International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 3, June 2020, pp. 3166~3175
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i3.pp3166-3175

Ransomware protection in loT using software defined networking

Azka Wani [1], S. Revathi [2]
[1]Department of Computer Applications, Crescent B S Abdur Rahman Institute of Science and Technology, India
[2]Department of Computer Science and Engineering, Crescent B S Abdur Rahman Institute of Science and Technology, India

Article Info

Article history:

Received Mar 23, 2019
Revised Dec 8, 2019
Accepted Jan 7, 2020

Keywords:

CoAP
Crypto ransomware
IoT
OpenFlow
Ransomware

ABSTRACT

Internet of things (IoT) is the network of physical objects connected to provide various services. IoT is expanding rapidly, and is positively influencing many areas. The impact of IoT is evident in medical field, manufacturing units and livestock. The IoT is also vulnerable to many cyber threats, owing to its limited resources and battery operation. In contemporary times the security threats like DDoS, botnet malware, man in the middle, flood attacks and ransomware are affecting the smooth functioning of IoT. Ransomware has emerged as one of the biggest threat in cyber world. Ransomware is a type of malware that stops the access to files by encrypting them and decrypts the files only when a ransom is paid. The negligence towards the IoT ransomware can result in disastrous outcomes. In this paper, the growth of ransomware attacks for past few years is shown with special focus on ransomwares threatening IoT. A detection mechanism for IoT ransomware attack is presented that is designed after study of ransomware for IoT. The proposed model monitors the incoming IoT traffic through Software Defined Network (SDN) gateway. It uses policies framed in SDN controller for detection and alleviation of ransomware in IoT.

Corresponding Author:

Azka Wani,
Department of Computer Applications,
Crescent B S Abdur Rahman Institute of Science and Technology,
Vandalur, Chennai- 600048, India.
Email: graceazka@gmail.com

1. INTRODUCTION

The Internet of Things (IoT) is formed by connecting physical devices. The IoT devices include ordinary objects from day to day life, which interact with each other to make human lives easier. The IoT devices are deployed at various environments for automation and smart data transfer from one IoT domain to another with least or no human intervention [1]. IoT devices are setup in places like homes, offices, hospitals, vehicles, roads, markets and industries etc [2, 3]. IoT has undoubtedly led to the innovation of smart world but IoT devices are highly vulnerable to a wide range of attacks. An indirect communication of individual to individual smart devices also makes IoT vulnerable to a range of attacks [4]. The security measures in IoT and the resistance of IoT devices against the recent attacks is one of the major concern faced by IoT [5]. IoT security has been in news recently, due to DDoS, botnet, malware and ransomware attacks on IoT devices[6]. The early variants ransomware first came up in the late 1980s [7]. The newer versions of ransomware have been around for a couple of years and lately have posed a big threat for IoT as well [8, 9]. Ransomware is a combination of ransom and malware. Ransomware encrypts the personal files of a victim and makes those unusable, allows decryption and release of the files after a ransom is paid to the ransomware creator. The attacker through cryptocurrency or credit card asks for the payment of ransom. Ransomware attacks are becoming stronger and it is hard to devise a prevention method. IoT devices, which already have

poor security profile, are easy targets for the ransomware attackers. Ransomware penetrates into a target through malware, spam, phishing or social engineering. Since ransomware attacks are irreversible after a deadline, these can result in a greater damage in a system constituting of computers and laptops. In case of IoT, ransomware attacks are craftier; these hit the target based on time and place. The hackers can track down the commuter of a smart car and may launch the ransomware once the car is at some remote location with no access to services. The victim is compelled to pay the ransom in such case. The smart health IoT are also crucial target of ransomware, if the attacker takes control of any such device, any delay in the payment of ransom can result in loss of human lives. Likewise, the ransomware can strike IoT devices associated with other fields and the force the victim to pay fee in timely manner.

The IoT security has been analyzed and evaluated for some years, and researchers have come up with many solutions for IoT protection [10-13] but, little has been proposed against ransomware prevention in IoT. The SDN is a modern way of networking which makes the networks programmable. The key concept introduced by SDN is segregation of control and data planes. The networking devices that include switches and routers are used for just traffic forwarding, while as the management of the network is by the centralized controller. The controller is the brain of the network, which takes decisions about the traffic movement and maintains a global view of network. SDN based networking is considered intelligent, [14] and has successfully removed plenty of shortcoming in traditional networks [15]. The SDN has also addresed majority of challenges faced in IoT. The security in IoT devices has also improved with the help of SDN [16, 17]. The paper can be summarized as:

- The ransomware attacks are briefly explained using a timeline of various types of ransomware that surfaced from the beginning of the attack.
- The recent research carried out in the area of ransomware attacks is discussed.
- The major contribution of paper is to (a) highlight the impact of ransomware on IoT, (b) propose a SDN based solution to detect and mitigate ransomware in an IoT environment, (c) evaluate the proposed solution and present the enhancements that can be included in the future work.

