Review of International Geographical Education | RIGEO | 2020

RIGE

ISSN: 2146 - 0353

Review of International
GEOGRAPHICAL EDUCATION

www.rigeo.org

Ransomware attack detection in Internet of Things (IoT) using IOTPOT platform with Ensemble Learning (EL)

* Ms. N. Ashwini,
Ph.D. Research Fellow, Reg. No. 19214012042058, Department of Criminology and Criminal Justice, Manonmaniam Sundaranar University, Tirunelveli

**Dr. Syed Umarhathab,
Assistant Professor, Department of Criminology and Criminal Justice, Manonmaniam Sundaranar University, Tirunelveli

Abstract

Internet of Things (IoT) has dramatically revolutionized in various purposes of humans in their past decade. It is a vast network device that may sense and store confidential data about its clients. The major issue faced by the clients using IoT platforms is security flaws that have mainly happened through small IoT devices. The latest ransomware attacks are TeslaCrypt, SimpleLocker, NotPetya, and WannaCry have broken the myth of protecting the digital data backup of organizations and it gets hacked by the intruder. In the IoT world, ransomware collides with each other; initiating cybercriminal activities more simpler. These activities are loading IoT devices with malware that generates an exact fire of cybersecurity arms race. The IoT platform has a large larceny view to the ransomware and intruder. However, it is highly dangerous that damages the complete security range services that result in the breach of sensitive information and life risks. Therefore, the robust Ransomware Attack Detection Honeypot (RADH) has been proposed with IoTPOT as a honeypot agent. It has addressed the challengeable security problems that consist of honeypot agents as a honey folder using IOTPOT. It is a decoy folder specifically to get intruded and perform as an earlier alrm system to signal the client at an apprehensive file actions. AuditWatch process act as an entropy module that certifies the files and folder entropy. CEP engine is assisted with Ensemble Learning (EL) has utilized for accumulating data from dissimilar security methods to train and test the behavior of ransomware, attack pattern, and immediately respond by confirming the ransomware attacks. Thus, the proposed RADH is trained with different samples from the dataset and tested experimentally with existing security attacks. Moreover, the outcome of the proposed RADH is comparatively produces better accuracy, precision, and recall in detecting ransomware attacks from the existing ransomware detection model. The organization of the paper is as follows. Section 1 a brief introduction on ransomware and its types; Section 2 presents a literature survey based on the various technique of Ransomware attack detection; Section 3 describes a proposed methodology for RADH architecture as a novel honeypot with IoTPOT and EL in the CEP engine; Section 4 describes the experimental setup followed by Section 5 that describes performance analysis based on detection of Ransomeware activities, accuracy, recall, and precision and Section 6 ends with the conclusion.

Keywords: Ransomware, Honeypot, Machine Learning (ML), security, IOTPOT, Honey folder, AuditWatch, CEP engine.

1. Introduction

The advancement of a worldwide network is said to be the internet that combined with the implementation of pervasive computing. The mobiles used with smart objects has given rise to the concept of an IoT, which has opened up new possibilities in developing digital solutions to various aspects of life. The IoT idea provides a network of items capable of communicating, interacting, and cooperating for a shared purpose. Every single gadget has stopped the work as a standalone device and becomes a part of a full connection system by IoT devices that has improved the human's daily life. It helps us monitor the properties far away from them and provides us better decision-making with the resulting data to be analyzed for tracking our businesses (Tankard, 2015). The interaction of sensors in IoT devices and decision-making has made independently with both internal and external environment conditions. The huge epoch of IoT is the dawning time in the digital world whereas practically all facets of our life have been experienced by big inventions. The effectiveness of today's IoT systems ranges from excessive data management to artificial intelligence.

In an IoT infrastructure, any interruption or malfunction of any devices may sustain disturbing threats to the process and reliability. IoT devices, ransomware attack has quite active while paralyzing and disrupting (Young and Yung, 2017). IoT Ransomware is a one of the malicious software type which prevents accessing of IoT devices unless a ransom has been paid (Su et al., 2019) and Crypto-ransomware (Almashhadani et al., 2019; Berrueta et al., 2019) are the two types of ransomware. The crypto-ransomware has encrypts the client files and prohibits the file accessing of user files from the client in the system, whereas the locker ransomware secures the overall system and restricts the system accessing (Khan et al., 2020). Most IoT ransomware uses the Locker version, which locks the overall device and prevents accessing. Meanwhile, the CryptoLocker is one of the attacks of ransomware is a hybrid form; which is the combination of locker and crypto-ransomware (Javaheri et al., 2018). In general, the model of an IoT ransomware attack differs from that of a traditional PC or smartphone. The IoT ransomware attack is considered to be serious threat since it gets launched at a time and location against the target IoT device. When the devices are unable to reorganize or prevent the ransomware's attacks that making them more eager to pay the ransom (Sharmeen et al., 2020). In an instance, hackers may place a certain thermostat to a high temperature in a smart home, or lock the control panel of a smart car without allowing access, or hacking an industrial IoT and also locking the smart power grids drug injection

pump hacking. Thus, set the drug composites for a propotion of abnormal during unlock the difficult and large ransom attack.

Moreover, some of the social media websites have been posting malicious links. When visitors visit the site, malicious parts contained present over the link gets downloaded automatically. For exploiting the flaws, ransomware obtained through such URLs may access the system and begin the encryption process. The ransomware has spread through downloaders namely portable media, drive-by download, botnets, water holing, and malicious. Malicious hackers are constantly looking for new ways to infect their victims. The user systems will be controlled by the attackers and encrypt all files in a variety of ways. The attackers take down the system that mainly exploits human weakness (Pathak and Vaidehi, 2015).

