International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7673
***Article Received**: 25 April 2023 **Revised:** 22 June 2023 **Accepted:** 09 July 2023*

Implementation of Decoy Deception based Detection System for Ransomware Attack

Mangesh D. Salunke[1], Subhash G. Rathod[2], Hemantkumar B. Jadhav[3], Meghna Yashwante [4], Vaibhav D. Rewaskar[5], Pranjali V. Deshmukh[6]

[1]Associate Professor,
Marathwada Mitra Mandal's Institute of Technology, Lohgaon, Pune,
Salunkemangesh019@gmail.com
[2]Assistant Professor,
Marathwada Mitra Mandal's Institute of Technology, Lohgaon, Pune
subhashrathod@gmail.com
[3]Associate Profeesor,
Adsul's Technical campus, Ahmednagar
[4]Assistant Professor,
Marathwada Mitra Mandal's Institute of Technology, Lohgaon, Pune
meghna@gmail.com
[5]Assistant Professor,
Marathwada Mitra Mandal's Institute of Technology, Lohgaon, Pune
vdrewaskar@gmail.com
[6]Assistant Professor,
Marathwada Mitra Mandal's Institute of Technology, Lohgaon, Pune
deshmukhpranjali26@gmail.com

Abstract— Ransomware poses a dangerous threat to cybersecurity. Data as well as rights owned by the user are adversely impacted. The situation has become considerably more critical as a result of the emergence of new ransomware varieties and Ransomware-as-a-Service. In this paper, we presented a novel deception-based and behaviour-based method for real-time ransomware detection. In order to avoid any loss before ransomware is discovered, we build pretend files and directories for nefarious behaviours. We conducted a pilot study using Locky, and the results demonstrate the effectiveness of our strategy with little system resource usage and geographical cost.

Keywords- Information security, Ransomware, Decoy deception, Network attacks, Attack detection systems, Cryptographic attack.

I. INTRODUCTION

Since the 1990s, researchers have been studying deception mechanisms. They are attempting to create detection warning technologies that would find any unauthorised access to servers or other crucial systems. After Wiki Leaks made a significant number of US federal and government information available to the public, deception methods grew, which led to a new security necessity to safeguard the data. This is especially true now that the market for ransomware virus has increased among cybercriminals.[1]

It should be emphasized that conventional intrusion detection systems (IDS) as well as firewalls are not adequate defensive structures against modern sophisticated ransomware and a threat approaches to safeguard your endpoints. As a result, a more complex model with more levels than just conventional Honeypot, honey tokens, and honey files is required. In order to identify any anomalous access, honey files were first introduced in and employ fake resources. Additionally, Honeypot were utilized in to find ransomware. [2].

The methodology used by ransomware to encrypt data has been developed for over twenty-five years, and it is always becoming better. Modern ransomware employs difficult-to crack asymmetric encryption techniques. In addition to taking the user's system's private data, ransomware typically encrypts the data so that the user can no longer access it. The user is then required to pay certain money as a ransom to get the key for decryption. The attacker does not give the user the decryption key if the user refuses to pay the ransom in accordance with attacker's directions. The file or data is unable to recover without the proper decryption key. In other instances, the attacker failed to send the decryption key even after the victim paid the ransom in accordance with the attacker's directions. There have also been instances of the same ransomware repeating its ransom.[3]

The Honeypot mechanism, which tempts attackers or harmful programmers' to attack the Honeypot system, is a deception

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7673
***Article Received**: 25 April 2023 **Revised:** 22 June 2023 **Accepted:** 09 July 2023*

technique frequently used to detect network infiltration. This approach has demonstrated excellent performance alongside can successfully lessen or stop attacks on the server. Counterfeit file is inserted to detect the ransomware based on the features of the Windows operating system. When ransomware damages the Honeypot file used as attraction, it instantly shuts down the machine to stop it from encrypting and deleting files, which can protect the user's data to the fullest extent possible and minimize losses. [4]

The discipline of secure network operations uses incident detection mechanisms extensively since they are both widely used and extremely helpful. By observing networks or infrastructure, which are additionally referred to as systems for intrusion detection, a system for identification or detection of attacks platform enables us or the system's user to notice inappropriate behaviors which may be potential of harm either through an a passive or active way. The best way to categories the detection strategy is by the way it is implemented, albeit there are many other approaches, strategies, and methodologies accessible. Anomaly-based detection as well as Signature-based detection is two distinct strategies that are accessible for detection procedures. Any method can be used to construct or build a detection system for protecting the network of your computers or individual systems of computers against hostile activity.

