Design of Low Power Artificial Intelligence Model for Resilience of IoT Devices

Ashwini.S, P. Shanmuga Prabha, S.Magesh kumar

Abstract: ***Internet users are keep on increasing every day and may reach billions and billions of users in the next year, the users of android mobiles for connecting their utilities with internet making them saving their time and allow fast and precise data transmission. Most of the communication, entertainment, medical, health, life and educational activities are showcased into the internet to increase the market place better. The increase in android users may also increase the lack of security on our personal data which is saved in the cloud. The study is focused on most of the devices connected with IoT and their decision making capability on sensible things like real word sensor data or malwares etc. The methodologies user in the industry to safeguard the data, the techniques involved in the detection of malwares etc. The study also motivate us to find out the extendable research focus on Resilient management in IoT devices during malware detection.***

Index Terms: ***IoT devices, Security in IoT devices, Malware detection, artificial Intelligence, algorithms.***

I. INTRODUCTION

At this moment the real time systems closely depends on Internet of things, the scope of the Things of Internet (IoT) is escalating with the overview of a diversity of applications such as patient condition monitoring, making the smart agriculture, automation of home, easy and flexible shopping, etc. Variety of Devices in a shared IoT network are based on the Android system due to tractability, strength and device support, which is crucial for sensors which is interfaced.

Variety of IoT devices provides several eminent services which is related to environment sensing, monitoring and controlling operations only. Accordingly, the number of users and scope of Android devices increasing each and every day. It is evaluated that there will be roughly more than 6 billion smartphone clients by 2020 [1], [2]. Hence forth, the malevolent activity can affect directly the functioning of many devices connected in a network. The increased usage of android users in shopping the things, transactions, entertainment activities, medical and sharing the technical information obviously the hackers also getting rapidly increased in the form of software malwares, Trojans and other unique way of getting the user information in the cloud which is stolen by the intermediate peoples by large number.

Revised Manuscript Received on October 21, 2019.

Ashwini.S, Assistant Professor, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai.

P. Shanmuga Prabha, Assistant Professor, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai.

S.Magesh kumar, Associate professor, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai.

The leakage of personal information, contact number, account numbers and communication text also getting shared in the cloud. Nowadays most of the communication in the form of sharing the images, the personal images, and images of the documents, finger print information, and personal identity numbers are easily passed over into the internet. Literally many android systems may not use anti-virus or malware detection software to control the anonymous activities Trojan enter into the mobile. In the current epoch many research work focused on detection of malware for android devices. Moreover android devices are the impressive target for hackers since the data stored in the clouds through online transactions, entertainments, shopping each and every websites requires registration and thus it is freely available for the hackers to grab the data and personal information. Most of the existing systems are not focused on accompanying the safety of Things Net devices. In most of the applications especially in android applications machine learning act as a safeguard module which protect the system from malware, software generated Trojans etc.

Machine learning uses variety of algorithms to detect, predict and analyze the data using deep data analytic methods which is a standard principle and proven concepts. Even through machine learning algorithms detect the malwares effectively the capability of miscellaneous activities generated by malware software also getting expanded. The tougher malware capacity leads to demand for strong machine learning concepts which are not already applied into the existing methodology. Henceforth most of the machine learning algorithms are now focused towards hybrid models in which more than one number of deep learning algorithm is incorporated with the highly predictive methods.

II. LITERATURE SURVEY

The research topic entitled Design of Self-healing Grid through Jamming Resilient Local Controller Switching, in the year 2015, Authors LiuHongbo, Yingying Chen, Mooi Choo Chuah, stated that key factor of a insolent grid or simply we call as smart grid is nothing but a programmable software module which is capable of collecting the useful information from power grid to estimate the current updates and occurrences of power factors and power states. These information are collected through smart grid and transferred to data centres through wire or wireless networks.[5]It is also evident that the growth of wireless technology also act as a back bone for the altitude that Internet of thing touches today. However countable attacks of software and IoT devices with serious impact situations are happen in

launching wireless systems, like jamming attacks. Self-healing the solution which is discussed in the present case study. [5]The presented paper research work focused on developing hardware based self-healing technology in which the Things Net hardware automatically heal its software issues which also act as a artificial intelligence model.

Another reference work here we took for analysis entitled Dynamic Connectivity Establishment technique and Cooperative Scheduling process for QoS-Aware WBANS research work done by author Mr.Amit Samanta and Sudip Misra, in the year of 2018 In a hospital environment, where the patients are connected with wireless network using body area model equipped with patients requesting continuous health care requirements and services after a surgery or critical treatments condition. The peoples are subjected to connect with monitoring sensors which transfer the real time signals into the wireless channels. Things internet act as a reliable platform to store the patients monitoring information into the cloud where the medical officers access easily.[2] To secure the communication robust techniques are used through biologically inspired model, standard data encryption techniques and AI based encryption algorithms.[2] In this paper he clearly depicts the advantage of AI and configurable software encryption model to secure the patient information.