Based on the colonial pipeline as the present attack with results has illustrated the experience of ransomware and threat operators whereas the response generated from the agencies of law enforcement have endure several primary re-shuffling in dissident cybercrime ecosystems. From the concealed forums of hacking have prohibiting the posts associated with ransomware gangs that purposely withdraw their operations and various changes are noticed. However, uncertainity occur when the control gets achieved over effective records of darkside infrastructure or the “exit scam” is performed from the group. Therefore, the positive enhancement is analyzed from the complete incidents and the main changes obtain from the operations by other ransomware operators such as REvil and Avaddon. In order to avert an annoy from law enforcement, te group of avaddon ransomware has specifically imposed the “rules”. Thus, the rules have directs connection for excluding targets from various organizations such as educational institute, health care and public sectors. In addition, the gang of avaddon ransomware has generally deploys three-pronged technique for leading their operation with ransomware operations to elicit money from the concern victims. Besides data encryption and exfiltrating if the victim gets compromised and the gang maintain under DDoS attack till the ransomware geg is communicated and cooperated. The victims are fixed with deadline of 10 days as maximum after the data gets leaked into their dark web portal.

To detect ransomware, all hosts in the network have a Honeypot agent deployed as a monitoring agent to monitor all users and file system operations. The main goal of this study is to present a new RADH based on ML that collects massive amount of data from a variety of sources, including SDN network, Honeyfolder, Audit Watch, hosts, and Firewall. Then, the aggregation rules usage has turned the data into event instances. It even evaluates the occurrences present in the CEP engine to analyze attack patterns, malware behavior and respond quickly. Generally, the business dispersed security systems that generate a large volume of data. From the data streams, predicting abnormal occurrences is a difficult task which needs several computing capacity. There are activities like predicting ransomware behavior, attack patterns, decision-making, the fast rule engine advancement for converting data into event streams, and collecting events in real-time. The ransomware behavior has been identified from user activity and various data sources like SDN controller, Honeyfolder, firewall, AuditWatch are used.

2. Literature Review

This section provides a comprehensive understanding of current state-of-the-art technologies in IoT ransomware security, such as Honeypot and ML, as well as their significant background. The real-time implementation of honeypot within the internal organization's network is described by (Eliot et al., 2018). They discussed the numerous Honeypot types along with its benefits. Their argument is about honeypot implementation under a firewall in a production environment would be more successful. Tian et al. (2020) recommend installing a honeypot over pheripheral of an external method to fight against emerging continual attacks. In order to acknowledge an entire design and architecture of honeypot, Fan et al., (2019) has introduced a new architecture of honeypot as dubbed HoneyDOC. The HoneyDOC is made up of modules that work together, including as captor, decoy and orchestrator.

Zahra et al. (2017) have introduced 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. Dash (2018) have evaluated

ransomware instanced for two years and estimated the evolution of ransomware attacks in the upcoming years. The authors have presented a detection mechanism that focuses on Cryptowall ransomware which is one of the family from Crypto ransomware. The proposed method monitors the traffic among the server of Cryptowall and the IoT devices is Command and Control (C&C). The behavior of Cryptowall is also analyzed and the TCP/IP headers from the traffic are acquired to detect the ransomware attacks. The work presented by Baykara and Sekin (2018) has 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 utilized for detecting the ransomware. As per the outcome of KNN shows better performance among the classifiers used in experiment. Science (2014) a solution is proposed to keep the files safe from ransomware. An operating system software is proposed that limits the accessing for the file system. The software is considered to sit on cloud servers and compressed the files into a single file using Message Digest (MD5) algorithm. The files are kept in non-write mode, so that the files can't be altered. A log file is also maintained that keeps record of all the actions done on the files.

Rizzardi et al. (2016) proposed a secure mechanism called as Authenticated Publish Subscribe (AUPS) by expanding the existing IoT protocol. A novel key management technique has been introduced with secure subscription system in the protocol which are more efficiently and control the data flow over a system. Tao et al. (2018) established a novel security architecture to introduce an improved services over IoT based smart homes using cloud techniques which develops the flow of data across devices from various companies. This model does not fit the standards of security based on live IoT network systems. Moosavi et al. (2016) provided a comprehensive security solution based on IoT healthcare system. A TLS datagram has ability to resume the sessions which has been utilized between the users. The evaluation metrics of latency, throughput and energy consumption has more efficiently works with suggested approach than the existing methods. Though the consumption of energy consumes a lot but which are not as per the standards. Sicari et al. (2016) designed a distributed middleware layer system that allows heterogeneous data to maintain and its responsibility is considered. Moreover, the IoT data reliability is monitored and evaluated. Perumal et al. (2015) suggested a model to aid IoT network forensic experts. It is based on a multilayer approach for the preservation of volatile data. Despite

the fact that the proposed methodology may aid researchers, it is currently challenging to implement in real-world IoT networks.

3. Research Methodology

This research has focused on introducing enhanced security in various small IoT devices that get compromised and misused by existing methods due to ransomware attacks. The concrete of this study has involved proposing RADH as a novel honeypot with IoTPOT as the decoy honey folder or agent. The IoTPOT is evaluated by the interaction of telnet protocol with several IoT devices involved in collections from the internet. However, the IoTPOT is enabled to configure for rejecting all authentication credentials in observing malware attempts. The honey folder shall monitor the decoy folder continuously during the transition from one CPU to another in IoTPOT. Therefore, it is capable of verifying the actions of users and ransomware. Thus, each IoT device executes on various CPU architecture and embedded Linux OS have been prepared in Multiple CPU architectures present in the IoTBOX for managing the different device interactions. There are parameters such as read frequency and write frequency that is considered with generated scores. Once the scores have crossed a specific threshold, then the process is made to be recognized and alarm the firewall for preventing or kill the process.

The proposed RADH high interaction Honeypot server and Networks RAD Security devices like SNS controller, firewall, and load balancer have implemented at an endpoint of the network. However, the honeypot server will be able to manage any kind of traffic and even analyze it. The direct attacks such as malicious links and websites redirect the network and the Honeypot folder gets detected and report the attacking behavior to the firewall. Hence, the correlation of the CEP engine with several events from hosts as Honeypot agents, Audit Watch, SDN controller, IP tables, firewall will be classified and predicted by training of stacking concept introduced by ensemble algorithm is shown in figure 1. According to the CEP engine outcome and scores obtained from the malicious process are recognized and killed. The solutions have randomly segregated in terms of features and labels during initial process whereas each feature consists of one malicious process and client processes with N number. The fitness of every process has been estimated and compared it with other available processes over the features and the labels. However,

the adaptive scoring is utilized for calculating the fitness and the thresholds have been modified as flexible as in each iteration related to the CPU state. Hence, the fitness is estimated to assist in identifying the processes of malicious. The score has been sent to the EL with the CEP engine as the concluding process of event folders.

