International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 1, ISSN No. 2455-2143, Pages 591-595
Published Online May 2020 in IJEAST (http://www.ijeast.com)

SECURE CYBER FORENSIC FRAMEWORKS FOR INTERNET OF THINGS

Prof Sagargouda S Patil
Department of CSE
JCER, Belagavi, Karnataka, India

Dr. Dinesha H.A.
Department of CSE
SGBIT, Belagavi, Karnataka, India

Abstract: The Internet of computers, tablets, and smart phones in our daily communications connects from leisure purposes to business tasks. An environment is deployed open and usage of resources limitedly make IoT vulnerable against attacks, whereas existing cyber Forensic frameworks and tools for investigation and processes are hard to obtain distributed and heterogeneous features of Internet of Things (IoT). Due to privacy and security protection of IoT, law enforcement agencies and investigators faces the challenges according to those characteristics. In this review, the various objectives in the cyber forensics researches were analyzed to understand the recent IoT techniques and its advantages. The limitation in the existing methods was also reviewed in this paper.

Keywords: Cyber Forensics, Frameworks, Internet of Things, Investigators, Security Protection

I. INTRODUCTION

The cyber security demand is rapidly increasing significantly on deployment of Internet of Things (IoT) for smart grid infra structure. However, the system is attacked by the hackers, where the credentials from the target vendor are stolen. The target is impacted on the type of attack and the type of consumers which performed cyber attacks. The attacks on the smart grid have been increased over the last few years. The losses on the attacks lead to increase in the environment concerns. The security in the cyber infrastructure of the smart grid is inappropriate to determine all the emerging and inadequate attacks [1,2,3]. The security of the system is ensured current posture of the existing and emerging smart grid security attacks in the data plane application with the associated interfaces [4,5]. The digital forensics is one of the branches in the forensic science that mainly investigates the crimes occurring in the digital field that attacks on digital devices. The categories include the computer forensics, mobile forensic, network forensics etc. The evidences are available directly on the digital investigation that is having the ability to carry the evidences within log files. The availability is included in the data bank for performing the investigation of the information retrieval about the causes in crime tracking their resources. The IoT digital forensics plays an important role for cyber crime investigation for IoT devices. The modern IoT attacks perform anti-forensics techniques for hiding the evidences that will be reflected for other attackers. However, in few cases, as the IoT devices increases in numbers in the amount of data transmission, processing and storing. However, IoT devices shows limited network for performing computation. That is the reason, reliable service in delivering the continuous information is challenging for the continuous information for constrained network environment [7]. The training platform for providing the security manages, designs and implements an expensive both in terms of efforts and time that needs objective for the clear vision. The maintenance, updates are essential for keeping the useful platforms interesting and faces the threats that are emerging [8,9]. The incentive mechanism offers a frame work in order to support potentially the smart city services securely for sharing the economy and interaction of cyber-physical with IoT block chain. The review on the unique contributions is justified by detailed system design and implementation of the framework [10]. The rest of the paper is organized as follows. Proposed Methodologies are explained in section II. Comparative analysis of existing system are presented in section III. Concluding remarks are given in section IV.

II. METHODOLOGIES FOR CYBER FORENSIC IN IOT ENVIRONMENT

The general architecture of IoT is shown in the figure [1]

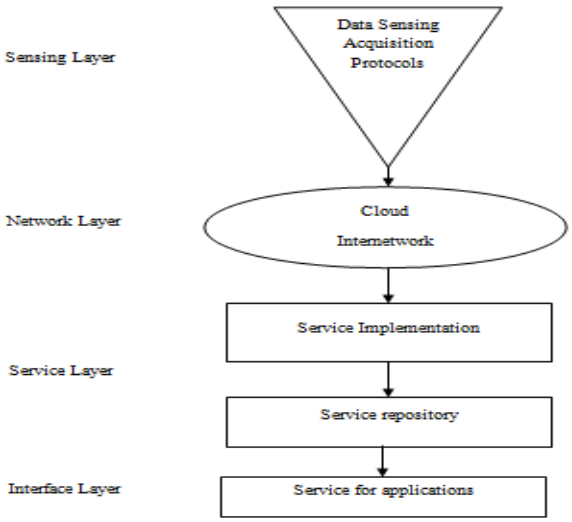

Figure 1: General IoT architecture

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 1, ISSN No. 2455-2143, Pages 591-595
Published Online May 2020 in IJEAST (http://www.ijeast.com)

In general, an IoT system includes large number of devices that consisted of infrastructure, applications and services of four layers as shown in the figure 1.

