

# **SECURITY AND PRIVACY IN IOT BASED HEALTHCARE SYSTEM**

Kiran Kumar Mohanraj, Abdulaziz Alahmed, Abdulaziz Alaskar

## **ABSTRACT**

The Internet of Things (IoT) is playing an ever-greater role in the healthcare sector. However, though it offers significant benefits for patients and health professionals in providing effective services and treatments, it also faces certain data security and privacy challenges. There is therefore a need to develop architecture and techniques to overcome these security and privacy problems. This paper undertakes a literature review and analysis of different proposals to maintain security and privacy in IoT-based healthcare applications. Solutions to various attacks on IoT-based health clouds are explored, to protect the patient's Personal Health Information (PHI). This paper also addresses the security and privacy issues related to wearable devices (WDs) designed for healthcare applications.

## **1. INTRODUCTION**

IoT applications help improve the collection and sharing of user's data, through a network of interconnected devices which support and exchange information with each other. In this way, computer technologies have had a major impact on real world practices across a range of fields. Healthcare is but one of the industries which has benefitted from this new technology. Increasingly, those working in this field are trying to find improved ways of providing health services, along with remote care options. This includes the development and use of sensory devices which can collect and then analyse patient data, to help administer effective treatments in a way which is convenient for the patient. The general preference is to limit the invasiveness of such devices rather than utilise implants. An IoT system typically comprises sensor devices, cloud-based interfaces, machine algorithms, along with a Wireless Sensor Network (WSN). The sensory devices collect patient data such as temperature, blood pressure and heartbeat. The algorithms analyse the gathered information, while the WSN provides communication facilities and the cloud functions storage (Amaraweera and Halgamuge, 2019).

This network nevertheless needs to be effectively secured, to protect patient data and privacy, particularly given the sensitive nature of what is collected. To do this, it is essential to analyse the different components of the application architecture in detail, which takes into account how it is interconnected and where vulnerabilities may therefore arise. In a WSN, nodes are recognisable through their unique identification numbers. These unique identification values enable sensor nodes to maintain communication between devices, so that data can be collected and exchanged over the application network and services provided (Elhoseny et al., 2018). However, this process presents significant privacy and security vulnerabilities, related to three overarching categories – data collection, data exchange, and data storage (Manogaran et al., 2018). Moreover, though it has significant advantages in terms of economies of scale reducing user costs, the cloud computing architecture upon which IoT networks are generally hosted

presents another significant potential vulnerability which application designers must be cognisant of (Amaraweera and Halgamuge, 2019). In this paper, a detailed review is presented, which examines various IoT-related security and privacy issues in the healthcare sector.

## **2. LITERATURE REVIEW**

There is a significant body of research regarding the implementation of the Internet of Things (IoT) in the healthcare sector. This study focuses on security and privacy requirements in Healthcare 4.0, healthcare-based IoT cloud, and wearable devices (WDs).

### **2.1 IoT-based Healthcare 4.0**

This section provides an overview of the security and privacy challenges of IoT-based healthcare applications. The healthcare industry has transformed from healthcare 1.0 to 4.0. Healthcare 1.0 was centred around doctors maintaining patients' medical records. This was replaced with Electronic Health Records (EHR) in Healthcare 2.0. Healthcare 3.0 was patient-centric and used WDs for monitoring patients. Healthcare 4.0 keeps the patient's record in the centralized EHR system to monitor the patients' health records and delivers uninterrupted services to them in real-time (Hathaliya and Tanwar, 2020). IoT technologies help in monitoring and providing services to patients located remotely. The applications built for healthcare are targeted to care for patients in medical care facilities as well as patients who reside in their own homes. The end node sensors are used to collect data from the patients, by gathering information through WDs and implants. The potential threat to these IoT applications is significant, however, because they deal with highly sensitive data (Amaraweera and Halgamuge, 2019).

Kodali, Swamy and Lakshmi (2015) presented the implementation of an IoT-based healthcare system with a zig bee mesh protocol that monitors the physiological parameters of the patients to provide quality care to the patient at a reduced cost. This IoT-based medical device is a combination of XBee S2 module interfaced with an LM35 temperature sensor. This device is connected with an Intel Galileo Generation 2 board which acts as the gateway. The drawbacks of this implementation are that zig bee provides limited coverage to connected devices, stealing of cryptographic keys by either remote or physical attack, along with packet capturing for conducting various attacks.