Adaptive threshold and scoring

There are several threads may available in each processor with various logical processors. The extraction of each thread consumed in the CPU and the overall CPU utilized by the process gets manipulated by accumulating all the values. Likewise, the system utilized by CPU at present is manipulated by accumulating the consumption of CPU for any kind of active processes. Hence, the threshold is estimated by formula as

$$\text{Adaptive Threshold} = \frac{\text{Total CPU consumed by single process}}{\text{Overall CPU consumed in the system}} \quad (1)$$

The estimation of threshold is done using maximum value setup as a major threshold in all iteration and the score gets distributed correspondingly to all features. Based on each malicious process deduction, the feature responsible probability gets increased whereas the maximum and minimum probability of the features get limited to 35% and 5% correspondingly. Thus, the demerits of single feature focuses are eliminated.

The client process and malicious is fixed as the ratio of N:1 for each row and every process fitness are made to be calculated in terms of Feature (F) array and Label (L) array. The algorithm of adaptive scoring will be able to estimate the scores for every process related to adaptive threshold. When the score of each process is generated will be compared with other process whereas the fitness comparison is done among client process (C) among malicious process (M). When the client process (C) fitness is lesser than M referes that the process is said to be malicious and similarly all the process in all kind of territories is made to be compared. Moreover, the Label (L) process fitness is compared with the C process. When the $C < L$, the label is considered to be client process which is placed into the territory. Hence, the C process is eliminated from the terrain and considered as L as well as C process with less fitness is eliminated from the terrain. Thus, the similar progress is endured for many iterations and the IoTPOT agent convergence is 25Secs. This IoTPOT has highlighted the M and send it to the EL assisted CEP engine for every 25 Secs.

According to the adaptive threshold, the extraction of feature by the Ransomware Mitigation System (RMS) has extracted the features and stored it in an array. The process of all kind of threads are listed and gets stored in the A_T as array. The processor data A_{Pi} array and CPU utilization per thread as A_{CPU} is stored as an array correspondingly. The total CPU T_{CPU} utilized in the process is estimated by accumulating all kind of values in the A_{CPU}. In addition, the CPU utilized by the system at present is O_{CPU} . Hence, the adaptive threshold A_{TH} is expressed in equation 2.

$$A_{TH} = \frac{T_{CPU}}{O_{CPU}} * 100 \quad (2)$$

Where,

T_{CPU} = Total CPU utilized for single process

O_{CPU} = Overall CPU utilized by all kind of active process

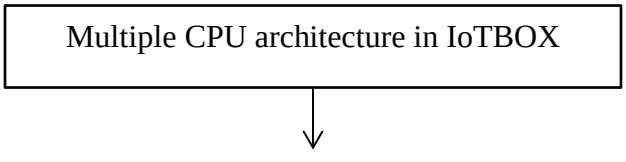
Similarly, the threshold value for memory usage has been calculated using the given below equation 3.

