INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

A Conceptual Model for Internet of Things Risk Assessment in Healthcare Domain with Deep Learning Approach

Mohd Nizam Zakaria[1], Nur Azaliah Abu Bakar[2]*, Hafiza Abas[3], Noor Hafizah Hassan[4]
Advance Informatics Department, Razak Faculty of Technology and Informatics
Universiti Teknologi Malaysia
Jalan Sultan Yahya Petra, 54100 Kuala Lumpur, Malaysia
[1]mohdnizam-1979@graduate.utm.my; [2*]azaliah@utm.my; [3]hafiza.kl@utm.my; [4]noorhafizah.kl@utm.my

Submitted: 04/07/2020. Revised edition: 18/08/2020. Accepted: 24/08/2020. Published online: 19/11/2020
DOI: https://doi.org/10.11113/ijic.v10n2.263

***Abstract*—The Internet of Things (IoT) has become a prevalent technology in the IT industry. One of the industries that can benefit extensively in this technology is healthcare. However, the healthcare IoT is still under debate with several studies suggesting it is lack of interoperability, security, and too much complexity. Even more, the risk involved in deploying it is still enormous. Many traditional risk assessment models are unable to provide a specific IoT risk guideline and specification, especially in the healthcare area. Thus, it is essential to understand the full extent of the IoT risk and how to manage its risk in the healthcare area. The risk management models, such as NIST SP 800-30, ISO/IEC 27005, OCTAVE, CRAMM, and EBIOS, which are among the leading and widely used in many areas and healthcare fields, have also been described. Besides, this paper includes a review of three IoT risk assessment models that are based on ABA-IDS, Deep Learning, and AHP-SVM. Based on the review analysis, we proposed a new enhanced healthcare IoT risk assessment model, which aims to provide a real-time monitoring and mitigating risks that incorporate the NIST SP 800-30 framework, ABA-IDS, and CNN deep learning. This shall constitute a better classification of each risk identified to find the best risk mitigation plan.**

Keywords—Risk Assessment, Internet of Things, Healthcare, Deep Learning, NIST SP 800-30, ABA-IDS, CNN

I. INTRODUCTION

Internet of Things (IoT) has become one of the hottest topics in recent technological and information technology-related fields of study. In simple terms, it described as an interrelated computing device, peripherals, mechanical systems, or even living beings; each has a unique identifier that enables them to send information to the digital world without any human intervention. Vermesan, *et al*. [1] described it as a medium where the physical and digital worlds connect. At the same time, Peña-López [2] stated that it is a framework that embeds computing and networking capabilities in any imaginable artefact. Although each IoT framework is different, the basis for each architecture of IoT and its general data process flow is essentially the same. AVSystem [3] describes IoT in its simplest architecture form, as represented in Fig. 1.

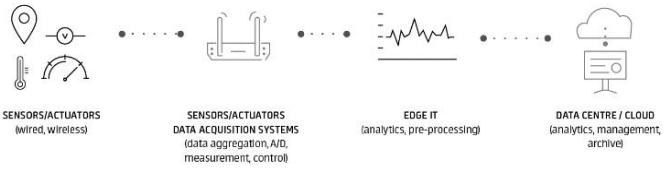

Fig. 1. IoT Architecture [3]

First, it consists of 'Things,' which are internet-connected devices that can sense the world around them through their embedded sensors and actuators and gather the information that is then passed on to IoT gateways. The next stage is IoT data collection systems and gateways collecting the overwhelming mass of unprocessed data, converting it into digital streams, filtering it, and preprocessing it, so it is ready for review. The third layer is edge tools responsible for further processing and enhanced data analysis. This layer also includes visualisation and machine learning technologies. Then, data is moved to data centres, either cloud-based or locally installed.

Data are stored, treated, and analysed in-depth for actionable insights.

The Industrial Internet of Things (IIoT) refers to the expansion and usage of the IoT in industrial industries and applications. IIoT focuses on machine-to-machine communications, big data, machine learning, and communication. This technology increases the performance and competitiveness of industries. It involves IIoT in robotic systems, manufacturing processes, and even software-driven devices [4]. Implementing IIoT provides enhanced data, increased awareness of the situation, and the ability to act more quickly and independently.

