AMERICAN INTERNATIONAL UNIVERSITY-BANGLADESH

Faculty of Science and Technology

Assignment Cover Page

Assignment Title:	*Final Assignment*			
Date of Submission:	8 May 2024			
Course Title:	**Research Methodology**			
Course Code:	01540		Section:	D
Semester:	Spring	2023-24	Course Teacher:	**DR. MD. ABDULLAH-AL-JUBAIR**

Declaration and Statement of Authorship:

1. I/we hold a copy of this Assignment/Case-Study, which can be produced if the original is lost/damaged.
2. This Assignment/Case-Study is my/our original work and no part of it has been copied from any other student's work or from any other source except where due acknowledgment is made.
3. No part of this Assignment/Case-Study has been written for me/us by any other person except where such collaboration has been authorized by the concerned teacher and is acknowledged in the assignment.
4. I/we have not previously submitted or currently submitting this work for any other course/unit.
5. This work may be reproduced, communicated, compared, and archived to detect plagiarism.
6. I/we permit a copy of my/our marked work to be retained by the faculty for review and comparison, including review by external examiners.
7. I/we understand that plagiarism is the presentation of the work, idea, or creation of another person as though it is your own. It is a formofcheatingandisaveryseriousacademicoffencethatmayleadtoexpulsionfromtheUniversity. Plagiarized material can be drawn from, and presented in, written, graphic and visual form, including electronic data, and oral presentations. Plagiarism occurs when the origin of the arterial used is not appropriately cited.
8. I/we also understand that enabling plagiarism is the act of assisting or allowing another person to plagiarize or copy my/our work.

* *Student(s) must complete all details except the faculty use part.*
** Please submit all assignments to your course teacher or the office of the concerned teacher.

No	Name	ID	Program	Permit No
1	SHUVA SAHA	21-45469-3	BSc [CSE]	00603859775
2	SAAD, TOUHIDUL ISLAM	22-46996-1	BSc [CSE]	00603611775

Faculty use only

FACULTY COMMENTS	**Marks Obtained**	
	Total Marks	

1.Introduction:

Ransomware, a pernicious malware, poses a significant threat to organizations and individuals, extorting money through data hijacking [1]. This form of cyber extortion has surged in recent years, causing widespread financial and operational damage. The WannaCry attack of 2017 underscored its disruptive potential, affecting entities worldwide [2]. It exploited vulnerabilities in outdated systems, highlighting the urgent need for robust cybersecurity measures. To address this escalating threat, dynamic analysis methods have emerged as crucial tools in malware detection. Sandboxing environments offer controlled settings for studying ransomware behavior, aiding in the development of effective countermeasures [3]. Our research focuses on leveraging Support Vector Machines (SVMs) to enhance ransomware detection on Windows systems. By analyzing API calls and standardizing vector representations, our approach aims to improve detection accuracy and mitigate the impact of ransomware attacks [4]. Through experimentation using tools like Cuckoo Sandbox, we validate the efficacy of our method in real-world scenarios [5]. This contributes to the ongoing efforts to strengthen cybersecurity defenses against evolving cyber threats.

2.Background:

Ransomware has emerged as a significant threat to individuals, organizations, and critical infrastructure, causing financial losses and operational disruptions. It is crucial to develop effective strategies for mitigating the risks associated with ransomware attacks. This research proposal aims to investigate and propose innovative approaches for ransomware mitigation, focusing on technical solutions and best practices.

The proposed research will build upon existing knowledge and practices in ransomware mitigation to develop novel and effective strategies. The research will incorporate a comprehensive analysis of the current threat landscape, examining the evolution of ransomware techniques and the impact of recent attacks. By studying contemporary trends and attack vectors, the research will identify the vulnerabilities that ransomware exploits and the common weaknesses in existing mitigation approaches.

The research will leverage a combination of quantitative and qualitative methods to achieve its objectives. Data will be collected from multiple sources, including security incident reports, case studies, and interviews with experts in the field. To ensure a comprehensive understanding of the subject, the research will explore various dimensions of ransomware mitigation, including technical measures, employee education and awareness, incident response planning, and policy frameworks. The goal is to identify the most effective and practical strategies for organizations to prevent, detect, and respond to ransomware attacks.

