since they are preventing interruptions and protecting data that has a huge value. Against the backdrop of the threat and being armed with an arsenal of sophisticated tools and techniques, organizations in different sectors face such critical challenges. While these entities are not the same and face other threats, each one should develop purposeful defense strategies. Achieving the necessary environment of anticipating and handling these threats is an essence for effective cybersecurity, and therefore threat modeling is a critical part of this quest.

Threat modeling implicates a methodical procedure of studying and analyzing threats, vulnerabilities, and risks in a certain system or environment. By looking at the assets, the associated weaknesses, and the possible intrusion paths, organizations will be able to start addressing these security concerns and will also strengthen their defenses. The strategic planning model which falls within the framework comprises such steps as scoping and goal definition, threat identification, environment characterization, threat evaluation, their selection, and implementing evaluated solutions.

Many legacy threat modeling frameworks combine structure methodologies into one to make sure that the threat analyses performed in certain contexts are complete. STRIDE, for instance, categorizes threats into six distinct types: the types of attacks that cause spoofing, result in tampering, service DoS, denial of service, data exfiltration, and escalation. By delineating these threat categories, STRIDE provides valuable insights into potential attack vectors, aiding organizations in identifying and prioritizing security measures effectively.

As opposed to this PASTA a risk-based strategy takes up a direction that enhances the Know-how crashing business operations. Such a strategy paves the way for organizations to ensure that resources are distributed effectively by primarily concentrating on minimizing the effects of those risks that will probably cause the greatest disruption to the continuity of their operations. On the other hand, DREAD sticks to both a novel grading scenario and offers an evaluative framework that assesses threats according to Damage, Reproducibility, Exploitability, Affected users, and Discoverability. Threat modelling gains strength through digitalization with visualization techniques. VAST (Visualization and Sensory Training) improves comprehension and communication of threats and vulnerabilities. Ultimately, TRIKE brings together the aspects of attack trees with passengers under the general classification of transportation. Connecting these models into one form, there is a broad range of analyzing methods in threat discussing, which enable companies to reinforce the level of their cybersecurity reliably.

Common Threat Models

1.Asset-centric Perspective:

- An asset standpoint should form the fulcrum of the system, whereby a comprehensive inventory of assets and their order of importance should be prepared [1].
- Offer a wide range of rationales for the allocation of assets because the protection of high-value assets always comes first.

2.Attack-centric Perspective:

- They elaborate on different ways by which attackers gain access to the computer system and the methods they use for the purpose of exploitation [2].
- Ensures the advantageous environment of recognizing the adversary's attack techniques and plans and hence, the prompt rebuttal planning.

3.Software-centric Perspective:

- Magnifies existing software applications and systems deficiencies and misuses by exposing the developers and implementation of the possibility [3].
- Risk identification in software-related domains such as code errors, design flaws, and insecure configurations is the intended purpose of this activity.

The purpose of this work is to help in the improvement of the framework by conducting a well-ordered evaluation of currently existing modeling techniques and proposing a single all-inclusive model that combines their strengths and deals with their weaknesses simultaneously. The formulation and synthesis of different approaches such as their appropriateness to various contexts of any organization will lead to creation of a proposed framework that will provide dynamic and robust basis for effective management of cybersecurity.

The importance of our research addition lies in the building of the framework which puts the iterative refinement and strict testing to verify the workability in prevention of threats under consideration. Acceptance of user-friendly web portals and the use of existing technologies fulfill the usability as well as real-time threats by emerging technologies.

Our methodology is examined in a systematic literature review and comparative analysis where

we find common grounds and differences between currently used methodologies, pointing out their strengths and weaknesses. This triad, which we will designate as: Investigation, Testing, and Maintenance, will be used in order to enhance the protection coverage on different forms of threats and vulnerabilities

The objective of the study is not to cover thoroughly every detail of risk modeling however the framework is holistic and the model can be easily adopted to fit different kind of environments. The proposed Model, which focuses on collective effort, cyclic polishing up, and progressivism, is intended to facilitate cybersecurity management development, thus, enabling systems to be resilient in the face of the rapidly changing cyber threat environment.