Among the top industries implementing IIoT are automobile, manufacturing, agrotechnology, healthcare, hospitality, energy and utilities, transportation, smart homes, and building. For example, in AgroTech, farmers use IIoT technology to generate more. They meet demand while in healthcare; it increases lifesaving abilities by helping to improve patients' quality of life in allowing self-monitoring and health management. Most of the infrastructure about medical technology such as health analysers, heart rate machines, x-ray, and scanner machines are maintained and monitored by every departments' authority. For example, hospital staff receives alerts for repairing and maintaining medical equipment such as MRI machines, ventilator machines, cardiac monitors, and other equipment by connecting them to the internet [5].

Studies have demonstrated that healthcare IoT is still lack of interoperability, security and too much complexity [6-8]. It is essential to understand the full extent of risk assessment models from the new scenario of the IoT healthcare perspective, which immensely involved not just in hardware technology but also from the intelligent learning aspect from the security risk data collected. Therefore, the emphasis of this work is on providing an enhanced IoT healthcare risk assessment model with deep learning for risk identification classification

II. Risk and Challenges of IoT in Healthcare

Still, there exists a question yet to be fully answered. "Which industry has the most risks affecting it, and what is the risk involved?" From a developer standpoint, four domains have critical risk when implementing IoT, such as smart meters, eHealth, security and emergencies, which from the results, two of those belongs to healthcare [9]. Healthcare industries are more prone to IoT risks because of the type of data it handles and the severity it can cause if something malicious happened to those data and information.

As discussed by the previous study, the breach of access occurs to life-sustaining equipment such as ventricular aids, pumps for injection of medications, baby inspectors, or incubators. The impact will be catastrophic [10]. In 2017, the United States Food and Drug Administration had to issue recalls on 500,000 heart pacemakers devices due to their lack of security which it happened that the pacemakers can be hacked to run batteries down or even alter a patient's heartbeat [11]. In certain situations, the intruder can have direct control over IoT devices, with potentially catastrophic results [12]. The following subsection explains the healthcare IoT risk from both technological and business perspectives.

Technological Challenges

From a technological perspective, the challenges highlighted are security, confidentiality, accessibility, the complexity of data management, and data flow.

1) Security Risk

As the number of connected devices grows, the opportunity to bypass security measures increases, creating countless attack paths for malicious actors to carry out their evil intentions. This leads to IoT developers to provide embedded system programming without considering the risks. In case of an emergency, most IoT devices don't have controls to protect their network from threats [8]. It therefore, poses a challenge for the health provider in maintaining and ensuring the protection of its assets, including the IoT application.

2) Confidentiality

Many IoT devices are deployed in the global scope. This leads to accounts of trust that these devices will collect peoples' data without respecting their privacy. Usually, system resources available for an IoT device is minimal, some only 8-bit. Hence, it makes it difficult to program more sophisticated security features in it and make it easy for hackers to target it and elicit confidential information from it [13].

3) Accessibility and Connectivity

With IoT technology racing, connecting so many devices will be a significant challenge for IoT's future. Current networking solutions have failed to handle an enormous number of devices at a time. The centralised server-to-client model has to adapt the peer-to-peer model so that devices will always stay online. Also, when dealing with healthcare applications, one cannot afford a delay in connectivity [13].

4) Compatibility

As for now, there are many different transport mechanisms existed for IoT. Different developers use different technology for their products. For instance, some vendors prefer ZigBee over Z-Wave. When these devices try to connect, there will be difficulties incompatibility for information exchange. In healthcare, power consumption and emitted radiation from IoT devices must be maintained as low as possible [14]. For different standards, a smooth transition in terms of speed and bandwidth is always challenging to maintain. With different bandwidths, the power consumed by the system will be adversely affected, and the efficiency will be lost.

5) Complexity

Different devices that interconnect with each other will need an interface hence would make heterogeneous

architecture challenging to manage [15]. This can also raise the risk of errors and make it challenging to communicate with other IoT devices [6].

6) Data Flow

Bandwidth is crucial for continuous data flow. With higher bandwidth, it will ensure smooth information exchange. Nevertheless, different or higher bandwidth can also lead to higher power consumption and emitted radiation [16].

7) Data and Analytics Complexity

The typical procedure seen in this industry is that they directly send their sensor data to the data centre or cloud [15]. This is not always the best option as it can make latency, drive costs, and unlock security risks. The massive amount of data collected through IoT devices also requires more processing time, as enormous extract-transform-load processes are required. [12].