In the year 2016, Authors named Fang Yie , Chia yin, Ilsun You b,Kim-Kwang, Raymond Choo c , Chi-Lun Ho started their research work entitled a Smart Mobile technology based wearable sensor device through WBSN model. This methodology is most popular in detecting the physiological parametrs of the patients which is almost equivalent to biologicaly inspired model or another famous name called CABA which is nothing but continuous authentication system for physiological data protection. Most of the networks are nowadays connected with freeware software clouds which is capable of getting attracted by the hacking tools where the pattern of malwares enter into the hardware IoT devices implicitly.

[9] In the year 2017, the research work entitles “Secure and Reconfigurable Multi-Layer Network Design for Critical Information” stated in the Things Internet category by the authors Muhammad Junaid Farooq, Quanyan Zhu, evaluated a Things of internet based automation system in which the sustainability of IoT devices to cyber-attacks. Internet of battlefield things (IoBT) networks. IoBT networks are expressively changed from outdated IoT networks due to explicit challenges such as the absence of substructure, and exposure to cyber-physical attacks. Battlefield networks are revolutionizing the management and control of smart security systems in health care, transportation, etc.[9] The methodologies adopted will get changed every time when the cyber security hacking software approach the IoT devices. This kind of continuously updating system help the Smart Grid Battlefield network to work in a most efficient way of communication. The things internet also grab the optimization algorithms for assisting the commands and leverage the stochastic network to the changing environment.

In the year 2015, authors Joshua Saxe, Konstantin Berlin, research topic entitled “Deep neural network based malware detection using two scalable binary program features” entirely focused on deep learning algorithm usage for the malware detection system, which achieves more than 95% detection rate and reduced false positive rate (FPR) based on large malware dataset commonly accommodated in to the global cloud or commonly available clouds. In addition, the proposed research work by this author enables the classification system to achieve accurate and reliable malware detection model.

III. TABULATION

SLNO	YEAR	AUTHORS	ANALYSIS
1	2009	Ashton	Scope of android devices
2	2015	Joshua Saxe, Konstantin Berlin	deep learning for Malware detection
3	2015	Liu Hongbo, Yingying Chen	Self-healing systems
			Resilient jammers
			Hardware based Self healing systems
4	2016	Fang Yie , Chia yin, Ilsun You b,Kim-Kwang, Raymond Choo c	Contonous authentication systems
5	2017	Muhammad Junaid Farooq	Smart grid
			multi layer network
			IOBT
6	2017	Newman	AOT challenges
7	2018	Mr.Amit Samanta	BIA- biologically inspired algorithms
			WBANS
			Dynamic connectivity

IV. DISCUSSIONS ON METHODS

IoT Decision Making Devices

Relevant decision making in IoT devices is always on the scope since the capability of the device is judged by the decision making speed and accuracy of the devices connected with internet. The author Mr. Power and Heaven

in the year of 2018 designed a research work entitled Computing Smart devices using Internet of Things. This paper is focused on analyzing the IoT decision making procedures. The capability of IoT devices on particular pattern of inputs, it may the image input, face detection, Audio track, video sequence etc. Computing the connected targets in common cloud is discussed and decision making algorithms that impact the more on IoT devices.

In the year 2017 Newman stated in the Forbes article which is ranked the highest position in things of internet and top trending category in 2018. From the article information we clarify that challenges faced in optimizing the decision making capability of IoT devices. Some of the discussed things are pointed out here.[9] Cyber Security is the most challenging task which is keep on increasing and adopting the internet environment for sustaining the changes becomes difficult to protect the highly sensitive privacy data and keeping the constant security on that data.

Fig. 1 Smart Android of things

Challenges of IoT Devices

Because of the impressive facilities available in android and global websites, the usage of Data analytics in every aspect of programs become wider. The theory of data analytics suggests that when analyzing the historical dataset, the practices, experiences, pitfalls and solutions it becomes easier for the IoT devices to make decision by self-correcting the mistakes and adapt the newly changing environment.

When talking about the role of IoT in decision making using machine learning techniques, it is also important to assess the ambient changes of people environment networked data sharing etc. The IoT act as a decision making device face challenges which is almost relevant to the human decision on particular problems. The solution identification is relevant to the humans also the generation of confusion also relevant up to the human's level.

Types of IoT Decisions

When discussing in detail about the IoT devices reacting on decision making, we also intended to intrude deeper about the types of decision that the devices can overcome will be considered. The decision of IoT devices may be direct decision, distributed decisions, networked decisions, Hybrid decisions etc. When a large set of sensor data flow into the IoT devices obviously the decision making capability of the devices get become resilient. Direct decision of the IoT devices is nothing but in the time of sensitive data coming into the IoT node, the values and threshold are closely related to the pre stored data range in the near memory.