Such a research project aims to score the highest marks in the threat modeling practices field, which is a rich source of existing methodologies, using them as a basis and adding to them a novel unlike anything seen before. An integrated threat model is proposed, which builds upon the strong points of already existing approaches and also eliminates their negative aspects. It will provide the challenge of cybersecurity from a holistic and adaptable view. The framework is designed iteratively to be regularly checked and tested so that organizations can strategically save on false alarms and predict, and deal with threats, effectively while enhancing their security stance in a continually changing threat atmosphere.

2. LITERATURE SURVEY

Many researchers, whose contribution has been instrumental in the foundation of the threat modeling practice, have been looking into the specific domains of the problem that have been pinpointed and working to fill up those gaps. For instance, while STRIDE, PASTA, and attack tree approaches are highlighted other advanced approaches are discovered, however, a combined methodology that pulls them from where they are good is created from them. Therefore, this framework looks into creating a platform for the improvement of the strengths of general threat modeling approaches while at the same time discarding their weaknesses - which in turn enhances the method for threat modeling in the real world.

The first method concentrates on increasing IT systems' robustness to cyber threats via the application of attack simulation toolkits together with developers' traditional methodology of danger modeling. This technique can be accomplished by building multiple attack scenarios and subsequently applying them to the specific system that is being examined thus, analysts are able to determine the vulnerabilities and possible consequences of different scenarios. But the fact is that this approach may require the developers to become specialists concerning the use of attack simulation tools, and the method's exactitude is entirely dependent on the quality and accuracy of the data that is given into the system, including any assumptions about the attackers' behavior and abilities [4].

The use of a security approach that fits perfectly into agile and DevSecOps approaches [5] is one of the methods that are embraced. This comprises a pragmatic risk modelling methodology specifically designed for the rapid development model and which allows security duties to being encompassed in the quick sprints. A general line that collaboration is often the key to development where security thinking cuts through the entire development process is portrayed. Security being the core design of systems is being executed at this point. This is a contradiction, though, tight deadlines might be insufficient to cover every authentication within it and the company has to bring up its technologies and culture along with the accelerating development of web security.

The researcher thoroughly and systematically digs into what such popularly used threat modeling tools provide. This assessment will be done on the parameter of whether the tool has the required capabilities, whether it is user-friendly or not, and to what level it can be integrated into development processes [6]. Even though tools examination could be dulled by the speed of change of threat mapping technologies currently exploding into the market effectiveness of it may vary from one organization to another based on their unique requirements.

The adaptation of the threat modeling existing frameworks for existing IoT devices addressed in one paper [7] is considered with the less processing power and communication protocols taken into further detail. Supported this with the cutting-edge development of the IoT to the point of obsolescence of areas that have been covered, leaving recommendations worthless.

A hybrid strategy is designed [8], which combines different threat modelling techniques that are appropriate for different activities. Comprising various approaches into a single threat model is the concept of the model - illustrating its application in a cloud solution case study. On the other hand, combining several methodologies may result in the need for complicated procedures.

The automation hybrid technique is suggested, which will adopt the most suitable methods according to the respective organizational function's needs. Constraints, for example, highly complex interactions inherent to the mixing of different methods; cost varies from time and workload and advanced equipment skills need are those which present the main limitations [9].

The STRIDE [10] threat model is renowned for its effectiveness in identifying and categorizing threats into six distinct types of attacks: masking, tampering, denial of service (DoS), data exfiltration (to alternative entities), service DoS, and escalation. Another factor, that contributes to its popularity, is its ability to identify critical systems, devices, and networks and ensure the protection of the same from possible attacks. Accomplishing this kind of input-based modelling, STRIDE makes it possible to see the security weaknesses allowing for preventive actions to be put into place and posture to be improved.

PASTA [11], which is an acronym for Pasteurise Attack Scenario and Stress Analysis Procedure, translates to a risk-focused procedure for threat modeling. First and foremost, giving a main focus to risk means PASTA will identify the specific risk factors that can potentially disrupt business operations. The addressing of IT infrastructure as a tool for achieving the goals of general business conduct implies the possibility of solving the issue of risk management accordingly. With risk assessment as its main principle, PASTA helps organizations direct their security processes from the viewpoint of business purposes successfully.