Alsubaei, Abuhussein and Shiva (2017) presented the taxonomy of security and privacy issues of IoMT and also provided a scheme to estimate IoMT risks and their mitigation strategies. The goal of this scheme is to increase security and privacy realisation among IoMT stack holders by authorisation and to also quantify the potential security and privacy risks of IoMT devices. The taxonomy is based on various parameters and methods. Namely, IoT layer, possible intruders, compromise level, attack impact, attack method, CIA compromise, attack origin, attack level, and attack difficulty. It provides protection against various threats such as perception layer, DoS, brute force, and replay attacks. The researchers have proposed a risk assessment model which can be used to compare the risks posed by different attacks on a single device by quantifying and comparing them.

Strielkina et al. (2018) proposed an IoT-based cybersecurity architecture to protect device and patients' health information. They focused on international healthcare cybersecurity rules and

standards to build a reliable hierarchical healthcare IoT model for advanced security assurance cases. The paper uses the proposed healthcare IoT model and ASAC (Advanced Security Assurance Case) for cybersecurity assessment. This increases the reliability of healthcare IoT models by reducing vulnerabilities and security threats. However, the proposed model lacks in the privacy aspect and therefore needs some improvement.

He et al. (2018) designed a smart healthcare system to monitor the health of the patient in real-time. They analysed the security issues of the existing system, such as password guessing and data privacy issues. They proposed a password strength meter (PI-PSM) which uses the personal information of the user to evaluate the strength of the password. They have compared and proved that the proposed PI-PSM performs better than the existing PSMs, namely NIST-PSM. Although the proposed model provides better privacy preservation of medical records, it is not particularly scalable.

S and Philip (2016) designed a Radio Frequency Identification (RFID) authentication approach for healthcare IoT. It provides IoT-based remote monitoring of patients' health for improvement. It automatically collects the data and reduces the risk of data error in regard quality of diagnosis. The researchers analysed the security issues related to IoT, like transferring the wrong information and access control issues arising from the RFID environment.

Amaraweera and Halgamuge (2019) investigated the security and privacy issues related to IoT healthcare applications. The author produced a structured guide for these issues by reviewing 30 peer-reviewed papers between 2016-2018. The healthcare applications used for this study were categorized into remote monitoring, clinical care, context awareness, and assisted living. Applications used for remote monitoring have shown the highest number of usages. An examination was conducted to analyse the end node medical sensors used to collect data from the patients using wearable smart devices. ECG sensors were found to be the most used sensory device. By analysing these publications, the author found that the highest threat to IoT healthcare applications is unauthorized access, with a value of 29%. The second highest threat is data breaches and impersonations, at around 8%. The most affected layer of the services architectures was found to be device layer of the applications architecture. This has the highest impact as a result of security threats. This study serves as basis for application developers and designers to improve the security and privacy of the health-related applications. It is also useful to design mitigation strategies to overcome the identified vulnerabilities and to provide appropriate controls to overcome the identified challenges.

## **2.2 IoT-based health clouds**

Electronic Patient Health Information (EPHI) is considered confidential for patients and healthcare providers. There are various challenges in storing and transferring EPHI while ensuring compliance with the Health Insurance Portability and Accountability Act (HIPAA). These are security and privacy challenges associated with e-health clouds which host not only applications but also software development tools and APIs. The use of hybrid public and private clouds also exacerbates the security situation, by causing billions of confidential data to be stored and transferred in cloud servers. Patients' sensitive personal and medical information could be tampered with, used or compromised in the absence of having real time monitoring. Due to IoT's ubiquitous and pervasive nature, the automatic data collection and

lack of verification, security breaches and privacy violations are highly likely (Alasmari and Anwar, 2017).

Mahajan and Sharma (2015) analysed the insider threat in the cloud, with the aim of detecting the presence of malicious insiders and then preventing them from undertaking any malicious activity in the cloud. This paper provided a solution to ensure the integrity of the data kept in cloud by the users, by getting a notification as a pop-up window whenever the file contents are being changed, along with a pop-up window showing the list of changes made. The authors also provided a solution to ensure confidentiality of the data kept in cloud by using One Time Password (OTP), though OTP is itself vulnerable to a number of attacks including man in the middle attack.