Decisions will be generated quickly and precisely during these kind of data entry. Distributed decision is defined as the decisions which are generated through a hierarchy of distributed models connected with the master IoT device. Henceforth the decision is based on the combined decisions of the all connected models. These kinds of decision making intended us to discuss two scenarios. One, when the distributed models are fully equipped with the required dataset information, the decision release will be faster and precise, other hand if any one of the distribution system doesn't equipped with required amount of information will make the system resilient and that can be carry forwarded to the fore coming blocks. Networked decisions are designed by combining more than one node information which is relevant for making the correct decision.

Device Resilience

The evident model of IoT systems or the always connected android of things which are present everywhere with sensors, gadgets connected with the internet in which billion billions of peoples and devices connected together. Having this large scale accountable connectivity model, there will be also the same amount of problems and issues faced by the devices when monitoring and handling the accessibility. The chapter discuss in detail about the resilient of IoT devices which is the prime factor of the overall capability of the IoT devices n long run. The reliability of the device also depends upon the dynamic changes and sensitivity of the devices to those occurrences matters. The future near is mainly embossed on current applications of IoT devices in various sectors. The adaptive nature of IoT devices is most important but still the implications on Resilience need to be adjusted or avoided to provide promising business benefits and research opportunities. The important factors need to discussed or analyzed here to find out the possible cause of resilience is discussed in sec(c). Some of the mandatory nature of IoT devices and system functionality is discussed below.

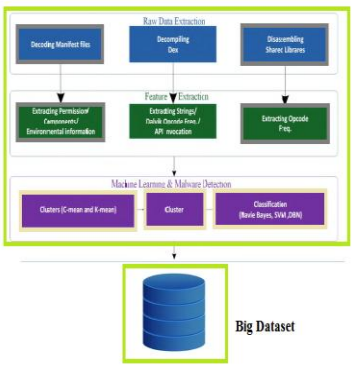

Fig. 2 Process of Malware detection

Self-Regulating Systems

The capability of the IoT devices to resist disturbances, crises, noise interference and evaluating the system control adaptable to changing environment and change in decision making model according to the previous decisions, experiences and dataset knowledge gathered will be proudly called as a self-regulating IoT devices in use. Most of the android of things model mentioned in Fig 1 will be the example for self-regulating model not the fully developed model.

Stabilized Model

The stabilized model of IoT architecture is capable of handling the fast and constant occurrences of the perturbances, noise interference and confusing nature of Malware triggers etc. Such IoT devices are more stable and capable of sustaining the system model until the changing nature of inputs get disappear.

Low Latencies

System with low latency is most important in the IoT devices of android of things devices in which the propagation delay of each data packets get carry forwarded to form a huge scalability of data which affect the response rate of the devices in sequence of IoT Cloud.

Static Analysis

Single class topographies: The benefits of single class topographies are easy to excerpt, and low power processing. The boundaries associated with this method are code barrier, simulated attack and low exactitude.

Multi class topographies: The advantages of multi class topographies are easy to excerpt, and poses high accuracy. The limitations associated with this method are Impersonation attack, high computation strategy, code mystification, and difficult to handle multiple topographies in the single system.

Dynamic Analysis

Single class topographies: it poses a better accuracy and easy to recover code clouding as compared with static analysis. Moreover, its topographies extraction process is difficult, and it consumes high resources in the IoT devices hence the device will overload from time to time.

Multi-category features: It gives better accuracy and easy to recover code obfuscation as compared with a static and dynamic single category. The limitations of this approach are:

1) Difficult to manage multiple topology conditions,
2) High resources handling and maintenance, and
3) More delay computation and latency.

Hybrid Analysis

The main advantages of hybrid analysis are to accomplish the highest accuracy as compared to static and dynamic analysis. The limitations are

1) Highest complication,
2) Context requirement to combine the static and dynamic topographies,
3) More assets deployment, and
4) Time consumption issues