The research proposal will also include a comparative analysis of existing ransomware mitigation solutions, evaluating their strengths, weaknesses, and applicability in different organizational contexts. This analysis will consider factors such as cost, ease of implementation, scalability, and compatibility with existing infrastructure.

3.Problem of Statement:

Ransomware attacks have become a significant and growing threat to individuals and organizations in recent years. Despite various efforts to prevent such attacks, ransomware attackers continue to find new ways to bypass prevention measures and cause harm. There is a clear need for more effective and reliable methods for detecting and preventing ransomware attacks.

This study aims to address the current gaps in the existing body of knowledge regarding ransomware detection and prevention. Specifically, this study will examine various aspects and perspectives of ransomware attacks, including the behavior of known ransomware strains, machine learning approaches, and security best practices. The existing body of literature has identified some key questions regarding ransomware detection and prevention, including:

- What are the most common behaviors associated with ransomware attacks, and how can these behaviors be detected and prevented?
- How effective are machine learning algorithms in detecting and preventing ransomware attacks?
- What are the best security practices for minimizing the risk of ransomware attacks?

While there is some existing research on these questions, there are still significant gaps in our understanding of how to effectively detect and prevent ransomware attacks. This study will aim to fill these gaps by conducting a comprehensive analysis of the existing literature, as well as by conducting new research to test various detection and prevention methods.

4.Objectives:

4.1. General Objective:

The study aims to investigate common ransomware entry points, vulnerabilities, and attacker tactics in organizations, proposing effective security measures and best practices. It also evaluates existing ransomware mitigation strategies, identifies integration opportunities for defense technologies, and suggests data recovery approaches to enhance organizational resilience.

4.2. Specific Objectives:

- Analyze known ransomware behavior to identify patterns for detection and prevention.
- Develop and compare machine learning models for effective ransomware detection and prevention.
- Identify and evaluate best security practices to mitigate ransomware risks and provide recommendations for enhancing existing detection and prevention measures.

5.Contribution of the Study:

This research proposal contributes to the field of cybersecurity in the following ways:

- Innovative Approach: Introducing a novel ransomware detection scheme utilizing support vector mechanisms (SVMs) for Microsoft Windows systems, enhancing existing methods with standardized vector representation models.
- Real-World Application: Exploring practical implementation of ransomware mitigation strategies, bridging the gap between theoretical research and tangible solutions through controlled environment experiments.
- Enhanced Security Measures: Improving the effectiveness of ransomware detection and prevention by analyzing known ransomware behaviors, developing machine learning models, and evaluating best security practices.
- Practical Recommendations: Providing actionable recommendations for improving existing ransomware detection and prevention measures, based on thorough analysis and experimentation with real-world data.
- Future Research Opportunities: Identifying avenues for further research and advancements in ransomware mitigation strategies, contributing to ongoing efforts to combat evolving cybersecurity threats.

6.Related Work:

In recent years, ransomware has become a significant threat to individuals and corporations. This review aims to identify effective practices for avoiding ransomware attacks and minimizing their impact. It explores various mitigation techniques such as the DAM framework, mini filter driver, and awareness initiatives. Additionally, it assesses ransomware attack mitigation strategies including Signature Based Detection, Host Based Defenses, and Firewall and malware defenses. The study also considers challenges in implementing these methods, such as cost and complexity, with the goal of providing readers a comprehensive understanding of effective ransomware prevention and mitigation strategies.

Kapoor, Gupta, Gupta, Tanwar, Sharma, and Davidson et al. [6] stress the necessity of regular software updates, caution with emails, disabling unsafe scripts in browsers, and enabling controlled folder access, while acknowledging the difficulties in devising generic detection solutions for diverse ransomware types. Joshi, Mahajan, Joshi, Gupta, and Agarkar [7] propose a signature-less detection method using a mini-filter driver that analyzes I/O requests, combined with Shannon's entropy and fuzzy hashing for enhanced security that's challenging to circumvent. Shinde, Veeken, Schooten, and Berg [9] point out the low awareness of ransomware threats, particularly among older populations, and suggest that while current mitigation strategies are adequate, their utilization is suboptimal. Alshaikh, Ramadan, and Hefny [10] recommend identifying ransomware behavioral patterns and maintaining offline backups to mitigate infection impacts, also highlighting the shortcomings of signature-based detection due to potential misclassification errors. Rehman, Hazarika, and Chetia [11] claim that a majority of malware originates from reputable sites and suggest adopting a multilayered web defense strategy to protect against increasingly complex threats. This summary encapsulates these contributions to guide readers toward a comprehensive understanding of the current landscape in ransomware prevention and mitigation.