The description for the four layers are shown,

1. The first layer is the sensing layer that sense the information acquired from the devices such as smart sensor, components of IoT clients, Radio Frequency Identification (RFID).
2. The second layer is the network layer that set up connection between internet and other devices having suitable infrastructure.
3. The third layer is the network layer provides services to the users and manages for other applications.
4. The fourth layer is the application interface layer that provides an interface between the user and other applications.

The increase in the popularity of the occurrences in the attacks of IoT devices are expected to be due to such attractiveness properties in the IoT devices for attacks that compromise the systems for data filtration. In other words, IoT devices like 3D printer composed of smart switch or a smart bulb for accessing the gain to the smart devices uses the personal data from the user.

Taxonomy of IoT for Cyber Forensic

The IoT systems are having settings and configuration differing from each other that analyses the IoT forensic device specifications. The home system involves the devices that are involved in differing from Industry IoT (IIoT) systems. The approaches performed various numbers of attempts for the reconstruction of crime events scenes. An analysis is documented for finding such events scenes that may be useful for the persons working under judiciary.

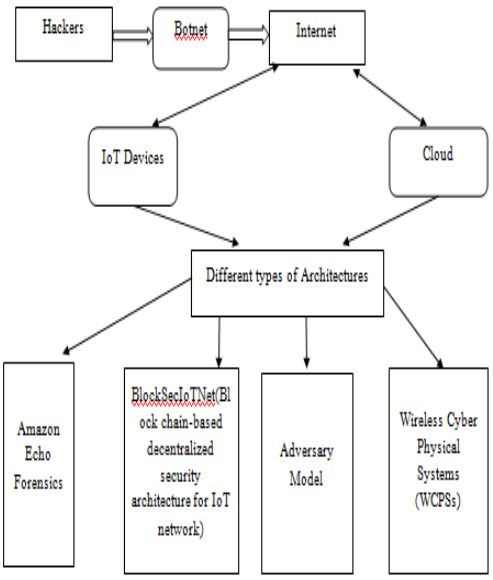

Figure 2: Taxonomy of IoT for Cyber Forensic

Amazon Echo Forensics

Amazon is a popular and an intelligent smart assistant also called as smart home assistant that takes the input commands into the system in the form of voice from users for controlling IoT devices or itself or sensors. The Amazon Echo examples includes smart kettles, lights, locks, doors and thermostats that uses voice recognition technology for interacting users with the IoT devices connected using the voice. In order to interact and to provide connection of IoT devices a sort of internet connection is required. The Amazon Echo is analyzed by involving prior work that reported the history of user data for the interaction with Alexa stored cache files in SQL database. During analysis of network, the JSON format is encrypted for performing the communication and analyzing parameters. The authors' analysis the communication between the API calls for the undocumented and revealed API calls to REST full Web services. From researches it was found that most of the data contained time stamps belonging to UNIX that was used for the creation of activities belonging to the timeline with an investigation. The application included in the API is to download the voice files such as iOS 10.1.1 + Alexa app, Android 4.4.2 + Alexa app, with, Windows 10 + Chrome, and OS X 10.10.5 + Chrome.

BlockSec IoT Net design overview

The present section shows the architecture design of the model consisting of layers such as sensing edge, cloud layers, edge, fog layers. The smart device is having a sensing layer that distributed widely the distinct environments of activities in the infrastructure publicly [11]. A huge amount of data is produced for data sensing and is forwarded to each layer of edge. The SDN enabled switches at each of the network's edge that performed low high power performance of the network. The SDN in the layer enabled the switch at edge layer connected the sensors of the network premises that analyses the data from sensors. The traffic is anomalously used for identifying the SDN controlling and manages the data responsible for updating with respect to the switches for instructing the attacks that are having low level of latency. The SDN delivers the results for the processing of data in the layer that controls and monitors a large scale cloud layer with long term monitoring condition in the analysis of data and behavior.