The rest of paper is arranged as follows; Section 2 contains an introduction to ransomware and its types. Section 3 highlights the vulnerabilities in IoT and discusses the ransomware attacks in context of IoT. Section 4 discusses the work related to ransomware in IoT. The proposed model is introduced in Section 5. The Section 6 includes performance evaluation of proposed system followed by its comparison with relevant methods. Section 6 is conclusion of the proposed work.

2. RANSOMWARE

This section explains the ransomware attack with special focus on IoT and basic types of ransomware. Ransomware is a malign software, developed in a way that it can halt access to any application or data. Ransomware blocks any system or data by encrypting it and the attacker demands a hefty amount from the victim for decrypting. The attacker sets a deadline for payment of fees and if victim fails to pay on time, the attacker may damage the asset permanently. The first instance of ransomware known as PC-Cyborg was reported in late 1980's. PC Cyborg used simple encryption and it was not a serious threat. There were not many instances of ransomware for the next 10 years. The next ransomware appeared in 2004, called GpCode, and it used asymmetric key encryption. In 2012, Reveton came into picture, which exploited credentials for law enforcement. In year 2013, CryptoLocker appeared as one of the most dangerous ransomwares. It had military grade encryption and kept the key, needed to release user data, on a remote server. Many instances of ransomware were reported for next few years, until Wannacry, which surfaced in 2017 as one of the most disastrous ransomware [18]. The ransomware infection on a host is depicted in Figure 1.The popular most ransomwares that appeared from the beginning until recently are shown in Table 1.

Table 1. The popular variants of ransomware

Ransomware	Year of Appearance	Intensity
PC Cyborg	1980's	Weak
GpCode	2004	Weak
WinLock	2007	Medium
Reveton	2012	Medium
CryptoLocker	2013	Strong
KeRanger	2016	Medium
Wannacry	2017	Strong
Petya	2017	Strong

- Crypto ransomware

The Crypto ransomware encrypts the important user data files with a strong encryption algorithm. The author of the ransomware provides the key for decryption only after the demanded ransom is credited into the attackers account. Crypto ransomware finds its way into a computer or any network operated device through a malware or spam mail. Once activated, it searches for files with extensions and then encrypts the vital files. Both symmetric and asymmetric cryptographic algorithms are used by crypto ransomware for exploiting the host. Some of the actively used crypto ransomwares are: Cryptowall, TelsaCrypt, CryptLocker, Cerber [19]. The Crypto ransomware is severe most and has been the reason for massive destructions in cyber-world. The encryption algorithms used by crypto ransomware are hard to crack and it is nearly impossible to decrypt the information without ransom.

- Locker ransomware

The Locker ransomware blocks the resource or the machine of the target. It makes the machine or other resources inaccessible for the victim. The user in unable to login into the system but the user data is not touched [20]. It occupies the resources like computer systems, screens etc. and then demands a payment to release the resources. The locker ransomware after activation allows user to interact with its interface only for payment or other related communication. In contrast to Crypto ransomware, the locker ransomware is easier to combat and can be cracked if one as technical knowledge. Some well-known locker ransomwares are Direct Memory Access (DMA) locker, Locky ransomware, Windows Locker, Torrent Locker etc [21].

- Hybrid ransomware

Hybrid ransomware are a combination of locker ransomware and crypto ransomware. Such malware involve both the resource and data. A hybrid ransomware attack has tendency to halting the entire IoT system, but such attacks are hard to execute. The Crypto ransomware has been responsible for the hype and success of the ransomware industry. The ransomware families have developed considerably over past few years. Some other notable types of ransomware include Scareware, Screen lockers, BadRabbit, Petya-esque and Wannacry ransomware, which was in news for quite some time in 2016. Wannacry ransomware has emerged as an evident threat to the IoT [22]. Although ransomware attack first occurred long back, these malwares restored lately with a greater strength.