7.Research Methodology in Flowchart:

Here is the proposed research methodology in the flowchart:

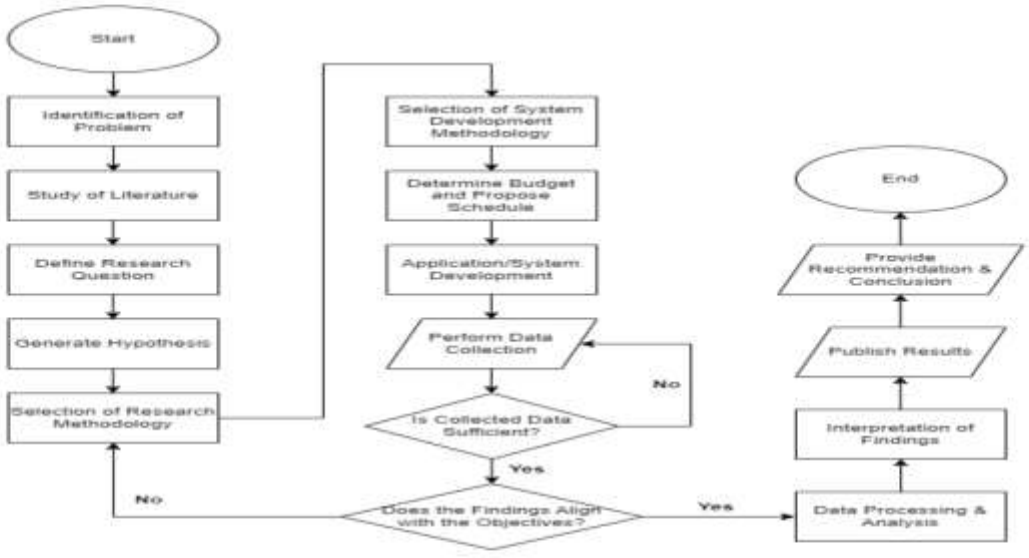

Start
Identification of Problem
Study of Literature
Define Research Question
Generate Hypothesis
Selection of Research Methodology
Selection of System Development Methodology
Determine Budget and Propose Schedule
Application/System Development
Perform Data Collection
Is Collected Data Sufficient?
No
Yes
No
Does the Findings Align with the Objectives?
Yes
Data Processing & Analysis
Interpretation of Findings
Publish Results
Provide Recommendation & Conclusion
End

Fig - 1: Flowchart of Research Methodology

8.System Development Methodology:

There are several system development methodologies available and for this research will use Extreme Programming (XP). Extreme Programming (XP) is a widely used software development model. It is an agile methodology that provides quality products and a chance to respond to ever-changing client needs [12]. It is a combination of iterative and incremental process models. XP is considered for a short-duration project as work happens in short iterations and can last from one to three weeks [13]. In this research, an outcome is required in a short amount of time and XP programming provides these facilities. Based on the short outcomes feedback can be taken and then the system can be improved. To apply XP, there are 12 practices to follow and those are:

- Practice 1: The Planning
- Practice 2: Small Releases
- Practice 3: System Metaphor
- Practice 4: Simple Design
- Practice 5: Continuous Testing
- Practice 6: Refactoring
- Practice 7: Pair Programming
- Practice 8: Collective Code Ownership
- Practice 9: Continuous Integration and Daily Build
- Practice 10: 40-Hour Work Week
- Practice 11: On-Site Customer
- Practice 12: Coding Standard

The reasons for selecting this model because:

Rapid Iterations: XP emphasizes short development cycles and frequent releases, allowing for quick adaptation to emerge ransomware threats and continuous improvement of mitigation strategies.

Customer Involvement: XP encourages close collaboration with stakeholders, including security experts and end-users, ensuring that the developed mitigation strategies are practical, effective, and aligned with organizational needs.