Methodological flow of BlockSecIoTNet

The proposed architecture uses a work flow approach performs bottom up approach that operates sensing layer at the end of cloud layer. The SDN operation enabled the edge layer switch for monitoring the traffic flow continuously in the sensor nodes. The sensing layer connected monitors the traffic flow at the sensor nodes and traces the fog node. The malicious traffic flow is analyzed from the sensor nodes that analyses the fog node identifies the flow of traffic from the sensor nodes. The SDN controller dynamically switches the SDN controller performance by means of traffic flow in the IoT devices. The actions consisted of applying the limits of rate of flow in the

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 1, ISSN No. 2455-2143, Pages 591-595
Published Online May 2020 in IJEAST (http://www.ijeast.com)

flow partially or fully in the block intervals observe the significant pattern of events in the fog node. The flow rules sets the SDN controller with respect to the switches dynamically. The SDN controller is defined by the SDN controller that performs action on the IOT devices based on the traffic flow that provides traffic flow decision about the traffic from the network located the IoT devices. Thus, the control of SDN assists the provision for providing security for the devices operated remotely that has no interventions at the end users. Similarly, from different clusters of events the waves incoming for attacking the devices from the network are concluded. Thus, the device helps in providing security with intelligence without intervention manually needed at the end users.

Adversary model

The adversary models are known for representation of an attacker and the potential actions for its value in representing the resources without using a cryptographic protocol. The capabilities for the adversary models derived from the previous researches are as described below,

1. Listen to channel or target: A communication channel is set
2. up to a target device and the adversary is allowed passively.
3. Transmits message to target: An adversary is allowed for transmitting the message to the destination, the adversary need to utilize capability of other message to obtain replies. Example: Listening
4. Modification of message to target: An adversary should be allowed for modifying particular message without device encryption. For an Example: If the file or configuration needs modification an adversary will be allowed only at particular condition without encrypting message because during transmission another adversary may misuse the situation
5. Intercept (Target): An adversary is allowed in order to receive all the messages at the target device. An adversary may choose to modify, drop or forward the message. This has the capability in providing combination of listening, transmitting and modifying the capabilities on the devices. However, the forensics contexts are not considered for this capability.

Corrupt (Target):

An adversary is allowed for obtaining control over the target device is having the ability to employ the capability to most of the attackers that are powerful. The capability of listening not makes any changes for evidential source forensically any differences and effects adversarial capability at the strict level. The classification was based on the modification and transmission for level of standard soundness and has the evidence of forensic at the potential. The attack is usually a part of real time of Intercept capability and is not used in post-event digital forensic investigation.

The data arbitrary is forwarded by the adversary over air and updates the devices that are matching to its firm ware. The adversary is added for the devices that are corrupting at the backgrounds are theoretically estimated. This is used as a powerful tool but infeasible attacker performs corruption and is not considered for the research.

Wireless Cyber Physical Systems (WCPSs)

An events of WCPSs is classified into three prototypes such as

- Data sending and receiving events
- Computing events
- Sensing and actuating events.

1. Data Sending and Receiving Events

Data used can send and receive the event pairs for sending the data flow from one node to another receives the data from one node to another having N nodes and are set to WCPS. DTMCs (Discrete-Time Markov Processes) pairs are used for performing sending as well as receiving processes from the event pair. The transceiver is computed based on the energy consumption in the equilibrium state in the DTMCs model.

2. Computing Events

The process of computing includes processing of main loop at the router, sensor or actuator or to control law for computing the task maintenance at the controller node. The computing events are set to present the procedures for the computation and executed at the node, The energy events are set for the energy evaluation to the memory and the MCU core parts for performing computational tasks at different execution stages on the embedded MCU.

3. Sensing and Actuating Events

The actuating event and the sensing event is set for denoting the sampling data rate at the sensor node and actuating event for denoting the actuator node. At the sensor node sampling events are triggered for sending the data events and computing data events at the same nodes is received the triggering events at another node. These all events organized as event chains that controlled loops at different flow of data. The event chain is extracted from the sampling rates of architecture model of the system that described the network data flows. Thus, the extraction of event chain rates the architecture model of the system describes the data flows and network nodes. The models are used for studying the energy models of these components that consumes energy of nodes and computes the energy from the control loops. This section presents the energy models for data transmission components of WCPSs.