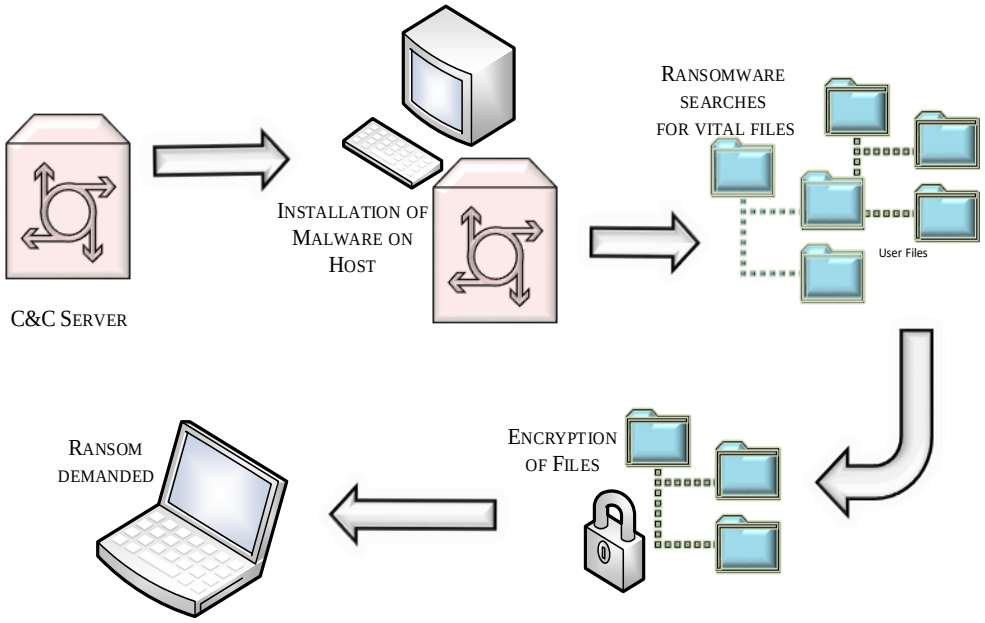

Figure 1. Ransomware hacking process

The reports of various anti-malware and anti-virus companies have reported considerable increase in ransomware as follows:

- The reports by Symantec depict that ransomware variants have increased by 46% [23].
- The Hollywood Presbyterian Medical Center lost 17,000 dollars to the ransomware attack that disabled the network of hospital in 2016 [24].

- The University of Calgary had to pay a ransom of 16,129 dollars after ransomware knocked down many systems of the institute [25]
- As per the statistics of 2018 [26], the ransomware attack rates on individual units have decreased considerably, but the ransomware attacks can still hit the small scale or average sized units in 2019**.**

3. RANSOMWARE AND IOT

In this section, the ransomware is discussed in context of IoT. The impact of ransomware on IoT and the way by which IoT devices are infected by ransomware is described. The ransomware attacks in IoT are more catastrophic. The ransomware in an IoT environment is able to shut off the entire network of physical devices, because it is easy for such strong malware to take the control of devices with constrained resources. Ransomware is capable of hitting on all the security aspects of IoT, which include authentication, integrity and availability. The ransomware in IoT have not only resulted in financial loss, but also posed a threat the human lives. As evident from the literature review, the earlier instances of ransomware were easier to tackle since there were less number of connected devices back then. With increasing number of connected devices, onset of IoT, introduction of cryptocurrency, exposure of personal data on social media, the ransomwares have become more powerful. The ransomware is able to penetrate into the IoT devices with lesser effort and collect the ransom from the users. The rightful owner of the IoT devices with user interfaces are locatable, while as finding the owner of IoT devices without user interface is difficult. The small IoT devices are not the target of ransomware. In case of ransomware hitting a computer system, an attacker can easily launch the attack and force the user to transfer the money from the same system. In case of IoT devices, a ransomware attack is launched from multiple devices, as there is lack of user interfaces in IoT. The ransomware has targeted the IoT devices that deal with critical real time data. These include the IoT devices connected to healthcare, smart vehicular system, smart manufacturing factories. The attacker can exploit users wearing critical smart health devices such as IoT monitored pacemakers or insulin pumps. The remotely located users can be forced to pay a ransom for the smart home or smart car under ransomware attack. The ransomware can penetrate in the IoT devices in many ways. The major methods of ransomware penetration are botnet, malvertisement or social engineering [27].

- Botnet: Botnets are the dwellers of malwares in any IoT network. Botnet cause the DDoS attacks or similar flooding attacks [28]. Ransomware are also entering into the IoT network with help of botnets.
- Social Engineering*:* Social engineering is the act of deceiving carried out by attackers, in which they pose to be the legitimate users and attain access to critical information. In an IoT environment, the adversaries penetrate in the system by acting as authorized owners of the devices.
- Malvertisement*:* The ransomware attackers can also infect IoT device through malvertisement [21]. The malware-filled content is broadcast through a Content delivery Network (CDN) that appears to be benign and is installed on the devices.

4. RELATED WORK

The authors in [29] have proposed a mechanism for detection of ransomware in IoT based on artificial intelligence. The detection method observes the battery consumption of the devices to confirm the presence of ransomware. The difference between battery consumption of genuine applications and malicious applications is recorded. The proposed method is executed using various machine learning algorithms. The results obtained from each algorithm are noted based on the various measures like detection rate, precision and recall. The authors in [30] have evaluated ransomware instanced for two years and estimated the growth of ransomware attacks in upcoming years. The authors have presented a detection mechanism that focuses on Cryptowall ransomware of Crypto ransomware family. The proposed method monitors the traffic between the Command and Control (C&C) server of Cryptowall and the IoT devices. The behavior of Cryptowall is also analyzed. The TCP/IP headers from the traffic are acquired to detect the ransomware attacks. The work presented in [31] have highlighted the various communication protocols used by IoT. The various applications of the IoT are also presented in the paper. The authors have introduced machine learning algorithms for classification purpose. The K Nearest Neighbour (KNN) and Random Forest classifiers have been used to detect the ransomware. As per the results the KNN shows better performance among the classifiers used in experiment. In [32] a solution is proposed to keep the files safe from ransomware. An operating system software is proposed that limits the access to the file system. The software is designed to sit on cloud servers. The software compresses the files into a single file using Message Digest (MD5) algorithm. The files are kept in non-write mode, so that the files cannot be altered. A log file is also maintained that keeps record of all the actions done on the files.