Attack trees [12] are useful graphical representations of how low-level attack activities of threats often interact and hence converge to achieve certain malicious objectives that are mostly harmful to victims. Reflecting the notions of roots symbolizing power and the branches down below covering subordinate activities, such trees are depicted as the framework for oppositional movements. In the form of a head node, the aim or goal of the attacker is specified at the base (root), whereas leaf nodes indicate particular activities the adversary is involved. Intermediate items represent the states or subgoals, while the AND/OR items indicate that certain activities are either in conjunction or in conflict with others. Frequently de-escalation is brought about by the attack which is after to be graver as one moves further up the tree. Performing visual risk analysis and identifying dependence and attack paths, attack trees make threat assessment comprehensive. They also play a vital role in developing up-to-date defense measures to prevent or reduce risks.

Honeypots [17] help us identify threats and vulnerabilities by studying all the actions performed by attackers in our server (honeypot). So, incorporating honeypots into the testing cycle of threat modeling will make it even more efficient. Additionally, organizations will also be able to deal with unknown threats through this integration.

The hybrid composite [18] methods will be exploited to bolster security against advanced and targeted cyber threats. In their work that was published in "Malware Detection", they proposed new techniques that can help in strengthening the cybersecurity and malware mitigation. Their approach combines various layers of defense which results in a really impeccable defense system against advanced cyber threats.

The discovery of a new technique for tailor-made detection of malware programs on web pages has been achieved by planting client honeypots [19]. By publishing their research in the "International Journal of Engineering Research and Applications," the authors have confirmed the fact that the security method that they have highlighted is effective enough to combat malevolent activities from the web-based sources. Through the use of client-side service in this approach, malware detection proficiency is surely enhanced; thus, the online security is guaranteed.

The approach focused on post-infection hacking activity breakdown [20], full information in the last Congress of International Information and Communication Technology. With their novel system architecture, the system can do expanded types of scrutiny on post-infection behaviors, thus allowing successful threat detection and reaction

mechanisms. Through behavior analytics, they increase situational awareness to strengthen cybersecurity settings and effectively deal with menacing threats that keep evolving.

Our modeling method will be set by the mixture of the previously mentioned approaches. They assist us in deleting the extraneous which we have in the different types of models. Thus, a complex and end-to-end risk model is developed that leads us to discover the threats that the software applications, assets and systems turn into by leaking in their vulnerabilities.

3. METHODOLOGY

3.1 Proposed Work

The integrated threat model's method is a multi-level approach developed to work on a system through and through. The process consists of three different cycles which every cycle plays a particular role of raising the system security.

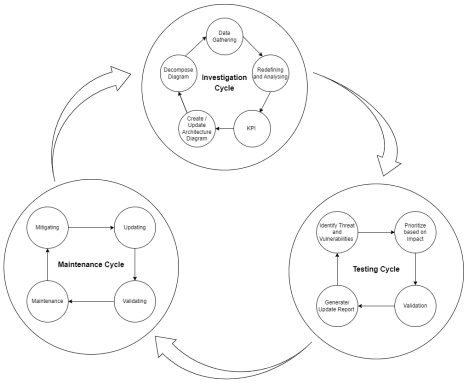

Figure 1: Proposed Integrated Threat Modeling Framework

The investigation phase of the Framework for threat modeling is the first critical step of our comprehensive project, where data is progressively collected and the complete data about the environment or system is reviewed. After that, the data is subjected to rigorous processing and analysis to find the meaningful pattern and trend applied for an effective understanding of the potential threat and vulnerabilities. Subsequently, the organization may have key performance indicators (KPIs), which serve as vital metrics to assess how well risk assessment and mitigation strategies have been implemented. These KPIs are the basis for designing structure and components representation, which is a visual diagram that clearly demonstrates how the whole system is created. This architecture diagram goes an iterative update and decomposed so that it can fit with the connections in the ongoing of understanding of threat sources and vulnerabilities, hence preparation to the following testing and maintenance phases of the framework.

Transitioning to the testing stage, the assets are carefully picked and investigated to discern the vulnerabilities they fall under the threat model. This part of the project is concerned with the confidentiality, integrity, and availability of the asset and each of them is dealt with through classification of data, design process, and adherence to best practices among others. The investigation goes further into the technological basis, including APIs, database tables, file storage systems, web hosting platforms, and other data repositories, which can all be examples of data inputs. Investigators ask whether the held data is confidential, integrated, or available (CIA), what risk could happen as a result of a data breach, who are the entities that the data, what methods are used to access it, and why it is kept. Languages that are being used within the program, such as JS, C, C++, HTML, JSON, Assembly, Python, P2P, etc., are included in the model in order to have a thorough knowledge of potential existing vulnerabilities. Then, in the execution phase, security procedures, such as user authentication, password encryption, and access restrictions, are thoughtfully built in rather than just being added as an afterthought, after the security problems and weaknesses have been identified. This step involves implementing strong authentication methods, such as Multi-Factor Authentication (MFA) and access control lists, embedded load balancers, firewalls, and so on. All security actions are made based on detailed specifications for the identified vulnerabilities that tend to appear during the investigation and testing phases so as to make it possible to choose the most appropriate steps to counteractively meet the threats. The top 25 vulnerabilities are precisely bordered by the Common Vulnerability Enumeration List (CVE) and each of them is examined in detail This is a combination of assessing the possible effects of threats on the system as well as