COMPARITIVE ANALYSIS of existing system

In this section, the expected outcome of exiting works in Cyber Forensic-IoT system is reviewed.

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 1, ISSN No. 2455-2143, Pages 591-595
Published Online May 2020 in IJEAST (http://www.ijeast.com)

Table 01: comparative analysis of existing methods

Authors	Proposed Methods	Advantage	Limitation	Performance Measure
Koroniotis, Net al [12]	Support Vector Machine (SVM), Recurrent Neural Network (RNN) and Long-Short Term Memory Recurrent Neural Network (LSTM-RNN)	The results obtained indicated that the developed dataset trained accurately using classifiers such as Recurrent Neural Networks and their permutation (LSTM) outperforming the SVM implementation.	With regards to the number of folds, we observed a loss of accuracy when a higher number of folds was chose	Accuracy= 88.37% Precision=100 Recall =88.37% Fall-out=0.0146
Al-Sharif, Z.Aet al [13]	Cyber–physical Systems	Our results show that a program's statescan still be extracted even after the garbage collector is explicitly invoked, the software is stopped, or the JVM is terminated. This research helps investigators identify the software used to launch the attack and understand its internal flows.	In the same time, the speed of securing these systems does not match the speed of our adaption of these CPS, which are vulnerable to be attacked and compromised by various means.	Experimentation time = 125.26sec
Sani, A.S.,et al [1]	Identity-Based Security Mechanism (I-ICAAAN) Intelligent Security System for Energy Management (ISSEM)	The I-ICAAAN provided an additional level of privacy to components, data and events in EI when compared to the smart grid privacy features.	The developed I-ICAAAN needed improvement in privacy and confidentiality to components, data and events in order to maintain components and events integrity	CPU time 1200 mA, radio transmit 20 mA , radio listen 25 mA)
Do, Qet al [14]	forensic active and passive system	The adversary implied that the role was passive in the initial instance that minimized the potential sources modifications evidence	However, the extension of potentials integrated the forensics adversary model used for identification and exploitation results	Experimentation time = 120.26sec
Keshk, M., et al [15]	Wireless Cyber Physical Systems (WCPSs)	The energy consumption for each control loop and each node is estimated as well as the overall energy consumption. All these energy consumption indexes can help us to design a performance and energy consumption balanced WCPS	However, the decrease in amount of current saved energy and also increased the retransmission probability during the recovery caused energy consumption at high quantity thus created divergent nodes.	Total energy of 59.2% of and energy consumption of 20.1% of total energy. Time interval between control loops from 200ms to 800ms
Azmoodeh, Aet al [16]	Independent Component Analysis (ICA)	The power was evaluated for performing and evaluating the performance using CPS dataset, and the results showed high privacy protection more effective compared to privacy-preservation techniques	The confidential information was preserved by using non-linear and non-normal functions however has the limitation of specifying the representative features of proper number.	Accuracy= 94.61 Detection Rate= 90.07 False Positive Rate (FPR)= 9.72
Hossain, M.,et al [17]	KNN, Neural Network, SVM, Random Forest.	Dynamic Time Warping (DTW) Found closer energy consumption pattern and consequently provided classification accurately when compared to the existing models	However, other classifiers failed to achieve performance optimally for the specific size of the window	Accuracy =87.56% Detection Rate = 95.65% Precision = 89.19%.

III. CONCLUSION

Nowadays, a study of intrusion detection technology in Cyber-Forensic is a hot topic, which is an important method to ensure the network security of IoT. Therefore, Cyber platform relies on advanced intrusion detection tools to identify malicious activities and enhance the security of IoT environments by inspecting compromised devices and collecting forensic evidence so as to determine the source of cyber-attacks. In this study, the existing techniques on cyber-forensic are reviewed along with their advantages, limitations. Based on the existing techniques, a taxonomy based on collection of evidence, architectures, tools and the process of the models and forensics data processing. Cyber based effective techniques are used as a solution to dematerializes the CoC process of recording and preserving a chronological history of digital evidences.

IV. REFERENCES

[1] DiMase, D., Collier, Z.A., Heffner, K. and Linkov, I., 2015. Systems engineering framework for cyber physical security and resilience. *Environment Systems and Decisions*, *35*(2), pp.291-300.