Business Challenges

From a business perspective, if a domain such as healthcare wants to embark on IoT enabled environment, a sound business model must satisfy all the requirements needed for it to succeed. Starting with high expectations, many companies embark on their IoT journey but ended up disappointed, as reported by Nesse, *et al.* [17]. Report by McKinsey and Co stated that IoT could create up to 40% potential value if only interoperability issues are solved [18]. While many reasons may affect in unsuccessful implementation of IoT, one of the main reasons contributing to it is a failure to assess the risk involved. In the next section, we will investigate the relevant risk assessment model for the IoT healthcare environment.

III. Related Works on Risk Assessment Model

From the literature, the need for an intelligent IoT risk assessment model with simulation and modelling that can boost risk prediction is suggested. [6, 19, 20]. From these current risk assessment models and the new design of IoT risk assessment models, there are many key concepts in IoT healthcare risk assessment, such as properties, weaknesses, risks, attack, probability, and impact or cyber damage.

Risk Management Methodologies

This study focuses on five widely used risk management methodologies in the information technology environment, namely 1) NIST Special Publication 800-30. Risk Management Guide for. Information Technology Systems (NIST SP 800-30), 2) Information technology — Security techniques — Information Security Risk Management (ISO/IEC 27005), 3) Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), 4) CCTA Risk Analysis and Management Method (CRAMM) and 5) Expression of Needs and Identification of Security Objectives (EBIOS).

1) NIST SP 800-30 Framework

NIST SP 800-30 Framework is a compilation of information security policies and standards established by the National Institute of Standards and Technology (NIST). Risk evaluation, according to NIST SP 800-30, is to determine the likelihood of a future adverse event, IT system risks must be balanced with the potential vulnerabilities and IT system controls in place. NIST SP 800-30 framework for risk management includes nine major steps: Step 1 System Characterisation, Step 2 Threat Identification, Step 3 Vulnerability Identification, Step 4 Control Analysis, Step 5 Likelihood Determination, Step 6 Impact Analysis, Step 7 Risk Determination, Step 8 Control Recommendations, and Step 9 Results Documentation [21]. The framework is commonly applicable to manufacturing businesses, insurance companies, medical providers, finance companies, governments and risk management firms.

2) ISO/IEC 27005

The ISO/IEC 27005 global standard which provides recommendations for the control of risks in information security and follows the ISO / IEC 27001 general principles. It is designed to help ensure the satisfactory implementation of information security based on a risk management approach and widely used in small, medium-sized or corporate, government or private organisations. The study mentioned, however, that even with a sophisticated risk management plan and a reasonable level of preventive measures the safety from emerging dangers and attacks is not guaranteed.[22]. The standard also quantitatively or qualitatively analyses the related security risks to assess the probability of incidents or accident situations and the potential business implications if they occur, taking into account security properties, challenges, current safeguards and sensitive variables.

3) OCTAVE

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a framework for identifying and managing information security risks introduced by the Software Engineering Institute in 1999. OCTAVE is aimed at companies with limited resources. This establishes a systematic framework for assessing resources that are essential for the organisation's mission, the threats to these assets, and the vulnerabilities that can expose the assets to the threats. The organisation can identify what information is at risk by analysing the data, risks and vulnerabilities of information to establish and execute a security policy to reduce potential risk exposure to the information assets [23].

4) CRAMM

CCTA Risk Analysis and Management Method (CRAMM) is a risk management methodology created in 1985 by the Central Computer and Telecommunications Agency (CCTA) in the United Kingdom [24]. The CRAMM method is focused on principles for the control of information security. It

describes the correlation between IT vulnerabilities and threats that IT vulnerabilities can affect. [25]. CRAMM contains three stages, each with objective questionnaires and instructions backed by objective questionnaires. During the first two steps, the vulnerability of the application is identified and analysed. The third step discusses how to handle these threats.

5) EBIOS

Expression of Needs and Identification of Security Objectives (EBIOS) is a method for analysing, assessing and acting on information systems risks. It generates an organisation-friendly security policy. The system was developed in 1995 and is now managed by the French Prime Minister's ANSSI department. EBIOS is explicitly intended to offer classified and protected security information to government and private entities functioning in cooperation with the Ministry of Security. This calls for well-informed protective behaviour. The aim is to evaluate and prepare for eventual future situations and defects to improve safety arrangements and identify and respond to them [14].