developing mitigating processes by customizing them. Considerations are developed focusing on program languages that may be found in the system (OS) and the particular security features that have been implemented in that system. Through this, organizations can utilize such findings for early action, operational strengthening of their security posturing, attack reduction, and resistance to attack.

The main aim of the maintenance phase is to permanently raise and retain the system security level. Besides responding to these threats promptly, addressing the newly discovered vulnerabilities and security have to be addressed in the right way. These frequent updates enable the security measures to be current and be ahead of the curve in terms of continually changing threats and technological advances. As well as that, penetration tests and inspections will be held on a regular basis to prove the effectiveness of the system in protecting the system. The maintenance mostly consists of repetitive operations that serves as the basis for detecting and fixing security flaws. Demonstration of these duties can be presented by analysis, audits, and system logs monitoring. Because of its interactive nature, it is possible to make changes to meet the new threats and vulnerabilities.

An integrated threat modeling risk assessment means an active rather than passive way to approach cybersecurity because this approach enables the organization to tackle and counter threats before they occur. Organizations should develop a risk assessment and mitigation system based on a development of a structured methodology covering an elaborate investigation, testing, and maintenance process to improve their security position. These components are constituted of series of processes that are continually reinforced and reorganized, which is imperative, considering the fact there are many cybersecurity threats and these are in a constant change every day.

The Figure 2 represents a structured security analysis process within an organization, consisting of three primary cycles: Investigation, Testing and Maintenance. It starts with the analyst logging into the system, followed by the Investigation Cycle, where data is gathered, analyzed, and redefined to update or create an architectural diagram which is then decomposed. Subsequently, the Testing Cycle commences, focusing on identifying threats or vulnerabilities, prioritizing these based on risk, generating or updating reports, and then validating these findings. The Maintenance Cycle involves mitigation of identified threats, validation of the mitigation measures, updating the system accordingly, and routine maintenance tasks. The process is iterative, with decision points after each cycle to determine whether additional work is required or if the process should be repeated, ensuring a continuous improvement approach to security analysis. At the end of the sequence, a review is conducted to evaluate the entire process for any new threats or changes, maintaining the integrity and security of the system in a dynamic threat landscape.