5. PROPOSED METHOD

Any mechanism developed to counter ransomware attacks in IoT environment should consider the varying nature of ransomware and underlying heterogeneous architecture of the IoT devices. The security solution for ransomware has to scan the traffic and check the behavior of devices at regular intervals. In this paper, a SDN based Crypto ransomware mitigation method is proposed for IoT environment, this method is termed as IoTSDN-RAN. All the variants of ransomware follow same procedure for acquiring the encryption key from the Command and Control (C&C) server of the adversary [30]. This process of communication between ransomware and the C&C server is used to detect the presence of ransomware. The attacker gets the target IoT device's IP address using the proxy server. The acquired IP address and an identifier is sent to the C&C server. The C&C server launches the ransomware attack. The C&C gets in contact with the IoT device and penetrates an encryption key into the device. After encrypting the IoT device, the C&C server sends the details of ransomware web portal to the owner of the hacked IoT device for payment of ransom. The details of the ransomware payment method are sent over a secure channel that cannot be intercepted. The hackers demand the payment to be done by bitcoin [21]

The proposed method or IoTSDN-RAN monitors the traffic between the IoT and the outside world, which includes communication between C&C server and IoT device as well, in case of a ransomware. IoTSDN-RAN is directly deployed in the SDN controller. It detects the presence of ransomware by extracting the COnstrained Application Protocol (CoAP) headers. The TCP/IP headers are also extracted and stored for further analysis. The proposed method is executed into three main steps. The first step is termed as *Sample Collection* in which the attack traffic and the normal traffic samples are collected using the realistic dataset. The second step is the *Training of IoTSDN-RAN* where the specific features of traffic collected in previous step are used to train the proposed algorithm .The parameters of the training algorithm are adjusted to attain accurate results. A combination of Naive Bayes and Principal Component Analysis (PCA) [33, 34] are used for detection of the ransomware in second and third step of the proposed method. The third and the final step is *Detection and Mitigation* where the ransomware infections are detected using the knowledge of previous steps. Once the presence of ransomware is confirmed, the ransomware is mitigated. The detailed working of each step in IoTSDN-RAN is discussed below and also described with the help of the flowchart as shown in Figure 2:

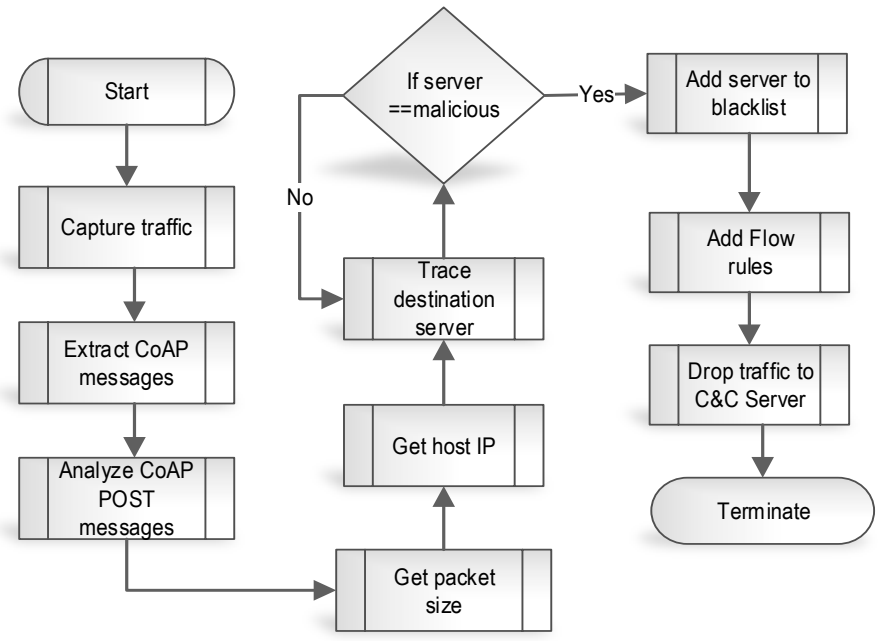

Figure 2. Work flow of IoT SDN-RAN

− Sample Collection

The sample collection step collects the network traffic that is used in next two steps of the IoTSDN-RAN, The samples of different ransomware attacks are taken from the dataset [35]. The IoT devices mostly use COnstrained Application Protocol (CoAP) at application layer. The CoAP traffic is captured and based

on the analysis of traffic, the attacker is traced. The CoAP POST messages are collected even if the non-standard ports are used. The messages are gathered to know the type of the devices, status of the devices, model and make of the devices.

