A critical review of IoT connected healthcare and Information security in South Africa

Khadija Hayat Naqvi[1], Elisha Didam Markus[1], Masinde Muthoni[1] and Adnan Abu-Mahfouz[2]

[1] Central University of Technology Free State South Africa
[2] Center for Scientific and Industrial Research, South Africa
emarkus@cut.ac.za

Abstract. South Africa as a developing nation is evolving in new healthcare technologies. With an increase in these innovations comes many challenges foremost among which is security. This paper presents a review of challenges faced in IoT connected healthcare and information security in South Africa. The study begins by providing an overview of IoT connectedness in healthcare in South Africa. An analysis on how this portends a threat to security is provided. A further study into how these threats have been mitigated with their pros and cons are presented. The study concludes by providing inherent gaps in security for IoT connected healthcare in South Africa.

Keywords: IoT connected healthcare, Information security, South Africa, IoT cyber security, Current research, Security issues, Intrusion detection systems.

1 Introduction

The integration of the internet into human life has brought about, in a positive sense, the advancement of technology and communication between people, and in a negative sense, the risks regarding personal security and privacy [1]. Previous studies have highlighted the need for IoT in healthcare facilities to improve quality of care, access to care, reduce cost of care and the need for information and connected device security due to data sensitivity. This paper provides an overview of IoT connected healthcare in South Africa and how the information security threats facing healthcare organisations affect them and their patients. The study provides an analysis on the proposed solutions to information security in health care from literature, along with their advantages and disadvantages. It is widely understood that the IoT environment especially in healthcare needs better security while maintaining efficiency and improving people's lives. The paper is organized as follows: First a background of connected healthcare and Internet of Medical Things (IoMT) is presented, next details of Intrusion detection systems (IDS), the types and groups of IDS are highlighted. The study discusses some effective frameworks used in the literature to identify, track, and detect attacks and traffic attack patterns. The study is concluded by providing the main findings of the study and recommendations on the type of IDS technique to design keeping the heterogeneity of IoT

networks in consideration and also ensure the IDS technique is secure and robust enough to be effective.

2 Security in Healthcare

Connected healthcare is believed to greatly impact, saving about one million lives in Sub-Saharan Africa in the coming few years. In connected healthcare, diverse distributed devices aggregate, analyse and communicate real time medical information to the cloud, making it possible to collect, store and analyse large amounts of data in several new forms and activate context based alarms [2]. According to research Africa's most developed country is South Africa [3]. South Africa is one of the countries experiencing growth with connected healthcare, with many connected medical devices, the security and privacy is important, it is becoming increasingly difficult and complex to maintain the privacy and security of these devices [4].

Cyber security is a clear risk factor for healthcare data, becoming a global concern due to the increase in data breaches and lack of resources to deal with breaches [4]. 83 per cent of the South African population rely on the public healthcare system [5]. Countries mostly affected by data breaches are ones where the citizens have health insurance [6]. Data breaches can incur massive losses in the health care sector [4]. Data breaches are not manageable for several reasons i.e. lack budget, work force, lack of awareness and expertise [6]. Attacks usually faced by healthcare sectors are: replay, man-in-the-middle, impersonation, privileged-insider, remote hijacking, password guessing, DDoS and malware attacks. Exposure to such attacks can end up in sensitive data being disclosed, altered and risk availability to unauthorized users [7].

Healthcare is one of the leading industries when it comes to security breaches, followed by government and retail [6]. As of 2018, the number of data breaches reported was 2216 from 65 countries. The healthcare industry faced 536 breaches. This implies that the healthcare industry has faced the highest number of breaches among all industries. In the year 2019, 2013 data breaches were reported from 86 countries. The total number of healthcare records that were exposed, stolen, or illegally disclosed in 2019 was 41.2 million in 505 healthcare data breaches. Hacking and information technology (IT) incidents are the most common forms of attacks behind healthcare data breaches [8]. In healthcare access to sensitive data is important and the aspects needed to be considered are; who can access the data, the training needed to handle this data, adequate security, motivation to use it extensively and maintaining a high availability, accompanied by vulnerabilities [9].

IoT has become popular in recent years due to its ability to decrease the strain on the healthcare system caused by a rise in chronic illnesses and an aging population [3]. Several African countries have also taken advantage of IoT technology, including

healthcare providers tracking the health of outpatients. In fact, Africa has excelled in several areas that other more developed countries find difficult [10]. Regardless of massive IoT impact globally, it is still in the early stages of development and the more objects that become internet-enabled the more difficult and complex it becomes to manage the security and privacy of the personal information generated, processed and stored by IoT devices [5]. As beneficial as IoT can be the growing number of devices and users is a cause for concern [6]. IoT is vulnerable to devastating intrusion attacks due to its connectivity to everything [7]. This vulnerability and challenges are peculiar to the African environment [3].