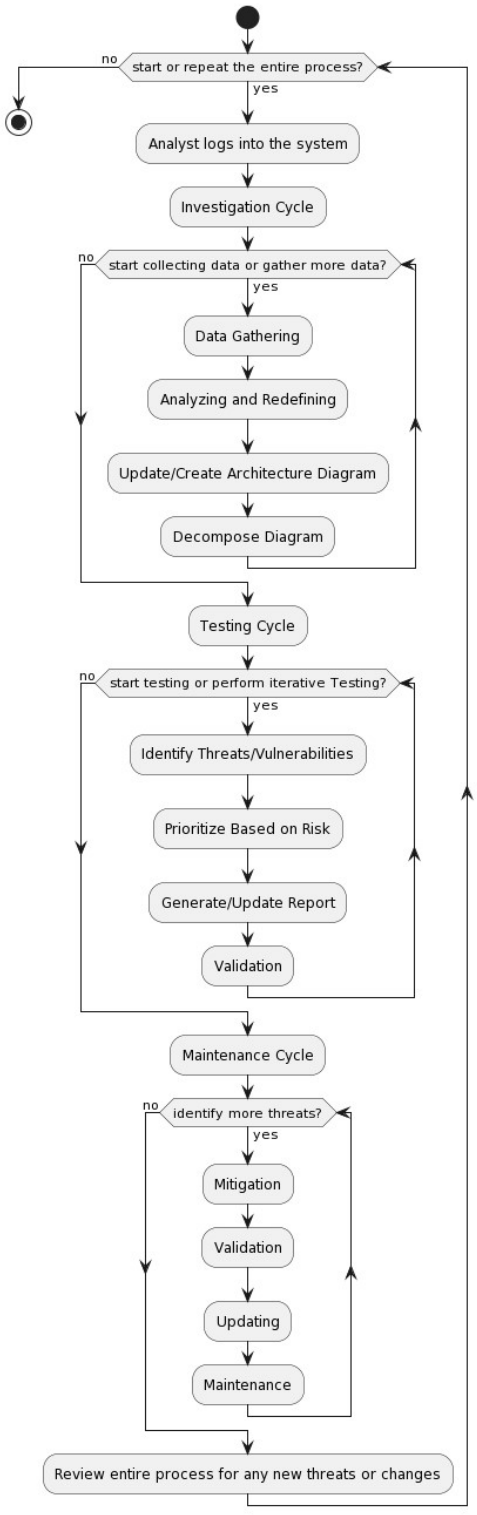

Figure 2: Control Flow Diagram of Integrated Threat Modeling Framework

3.2 Implementation

The implementation of the integrated threat model in the testing phase involves three major steps:

1. **ADDING A NEW THREAT MODEL**

Adding a new threat model to the system is the first stage in this process. It has operations like 'deleteThreatFromDB' that remove a threat model from the database and 'addThreatToDB' that adds the threat model to the database. The local application state is updated in accordance with the interactions managed by these functions with the database.

function addThreatToDB(name, SecurityFocus, onCloseDialog, user, setThreat, Threat):
// Add Threat to the Firestore database
// Update the local state with the new Threat
function deleteThreatFromDB(threatId, user, toast, navigate):
// Delete the model from the Firestore database
// Remove the model from the local state
// Navigate to the specified route

2. **ADDING TECHNOLOGIES TO THE MODEL**

Adding technologies to the threat model is the next step once it is created. Technologies can be added or removed from the threat model in the database using functions like 'removeTechFromDB' and 'addTechToDB' . The local application state is updated to reflect these changes using these functions, which also handle the addition and removal of technologies.

function addTechToDB(chips, tech, user, onClose, techStack, setTechStack, threatId):
// Add technology to the Firestore database
// Update the local state with the new technology
function removeTechFromDB(user, assetName, techName, allTech, setTech, threatId):
// Remove technology from the Firestore database

// Remove the technology from the local state

3. ADDING SECURITY DETAILS AND GENERATING RELATED THREATS

The last stage is to add security features and generate relevant threats after the threat model and technologies have been defined. The functions 'check_condition' and 'check_security_stack_does_not_contain_assets' evaluate conditions according to technology details and rules, respectively, and 'applyRulesToTech' applies security rules to the technology stack. These features ensure that the security mechanisms established for the system are strong and in accordance with the threats and vulnerabilities that were previously identified.

```
function check_condition(is_is_not_condition, rule_is_is_not, technology, data_type, is_condition):
// Check if the condition is met based on the rule and technology details
function check_security_stack_does_not_contain_assets(asset_to_find, tech):
// Check if the security stack does not contain specific assets function applyRulesToTech(rules, allTech, securityStack):
// Apply security rules to technology stack
// Return matched rule
```

4. RESULTS

The threat modeling is performed the same way as we framework as the guide to conduct the iterative assessments to see if the security solution is effective. Stats of accuracy have been done on several runs of the model and are depicted below as Figure 3. To this end, our examination has shown that the precision is steadily increasing. Precision increased from 78% to 83%, next to it 87%, and at the last stage reached 92% easing our way and achieving the goal. I admit that it was okay initially but the performance deteriorated after that and there were just marginal changes in the following versions which were called insignificant. Contrasting this, the proposed model achieved the accuracy of 94.2% at the seventh crop. Certainly, it led us to the truth that our way seems to work quickly at first but its impact is low when it is measured after a few repetitions. On this chip, the fourth iteration performance is responsible for and therefore the framework has successfully handled the major categories of security threats which finally lead to a good performance very close to perfect. An evaluation of our threat modelling framework was definitely performed at the last stage of the iterative refinement but it contributed to the gradual development of system security at all the points of mission execution.