[2] Rahman, M.A. and Hossain, M.S., 2017. A cloud-based virtual caregiver for elderly people in a cyber physical IoT system. *Cluster Computing*, pp.1-14.

[3] Ahmed, U., Raza, I., Hussain, S.A., Ali, A., Iqbal, M. and Wang, X., 2015. Modelling cyber security for software-defined networks those grow strong when exposed to threats. *Journal of Reliable Intelligent Environments*, *1*(2-4), pp.123-146.

[4] Rahman, M.A., Rashid, M.M., Hossain, M.S., Hassanain, E., Alhamid, M.F. and Guizani, M., 2019. Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city. *IEEE Access*, *7*, pp.18611-18621.

[5] Noura, H.N., Salman, O., Chehab, A. and Couturier, R., 2019. DistLog: A Distributed Logging Scheme for IoT Forensics. *Ad Hoc Networks*, p.102061.

[6] Jia, X., He, D., Kumar, N. and Choo, K.K.R., 2018. Authenticated key agreement scheme for fog-driven IoT healthcare system. *Wireless Networks*, pp.1-14.

[7] Matheu-García, S.N., Hernández-Ramos, J.L., Skarmeta, A.F. and Baldini, G., 2019. Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices. *Computer Standards & Interfaces*, *62*, pp.64-83.

[8] Chen, J. and Zhu, Q., 2019. Interdependent strategic security risk management with bounded rationality in the internet of things. *IEEE Transactions on Information Forensics and Security*.

[9] Dovom, E.M., Azmoodeh, A., Dehghantanha, A., Newton, D.E., Parizi, R.M. and Karimipour, H., 2019. Fuzzy pattern tree for edge malware detection and

categorization in IoT. *Journal of Systems Architecture*, *97*, pp.1-7.

[10] Deng, L., Li, D., Yao, X., Cox, D. and Wang, H., 2018. Mobile network intrusion detection for IoT system based on transfer learning algorithm. *Cluster Computing*, pp.1-16.

[11] Li, S., Choo, K.K.R., Sun, Q., Buchanan, W.J. and Cao, J., 2019. IoT forensics: Amazon echo as a use case. *IEEE Internet of Things Journal*.

[12] Rathore, S., Kwon, B.W. and Park, J.H., 2019. BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. *Journal of Network and Computer Applications*, *143*, pp.167-177.

[13] Koroniotis, N., Moustafa, N., Sitnikova, E. and Turnbull, B., 2019. Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. Future Generation Computer Systems, 100, pp.779-796.

[14] Al-Sharif, Z.A., Al-Saleh, M.I., Alawneh, L.M., Jararweh, Y.I. and Gupta, B., 2018. Live forensics of software attacks on cyber–physical systems. *Future Generation Computer Systems*.

[15] Sani, A.S., Yuan, D., Jin, J., Gao, L., Yu, S. and Dong, Z.Y., 2019. Cyber security framework for Internet of Things-based Energy Internet. *Future Generation Computer Systems*, *93*, pp.849-859.

[16] Do, Q., Martini, B. and Choo, K.K.R., 2018. Cyber-physical systems information gathering: A smart home case study. *Computer Networks*, *138*, pp.1-12.

[17] Wang, P., Liu, J., Lin, J. and Chu, C.H., 2018. Model Based Energy Consumption Analysis of Wireless Cyber Physical Systems. *Journal of Signal Processing Systems*, *90*(8-9), pp.1191-1204.

[18] Hossain, M., Islam, S.R., Ali, F., Kwak, K.S. and Hasan, R., 2018. An Internet of Things-based health prescription assistant and its security system design. *Future generation computer systems*, *82*, pp.422-439.

[19] Keshk, M., Moustafa, N., Sitnikova, E. and Turnbull, B., 2018. Privacy-preserving big data analytics for cyber-physical systems. *Wireless Networks*, pp.1-9.

[20] Azmoodeh, A., Dehghantanha, A., Conti, M. and Choo, K.K.R., 2018. Detecting crypto-ransomware in IoT networks based on energy consumption footprint. *Journal of Ambient Intelligence and Humanized Computing*, *9*(4), pp.1141-1152.