$$A_{TH} = \frac{T_{MU}}{O_{MU}} * 100 \quad (3)$$

Where,

T_{MU} = Total memory usage by single process

O_{CPU} = Overall memory usage by all kind of active process



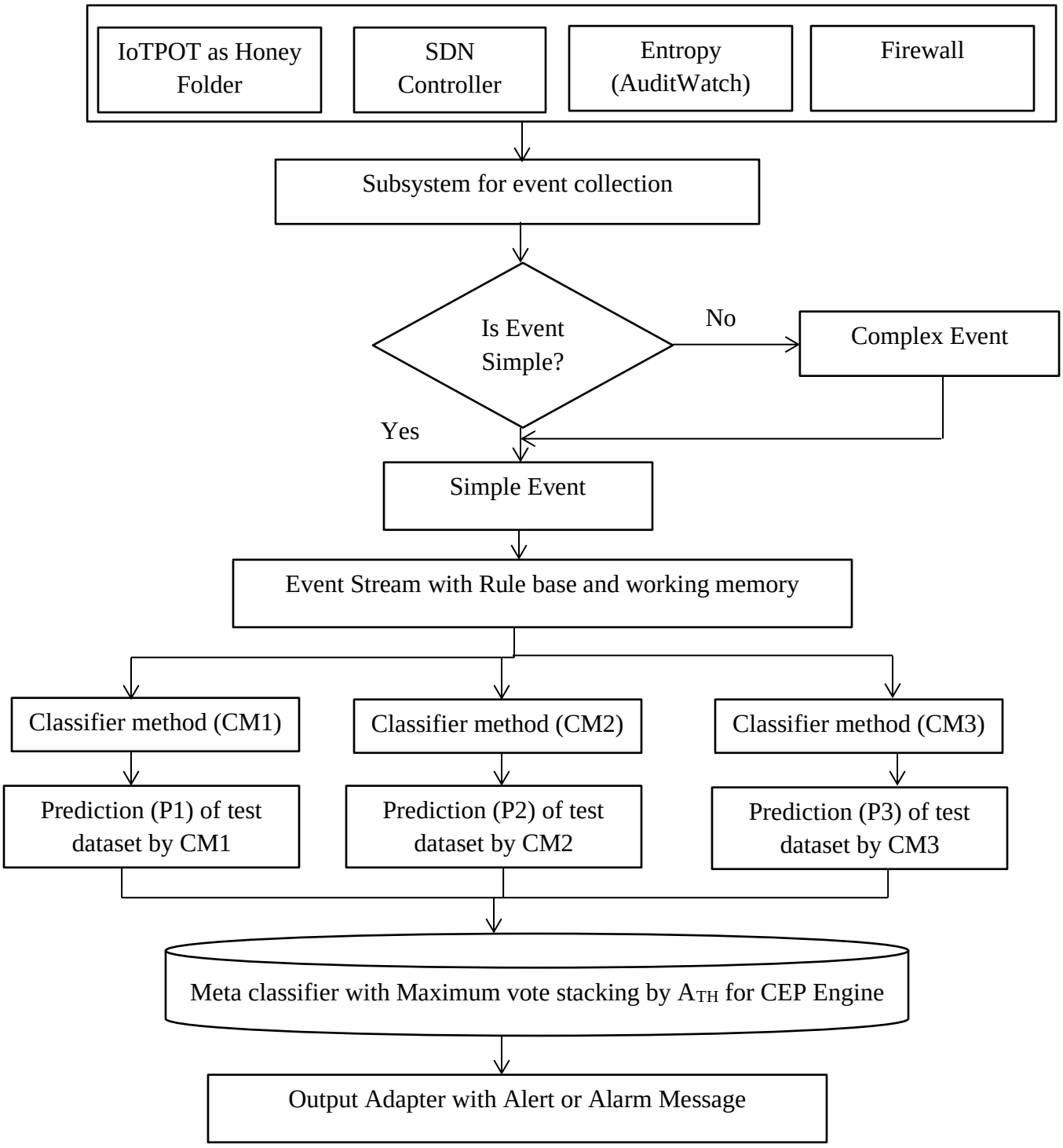


Figure 1 Proposed RADH architecture with EL

Moreover, the maximum threshold (M_{TH}) for the each iteration is fixed whereas the CPU extraction is detected and verified based on the range provided is $M_{TH} + n$ and $M_{TH} - n$. Where,

n = sample size auto tuning features for proposed RADH

Therefore, the sample size is fixed to be constant with value 10 due to highly tuned and hardened value for adaptive score. Thus, the similar process is done for memory usage that has been considered as M_{TH} for memory usage and even the threshold may be varied in all iterations depends upon system state.

Once the event collection is done and verified as simple event or complex event, the event stream has progress the events to the CEP engine by manipulating the rule base and working memory. EL is a technique of obtaining the task by organizing and merging various learners. Initially, it is essential for explaining the significance idea named with hypothesis over the area of ensemble learning. The collection of features function that estimate the adaptive score with several hypotheses such as $h_1, h_2, \dots, h_n$. The purpose of ensemble learning is to classify the events level based on the events sensor from the multiple CPU architecture of IoTBOX. The level of the events is obtained from the events sensors whereas the levels are mentioned as follows

1. Level 1- Collection of events
2. Level 2 – Refinement and preprocessing events
3. Level 3 – Refinement status
4. Level 4 – Threat Estimation

1. Level 1 – Collection of events

There are several events are collected as the input as an event sensors from multiple CPU architecture which get integrated with IoTBOX whereas the IoT devices are collected and stored in the IoTBOX. The sources available in the events sensors are Honeyfolder, SDN controller, Audit Watch, Firewall and IP address tables inclusive of timestamps reported through events stream to the CEP engine. Thus, the subsystem of event Collection has assisted in reading the inputs based on the frequency from different sources and the events.

2. Level 2 – Collection of events

In CEP engine process, the general step involved is collection of events from several sources is verified to noise, missing values, and various divergences and filtered. The major feature

extraction, selection and normalization are performed with ensemble learning. Events from various sources have been transformed into an appropriate format to be processed by CEP Engine with ML.

3. Level 3 – Refinement status

This level has discrete classification of event with various ML algorithms such as Logistic Regression (LR), K-Neural Network (KNN) and the Naïve Bayes to accomplish the usual or unusual events depend upon the adaptive score event range value. In RADH, the adaptive threshold (A_{TH}) represent the adaptive score of missing net flow present in the blocked processes, firing firewall rules, controller flow table, and diverse entropy range.

4. Level 4 – Treat Estimation

This level correlates the prediction of all three classifier whereas the maximum vote stacking is considered for the training event dataset for Meta classifier for predicting the complex event using a Support Vector Machine (SVM). However, the models of ransomware attacks are analyzed and compared using trained rule base of client process activities with ransomware activities. Hence, the refinement status has listed out the tuned and updates the decision variable for detecting the ransomware attack. Thus, it improves the performance of multi CPU architecture present in the IoTBOX.

However, SVM has the capability to provide better adaptive score for detecting ransomware attacks using the refinement status. Therefore, the proposed IoTPOT with EL technique is implemented in RADH architecture for providing an enhanced security from ransomware attack.

4. Experimental setup

This research has implemented the proposed RADH architecture for detecting the mitigating the CryptoLocker. The proposed RADH implementation shown in figure 2 contains IoTBOX with multi CPU architecture, event sensor devices and CEP engine with EL as a module. Based on the scenario, the user misguidedly opened the email of spear-phishing and gets attacked by the CryptoLocker. The event files and folders used from the IoTBOX for experiment is a single partition and get configured with IoTPOT as Honey folder which consists of various attracting images, videos, download archives. During an experiment analysis, it is identified that certain ransomwares have utilized asymmetric cryptography for dealing with harder threat to attack.

However, the provision of malicious process with client process with ratio of 1:N is progressed in the IoTPOT which perform as honey agent. Hence, IoTPOT assist the SDN controller infrastructure in filtering the apprehensive traffic and interrupt the transmission among the CryptoLocker and client honeypot server before the encryption process begins. When the ransomware has utilized symmetric cryptography whereas the key has made to be hardcoded in the malware that acknowledge itself for initiating the process of encryption. For this kind of secanario, IoTPOT as Honey agent has decoy the CryptoLocker for performing the action in the Honey folder. If the files are started to encrypt by CryptoLocker, the Honey folder has sends an alarm based on the activities of malicious process and the process is turned to stop.