- Training of IoTSDN-RAN

The traffic captured in the previous step is analyzed. The CoAP POST messages sent by the attacker are considered and the features are extracted. The features are extracted for experimental use. The features extracted from the traffic traces are files in the (packet capture).pcap and (comma-separated values).csv format. The learning of the IoTSDN-RAN is done by using the features of the extracted traffic and the dataset [35]. The dataset includes data from the crypto ransomware. The IoTSDN-RAN finally calculates all the important parameters that are used later for the detection step.

- Detection and Mitigation

The CoAP traffic is analyzed for detection of any potential ransomware. The analysis of the traffic is carried out in two phases. The first phase of analysis focuses on the training of the algorithm. The second phase is used for real-time detection of the ransomware infections. In both the phases of detection the TCP/IP traffic segments that contain CoAP traffic are monitored. The packet size and the host IP address are acquired from the CoAP header. The extracted information is used to trace the destination server, which could be C&C server. The server is tested and if it is found to be malicious then the server is added to the blacklist, and communication between such servers and the IoT devices is stopped by dropping the traffic destined to or from the servers. The traffic to the blacklisted servers is dropped using the OpenFlow flow rules [36].

The above steps are followed in case the ransomware has not yet encrypted the user data. In case the ransomware has infected the user data of an IoT device, the owner of the encrypted data gets a prompt on screen about the hacking and a link for the payment. In case of the compromised IoT device following steps are taken:

- Get the details of the ransomware family used to infect the IoT device.
- Evaluate the user data encrypted and checked whether the data is important enough to decrypt and pay the ransom.
- In case the data is important, decryption of the compromised file is tried on an uninfected computer.
- There are a number of tools that help in decryption of ransomware encrypted files like Troldesh, Apocalypse, Nemucod, BadBlcok, LeChiffre, Crypt888, Legion, SZFLocker, and TeslaCrypt [32].
- The owners of devices need to update the firmware. In many cases, restarting of the devices also helps in removal of the malware. The strong authentication also prevents the devices from ransomware attacks.
- The practice of taking a backup of user data and configuration data periodically can save the users from paying the ransom even if the devices are compromised.

6. RESULTS AND DISCUSSION

This section presents the detailed working of the ransomware detection algorithm, and the results obtained. The experiment is carried out using the simulation environment on Mininet-WiFi [33]. The dataset is used to simulate the experiment. The proposed method mainly focuses on the CryptoWall ransomware. The OpenFlow protocol is used in a SDN environment and SDN controller monitors and manages the network devices. The gateway for the IoT is the Openflow enabled switch, the traffic towards the IoT always passes through it. The experimental setup uses Floodlight controller which is based on python [37]. The CoAP traffic passes through the IoTSDN-RAN application that is deployed on the SDN controller that takes the decision on the traffic. As the experiment started, the samples from the dataset were run, the communication to the C&C server helped in detection of the ransomware in IoT.

The decision on blocking or allowing the traffic were taken based on size of the CoAP POST messages. If presence of ransomware was confirmed, the flow rules were inserted in the OpenFlow switch. The flow rules were inserted to block the communication with the C&C server. In an ideal system all, the instances of malware are reported, while as in a real system few of the malicious traces cannot be flagged. The True Positive Rate (TPR) is calculated as a ratio reported malwares and the total number of samples taken in the experiment. The FPR (False Positive Rate) is the ratio of the normal traffic reported as malicious to the total number of samples. Then traffic samples were taken from the CryptoWall C&C servers and the infected host. The total number of packets taken were 700, out of which 78 samples were used for training the application and rest of the samples were used during the actual experiment. The confusion matrix for IoTSDN-RAN is given in Table 2. The detection rate of the proposed method is 98% and the FPR is 2.1%.

Table 2. Confusion matrix FOR IoTSDN-RAN

Measure	Value	Derivations
Sensitivity	0.9801	TPR = TP / (TP + FN)
Specificity	0.9781	SPC = TN / (FP + TN)
Precision	0.9769	PPV = TP / (TP + FP)
Negative Predictive Value	0.9812	NPV = TN / (TN + FN)
False Positive Rate	0.0219	FPR = FP / (FP + TN)
False Discovery Rate	0.0231	FDR = FP / (FP + TP)
False Negative Rate	0.0199	FNR = FN / (FN + TP)
Accuracy	0.9791	ACC = (TP + TN) / (P + N)
F1 Score	0.9785	F1 = 2TP / (2TP + FP + FN)
Matthews Correlation Coefficient	0.9582	TP*TN - FP*FN / sqrt((TP+FP)*(TP+FN)*(TN+FP)*(TN+FN))