Accordingly, our framework effectiveness was measured by comparing mitigations options generated versus already existing ones shown in Figure 4. In this instance our model turned out to be exceptional because it had a wide ample of 13 mitigation measures. This significantly surpassed the number of recommendations offered by other widely used frameworks: STRIDE (11), DREAD (9), PASTA (12), Attack Trees (7), TRIKE (9), and VAST (8). The findings of the scenario support the adequacy of our model to address security risks in their holistic approach. By developing a more effective shield with a higher number of mitigation recommendations, our framework will practically eliminate the risk of successful attacks. The outcomes of our established threat modelling framework not only prove the superiority of our approach but also demonstrate the practical applicability in the real-world security problems.

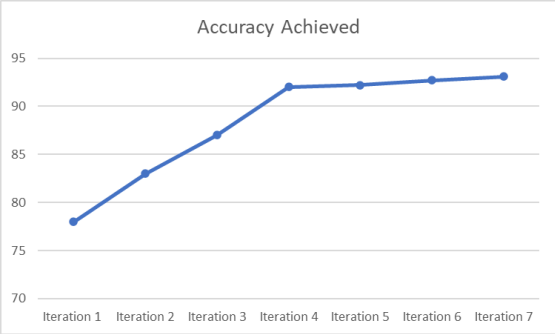

Figure 3: Accuracy Achieved In Successive Iterations

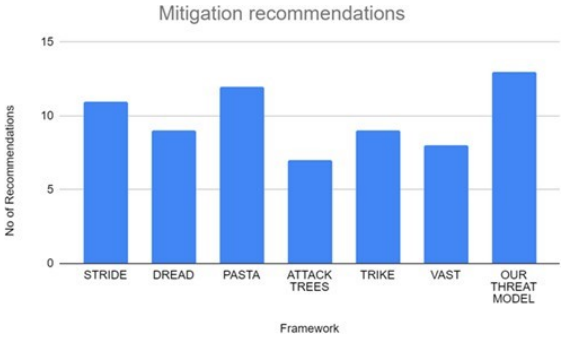

Figure 4: Number Of Mitigation Recommendations Suggested By Multiple Frameworks

Contrary to the middle of the road approaches which include just three or four parameters such as STRIDE, PASTA, Attack Trees, TRIKE, and VAST, our framework includes eight parameters as shown in Figure 5. The consideration of the system's interconnected nature that this approach affords facilitates an exhaustive risk assessment and detection of weaknesses within the system. Our framework account for many factors, hence it leads to a more complete and complex view of security. The aspect of the eight parameters is Confidentiality, Integrity, Availability, Authentication, Authorization, Non-Repudiation, Access control, and Assets, which refer to the technical, organizational, and environmental factors that need to be considered when securing information and assets. This empowers in more depth exploration of possible vulnerability channels and the possible consequences they cause to the entire system. Multiple factors being considered brings the advantages of; categorizing and also prioritizing threats. By looking at the threats from different perspectives, our approach compiles gaps or blind spots which could otherwise, not be spotted. Thus, organizations with limited resources can address the major risks first before using up all their sources on other threats.

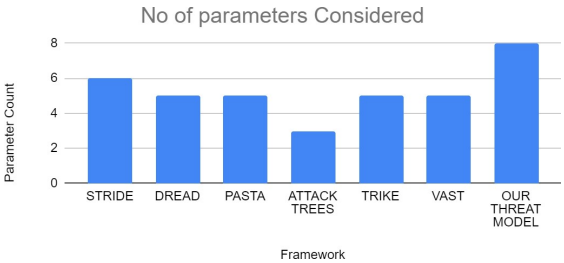

Figure 5: Number Of Parameters Considered By The Different Frameworks

Our framework reached 94.2% in its seventh iteration when tested on our local computing environment, as presented in figure 6. Concerning the results, the accuracy score of 92% significantly outperforms many other well-renowned frameworks, for instance, STRIDE (89%), DREAD (81%), PASTA (86%), Attack Trees (87%), TRIKE (83%), and VAST (74%). The great accuracy, in itself, is an embodiment of the efficiency and excellency of the framework that we have in place to determine and counter the existing network threats. Iterative method lies at the core of the proposed framework and ensures continuous refinement and betterment with time. The developed method of threat modeling and analysis can be adapted easily to different types of threats that arise in future and changing networks conditions the cyclic return leads to process of learning and improvement, which in turn hold the threat analysis, more accurate at each iteration.