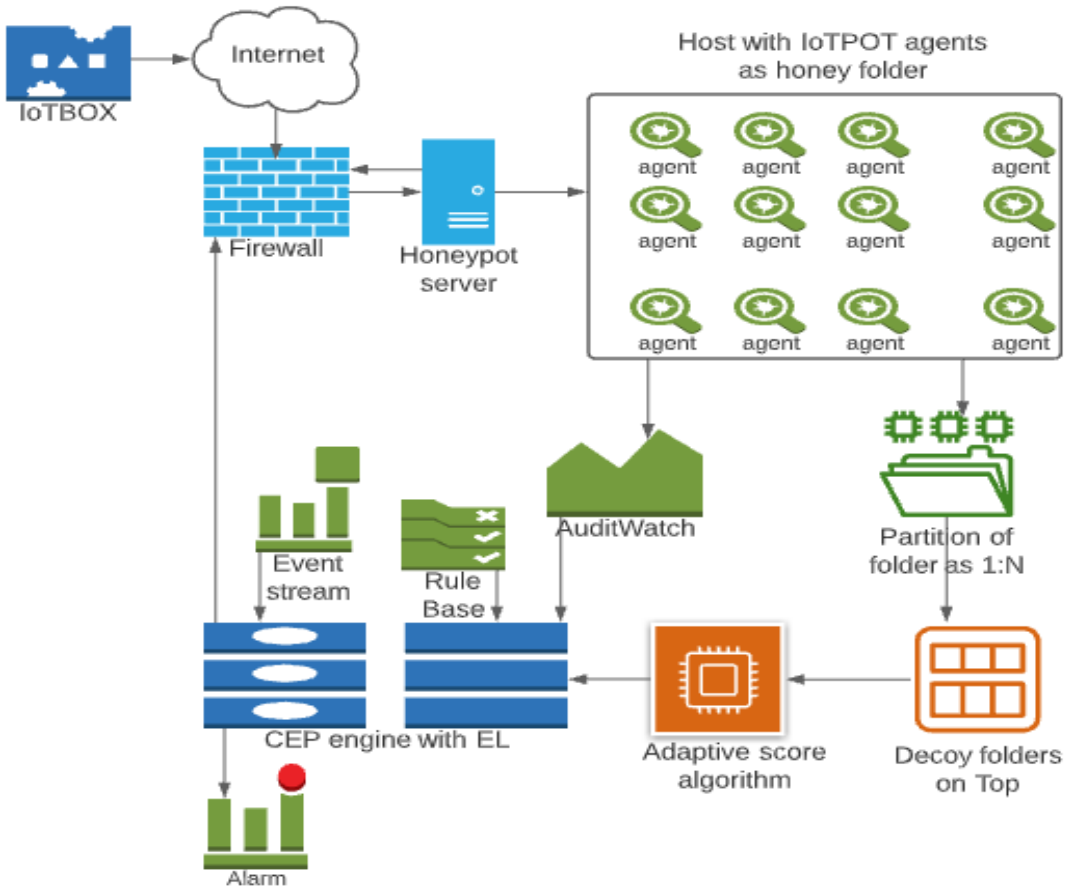


Figure 2 Deployment of RADH architecture in experimental setup

Moreover, the process is verified and the AuditWatch is used to estimate the entropy value to encrypt files and folders as well as entropy value is send to the CEP engine. Simultaneously, the CEP engine with EL may assist in correlating the adaptive scores progressed by IoTPOT Honey folder, AuditWatch, and SDN application are estimated and compared with A_{TH} and makes an

alarm with respect to the rule base which provides a high degree security from ransomware attacks and other attacks. Thus, the proposed RADH architecture has effectively stops the ransomware attacking process with nominal loss.

5. Result and discussion

Based on the technology of remote scanning, the prediction of an outcome with high accuracy and more authenticity is the focus of the experiment in the original honeypot servers and normal servers. The experimental procedures are implemented with i7-7700HQ CPU, 16 GB of memory, GTX 1050ti GPU, and python scikit-learn library for accomplishing ML model training. The proposed experimental procedure has been implemented on the system with multiple CPU architectures by considering the ransomware scenario like CryptoLocker. There are several processes included in CryptoLocker are illustrated. According to the infected folder assume that a CryptoLocker has utilized for compromising the victim via an email of exploit kit. Moreover, the exploit kit has targeted the vulnerabilities in the untracked security for the executed software on the user devices. Hence, the Angular Exploit Kit (AEK) is used for the CryptoLocker to obtain more performance. Thus, the AEK has been introduced due to better focuses in the identified vulnerabilities over an authentication and network services.

This repository consists of the dataset with ransomware seed and development procedure illustrated in the Ransomware Payments in the Bitcoin Ecosystem paper. Based on the consideration of an automated python script get executed in the ransomware dataset (Ransomware, 2020) for extracting all kinds of features as listed over the dataset. The execution of this extracted job needed an executing cluster with a GraphSense implementation and all pre-computing data. However, there are certain hosts and network features that have been considered. The samples send as the multiple DNS requests at the network from the client process and ransomware attack related to timestamp are considered in this research shown in figure 3.