7. COMPARISON WITH RELATED METHODS AGAINST RAMSOMWARE

The performance of the proposed mechanism is compared with several other related works using various matrices like detection rate, precision rate. The work presented in [31] has a detection rate of 93.76%. The detection rate of IoTSDN-RAN is 98.01% and a precision rate of 97.69%.The work in [31] is abbreviated as IoT-ML. The detection rate of IoTSDN-RAN is greater by 4.43%. The precision rate of IoTSDN-RAN is also greater by 8.36%. The comparison of results is shown in Figure 3. As clearly indicated by two major matrices i.e. precision and detection rate, the performance of proposed solution is better than the previous related work. The results of the detection mechanism proposed in [38] have the Accuracy and the False Negative Rate (FNR) as 97.48% and 1.64%. When compared to IoTSDN-RAN the, Accuracy is 97.91% and FNR is 1.99%. Thus, accuracy increases by 0.44 % while as FNR increases by 19.28%, so even though the accuracy increases but FNR does not decrease. The variation in the results can be due the size of the samples, which is greater in case of IoTSDN-RAN. The results are shown graphically in Figure 4. The accuracy has shown a slight increase in IoTSDN-RAN. The work presented in [30] shows a conceptual way of safeguarding IoT against ransomware. The TCP/IP headers have been used for the purpose of ransomware detection while as for IoT traffic the network protocols/headers differ as compared the normal internet traffic. The results in terms of matrices can be a future project for the authors. The fresh incidents of ransomware [39, 40] that hit the cyber world have made it important to create counter solutions for threats that IoT is posing.

IoTSDN-RAN is a realistic approach towards ransomware detection in IoT because of following reasons:

- It does not report presence of ransomware based on the status of battery consumption, the battery may be drained during peak hours of usage or due to some other attack like DDoS.
- IoTSDN-RAN extracts information from CoAP headers for detection of ransomware, as CoAP protocol is specific to IoT communication.

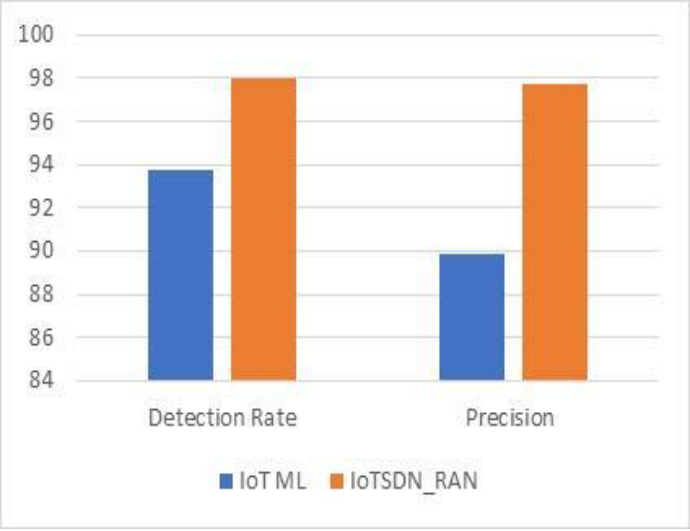

Figure 3. Comparison of IoTSDN-RAN with IoT-ML [31]

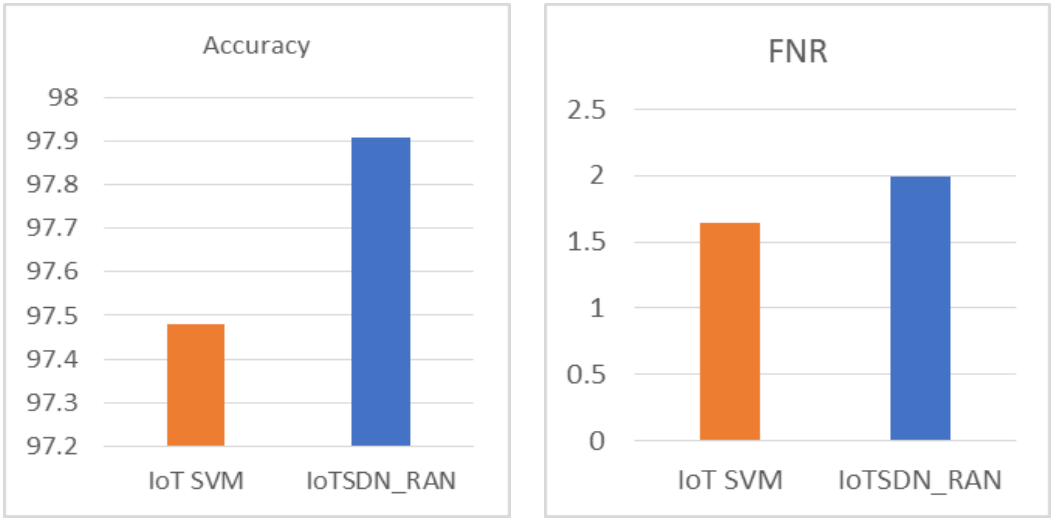

Figure 4. Comparison of IoTSDN-RAN with IoT-SVM [38]

8. CONCLUSION

Ransomware has been there for three decades but the increased number of connected devices resulted in the gruesome comeback of ransomware. The ransomware has been in news for past few years, it has affected the user data and resources severely. The ransomware poses a serious threat to IoT as well. In this paper the ransomware is discussed in context of IoT and some measures are mentioned in the paper that can be taken to prevent ransomware from attacking the Internet of Things. The prevention measures against ransomware are much easier to follow as compared to the detection and mitigation procedure. A SDN based solution is also proposed that detects the presence of crypto ransomware in IoT environment. The detection process is followed by the mitigation. The alleviation of ransomware is done using the flow rules of OpenFlow protocol. The results of the experiment demonstrate that the proposed solution improves the accuracy and detection rate of the ransomware attack. The future work should include detection of all ransomware variants and other prevalent malwares that threaten the IoT environment with a reduced false negative rate.