Garkoti, Peddoju and Balasubramanian (2014) presented a paper in which a framework was proposed to address the secure transmission of medical records between the healthcare organisations based on the cloud. Moreover, it also ensures the integrity of medical records by proposing a model that would detect any modification made in the data and the person responsible for that alteration. The proposed model makes use of watermarking and auditing techniques to ensure the integrity of the medical records and identify any modification made along with the person responsible for modifying the data. This model thus introduced a new feature of accountability in already proposed frameworks. Spatial domain watermarking has been used in the proposed model to detect any modification of the data. The drawback of this technique is however that it can be changed by noise, compression or interpolation. This may lead to false detection of modification even if it is not carried out. Moreover, the solution proposed only identifies any alteration or malicious insider inside the healthcare organisation. It does not deal with malicious insiders residing in the cloud.

To mitigate the insider threats, Gunasekhar et al. (2015) proposed a technique to counter the insider attacks through use of multi-cloud. The data of the organisation is first encrypted and then kept in a trusted cloud, while the keys that are used to encrypt that data are kept in another cloud. If a malicious insider gets access to the encrypted data, then he/she would be unable to get access to the keys, and vice versa. In this way, the data of the organisation remains protected from malicious insiders. This is one of the best ways to secure data kept in the cloud. However, even though the data gets secured through the proposed framework, the key management issues are still there. Moreover, some attacks like side channel attacks are still possible.

Similar to Gunasekhar et al. (2015), V.R. and S. (2014) introduced an architecture where multi-clouds are used to keep the data secure. The data of the organisation is encrypted and then split into two or three parts and stored in separate clouds. The metadata information such as passwords and secret keys of the encrypted data are stored in a private cloud. This scheme works well provided the two cloud providers are trustworthy and do not have an idea of the other CSP who is storing the other part of organisational sensitive information, whether the encrypted data or the secret used to encrypt that data. This architecture does not consider collusion attacks, however. Furthermore, intensive computation is needed during the decryption process as the file access paths are continuously being updated in the proposed scheme.

Another architecture named Homomorphic Encryption with Random Diagonal Elliptical curve cryptography integrated with Multi-nominal smoothing Naive Bayes (HERDE-MSNB) was proposed by Vedaraj and Ezhumalai (2021), to provide effective security and predict disease

from patient data stored in an IoT health cloud system. The patient data is encrypted along with the keywords through the HERDE algorithm and uploaded into the cloud. The uploaded cloud data is then decrypted by the medical person. The deciphered data is thereafter processed in the MSNB prediction model to predict the disease of the patient. The drawback of this model is it can predict only heart disease and diabetes, and very minimal features (only 8) are considered, which will produce less accuracy when the model is scaled.

To provide multilevel privacy of patient's Personal Health Information (PHI), Zhou et al. (2015) proposed a white-box traceable and revocable multi-authority attribute-based encryption named TR-MABE. This paper helps the primary physicians to securely access a patient's PHI content and verify her/his real identity. The author utilises attribute revocation to achieve the patient's multilevel (conditional) identity privacy. Without introducing extra special signatures, the multilevel privacy preservation is efficiently realised by outsourcing the storage revocation to the e-healthcare cloud.

### **2.3 Wearable devices for healthcare application**

Wearable-based devices (WDs) are devices which are worn by individual users to record and transmit unique biometric information. This includes measures such as heartrate, temperature, blood pressure, as well as sleep cycles and workout statistics. The collection of this information can help to improve users' life and health outcomes and for this reason WDs are therefore becoming ever more widely adopted. There are a range of different WDs and schemes to collect and transmit data. The generated data is then transferred from the WD to the user's smartphone, through several different possible communication channels, like zig-bee and Bluetooth. However, this process involves significant security and privacy challenges, which designers must confront.

In regard the issue of WD security, Srinivas et al (2018) favoured a cloud-based authentication scheme, based around the automated validation of internet security protocols and an applications (AVISPA) tool. The scheme would also undertake informational verification in regard to Man in the Middle (MIM) and Denial of Service (DOS) attacks, among others. It is a scheme that has significant advantages in terms of the costs related to computation and communication. However, on the downside, it is vulnerable to stolen attacks. This problem of stolen attacks was addressed by Das et al. (2018). Their solution was based around use of a secure authentication protocol, wherein the user's WD and mobile device undertake a process of mutual authentication through the generation of a session key, with a real-or-random model and AVISPA tool used.