The fact that our methodology did top the other frameworks which includes STRIDE (11), DREAD (7) PASTA (15), Attack Trees (10), TRIKE (5), and VAST (5) that is shown in figure 7 clearly reveals how powerful and progressive our proposal is. Through multi-factor analysis and in-depth exploration, our framework turns the inherited system defenses inside-out and exposes latent flaws. Part two, a mitigating phase appears in each iteration because as a result of that the identified vulnerabilities become less likely to be revealed overtime and we can be certain that we are building a more secure network. Stressed strategically the frameworks will secure the network through identifying and eliminating vulnerabilities which in turn will build the security culture within the organization teaching the need to be always updated and ever adaptable. After all, our framework which shows up the vulnerable areas fast and determines the most suitable measures of attempts to create secure and unwavering environment.

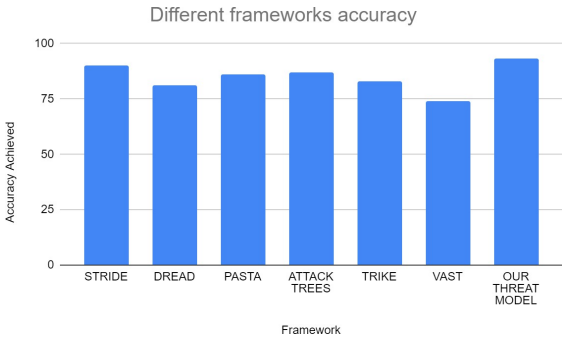

Figure 6: Accuracy Achieved By Different Threat Modeling Frameworks

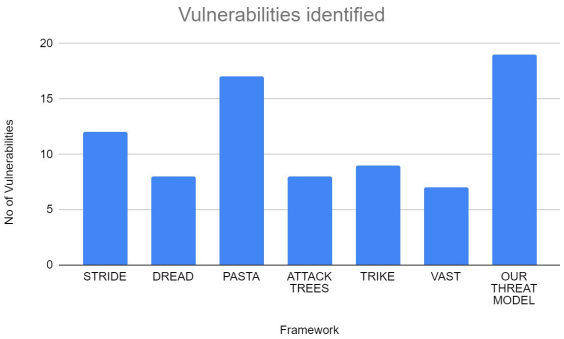

Figure 7: Number Of Vulnerabilities Identified By Different Threat Modelling Frameworks

5. CONCLUSION AND FUTURE SCOPE

Finally, we will return to the principles of human centering and scalability since they form the core of the suggested framework. From the very simple man's point of view, our approach is concise and has the direct application of pertinent solutions for problems concerning the security of the systems in the beginning, the framework will be tailored for small organizations and application, but a progressive design will raise security standards of systems on a system basis. Furthermore, our testing web portal helps the ease of use and accessibility and the users can carry out the threat modeling even if they do not know anything about the subject. Our strategy is based on new and advanced technology that is regularly updated together with the most efficient security measures. These are the issue of risks arising from the use of new technology.

The framework, in its current version, holds much potential for thorough perusal and planning within the whole upgrade and advancement programs. The main aim of this project is to widen the number of web portal modules being connected to the security and the technology stack, which gives a chance to serve needy applications and various industries. However, concentrating on critical vulnerabilities and dominating the threat space within the limitations of the portal will lead to better management of resources and more effectiveness in procedure. This final section should consist of the review of the framework to be compatible with incorporation to other organizations' digital ecosystem. It should provide a firm ground for the digital transformation of such companies.

The proposed framework presents an organizational, human-centered and scalable integrated threat modeling framework for cybersecurity that can be employed and applied in the offices of organizations irrespective of their sizes (small, and medium through possible modification also for larger entities). The halmark of the framework was to ensure it kept evolving for adaptability and scalability. Web-based interface giving the ability to run tests without having to be an expert becomes aforementioned tool allowing everybody to more easily run such tests. Exploiting new technology, the device foresees and counteracts cyber threats that are cropping up in the first place. Nevertheless, there are concerns about future risks and those concerned if the process is equipped enough, the framework should be updated more often and even security and privacy should be considered. Creation of joint efforts among different cybersecurity players is obligatory for obtaining a successful online environment. Further study should face with existing literature and adopt qualitative approaches to performance tracking. Above all, ethical issues and data privacy issues should be seriously considered.