2.1 Internet of Medical Things

The emergence of the IoMT has introduced massive changes in the healthcare system. IoMT combines technologies with healthcare services to provide real-time remote patient monitoring, management of diseases, reduced cost and errors, improved disease diagnostics and treatment methods [11]. IoMT is growing fast with internet-enabled devices helping track patient health [12]. The security of IoMT is important [13]. Threats in the healthcare system can be found through medical devices, anything connected to the internet will face the same vulnerabilities as the computer systems [4]. Medical devices and applications that are connected to health IT systems through computer networks. These medical devices can be converted and deployed as medical technology [6]. IoMT makes patient and medical staff lives easier as it gives doctors access to their patients with the help of wearable devices as part of their medical kits [14]. Wearable devices are used to collect, store, and analyse patient data to keep up with their health status with very little research to address the privacy and security issues of these devices [15]. Health sensors in a patient's body can sense the level of sugar, blood pressure and heartbeat, the sensor can notify the health practitioners immediately if any of them elevate higher than normal [16]. In this case smart sensors monitor the health of patients daily and send the data to the cloud server which is later processed by healthcare practitioners with their smartphones [16]. Mobile sensing devices aid in monitoring patient health but because of moving around and connecting to different network configurations and data transmission to the cloud servers, maintain the security of sensing devices becomes challenging [16]. The communication in the IoT based environment suffers from breach of patient's data privacy [16].

Electronic collection of patient information is a common practice across healthcare organisations in South Africa [17]. Personal electronic health records (PEHRs) a personal and secure set of online tools that connect patients to their health records and empower them to manage their own health and healthcare. PEHR is a new concept in South African healthcare sector. The privacy and security standards to protect patients using PEHR have not been implemented yet, leaving patient records vulnerable. Healthcare organisations suffer financially due to external maintenance of PEHRs [17].

2.2 Intrusion detection system (IDS)

An Intrusion Detection System (IDS) monitors and analyses malicious traffic to protect the devices from various attacks [16]. In an IoT and wireless sensors environment, IDS verifies incoming traffic and searches for intrusions, if an intrusion is identified, the appropriate mechanism is deployed to take the appropriate action. IDS can be divided into the following categories [16]:

- **Network based intrusion detection system (NIDS):** used in a network for the prevention and detection of different network attacks. It monitors the entire network by doing an analysis of activities on the network.
- **Host based intrusion detection system (HIDS):** used to monitor a single host for signs of malicious activities and analyses the activities inside the host.

For IDS to be effective it should be ensured that it does not introduce new weaknesses, should be designed in such a way it exhibits less computation and communication costs, should be reliable enough to produce less numbers of false positives and false negatives. IDS can be divided into three groups [16]:

- **Anomaly-based detection:** based on statistical behaviour methods. Two types of flows are defined under this: normal and abnormal flow. Any deviation from the normal flow is detected as an anomaly. This is an accurate and consistent form of detection with less false negatives and positives. This is perfect for unknown attacks, however the profile for normal activities needs to be updated regularly as the changes occur daily.
- **Misuse-based detection:** also known as rule-based or signature-based. The signature of an attack is generated when it happens, which is used to detect future attacks. This method is perfect for detecting known attacks with low false rates. Installed much like an antivirus in a system.
- **Specification-based detection:** defines the constraints and specifications that describe the correctness of the detection process. The network behaviour is monitored based on the specifications and constraints. This technique combines the advantages of the anomaly and misuse based detection by using manually developed specifications and constraints to identify the abnormal behaviour, with low false positive rates. This technique detects both known and unknown attacks however it can be time consuming.

The advantages and disadvantages of the below solutions suggested by researchers are presented in Table 1:

- **IoMT Security Assessment Framework**, a web-based application to ensure security in IoMT solutions. IoMT-SAF uses a list of attributes to assess necessary security measures. This framework can be used to assess and verify the security in products, allowing transparency with other security providers [11].
- **The trust-based Bayesian management** is a result of a survey done by 12 hospitals in different countries; the survey collected system design requirements in

medical networks and came up with the trust-based approach. The authors then focused on identifying insider attacks in healthcare Software-Defined Networks (SDNs) due to researchers exploring the deployment of SDNs in healthcare organisations [13]. SDN can be used to defend healthcare organisations against several attacks [13]. This approach can be applied to a generic SDN-based network [13].

