In recent years, ransomware has emerged as a common danger to both people and corporations. It is a form of malware that encrypts the data of a victim and demands money in return for the key to unlock them. Attacks using ransomware have resulted in large financial losses, halted commercial activities, and compromised private data. The development of efficient preventive and mitigation strategies is essential to lessen the impact of ransomware attacks as their complexity and frequency rise. An overview of the most recent findings in the field of ransomware prevention and mitigation is given in this review of the relevant literature. The goal of the review is to determine the best practices for avoiding ransomware attacks and lessening their effects when they do happen. The review starts out by looking at the many technique to mitigation of ransomware and their process, including DAM framework and mini filter driver, awareness, The research also looks at the various ransomware attack mitigation strategies that are accessible to enterprises like Signature Based Detection, Host Based Defenses, Firewall and malware defenses. They consist of ransomware-specific decryption tools, incident response strategies, and data backups.

The literature study also looks at the difficulties in putting these methods into practice, such as the expense and complexity of preventative and mitigation plans. Ultimately, the goal of the literature study is to give readers a thorough grasp of the various preventative and mitigation strategies for ransomware attacks.By examining the current research, it aims to identify the most effective strategies for organizations to protect themselves against this growing threat.

-------------------------------------------------------------------------------------------------------------

To prevent ransomware , according to Kapoor, Gupta, Gupta, Tanwar, Sharma and Davidson et al. [1] proposed the DAM framework to classify potential defense techniques, tools and strategies for countering the menace of Ransomware. They found that detection are created mostly to detect a single or a single type of ransomware, so generic solutions do not exist as they are extreamly challenging to develop. So , they suggests some key points .. which are Regular Patches and Updates, Avoid e-Mails from unknown sources and attachments, Disable JavaScript and Java for Browsers ,Controlled Folder Access .

The DAM framework evaluates different combat strategies for preventing ransomware attacks and widespread financial losses.

Signature-less ransomware detection and mitigation is also proposed by Joshi, Mahajan,Joshi, Gupta and Agarkar [2] They proposed that a mini filter driver that allow then to analysis the Input Output request to the file system driver . The mini-filter driver is deployed at a certain altitude such that it has access to most of the objects of the operating system. This detection technique is robust because, to bypass the security of the mini-filter driver, a new mini-filter driver needs to be developed and deployed whose altitude needs to be equal to or less than the proposed mini-filter driver. The implementation of the signature-less technique is done by combining the working of Shannon’s entropy and fuzzy hash.

Chesti, Sama, Humayun and Jhanjhi [3] discussed about how to dealing with infected machine. As, Ransomware is a dangerous thing and dealing with it is

complex as well as expensive. Due to ransomware, a person is restricted to use hisdevice even if a backup is available still it will take 2 to 3 weeks to restore data back and during this time the businesses have to face a major loss. So, They Suggest some step like, Separate the infection, Identify the infection, Report about the infection, Determine the best option, Restore and refresh the device, Plan to protect the device against the reoccurrence of

ransomware.

Shinde, Veeken, Schooten and Berg [4] they suggest that Transformation of ransomware has become pretty easy with growing Internet. They found that Awareness of ransomware is incredibly low, especially of older persons . Nearly all victims are unwilling or unable to pay the ransom. They have given the solution that Existing mitigation strategies generally work well enough, but too few people make use of them. But They did not do the proper research on several ways of mitigating ransomware they discussed previously like: Off-side backups, capable anti-virus software and user training

Alshaikh, Ramadan and Hefny [5] they have found that many Ransomware families exhibit similar characteristics. They have suggested that availability of offline backup will mitigate the impact of ransomware infection. They also suggest to Identify the ransomware behavioural pattern. Their research paper demonstrates the limitation of signature-based detection methods, and emphasize the behaviour-based detection mechanism capability to detect crypto ransomware. But They didn’t suggest a specific solution to prevent or detect ransomware infection and Misclassification may happen due to decision boundary errors.

Malware threat and mitigation strategies are discussed by Rehman, Hazarika and Chetia [6]. They Claimed That 70% of the malware comes from popular sites. Discussed About latest Mitigation strategies like Signature Based Detection, Host Based Defenses, Firewall and malware defenses. They Have Suggested to Adopt a multilayer Web defence strategy that can protect users and networks from increasingly sophisticated threats.

# **[1]** Kapoor, A. , Gupta, A. , Gupta, R. , Tanwar, S. , Sharma, G. and Davidson, I. E.,Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions. MDPI (2021)

[2] Joshi, Y. S. , Mahajan, H. ,Joshi, S. N. , Gupta, K. P. and Agarkar, A. A., Signature-less ransomware detection and mitigation . Springer (2021)299–306

[3] Chesti, I. A. , Sama, N. U. , Humayun M. and Jhanjhi, NZ. , Evolution, Mitigation, and Prevention of Ransomware . 2nd International Conference on Computer and Information Sciences (ICCIS), 2020

[4] Shinde, R. , Veeken, P.V.D. , Schooten, S.V. , and Berg, J.V.D., Ransomware: Studying Transfer and Mitigation . 2016 International Conference on Computing, Analytics and Security Trends (CAST), 2016

[5] Alshaikh, H. , Ramadan, R. , and Hefny, H.A., Ransomware Prevention and Mitigation Techniques . International Journal of Computer Applications ,2020

[6] Rehman, R. , Hazarika, G.C. , and Chetia, G. , Malware Threats AND Mitigation Strategies. Journal of Theoretical and Applied Information Technology, 2011