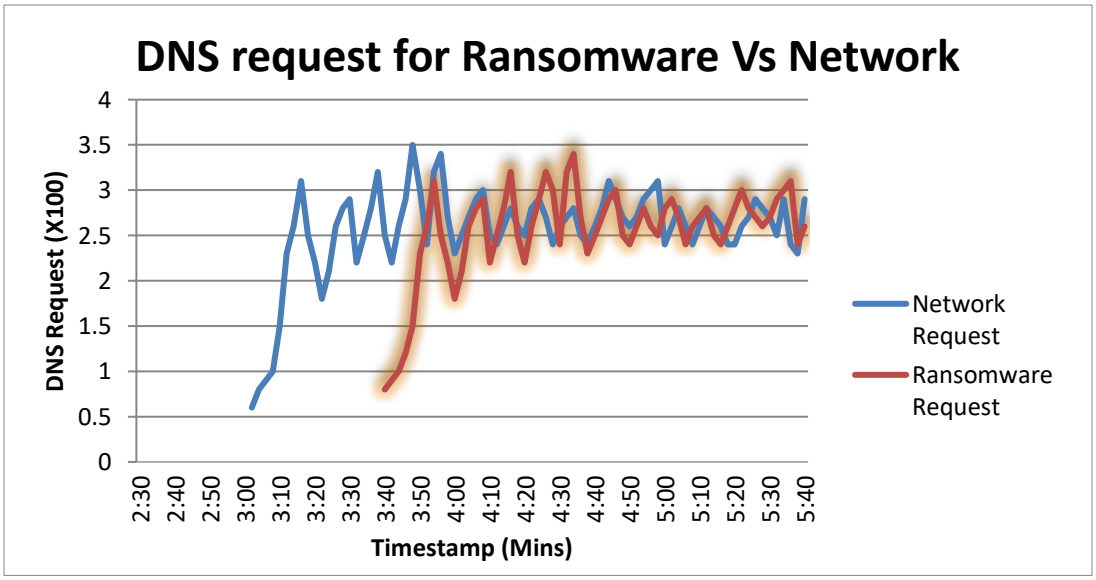


Figure 3 Comparison of DNS Request for Ransomware Vs Network

In the ransomware attacks, the samples are send as the multiple DNS requests at an appropriate interval of timestamp are detected using proposed RADH architecture is shown in figure 4. Therefore, the experimental analysis has identified more than 180 private proxies provided as well as more than 100 onion websites have been used to ransomware communication.

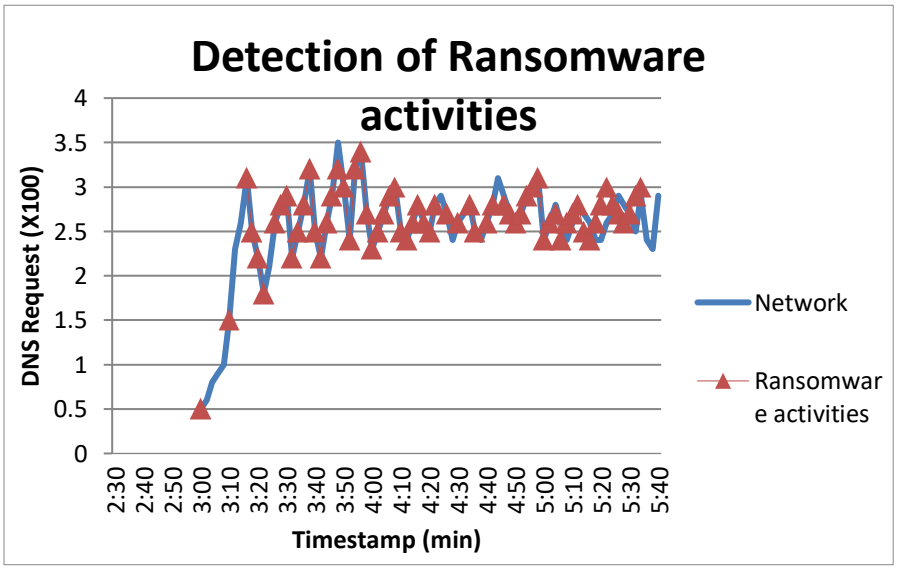


Figure 4 Detection of Ransomware activities using proposed RADH architecture

In addition, the SDN controller is used for filtering and blacklisting the domain traffics. When all infected host is annoying for communicating with all domains of blacklisted have been

assisted as automatic controller which obstruct the communication and alarms the system of multiple CPU architecture.

Based on the estimation of event sensors values for honeyfolder, SDN controller, firewall, Auditwatch are calculated through CEP engine. EL with CEP engine model is evaluated by maximum voting of adaptive score with significant model training part. Thus, the evaluation of model purpose is for accessing the performance of final ensemble model. This research has involved the accuracy, precision and recall to evaluate the RADH prediction. The determination of prediction the model Quality of Service (QoS) metrics with True positive (TP), False positive (FP), True negative (TN) and False negative (FN).

- TP = Honeypot servers number is classified in the honeypot servers.
- TN = Normal servers number is classified in the normal servers.
- FP = Normal servers number is classified in the honeypot servers.
- FN = Honeypot servers number is classified in the normal servers.

The accuracy of the ransomware detection model is calculated based on exact classification of transmission of files to honeypot server and normal server from the overall transmission of files to the honeypot and normal servers. The recall is calculated based on amount of honeypot server classified from the overall honeypot server number classified in both honeypot server and normal server. Similarly, the precision is calculated amount of honeypot server classified from the overall classification of honeypot server. However, the performance of RADH model is compared with the existing ransomware detecting models from (Cabaj and Mazurczyk, 2016 ; Du et al., 2020 ; Lee et al.,2019) have introduced for evaluating the QoS metrics. Figure 5 illustrates the accuracy of detecting ransomware attacks whereas the accuracy score from 10 samples to 150 samples are manipulated. The accuracy score gets increased with increase of sample files and from sample 100 there is a steady in accuracy score for all ransomware detecting method. The accuracy score has determined that proposed RADH method score high while comparing with the existing ransomware detection methods.