Figure 1 shows the category approaches for detection the network attack, two ways for detecting cyber attack are anomaly based detection and signature based detection

Figure 1: Attack Detection approach

In the present study, we develop the Ransomware Detection System framework which enables us recognize any un-authorized intrusion to system servers (documents as well as files) as well as network technology. The model is capable of finding ransomware on any server and alerting the network administrator or security measures.

Structure of Paper the rest of this paper is organized as follows: The associated work for ransomware and intrusion detection is covered in Section 2 along with servers, honey tokens/ files, and decoy resources. Section 3, Architecture of the Ransomware and Intrusion Detection System (RIDS). The RIDS system design and experiment results are described in Section 4. And in Section 5 Conclusions and future Work.

II. RELEATED WORKS

Sajad Homayoun et.al. (2017), suggested a system that distinguishes between Ransomware and benign apps using a sequential pattern matching technique. uses 3 ransomware variants, including LockyRansom (517 samples), CerberRansom (535 samples), and TeslaCryptRansom (572 samples), and uses the J48, MLP,

bagging, and Random Forest classification methods to detect Goodware with 99% accuracy and Ransomware with 96.5% accuracy in less than 10 seconds. [5]

Eugene Kolodenker et.al. (2017), outlines the PayBreak method, which was tested with 170 ransomware variants from 20 current families of ransomware that were gathered by employing RADDAR, or “Real-time Automation to Discover, Detect, and Alert of Ransomware”, to eliminate the danger of Crypto-based-ransomware on Windows PC Platform. Obtainable via VirusTotal Intelligence, Malc0de,

and VXVault, these 12 ransomware families can decrypt data, and they can also recover decrypted data. [6]

Monika et.al. (2016), Examine the characteristics of the ransomware assault and how they have changed. Various Ransomware samples are examined using the PEiD tool on the Windows (17 families) and Android (8 families) platforms. And the outcome demonstrates that while ransomware families utilize various payloads, they all function similarly. Additionally, it is feasible to identify ransomware on the Windows platform by analyzing unusual disk and registry behavior. [7]

Juan A. Herrera Silva et.al. (2017), analyzes unstructured data gathered from EcuCERT logs using a machine learning algorithm on the Windows platform to construct a model for Ransomware prevention and detection. These logs aid in choosing the attack

determining qualities. These logs are produced using a machine learning method by identifying treat behavior while maintaining cognitive security. [8]

Aaron Zimba et.al. (2017), leverages the most prevalent infection channel for ransomware attacks, such as spam emails, to construct a system for ransomware enables to employs Bayesian network statistics for detection or proof of the most poular sort of ransomware assault contamination. Working to identify the crypto ransomware family. [9]

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7673
***Article Received**: 25 April 2023 **Revised:** 22 June 2023 **Accepted:** 09 July 2023*

Nolen Scaife et.al. (2016), demonstrates CryptoDrop, an timely warning-based detection system that notifies users of any unusual folder movement. By means of a group of behavioral traits that are typical of ransomware, one may identify it. With a perfect rate for detection and a loss of 10 files out of a total of 5100, they analysis their method alongside 492 real-time Ransomware instances. [10]

Shreya Chadha et.al. (2017), introducing a self-learning system that uses machine learning to identify ransomware attacks. The dataset was created by analyzing network traffic for one day of an organization and comprises 3473 valid and 131 malicious entries. [11]

Routa Moussaileb et.al. (2018), provides a graph-based ransomware defense that uses machine learning techniques to identify ransomware activity based on file system monitoring. On Windows 10, Windows 11, as well as 417 kindly samples gathered on Windows 10, testing is conducted on more than 770 active Ransomware variants. and obtain a rate of detection of 99.35% with a false positive rate of less than 1%. [12]

Pratyush Raunak et.al. (2017), developed a system to stop and identify ransomware attacks. By utilizing the certificate Authority Checker provided by the framework, users are able to stop data from being encrypted. Additionally, it uses static with dynamic analysis, network packets patterns, and the Ransomware attack pattern signature to detect illicit interaction with the use of SDN. [13]