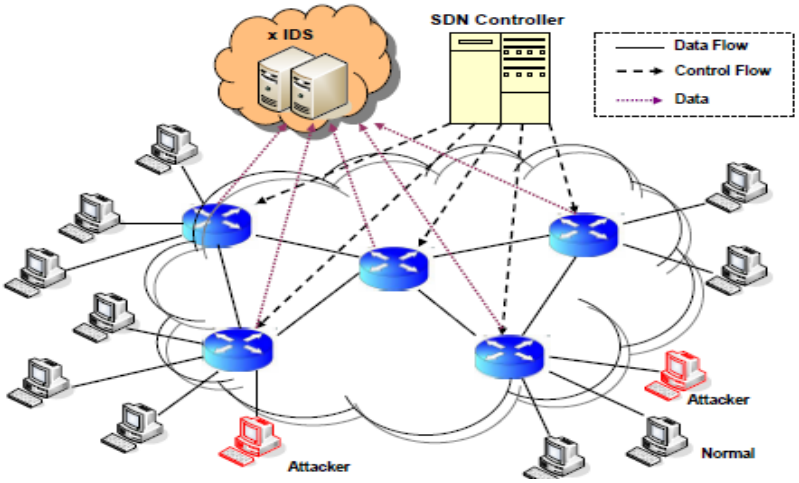

Figure 1: An architecture of healthcare SDNs [13].

- **The DDoS detection method**, using ANN for IoT network, is based on categorisation of legitimate traffic patterns and attack traffic patterns. This system can identify the attack traffic and performs well in true and false positive accuracy. The system is composed of eight node sensors, seven client nodes and one server relay node for analysis, to compose an IoT network. Data is sent and acknowledged by client and server nodes to analyse their behaviour and response phenomenon [17].

- **Local Outlier Factor (LOF)-based data analytics technique,** analyst in the loop and visualisation to safeguard EPR data. The system allows detecting anomalous behaviour within EPR audit activity using the following multi-stage process:
    - Data Pre-processing.
    - Machine learning.
    - Feature testing [19].

3 Comparison and Discussion

This paper reviews previous studies, discussing the proposed solutions to current information security problems. Information security is a major concern in a developing country where security channels for new devices are yet to be developed. The table highlights studies that have proposed solutions that detect and assess security in the IoT/IoMT environment. Further research is needed on the topic of IoT connected

healthcare and the need and benefits information securities in that sector within South Africa, as healthcare organisations are the most trusted entities.

Ref.	Proposed framework	Advantages	Disadvantages
11.	IoMT Security Assessment Framework	• Granular • Extensible • Adaptable	Lengthiness and complexity of defining security profiles.
13.	Bayesian interference-based Trust management.	• Dynamic • Flexible in recovering false detected devices. • Flexibility for IT administrators to control and manage the network in SDN controller. • Effective in identifying malicious devices in a healthcare SDN environment. • Scalable.	• Increase in CPU load. • Threshold. • Behavioural profiles. • Large traffic volume • IT experts in the healthcare area. • Security policy enforcement. • Implementation of additional security mechanisms.
16.	Deep learning-based method Deep Belief Network (DBN) algorithm for intrusion detection system.	• Accurate • Precise • Recall • Detection rate • F1-score	Can only detect limited types of attacks and data sets.
17.	A DDoS detection method using ANN for IoT network	• The system was 99% accurate in detecting attack patterns. • The system successfully identified attack traffic and performed well in true and false negative accuracy.	• This system is not trained for latest threat patterns. • The reliability of the system with modern technology is uncertain.
19.	Local Outlier Factor (LOF) and Density-Based Spatial Clustering of Applications with Noise (DBSCAN) algorithm.	• Complementary to existing security perimeter solutions. • Increase in situational awareness of data flow and actively address the misuse of data.	• Cannot learn or observe patterns of data and profile user's data behaviour.

4 Conclusion

This study has demonstrated the pros and cons of IoT and connected healthcare highlighting the security and privacy issues encountered globally and what that means for a developing country like South Africa. Wearable devices that aid hospitals in keeping track of patient's health could prove to be life threatening to patients if necessary precautions from cyber and physical attacks are not taken. Many of the studies have proposed frameworks that can help detect attacks and traffic attack patterns. The study further investigated the advantages and disadvantages of the proposed frameworks. Common disadvantages among the solutions are that the systems are unable to learn new patterns, behaviours and defining security profiles is a long and complex task for them. It is crucial to design intrusion detection techniques that can address the

disadvantages and are robust and secure against different attacks, even simultaneously. Heterogeneity of IoT networks should also be considered. This can create a problem when designing an effective detection system, which is strong and efficient enough to perform detection over multiple IoT platforms. The shortage of research in connected healthcare and lack of health employees, patient and the organisation awareness on security and privacy issues could be dangerous as a patient's information flows through many "users" and there is no way to ensure confidentiality and integrity of information.