ACKNOWLEDGEMENTS

The authors are grateful to MANF UGC, Govt. of India for providing financial support under MANF- UGC (MANF-2015-17-JAM-60506) programme to carry out this work.

REFERENCES

[1] M. Y. Idris, D. Stiawan, N. M. Habibullah, A. H. Fikri, M. R. A. Rahim, and M. Dasuki, "Iot smart device for e-learning content sharing on hybrid cloud environment," *Int. Conf. Electr. Eng. Comput. Sci. Informatics*, vol. 4, no. September, pp. 25–29, 2017.

[2] M. I. Mahali, E. Marpanaji, S. A. Dewanto, B. Wulandari, U. Rochayati, and N. Hasanah, "Smart Traffic Light based on IoT and mBaaS using High Priority Vehicles Method," *2018 5th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, no. 22, pp. 703–707, 2019.

[3] M. Husni, H. T. Ciptaningtyas, R. R. Hariadi, I. A. Sabilla, and S. Arifiani, "Integrated smart door system in apartment room based on internet," *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, vol. 17, no. 6, pp. 2747–2754, 2019.

[4] S. Andy, B. Rahardjo, and B. Hanindhito, "Attack scenarios and security analysis of mqtt communication protocol in iot system," *Int. Conf. Electr. Eng. Comput. Sci. Informatics*, vol. 4, no. September, pp. 600–604, 2017.

[5] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, vol. 38, no. February, pp. 8–27, 2018.

[6] M. De Donno, N. Dragoni, A. Giaretta, and A. Spognardi, "DDoS-Capable IoT Malwares : Comparative Analysis and Mirai Investigation," *Security and Communication Networks*, vol. 2018, no. 4, pp. 1-30, 2018.

[7] A. Tandon and A. Nayyar, "Data Management, Analytics and Innovation," *Springer* Singapore, vol. 839, 2019.

[8] S. Cobb, "RoT: Ransomware of Things," *ESET*, 2017.

[9] T. B. Laboratories *et al.*, "Ransomware and IoT among leading threats," *Netw. Secur.*, vol. 2017, no. 9, pp. 2, 2017.