Manish Shukla et.al. (2016), uses a method to keep an eye out for unusual behaviour in a POSTER directory system. a solution based on how Windows 7 platform based ransomware behaves. The outcome demonstrates the ability to identify both the old and new Ransomware variants. [14]

Salunke M. D et al Researchers concentrate on recovery and mitigation strategies for the ransomware assault in this study. The use of mitigation or recovery techniques is particularly challenging since ransomware relies on cryptographic methods that are exceedingly hard to decipher.[15]

III. DECOY DECEPTION TECHNIQUES FOR DETECTION OF RANSOMWARE ATTACKS SELECTING A TEMPLATE

A. Deception technique

The deception technique is nothing but trap or decoy that exist for being attacked or attract the attacker to be trapped that works as in the stages like decoy objects, monitoring, and alert for malicious activity which is also known as deception components. The decoy objects can be any of files, database, images which act as wrong target for attackers and to which attackers attack by sensing real objects which monitors by deception technique and finally generate alert to administrator which state that ransomware attack is happened on your system. With the help of decoy deception technique we added one advantage to our detection approach. So with the help of these deception techniques we can trap attacker with using decoy files which does not harm your system or network.

B. Decoy files

A document made with the intention of misleading a foe. Defenders employ lures and decoys to trick attackers into thinking they have a foothold in the network and revealing themselves in the context of cybersecurity. Any security staff might become worn out by false positives. Few are naturally produced through deception; only an attacker should have any motive to communicate with a decoy. Additionally, the warnings give background information regarding an attacker's goal. The majority of behaviour analysis uses machine learning to highlight deviations from the norm, which frequently results in false positives. Deception creates a baseline of zero activity, making any activity justify scrutiny, and provides specific signs of compromise.

C. Proposed methodology

Figure3: Proposed model for Ransomware Detection.

The figure shows that the detection system uses event handler and decoy file systems with file system activity watcher such as changed, created, deleted and rename watcher for file system activity for ransomware detection system building approach as the architecture of system for detection of ransomware attack.

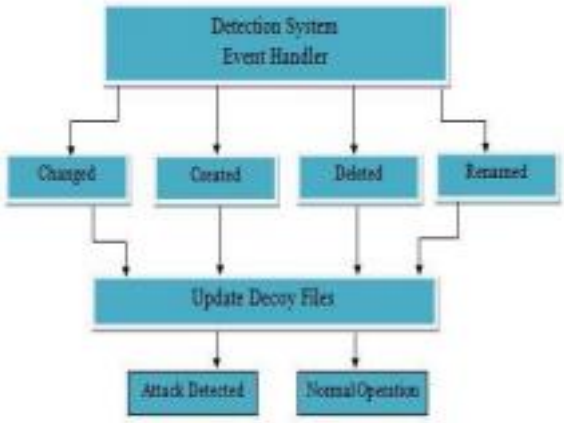

Figure2: Ransomware Detection System Architecture

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7673
***Article Received**: 25 April 2023 **Revised:** 22 June 2023 **Accepted:** 09 July 2023*

. (1) Decoy deception technique:

Deception techniques are the important one and mostly used approach for building the detection system for countermeasure the any type of attack. As ransomware attack directly process on file systems as they change the file format or extension of file or some time delete the original file by creating the encrypted version of that file. So it is very important for developing the detection system to take care these things of file system activity. The deception technique works for finding error in the system for betterment of that system. The need of deception based systems comes in reality because of attackers.

(2) File System Activity:

Read, write, create, rename, delete are some activities or the file related operations that are perform by attacker or ant variant of ransomware attack. Every time when attack is happened on system then at that time .txt or one text file is created at early stages of attack so here create activity of file system is done by attack. Some of the ransomware variants uses or created new files and read the contain from old file encrypt it and then write that encrypted data into new file and lastly deleted that old original file which is then replace by new encrypted file which has attack as its extension.

So in this way attack can use create, read, write, rename and delete activities related to file system activity or operations. So while designing or building a detection system for ransomware attack we must have to consider all these parameters or features or file system activities.

Algorithm for proposed system

Working of module:

Let's see actual working of ransomware detection module.

The figure shows about the algorithmic steps for detection system for ransomware attack.