V. IMPLEMENTATION

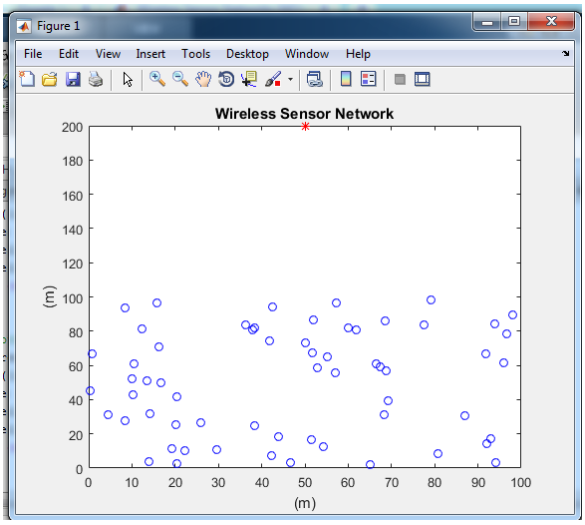

Fig. 3 Node Creation

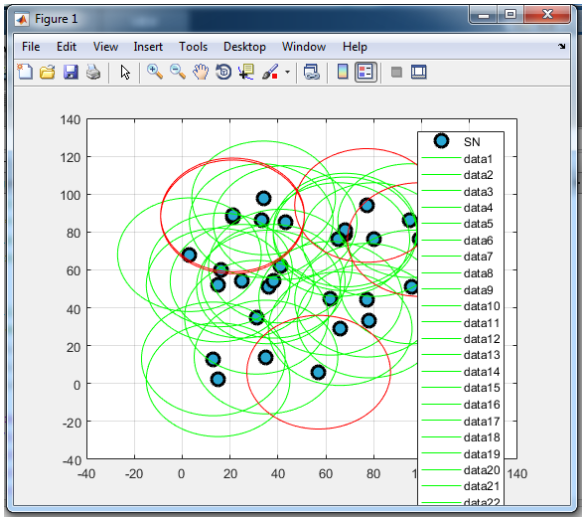

Fig. 4 Node Deployment

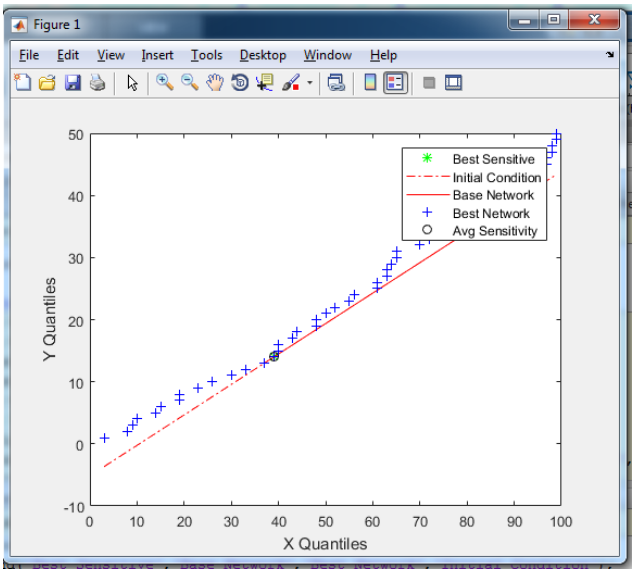

Fig. 5 Sensitivity Plot

VI. RESULT AND CONCLUSION

The overall study focused on analyzing the various methods and algorithms available for IoT devices security and cyber security. The study stated to focus on gathering papers related to IoT device configurations, methods involved in IoT device management, sensitivity handling, stability, static and dynamic response etc. The Resilience of decision making in IoT devices are clearly discussed here. Android based IoT devices and applications are working time to time to realize IoT dreams. Henceforth the discussion is focused on finding the solution or reliable model to extend the framework to next level of research. The detailed decision making problems and types are discussed here. The upcoming extension of this work should go with the creation of hybrid algorithms which are working together the highly stable machine learning concepts together to form a new model. The extension of the study will focus on generation power conscious and reliable machine learning algorithms which make the IoT devices more sensible and accurate on decision making.

REFERENCES

1. Ashton,survey of Internet of Things, RFID Journal, published June 22, published in the year 2009
2. Author Hullum, Research entitled Threats and 3 Benefits of the Internet of Things in real time applications, January 2018 Published in Intel Corp. blogs
3. Author Heavin, Research entitled Random Data based Decision Making and Digital Transformation systems, in the year 2018
4. Author Puri, "Development of IoT decision making improved with impact-sourced human experts a novel approach, published in 2016
   In 2009 Mr.Ashtom, research paper titled “Enabling IoT Precision mdules” IEEE transaction.
5. Authors Joshua Saxe, Konstantin Berlin, 2015 on Conference about” Deep learning malware detection”
6. Year 2015, Yingying Chen, “Research on Resilient jammers” on IEEE transactions
7. author Fang Yie , Chia yin, Ilsun You b,Kim-Kwang, Raymond Choo c, in the year 2016, published research paper on CABA – continuous authentication on IEEE transactions.
8. Newman, in the year 2017, published articles on Forbes , discussing about WBANS, Android of things challenges”, Forbes India.
9. author Park, T. Y. Youn, H. B. Kim, K. H. Rhee,”Smart Connectivity based system for an IoT data marketplace,"published in Sensors, IEEE 2018