Continuous Testing: XP promotes automated testing throughout the development process, ensuring the reliability and robustness of ransomware detection and prevention mechanisms.

9.Budget and Schedule:

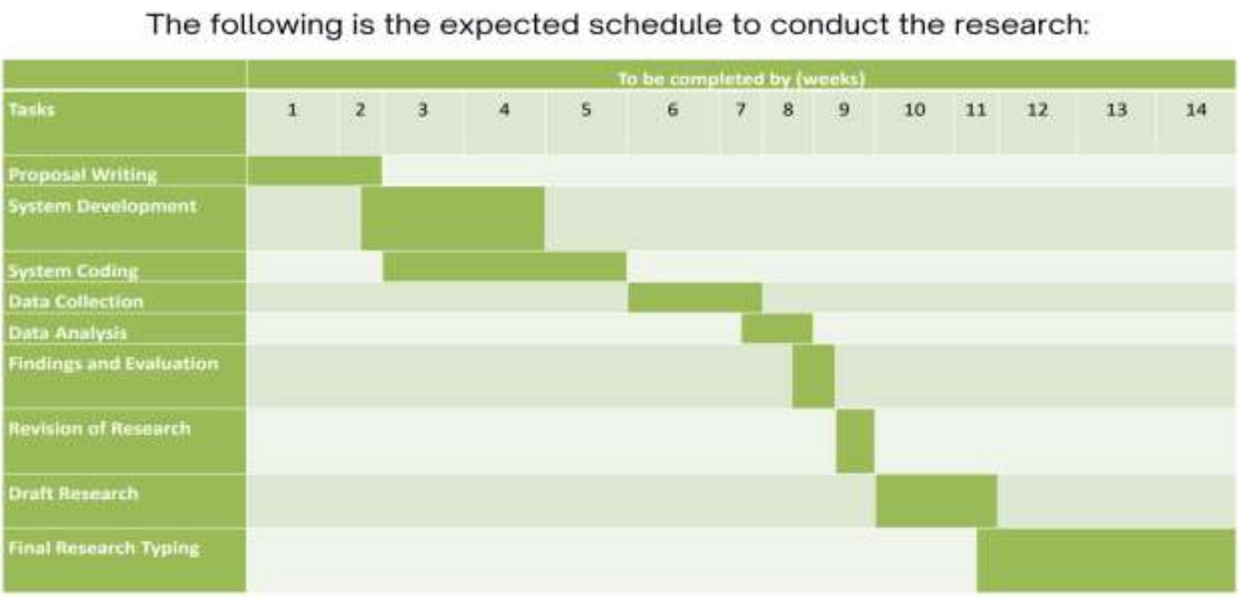
To perform the following research, a budget can be proposed as follows:

Table-1: Proposed Budget of Research

Budget Category	Budget Type	Cost
Computer Hardware & Software	Ransomware analysis tools, sandboxing tools	$7500
Equipment & Technology	Network monitoring tools	$5,000
	High-performance computing cluster (optional)	$20000+
Cloud Storage Costs	Storage for research data	$2,000
Data Processing Tools	Data analysis software	$3,000
Travel & Accommodation	Conference travel	$2,000
	Workshops	$2,000
Miscellaneous	Salary for research assistant (1 year)	$4,500
	Printing and supplies	$1,000
	Contingency funds	$10,000
Grand Total		$48,000

To perform the whole research, an appropriately distributed schedule is necessary. Maintaining this schedule would be crucial for all the researchers involved in the project. Here is the proposed schedule to perform our research:

Table – 2: Project Schedule in Gantt Chart



The following is the expected schedule to conduct the research:

	To be completed by (weeks)													
Tasks	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Proposal Writing	🟩	🟩												
System Development		🟩	🟩	🟩										
System Coding			🟩	🟩	🟩									
Data Collection						🟩	🟩							
Data Analysis							🟩	🟩						
Findings and Evaluation								🟩	🟩					
Revision of Research									🟩					
Draft Research										🟩	🟩			
Final Research Typing											🟩	🟩	🟩	🟩

10.Data Collection Method:

The chosen data collection method for this research is the quantitative method and the quantitative method includes the given methods:

Surveys: Conducting surveys can help collect data on the prevalence of ransomware attacks in a particular industry or organization, the types of attacks that are most common

Interviews: Interviewing IT professionals or security experts can provide more in-depth information on the specific ransomware threats they have encountered

Observations: Observing the security measures that organizations have in place to mitigate the risk of ransomware attacks can help identify common vulnerabilities and areas where additional measures may be needed.