1. Detection System will monitor the decoy file system which is specified by user.

2. When first layer executes attack samples that is when first attack threat model gets executed it will encrypt the files from victim's machine for executing the Java Ransomware variant of ransomware attack

3. Detection system then listen for create, rename, change and delete event handler of file system activities file system watcher functionality for monitoring or detecting the any change in to the file system on users machine.

4. Detection system also watches for any change in decoy file system of user's machine for all these event handler activity.

Figure4: Ransomware Detection System Steps

Activities Such as encryption processes on file with create; change and delete file system event handlers. As most of ransomware attack lastly change the extension of file with its own extension type such as JLocked in our case, the proposed systems detection module then check for list of valid extension type and matches this new extension with that list. If extension is valid and no encryption is done then it will generate alert as Benign application, but if extension is not matched with

valid extension list then it will generate alert for user for ransomware attack on the machine.

IV. DATASET

Datasets plays important role while counter the attack, they are key factor in most of network or intrusion or attack detection systems. So, while designing the ransomware countermeasure system I consider this factor.

It is very important to have not only large dataset but also good available dataset collection for countermeasure the ransomware attack. It is very difficult at first sight to have correct dataset ransomware samples. In proposed system I have used datasets for detection as well as mitigation of ransomware attack. The various attack samples are collected from these sources for experimental process that will check the proposed systems performance. These collected samples from various sources are then executed in controlled environment for detection module testing that is they are used as input to third layer of proposed system that is detection module to check the performance of detection module against these collected samples.

TABLE I
DATASET COLLECTED

Sr. No.	Name Of Ransomware Variant	Total Samples
1	CryptoWall	64
2	TeslaCrypt	57
3	Cerber	132
4	CTB-Locker	29
5	Jigsaw	52
6	TorrentLocker	41
7	Locky	74
8	CryptoLocker	42
9	CryptoDefence	26

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7673
***Article Received**: 25 April 2023 **Revised:** 22 June 2023 **Accepted:** 09 July 2023*

10	Hidden Tear	22
11	CryptoFortress	38
12	CryptVault	37
	Total	614

In our research we have collected dataset of different variant of ransomware attack from different sources of about total 614 files encrypted and extension.

V. RESULT

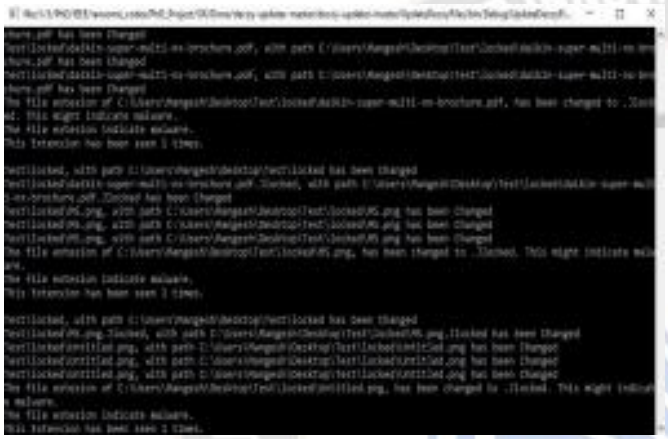

Figure 5: Result of Detection system

The figure 5 shows that the one of the result of the proposed systems detection module of, in that it shows the malware detected with the help of proposed system. The diagram demonstrates that the suggested system's detecting structure is capable of detecting attack by ransomware variants that are produced by or assisted by the attack generating component. This diagram illustrates how the malware component affects the user's workstation decoy files by encrypting them and altering their JPG extension to JLocked. Therefore, the suggested ransomware attack detection system may be able to identify the attack.

As we have two datasets for detection system or for detection of ransomware attack, one is dataset created with the help of first module that is attack dataset module and another one is dataset that is collected from several malware websites. So our result of this module is also divided into two parts first for created dataset and second part for collected dataset.