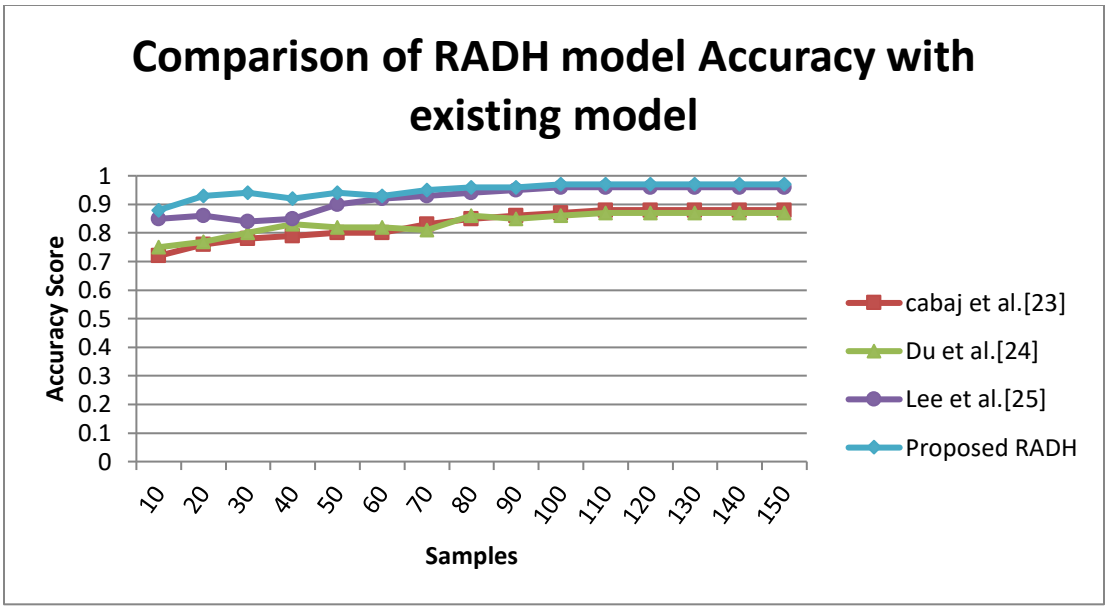


Figure 5 Comparison of RADH method Accuracy score with existing method

Figure 6 illustrates the recall of detecting ransomware attacks whereas the recall score from 10 samples to 150 samples are manipulated by confusion matrix metrics. The recall score gets increased with increase of sample files for all ransomware detecting method. The recall score has determined that proposed RADH method scored high while comparing with the existing ransomware detection methods.

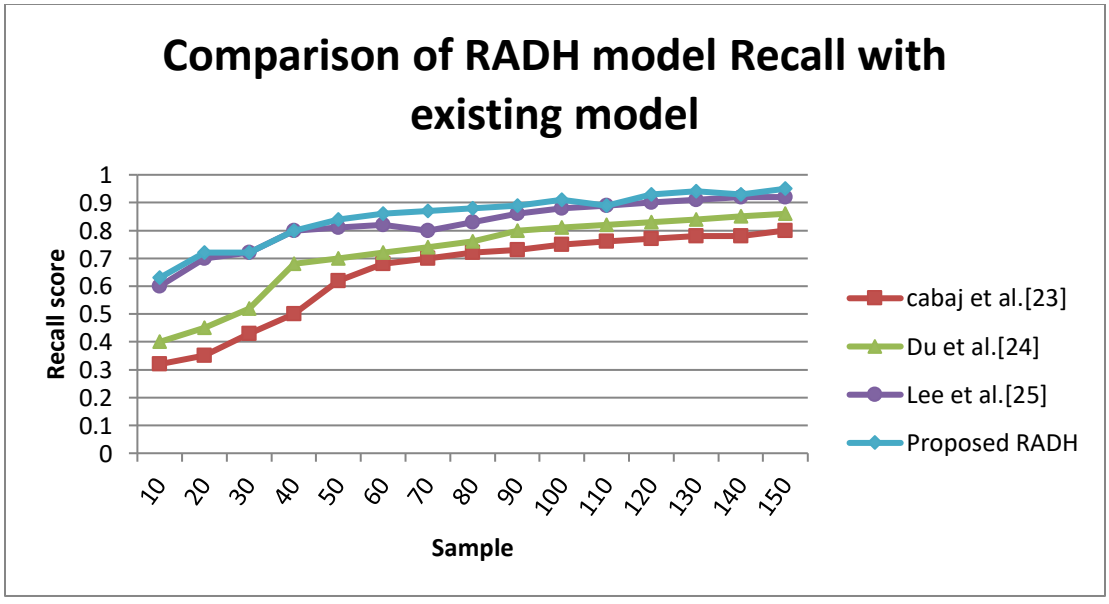


Figure 6 Comparison of RADH method Recall score with existing method

Figure 7 illustrates the precision of detecting ransomware attacks whereas the precision score from 10 samples to 150 samples have been manipulated. The precision score gets increased with increase of sample files for all ransomware detecting method. The precision score has determined that proposed RADH method score high while comparing with the existing ransomware detection methods.

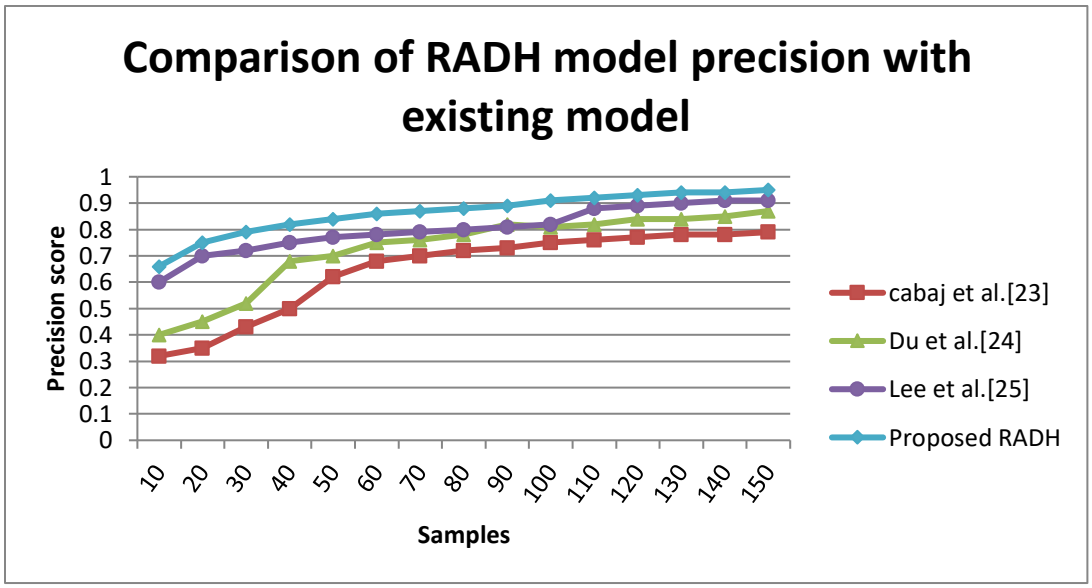


Figure 7 Comparison of RADH method Precision score with existing method

Therefore, the confusion matrix metrics have determined that proposed RADH model has detected the ransomware attack with high accuracy, recall and precision while compared to existing ransomware detection models.