From the discussion, we summarise each of the risk management methodologies in Table 1.

TABLE I. SUMMARY OF COMMON RISK ASSESSMENT MODELS

Risk Assessment Model	NIST SP800-30	ISO/IEC 27005	OCTAVE	CRAMM	EBIOS
Main evaluation	Catered for the current threat organisation landscape	Global standardisation of risk assessment	Preferred methodology for HIPAA compliance	Catered around organisation critical asset	Catered around critical asset
Level of detail	16 risk assessment tasks	Four stages with 13 steps	3 phases:	Three stages with eight steps	Five steps
Assessment Approach	Compliance (standards and guidelines with documentation)	Compliance (Standards and guidelines with documentation)	Qualitative method	Quantitative method	Qualitative method
Probability estimation	Not exist	Not exist	Not exist	Not exist	Not exist
Period of assessment	Depends on complexity	Depends on complexity	Depends on complexity	Depends on complexity	Depends on complexity
Overall Advantages	A thorough framework in managing cyber risks	Promotes security risk standardisation and embraces foreign awareness and practice	An iterative methodology slowly raises the depth of the risk identification and low labour costs for the study and evaluation of risk	The availability of tools to automate risk analysis minimises the time and effort spent on risk analysis and management.	The method takes both technological entities (software, equipment, networks) and non-technical entities (organisation, human dimensions, physical security) into consideration.
Overall Disadvantages	The framework is documented, but it is not an automated and a risk quantification tool	International standardisation requires conformity, but there is no comprehensive supporting information	The lack of capacity to quantify risks in resources and the high difficulty of raw data collection trigger a high resource use and time for the study and evaluation of risk.	the high complexity of collecting raw data; high consumption of resources and time to implement IT risk analysis and management processes	The qualitative essence of EBIOS is that complicated or changing operational environments are challenging for the risk analysis to reflect

From Table 1, we can conclude that the existing risk assessment methodologies need to perform a thorough investigation before making any risk-based decisions that involved quantitative and qualitative assessment. Most of the existing risk assessment is periodic, which means that the assessment will be conducted at a particular stipulated time. In contrast, the healthcare IoT solution keeps increasing daily and requires real-time processing. Eventually, this means a high likelihood that a new IoT healthcare solution will be deployed between that periodic evaluations.

IoT Risk Assessment Model

As IoT technology availability increases, it is vital to measure its associated threats and risks. Primarily, the IoT healthcare environment, where patients, medical practitioners and medical devices are highly connected, is associated with privacy exposure that adversely affects the threat. Studies have shown that the complexity of this IoT environment makes it difficult for policymakers to assess the situation [5, 12] accurately. Each of the approaches applies technological solutions for the problem of dynamically enhance the IoT ecosystem. To understand it better, we analyse three types of IoT risk assessment models to get the insights of those concerns.

6) Anomaly Behavior Analysis using Intrusion Detection System (ABA-IDS)

Pacheco *et al.* [26] introduced the concept of detecting anomalies using an Intrusion Detection System (IDS) for dynamically monitoring the systemic behaviour of an IoT

system. The framework consists of four layers, namely devices, networks, services, and applications. A general threat model was developed, covering risks at every stage. The system includes an ABA-IDS to detect abnormalities that could be caused by attacks on elements in each layer. Firstly ABA-IDS model defines a baseline model, so-called 'normal behaviour' through offline training. When it detects unusual activities, it will classify it as abnormal, which may be caused by an attack. ABA-IDS model is illustrated in Fig. 2.

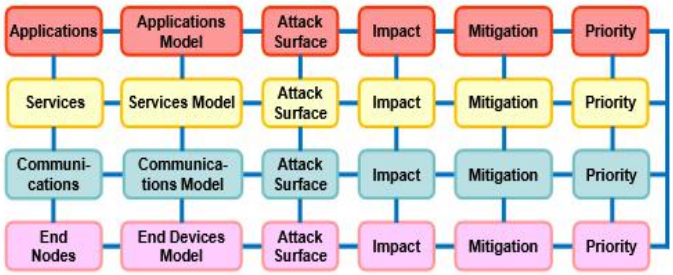

Fig. 2. ABA-IDS Model [26]

During experimentation, the researchers run tests for each layer to obtain results using the model. Node and communication layer results are depicted in Tables 2.