Experiments: Conducting controlled tests, like those in Cuckoo Sandbox, enables observation of ransomware behavior, aiding in the evaluation of detection and mitigation strategies in practical settings.

11.Significance of a study:

The significance of a study on mitigating the risk of ransomware attacks lies in its potential to address a critical issue that affects businesses, organizations, and individuals worldwide. Ransomware attacks have become increasingly common and sophisticated, causing significant financial losses and disrupting operations. By exploring ways to mitigate the risk of ransomware attacks, the study can help organizations develop more effective strategies and tools to protect their systems and data.

Additionally, the study can contribute to the broader body of knowledge on cybersecurity, particularly in the context of ransomware attacks. It can shed light on the current state of ransomware attacks, their impact, and the challenges organizations face in preventing them. The findings can inform policy and decision-making, as well as guide future research in the field.

Overall, the study on mitigating the risk of ransomware attacks is significant as it can help reduce the negative impact of ransomware attacks on organizations and individuals, enhance cybersecurity, and contribute to the advancement of knowledge in the field.

12.References:

1. Alshaikh, M. A., Ramadan, R. A., & Hefny, H. Y. (2020). Ransomware prevention and mitigation techniques. International Journal of Computer Applications, 178(13), 23–28.
2. Chesti, I. A., Humayun, M., Sama, N. U., & Jhanjhi, N. (2020). Evolution, mitigation, and prevention of ransomware. In 2020 2nd International Conference on Computer and Information Sciences (ICCIS) (pp. 1-6). IEEE.

3. Colonial Pipeline paid hackers $5 million in ransom. (2021, June 8). The New York Times. https://www.nytimes.com/video/us/100000007803121/colonial-pipeline-ransom-justice-department.html
4. Cuckoo Foundation. (n.d.). Cuckoo Sandbox - Automated Malware Analysis. https://cuckoosandbox.org/
5. Cybersecurity Ventures. (2021, August 9). Ransomware damages to hit $265 billion by 2031. [https://cybersecurityventures.com/ransomware-damages-to-hit-265-billion-by-2031]
6. Firdausi, I., Erwin, A., Nugroho, A. S., et al. (2010). Analysis of machine learning techniques used in behavior-based malware detection. In Advances in Computing, Control and Telecommunication Technologies (pp. 201–203). IEEE.
7. Joshi, Y. S., Mahajan, H., Joshi, S. N., Gupta, K. P., & Agarkar, A. A. (2021). Signature-less ransomware detection and mitigation. In Advances in Intelligent Systems and Computing (pp. 299–306). Springer.
8. Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2021). Ransomware detection, avoidance, and mitigation scheme: A review and future directions. MDPI.
9. Moser, A., Kruegel, C., & Kirda, E. (2007). Limits of static analysis for malware detection. In Computer Security Applications Conference (pp. 421–430). IEEE.
10. Rehman, M. A., Hazarika, S. M., & Chetia, M. (2011). Malware threats and mitigation strategies. Journal of Theoretical and Applied Information Technology, 21(1), 74-80.
11. Rieck, K., Trinius, P., Willems, C., & Holz, T. (2011). Dynamic analysis of unknown viruses with Cuckoo Sandbox. Journal of Computer Security, 19(4), 639-668.
12. Scaife, N., Carter, H., Traynor, P., & Butler, K. R. B. (2016). CryptoString (and drop it): Stopping ransomware attacks on user data. In International Conference on Distributed Computing Systems (pp. 303–312). IEEE.
13. Shinde, S., Veeken, A., van Schooten, B., & Berg, H. W. (2016). Ransomware: Studying transfer and mitigation. In 2016 International Conference on Computing, Analytics and Security Trends (CAST) (pp. 353-358). IEEE.
14. Vinod, P., Laxmi, V., Gaur, M., & Rajasthan Jaipur, V. (2009). Survey on malware detection methods. In 3rd Hacker's Workshop on Computer and Internet Security (pp. 74–79).