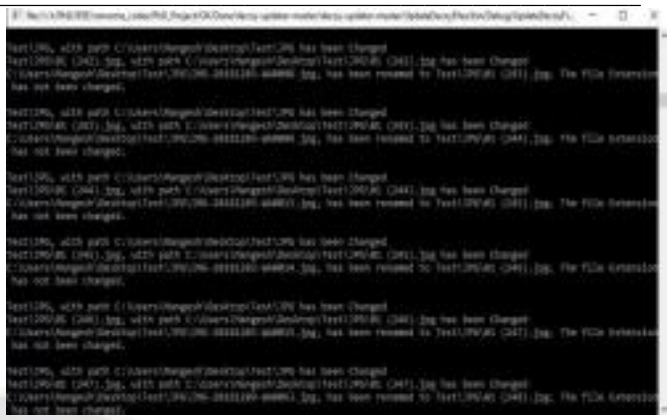

Figure 6: Result of Detection system. (Rename)

Another output of the proposed system's detection module is shown in Figure 6, which depicts a system user's renaming action. The output for users' actions on the system is shown in the figure. This occurs when a user renames numerous files at once, which is when more than one file is changed by the user at once. Because this is a benign procedure from the user, our ransomware detection system flags it as a benign application..

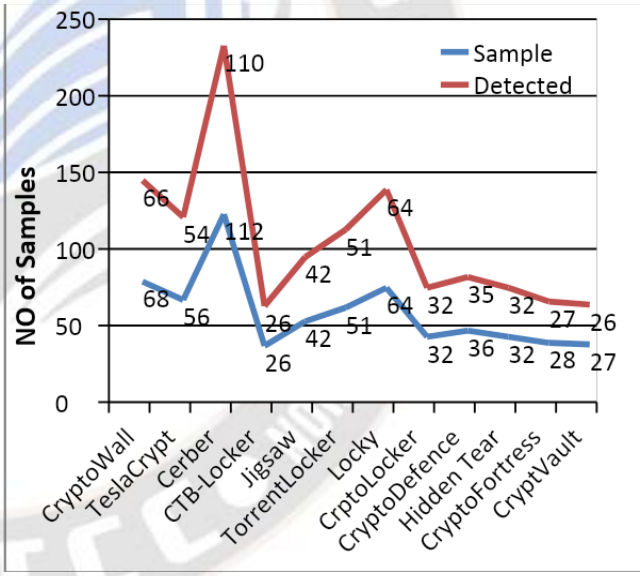

Figure 7: Fig System Architecture (Detection Module)

The figure 7 shows the graphical representation of result that obtain as an output of this proposed systems module that is Ransomware detection system module. In that the figure shows about graph of variants of ransomware attacks for number of attack samples used and number of attack samples are detected by proposed systems ransomware detection module. Figure demonstrates the ratio between the number of attack samples used and the number of attack samples actually detected during a ransomware attack. For example, during testing of the system, 68 samples of the CryptoWall variant of ransomware were used, of which 66 samples were actually detected by the proposed module's ransomware detection system. Additionally, it employs

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7673
***Article Received**: 25 April 2023 **Revised:** 22 June 2023 **Accepted:** 09 July 2023*

56 attack samples for other variations like TeslaCrypt, from which the system properly detects 54 attack samples. For the Cerber ransomware type, 112 attack samples are used, and 110 attack samples are detected by the system. It requires 26 attack samples for CTB-Locker, of which the system accurately detects 26 of them. For the Jigsaw ransomware version, the system detected all 42 attack samples, which are required for detection.

VI. CONCLUSION

We developed new approach for detection of this very popular and complex type of attack that is ransomware attack. The new developed approach is uses combine techniques to detect the complex ransomware attack. In that it uses deception techniques such as decoy files and folder which combine with file system activity which is again having file system watcher for monitoring the file system activity and events such as rename, delete, create and read or write events. So all these approaches or techniques are combined to monitor the system or network in real time will allow its user to detect the ransomware attack.

REFERENCES

[1] **J**ames A. Sherer, Melinda L. McLellan, Emily R. Fedeles, and Nichole L. Sterling, "RANSOMWARE – PRACTICAL AND LEGAL CONSIDERATIONS FOR CONFRONTING THE NEW ECONOMIC ENGINE OF THE DARK WEB", Richmond Journal of Law & Technology Volume XXIII, Issue 3

[2] Dean F. Sittig, Hardeep Singh, "A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks", Appl Clin Inform 2016; 7: 624–632 http://dx.doi.org/10.4338/ACI 2016-04-SOA-0064

[3] Francesco Mercaldo, Vittoria Nardone, Antonella Santone, "Ransomware Inside Out", 2016 11th International Conference on Availability, Reliability and Security, 978-1-5090-0990-9/16 $31.00 © 2016 IEEE DOI 10.1109/ARES.2016.35.