TABLE II. NODE LAYER RESULT [26]

Layers	Attack Type	Detection Rate
Node	Replay	98%
	Delay	98%
	DoS	99.9%
	Flooding	98%
	Sensor Impersonation	97.4%
	Pulse DoS	96%
	Noise Injection	100%
Communication	Flooding	94.2%
	Replay	96.3%
	Pulse DoS	92.3%
	HTTP GET	98.0%
	Replay + HTTP GET	99.2%

For the services layer, a Bayesian model is used to classify each anomaly and based the decision using a fuzzy logic system. At the same time, for the application level, the researchers do not provide any form of measurements. This is because the model is focused on the node and communication layer, as any IDS would have functioned.

7) Intelligent Security Risk Assessment Model using Deep Learning:

Abbass *et al.* [20] used a deep learning algorithm called Convolutional Neural Network (CNN) to further classify anomalies By introducing deep learning, and they hoped to introduce an intelligent security risk assessment model. Fig. 3 displayed the underlying concept of intelligent security risk assessment.

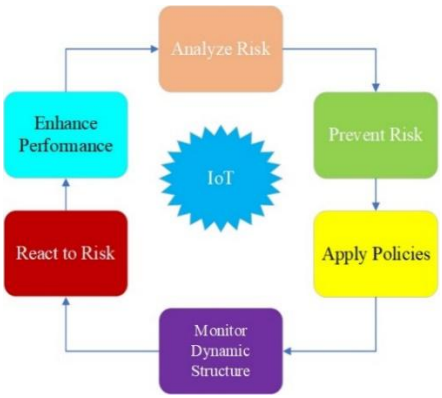

Fig. 3. Intelligent Security Risk Assessment Model [20]

When applying deep learning algorithms, the researchers did a comparative study to decide which algorithms suit best for accuracy and performance, namely Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Restricted Boltzmann Machines (RBMs) and Deep Stacking Networks (DSNs). The results obtained through experimentation stated that using CNN improves the performance of classifying each threat, and it can learn features from unlabeled data. It is also faster than any other deep learning algorithm. Fig. 4 depicts the IoT Risk Assessment developed.

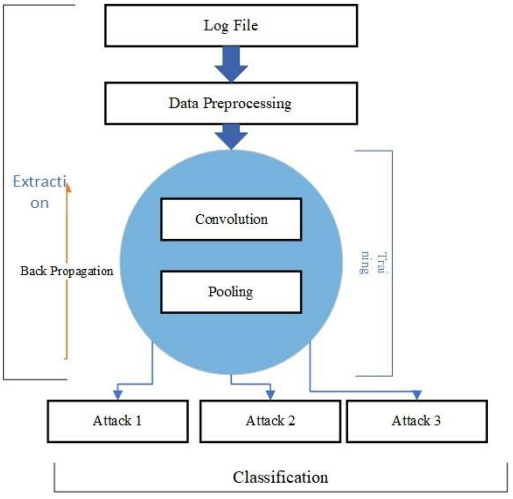

Fig. 4. Intelligent SRA Model [20]

8) AHP –SVM

Huang *et al.* [27] proposed an Analytical Hierarchy Process (AHP) analytical risk assessment model using a one-class Support Vector Machine (SVM). It is a machine learning algorithm used for classifications. There are three layers in this model which are 1) Processing and Result Block, 2) Data Block, and 3) Nodes. To further classify the type of attack or risk involved, data must be preprocessed, with SVM and machine learning algorithm, the data must be structured and labelled correctly. Risk assessment comes after data processing and analysis. Using the AHP weighted score, they determine

and evaluate the model for its security. The weighted score consists of three other models; feedback mechanism, comparison matrix calculator, and variable weight calculator. It is a complex process of mathematical calculations and precise enough for users to manage risks in IoT. The model is portrayed in Fig. 5.