References

1. Solic, K., Plesa, M., Velki, T. and Nenadic, K., 2019. Awareness About Information Security and Privacy Among Healthcare Employees. Southeastern European Medical Journal: SEEMEDJ, 3(1), pp.21-28.
2. Kodali, R.K., Swamy, G. and Lakshmi, B., 2015, December. An implementation of IoT for healthcare. In 2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS), pp. 411-416. IEEE.
3. Ndubuaku, M. and Okereafor, D., 2015, April. Internet of things for Africa: Challenges and opportunities. In 2015 International Conference on Cyberspace Governance–CYBERABUJA2015, pp. 23-31.
4. Van Niekerk, B., 2017. An analysis of cyber-incidents in South Africa. African Journal of Information and Communication, 20, pp.113-132.
5. Ngobeni, V., Breitenbach, M.C. and Aye, G.C., 2020. Technical efficiency of provincial public healthcare in South Africa. *Cost Effectiveness and Resource Allocation*, *18*(1), p.3.
6. Fuentes, M.R., 2017. Cybercrime and other threats faced by the healthcare industry. Trend Micro.
7. Wazid, M., Das, A.K., Rodrigues, J.J., Shetty, S. and Park, Y., 2019. IoMT malware detection approaches: Analysis and research challenges. *IEEE Access*, *7*, pp.182459-182476.
8. Seh, A.H., Zarour, M., Alenezi, M., Sarkar, A.K., Agrawal, A., Kumar, R. and Khan, R.A., 2020, June. *Healthcare Data Breaches: Insights and Implications.* In *Healthcare*, Vol. 8, No. 2, p. 133. Multidisciplinary Digital Publishing Institute.
9. Salih, F.I., Bakar, N.A.A., Hassan, N.H., Yahya, F., Kama, N. and Shah, J., 2019. *IOT Security Risk Management Model for Healthcare Industry*. *Malaysian Journal of Computer Science*, pp.131-144.
10. Baker, S.B., Xiang, W. and Atkinson, I., 2017. Internet of things for smart healthcare: Technologies, challenges, and opportunities. IEEE Access, 5, pp.26521-26544.
11. Alsubaei, F., Abuhussein, A., Shandilya, V. and Shiva, S., 2019. IoMT-SAF: Internet of medical things security assessment framework. *Internet of Things*, *8*, p.100123.
12. Alsubaei, F., Abuhussein, A. and Shiva, S., 2018, November. A framework for ranking IoMT solutions based on measuring security and privacy. In *Proceedings of the Future Technologies Conference*, pp. 205-224. Springer, Cham.
13. Meng, W., Choo, K.K.R., Furnell, S., Vasilakos, A.V. and Probst, C.W., 2018. Towards Bayesian-based trust management for insider attacks in healthcare software-defined networks. *IEEE Transactions on Network and Service Management*, *15*(2), pp.761-773.
14. Banka, S., Madan, I. and Saranya, S.S., 2018. Smart healthcare monitoring using IoT. *International Journal of Applied Engineering Research*, *13*(15), pp.11984-11989

15. Cilliers, L., 2020. Wearable devices in healthcare: Privacy and information security issues. *Health Information Management Journal*, *49*(2-3), pp.150-156.
16. Pundir, S., Wazid, M., Singh, D.P., Das, A.K., Rodrigues, J.J. and Park, Y., 2019. Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges. *IEEE Access*, *8*, pp.3343-3363.
17. Els, F. and Cilliers, L., 2017, March. Improving the information security of personal electronic health records to protect a patient's health information. In *2017 Conference on Information Communication Technology and Society (ICTAS)*, pp. 1-6. IEEE.
18. Ahanger, T.A., 2018. Defense scheme to protect IoT from cyber-attacks using AI principles. *International Journal of Computers Communications & Control*, *13*(6), pp.915-926.
19. Hurst, W., Boddy, A., Merabti, M. and Shone, N., 2020. Patient Privacy Violation Detection in Healthcare Critical Infrastructures: An Investigation Using Density-Based Benchmarking. *Future Internet*, *12*(6), p.100.