6. Conclusion

This paper has introduced the RADH method in which the IoTPOT plays a major role as the honey folder that assists in collecting files from IoTBOX. The IoTBOX transmits the IoT device outcome through multiple CPU architectures are collected through event sensors. The proposed RADH with IoTPOT has utilized an adaptive score algorithm that assists in manipulating the score of client process features, labels and compares it with the adaptive threshold. When the estimated score of the client process is lesser than the threshold is said to be a malicious process. However, the components of the even sensor used are honeypot agent, firewall, Auditwatch, and IP tables. Therefore, the proposed RADH has used the CEP engine with EL for correlating the network features, host features and even calculates the scores from several events such as Firewall

and AuditWatch. Thus, the adaptive score is estimated by aggregating the event scores and feature scores to accomplish better accuracy in ransomware detection over IoT platforms. The experimental results illustrated that the deployment of Honeyfolder for monitoring the host system is highly efficient at representing attention for the host's ransomware. In addition, it is identified that the SDN controller usage has effectively improved the network security by implementing a controlled rule base. This proposed RADH has defended an organization by discovering the surfaces of the attack and creating digital risk profile that assist in predicting the imminent attacks by personalized cyber intelligence. In addition, it decode the cyber threat and even receives earlier alarm before cyber threat has been attacked. Future work has focused on restricting the ransomware activities while transmitting files from the host by optimizing the load balancer for accomplishing resource-constrained devices in an IoT environment.

Reference

Almashhadani.A.O, Kaiiali.M, Sezer.S, and Kane.P.O. (2019). A multi-classifier network-based crypto ransomware detection system: A case study of locky ransomware. IEEE Access, 7, 47053-47067.

Baykara.M and Sekin.B. (2018). A novel approach to ransomware: Designing a safe zone system. 6th Int. Symp. Digit. Forensic Secur. ISDFS 2018 - Proceeding, 1–5.

Berrueta.E, Morato.D, Magana.E, and Izal.M, (2019). A survey on detection techniques for cryptographic ransomware. IEEE Access, 7,144925-144944.

Cabaj K., and Mazurczyk.W. (2016). Using software-defined networking for ransomware mitigation: The case of CryptoWall. IEEE Netw, 30(6), 14-20.

Dash A. (2018). Ransomware Auto-Detection In IoT Devices Using Machine Learning. 0–10.

Du.M and Wang.K. (2020). An SDN-enabled pseudo-honeypot strategy for distributed denial of service attacks in industrial Internet of Things. IEEE Trans. Ind. Informat, 16(1), 648-657.

Eliot.N, Kendall.D, and Brockway.M. (2018). A flexible laboratory environment supporting honeypot deployment for teaching real-world cybersecurity skills. IEEE Access,6,34884-34895.

Fan.W, Du.Z, Smith-Creasey.M, and Fernandez.D. (2019).HoneyDOC: An efficient honeypot architecture enabling all-round design. IEEE J. Sel.Areas Commun. 37(3), 683-697.

Javaheri.D, Hosseinzadeh.M, and Rahmani.A.M. (2018). Detection and elimination of spyware and ransomware by intercepting kernel-level system routines. IEEE Access. 6, 78321-78332.

Khan.F, Ncube.C, Ramasamy.L.K, Kadry.S, and Nam.Y. (2020). A digital DNA sequencing engine for ransomware detection using machine learning. IEEE Access, 8, 119710-119719.

Lee.K, Lee. S,Y, and Yim.K. (2019). Machine learning based file entropy analysis for ransomware detection in backup systems. IEEE Access, 7, 110205-110215.

Moosavi SR, Gia TN, Nigussie E, Rahmani AM, Virtanen S, Tenhunen H, et al. (2016). End-to-end security scheme for mobility enabled healthcare Internet of Things. Futur Gener Comput Syst [Internet], 64,108–24.

Pathak.R and Vaidehi.V. (2015). Complex event refinement by statistical augmentation model. Int. J. Intell. Inf. Technol,11(2),55-69.

Perumal S, Norwawi NM, Raman V. (2015). Internet of Things(IoT) digital forensic investigation model: Top-down forensic approach methodology. In: 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC) [Internet]. IEEE,19–23.

Ransomware Dataset. Accessed: Feb. 22, 2020. [Online]. Retrived on 18.03.2021 from https://github.com/behas/ransomware-dataset

Rizzardi A, Sicari S, Miorandi D, Coen-Porisini A.(2016). AUPS: An Open Source AUthenticated Publish/Subscribe system for the Internet of Things. Inf Syst [Internet]. 62, 29–41.

Science C. (2014). Naive Bayesian Classifier And Pca For Web Link Spam. 1(1).

Sharmeen.S, Ahmed.Y.A, Huda.S, Kocer.B.S, and Hassan.M.M.(2020). Avoiding future digital extortion through robust protection against ransomware threats using deep learning based adaptive approaches. IEEE Access, 8, pp. 24522-24534.

Sicari S, Rizzardi A, Miorandi D, Cappiello C, Coen-Porisini A. (2016). A secure and quality-aware prototypical architecture for the Internet of Things. Inf Syst [Internet] 58, 43–55.

Su.D, Liu.J, Wang.X, and Wang.W. (2019). Detecting Android locker- ransomware on Chinese social networks. IEEE Access, 7, pp. 20381-20393.

Tankard, Colin. (2015). The security issues of the Internet of Things. Computer Fraud and Security, 9, 11-14.

Tao M, Zuo J, Liu Z, Castiglione A, Palmieri F. (2018). Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. Futur Gener Comput Syst [Internet] 78,1040–51.

Tian.W, Ji.X, Liu.W, Liu.G, Zhai.J, Dai.Y, and Huang.S. (2020). Prospect theoretic study of honeypot defense against advanced persistent threats in power grid. IEEE Access,8, 64075-64085.

Young.A.L and Yung.M. (2017). On ransomware and envisioning the enemy of tomorrow. Computer, 50(11), 82-85.

Zahra.A and Shah.M.A. (2017). 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, 7–8.