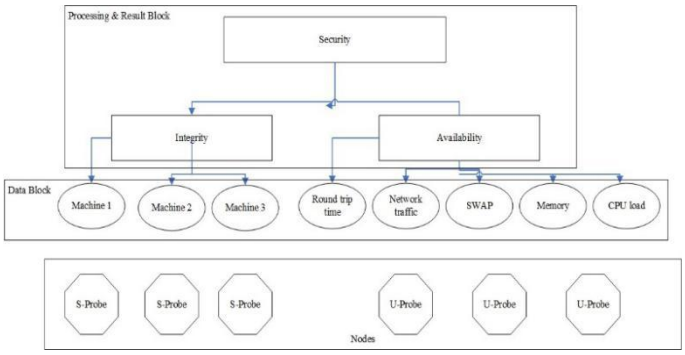

Fig. 5. Three Layer AHP-SVM Risk Assessment Model [27]

From the review of these IoT Risk Assessment Models, firstly most of the risk assessment model involves many steps; hence it will take much time to complete. Hence, these extensive processes will be ineffective with a high paced and dynamic system of IoT itself. There are also limited results due to the periodic assessment approach, which is workable for standard IT systems and will not change significantly in the short term. The traditional risk assessment also focused on well-evaluated assets whereby for IoT, each asset is interdependent, and risk may become greater through that interdependency. We can therefore conclude that the IoT risk assessment model can predict and consider possible systems and connections before the next assessment. This motivates the need for an alternative approach where the risk management methodology for IoT healthcare area should be able to provide a fast risk assessment based on real-time data collected.

IV. Proposed Risk Assessment Model For Healthcare IoT

This study proposes a risk assessment model that combines NIST SP 800-30, ABA-IDS, and classifying threats using the CNN Deep Learning algorithm. The NIST SP 800-30 framework as a basis offers functional threat analysis that better suited with the dynamic nature of the IoT landscape. ABA-IDS offers complete anomaly detection that can be utilised and CNN algorithm to classify better the threats encountered when properly deployed at the Service level of ABA-IDS. The combination of various models into one singular entity can complement each other's advantages and hopefully rectified each weakness. The proposed model is as shown in Fig. 6.