In essence, our threat models method that is integral will offer a pro-active and dynamic cybersecurity solution, taking care of any negative scenario that may endanger the operations of the organization or any business type before it even happens. Our team aims to achieve it by continuous working on new and useful technologies and collaboration methods which are intended to help in improving the cybersecurity safety level and resilience through avoiding the immediate emergence of new cybersecurity threats and elimination of residual risks that keep being often ignored.

REFERENCES:

[1] Nweke, L. O., & Wolthusen, S. (2020). A review of asset-centric threat modelling approaches.

[2] Viswanathan, G. (2021, January). A hybrid threat model for system-centric and attack-centric for effective security design in SDLC. In Web Intelligence (Vol. 19, No. 1-2, pp. 1-11). IOS Press.

[3] Potteiger, B., Martins, G., & Koutsoukos, X. (2016, April). Software and attack centric integrated threat modeling for quantitative risk assessment. In Proceedings of the Symposium and Bootcamp on the Science of Security (pp. 99-108).

[4] Xiong, W. (2021). Enhancing IT Systems

Cyber Resilience through Threat Modeling : Cyber Security Analysis of Enterprise Systems and Connected Vehicles (PhD dissertation, KTH Royal Institute of Technology). Retrieved from https://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-300046

[5] Martelleur, J., & Hamza, A. (2022). Security Tools in DevSecOps : A Systematic Literature Review (Dissertation). Retrieved from https://urn.kb.se/resolve?urn=urn:nbn:se:lnu:diva-118400

[6] Yeng, P. K., D., S., & Yang, B. (2020). Comparative Analysis of Threat Modeling Methods for Cloud Computing towards Healthcare Security Practice. International Journal of Advanced Computer Science and Applications, 11(11).

[7] Liebl, Simon. (2023). Threat Modelling for Internet of Things Devices.

[8] Eng, D. (2017). Integrated Threat Modelling (Master's thesis, University of Oslo). Retrieved from http://hdl.handle.net/10852/55699

[9] Krishnan, Sriram. (2017). A Hybrid Approach to Threat Modelling A Hybrid Approach to Threat Modelling. 10.13140/RG.2.2.33303.88486.

[10] Lowe, H. J., Ferris, T. A., Hernandez, P. M., & Weber, S. C. (2009). STRIDE–An integrated standards-based translational research informatics platform. In AMIA annual symposium proceedings (Vol. 2009, p. 391). American Medical Informatics Association.

[11] Wolf, A., Simopoulos, D., D'Avino, L., & Schwaiger, P. (2021). The PASTA threat model implementation in the IoT development life cycle. INFORMATIK 2020.

[12] Saini, V., Duan, Q., & Paruchuri, V. (2008). Threat modeling using attack trees. Journal of Computing Sciences in Colleges, 23(4), 124-131.

[13] Tatam, M., Shanmugam, B., Azam, S., & Kannoorpatti, K. (2021, January). A review of threat modelling approaches for APT-style attacks. Heliyon, 7(1), e05969. https://doi.org/10.1016/j.heliyon.2021.e05969

[14] Shostack, A. (2014). Threat modeling: Designing for security. John Wiley & Sons.

[15] Parsons, D. (2024, February 26). ICS Layered Threat Modeling | SANS Institute. https://www.sans.org/white-papers/38770/

[16] Hutchins, Eric & Cloppert, Michael & Amin, Rohan. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Leading Issues in Information Warfare & Security Research. 1.

[17] Subhash, P., Qayyum, M., Likhitha Varsha, C., Mehernadh, K., Sruthi, J., & Nithin, A. (2023, October). A Security Framework for the Detection of Targeted Attacks Using Honeypot. In International Conference on Computer & Communication Technologies (pp. 183-192). Singapore: Springer Nature Singapore.

[18] Sidiroglou, S., & Keromytis, A. D. (2007). Composite Hybrid Techniques For Defending Against Targeted Attacks. In Malware Detection (pp. 213-229). Boston, MA: Springer US.

[19] Kaur, Supinder, and Harpreet Kaur. "Client honeypot based malware program detection embedded into web pages." International Journal of Engineering Research and Applications 3.6 (2013): 849-854.

[20] Kamati, Toivo Herman, Dharm Singh Jat, and Saurabh Chamotra. "Design and Development of System for Post-infection Attack Behavioral Analysis." Proceedings of Fifth International Congress on Information and Communication Technology: ICICT 2020, London, Volume 2. Singapore: Springer Singapore, 2020.