[4] Sileshi Demesie Yalew1;2, Gerald Q. Maguire Jr.2, Seif Haridi2, Miguel Correia, "Hail to the Thief: Protecting Data from Mobile Ransomware with ransomSafeDroid", 978-1-5386-1465-5/17/$31.00 c 2017 IEEE

[5] Sajad Homayoun, Ali Dehghantanha, Marzieh Ahmadzadeh, Sattar Hashemi, Raouf Khayami, "Know Abnormal, Find Evil: Frequent Pattern Mining for

[6] Ransomware Threat Hunting and Intelligence", IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING, 2168-6750 (c) 2017 IEEE

[7] Eugene Kolodenkerz, William Koch, Gianluca Stringhiniy, and Manuel Egele, "PayBreak: Defense Against Cryptographic Ransomware", 2017 ACM. ISBN 978-1-4503-4944-4/17/04

[8] Monika , Pavol Zavarsky, Dale Lindskog, "Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization", The 2nd International Workshop on Future Information Security, Privacy & Forensics for Complex Systems, Elsevier

[9] Juan A. Herrera Silva, Myriam Hernández-Alvarez, "Large Scale Ransomware Detection by Cognitive Security", 978-1-5386-3894- 1/17/$31.00 ©2017 IEEE

[10] Aaron Zimba, Luckson Simukonda, Mumbi Chishimba, "Demystifying Ransomware Attacks: Reverse Engineering and Dynamic Malware Analysis of WannaCry for Network and Information Security", ZAMBIA INFORMATION COMMUNICATION TECHNOLOGY (ICT) JOURNAL Volume 1 (Issue 1) (2017) Pages 35-40

[11] Nolen Scaife, Henry Carter, Patrick Traynor, Kevin R.B. Butler," CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data", 2016 IEEE 36th International Conference on Distributed Computing Systems

[12] Shreya Chadha, Utham Kumar, "Ransomware: Let's Fight Back!", International Conference on Computing, Communication and Automation (ICCCA2017), ISBN: 978-1-5090-6471-7/17/$31.00 ©2017 IEEE.

[13] Routa Moussaileb, Benjamin Bouget, Aurélien Palisse, Hélène Le Bouder, Nora Cuppens, Jean-Louis Lanet, "Ransomware's Early Mitigation Mechanisms", ACM ISBN 978-1-4503-6448-5/18/08. . . $15.00, https://doi.org/10.1145/3230833.3234691

[14] Pratyush Raunak and Prabhakar Krishnan, "NETWORK DETECTION OF RANSOMWARE DELIVERED BY EXPLOIT KIT", VOL. 12, NO. 12, JUNE 2017 ISSN 1819-6608 ARPN Journal of Engineering and Applied Sciences ©2006-2017 Asian Research Publishing Network

[15] Manish Shukla, Sutapa Mondal, Sachin Lodha, "POSTER: Locally Virtualized Environment for Mitigating Ransomware Threat", CCS'16 October 24-28, 2016, Vienna, Austria c 2016 Copyright held by the owner/author(s). ACM ISBN 978-1-4503-4139-4/16/10. DOI: http://dx.doi.org/10.1145/2976749.2989051.

[16] Salunke, M.D., Kumbharkar, P.B., Kumar, P. "A Proposed Methodology to Mitigate the Ransomware Attack", Advances in Parallel Computing, 2021, 39, pp. 16–21

[17] Salunke, M., Kabra, R., & Kumar, A. (2015). IRJET-Layered architecture for DoS attack detection system by combine approach of Naive bayes and Improved K-mea Layered architecture for DoS attack detection system by combine approach of Naive bayes and Improved K-means Clustering Algorithm. International Research Journal of Engineering and Technology. www.irjet.net

[18] Salunke, M., Kumbharkar, D. P. B., & Sharma, D. Y. K. (2020). A Proposed Methodology to Prevent a Ransomware Attack. International Journal of Recent Technology and Engineering (IJRTE), 9(1), 2723–2725. https://doi.org/10.35940/ijrte.a2860.059120