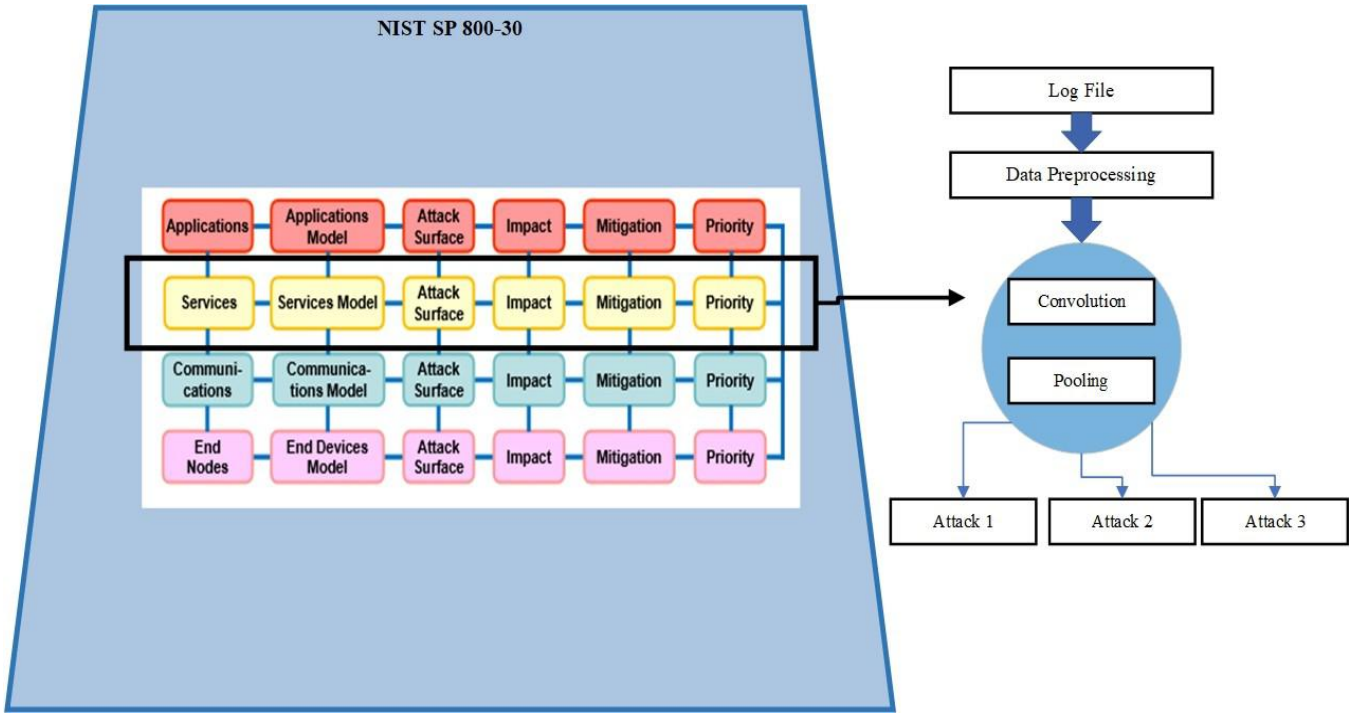

Fig. 6. Proposed Conceptual Risk Assessment Model for Healthcare IoT

The proposed model in Fig. 6 has the potential to identify threats accurately and can provide an accurate prediction when supplied with adequate data. A deep learning practitioner will have to tweak the algorithm in such a way that it can predict threats accurately. It is deployable because there are extensive open-source deep learning libraries available such as Keras, Tensor Flow, and PyTorch. Moreover, computer systems nowadays have an excellent GPU that's needed to support deep

learning executions. Through experimentations, risk assessment using CNN must be trained extensively to classify each intrusion that is detected. It needs a large amount of data to perform accurately.

Although the model successfully identified each attack, it does not guarantee absolute accuracy. It requires much experimentation to distinguish an optimal parameter. Other than that, it requires a vast amount of data for the algorithm to predict accurately. The idea from this model is to provide intelligent and automatic learning without any human intervention. The implementation is feasible in healthcare because the solution is deployed at the back end and does not interfere directly with the patient's telemetric devices, thus nulling any extra-emitted radiation.

V. CONCLUSION

This study explained the risk and challenges of IoT in the healthcare area from both technology and business aspects. This lead to analysing the existing risk management methodologies and the specific IoT risk assessment models used by industry and researchers. We found the utmost IoT healthcare risk factor, is to provide a fast and real-time data risk assessment result as needed. Based on the gap identified, we found out that unlike machine learning, using deep learning does not need an expert to identify the applied features used to solve a problem. It is very well suited for a highly dynamic IoT domain that grows exponentially. Having interventions at every stage of the risk assessment will undoubtedly bring down the performance that is needed to tackle the IoT fast-paced problem.

We therefore, introduced an IoT healthcare risk assessment model that coincided with the process structure defined in NIST SP 800-30 frames, which encourages risk assessment before choosing targets and controls using a CNN deep learning methodology. Efficiency and deployability need limited specialist involvement to make it IoT-friendly. The model shall also include replicated outcomes that cover the history, security sensitivities, challenges, hazards, safety targets and protection specifications, which are eligible for future IoT risk evaluation iterations. The healthcare domain can benefit extensively from it by having risk factors significantly reduced with up to date risk mitigation measures as a result of a model that can keep up with an exponentially growing environment.

ACKNOWLEDGMENT

The research is financially supported by Universiti Teknologi Malaysia (UTM) Transdisciplinary Research (TDR) Grant Q.K130000.3556.06G26.

REFERENCES

[1] O. Vermesan *et al.* (2011). Internet of Things Strategic Research Roadmap. *Internet of Things-global Technological and Societal Trends,* 1(2011), 9-52.

[2] I. Peña-López. (2005). ITU Internet Report 2005: The Internet of Things.

[3] AVSystem. (2019, 15/05/2020). *What is the IoT Architecture?* Available: https://www.avsystem.com/blog/what-is-iot-architecture/.

[4] TrendMicro. (2019, 15/05/2020). *Industrial Internet of Things (IIoT)*. Available: https://www.trendmicro.com/vinfo/us/security/definition/industrial-internet-of-things-iiot.

[5] F. I. Salih, N. A. A. Bakar, N. H. Hassan, F. Yahya, N. Kama, and J. Shah. (2019). IoT Security Risk Management Model for Healthcare Industry. *Malaysian Journal of Computer Science,* 131-144.

[6] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain. (2020). Machine Learning in IoT Security: Current Solutions and Future Challenges. *IEEE Communications Surveys & Tutorials.*

[7] M. N. Alraja, M. M. J. Farooque, and B. Khashab. (2019). The Effect of Security, Privacy, Familiarity and Trust on Users' Attitudes Towards the Use of IoT-based Healthcare: The Mediation Role of Risk Perception. *IEEE Access.*

[8] H. Zakaria, N. A. A. Bakar, N. H. Hassan, and S. Yaacob. (2019). IoT Security Risk Management Model for Secured Practice in Healthcare Environment. *Procedia Computer Science,* 161, 1241-1248.