[10] A. K. Simpson, F. Roesner and T. Kohno, "Securing vulnerable home IoT devices with an in-hub security manager," *2017 IEEE International Conference on Pervasive Computing and Communications Workshops* S. Zahra *et al.*, "Fog Computing Over IoT : A Secure Deployment and Formal Verification," vol. 5, 2017.
[11] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 395–411, 2018.
[12] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 761–768, 2018.
[13] P. Goransson, C. Black, and T. Culver, "Software Defined Networks: A Comprehensive Approach," Morgan Kaufmann, Oct. 2016.
[14] F. D. S. Sumadi, D. Risqiwati, and Syaifuddin, "Semi-reactive Switch Based Proxy ARP in SDN," *Proceeding of the Electrical Engineering Computer Science and Informatics*, pp. 478–482, 2019.
[15] Martinez-Julia, P., Skarmeta, A.F., "Empowering the Internet of Things with Software Defined Networking," White paper 2014; IoT6: Geneva, Switzerland, 2014
[16] O. Salman, I. Elhajj, A. Chehab, and A. Kayssi, "Software Defined IoT security framework," *2017 4th Int. Conf. Softw. Defin. Syst. SDS 2017*, pp. 75–80, 2017.
[17] B.A.S. Al-rimy, M.A. Maarof, and S.Z.M. Shaid, "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions," *Comput. Secur.*, vol. 74, pp. 144–166, 2018.
[18] Pippa Thirkettle, "SentinelOne : Global Ransomware Study 2018," Vanson Bourne, 2018.
[19] I. Yaqoob *et al.*, "The rise of ransomware and emerging security challenges in the Internet of Things," *Comput. Networks*, vol. 129, pp. 444–458, 2017.
[20] R. Richardson and M. North, "Ransomware: Evolution, Mitigation and Prevention.: EBSCOhost," *Int. Manag. Rev.*, vol. 13, no. 1, pp. 10–21, 2017.
[21] A. Zimba, M. Mulenga, and I. Technology, "A Dive Into the Deep : Demystifying Wannacry Crypto Ransomware Network," *International Journal on Information Technologies & Security*, vol. 10, no. 2, pp. 57–69, 2018.
[22] N. N. Rabalais, B. A. McKee, D. J. Reed, and J. C. Means, "Executive Summary," *Fate Eff. nearshore discharges OCS Prod. waters*, vol. 1, 1991.
[23] "Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers | Technology | The Guardian," *The Guardian*, 2016. [Online]. Available: https://www.theguardian.com/technology/2016/feb/17/los-angeles-hospital-hacked-ransom-bitcoin-hollywood-presbyterian-medical-center. [Accessed: 03-Feb-2019].
[24] "University of Calgary paid $20K in ransomware attack | CBC News," *CBC News*, 2016. [Online]. Available: https://www.cbc.ca/news/canada/calgary/university-calgary-ransomware-cyberattack-1.3620979. [Accessed: 03-Feb-2019].
[25] V. J. Reddi and H. Kim, "On the Internet of Things," in *IEEE Micro*, vol. 36, no. 6, pp. 5-7, 2016
[26] M. Poriye and V. Kumar, "Review Paper Ransomware : Detection And Prevention," no. 5, pp. 900–905, 2018.
[27] E. Bertino, "Botnets and Internet of Things Security," *Computer*, vol. 50, no. 2, pp. 76-79, 2017.
[28] A. Azmoodeh, A. Dehghantanha, M. Conti, and K.K.R. Choo, "Detecting crypto-ransomware in IoT networks based on energy consumption footprint," *J. Ambient Intell. Humaniz. Comput.*, vol. 9, no. 4, pp. 1141–1152, 2018.
[29] A. Zahra and M. A. Shah, "IoT based ransomware growth rate evaluation and detection using command and control blacklisting," *ICAC 2017 - 2017 23rd IEEE Int. Conf. Autom. Comput. Addressing Glob. Challenges through Autom. Comput.*, no. September, pp. 7–8, 2017.
[30] A. Dash, "Ransomware Auto-Detection In IoT Devices Using Machine Learning," no. December, pp. 0–10, 2018.
[31] M. Baykara and B. Sekin, "A novel approach to ransomware: Designing a safe zone system," *6th Int. Symp. Digit. Forensic Secur. ISDFS 2018 - Proceeding*, vol. 2018-Janua, no. March, pp. 1–5, 2018.
[32] C. Science, C. Science, C. Science, "Naive Bayesian Classifier And Pca For Web Link Spam," vol. 1, no. 1, 2014.
[33] T. Karthikeyan and P. Thangaraju, "PCA-NB Algorithm to Enhance the Predictive Accuracy," vol. 6, no. 1, pp. 381–387, 2014.
[34] D. Sgandurra, L. Muñoz-González, R. Mohsen, and E. C. Lupu, "Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection," *arXiv:1609.03020*, Sep. 2016.
[35] "SDN/OpenFlow," Flowgrammable, 2015. [Online]. Available: http://flowgrammable.org/sdn/openflow/. [Accessed: 27-Mar-2018].
[36] V. B. Harkal, "Software Defined Networking with Floodlight Controller," *Int. Journal of Comput. Appl.*, pp. 975–8887, 2016.
[37] Y. Takeuchi, K. Sakai, and S. Fukumoto, "Detecting Ransomware using Support Vector Machines," *Proc. 47th Int. Conf. Parallel Process. Companion - ICPP '18*, pp. 1–6, 2018.
[38] "Yet another company has been hit by a ransomware attack," *CNN Business*, [Online]. Available: https://edition.cnn.com/2019/10/15/business/pitney-bowes-ransomware-trnd/index.html. [Accessed: 18-Oct-2019].
[39] "Ransomware: These are the most common attacks targeting you right now," *ZDNet*. [Online]. Available: https://www.zdnet.com/article/ransomware-these-are-the-most-common-attacks-targeting-you-right-now/. [Accessed: 18-Oct-2019].
[40] "As Oil and Gas Data Multiply, so Do the Cybersecurity Threats," *JPT Journal of Petrolium Technology*, [Online]. Available: https://pubs.spe.org/en/jpt/jpt-article-detail/?art=5992. [Accessed: 18-Oct-2019].

BIOGRAPHIES OF AUTHORS

Azka Wani is is a full-time Research Scholar in the Department of Computer Applications, B S Abdur Rahman Crescent Institute of Science and Technology, Chennai. She completed her Bachelors in Information Technology in 2009 from Kashmir University, Kashmir and Masters in Information Technology in 2012 from Central University of Kashmir, Kashmir. Her research areas include IoT, Security in IoT, Software Defined Networks, and Network Security.

S. Revathi is working as an Assoc. Professor in Department of Computer Science and Engineering, B S Abdur Rahman Crescent Institute of Science and Technology, Chennai. She received her Ph.D. from Anna University in 2014. She has published good number of papers in the international journals and conferences. She is supervising six PhD scholars, and her research areas include Internet of Things, Mobile Ad-hoc networks.