[9] V.-V. Fireteanu. 2019. Risk Assessment Parameters for the Internet of Things Projects. *2019 15th International Conference on Engineering of Modern Electric Systems (EMES)*, 41-44, IEEE.

[10] K. Routh and T. Pal. (2018). A Survey on Technological, Business and Societal Aspects of Internet of Things by Q3, 2017, *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)*, 1-4, IEEE.

[11] T. Guardian. (2019, 15/05/2020). *Hacking Risk Leads to Recall of 500,000 Pacemakers Due to Patient Death Fears*. Available: https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update.

[12] N. A. Bakar, W. M. W. Ramli, and N. H. Hassan. (2019). The Internet of Things in Healthcare: An Overview, Challenges and Model Plan for Security Risks Management Process. *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS),* 15(1), 414-420.

[13] S. Anand and S. K. Routray. (2017). Issues and Challenges in Healthcare Narrowband IoT, *2017 International Conference on Inventive Communication and Computational Technologies (ICICCT)*, 486-489, IEEE.

[14] N. Židková, M. Maryška, P. Doucek, and L. Nedomova. (2020). Security of Wi-Fi as a Key Factor for IoT.

[15] H. Abie. (2019). Cognitive Cybersecurity for CPS-IoT Enabled Healthcare Ecosystems, *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)*, 1-6, IEEE.

[16] M. A. Salahuddin, A. Al-Fuqaha, M. Guizani, K. Shuaib, and F. Sallabi. (2018). Softwarization of the Internet of Things Infrastructure for Secure and Smart Healthcare, *arXiv preprint arXiv:1805.11011.*

[17] P. J. Nesse, H. S. Hallingby, O. B. Erdal, and B. Evjemo. (2020). Business Ecosystem and Internet of Things (IoT): Learnings from an Experimental Ecosystem Approach in Norway, *Economics and Finance Readings*, Springer, 109-124.

[18] M. G. Institute. (2015). The Internet of Things: Mapping the Value Beyond the Hype, McKinsey Co2015.

[19] P. Kaviya. (2018). Intelligent Healthcare Monitoring in IoT, *International Journal of Advanced Engineering, Management and Science,* 4(6).

[20] W. Abbass, Z. Bakraouy, A. Baïna, and M. Bellafkih. (2018). Classifying IoT Security Risks Using Deep Learning

Algorithms. *2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM)*, IEEE, 1-6.

[21] M. Barrett *et al.* (2020) Approaches for Federal Agencies to Use the Cybersecurity Framework. National Institute of Standards and Technology 2020.

[22] M. M. Hassan, A. Gumaei, S. Huda, and A. Almogren. (2020). Increasing the Trustworthiness in the Industrial IoT Networks Through a Reliable Cyberattack Detection Model, *IEEE Transactions on Industrial Informatics,* 16(9), 6154-6162.

[23] K. Kandasamy, S. Srinivas, K. Achuthan, and V. P. Rangan. (2020). IoT Cyber Risk: A Holistic Analysis of Cyber Risk Assessment Frameworks, Risk Vectors, and Risk Ranking Process. *EURASIP Journal on Information Security,* 2020, 1-18,

[24] C. CRAMM. (1996). CCTA Risk Analysis and Management Method. *Central Computer and Telecommunication Agency, United Kingdom, User Manual Edition.*

[25] V. Dokuchaev, V. Maklachkova, D. Makarova, and L. Volkova. (2020). Analysis of Data Risk Management Methods for Personal Data Information Systems. *2020 Systems of Signals Generating and Processing in the Field of on Board Communications*, IEEE, 1-5.

[26] J. Pacheco, X. Zhu, Y. Badr, and S. Hariri. (2017). Enabling Risk Management for Smart Infrastructures with an Anomaly Behaviour Analysis Intrusion Detection System. *2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS* W)*, IEEE, 324-328.

[27] Y.-L. Huang, W.-L. Sun, and Y.-H. Tang. (2019). 3aRAM: A 3-Layer AHP-Based Risk Assessment Model and its Implementation for an Industrial IoT Cloud. *IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, IEEE, 450-457.