Another scheme was designed by Liu et al. (2016a). It centred around the use of a yoking-proof-based protocol provided simultaneous authentication and identification for cloud-assisted WDs. A physical unclonable function, coupled with lightweight cryptographic operators, were utilised in order to facilitate mutual authentication, with the yoking protocol enabling the cloud server to undertake simultaneous authentication. Through the employment of the Rubin logic-based security analysis it was determined that the yoking-proof-based authentication protocol had theoretical design correctness. Moreover, Liu et al. (2016b) proposed the adoption of an asymmetric three-party-based authentication method. Through use of QR codes and the out-of-band channel, this approach worked to pair the mobile and wearable devices, in a secure way which undertook mutual authentication and enhanced the Bluetooth connection. That said, this approach remained vulnerable to impersonation and DDOS attacks.

Therefore, Liu et al. (2016a) proposed another scheme to overcome this problem. This scheme has the crucial feature of being able to protect against various attacks, in a way which can be applied in practice.

Kumar et al. (2014) also suggested a scheme to provide remote monitoring for patients, based on recognition of the fact that user data security and privacy remains an important unresolved issue and that finding the flaws in systems can be difficult, because each is to a significant degree unique. The privacy-preserving e-healthcare scheme the researchers proposed utilises the aspects of IoT infrastructure and cloud-based storage, based around the adoption of message authentication codes and symmetric encryption. However, the scheme is limited, in that it is inappropriate for implementation on battery-constrained devices, although it is possible to implement GCM services for enhanced battery performance and improved message delivery. On the other hand, Yang (2017) proposed a scheme which, utilising emerging cloud storage and IoT infrastructure, offered a reliable, searchable and privacy preserving remote monitoring healthcare system, which displayed superior results in message delivery and battery performance. It was a scheme that was centred upon symmetric encryption, with forward privacy and delegated verifiability. These elements were achieved through a design which incorporated a novel combination of the increasing counter, Bloom filter and aggregate MAC. The research demonstrated the practical efficiency of this novel scheme in relation to real-world healthcare settings, which can meet both desired performance and security requirements.

Meanwhile, Sathya et al. (2017) have suggested a scheme which uses a wireless sensor network, which as the researchers note is more susceptible to attack than wired systems. This scheme collects user data in real-time, so that remote monitoring and diagnosis can be undertaken. The blowfish algorithm was utilised for data encryption, with CP-ABE utilised to ensure that data is only accessible to authorised users. In the researchers view, this approach produced the best results in regard to both security and fast transmission of data, as compared with other proposed schemes. In addition, Sadki (2014) also designed a privacy-preserving remote healthcare scheme, wherein users accessed their data via mobile, with third-party privacy policies instituted to protect and secure the collected information. This scheme allowed for users to control their own sensitive data, through use of an intelligent mobile application which can determine and predict users' privacy preferences. These preferences are in turn transformed into privacy policies. Third parties such as cloud and healthcare providers are thereafter required to adhere to these policies through an agreement.

Zhang et al. (2015) also developed an architecture for mobile healthcare, with the aim of enhancing user protection and privacy. It was centred around attribute-based encryption, which was deployed to ensure the security of users' data, through adjustable security protections provided at fine-grained access levels. The adjustable nature of these levels was designed with the aim to satisfy the requirements of individual users, in regard such aspects as experience, protection and service. However, the researchers acknowledged that there is a difficult trade-off that must be resolved in relation to security and data processing complexity.

### **3. CONCLUSION**

In this paper, the security and privacy issues facing the IoT-based health sector have been reviewed. The discussion considered various IoT architectures, along with their security problems and potential mitigations. The basis of IoT clouds were reviewed and the privacy challenges encountered by the consumers were discussed. The possible solutions in the literature were studied and presented. In addition to IoT devices, wearable devices in healthcare applications were reviewed to examine the security challenges they face. Most studies are focused primarily on providing solutions to specific security and/or privacy problems. However, there is a need for IoT application designers to consider the wider process, in a holistic manner which considers all potential vulnerabilities, to help develop secure applications which can improve health outcomes.

### **4. INDIVIDUAL REFLECTION**

When the coursework was published, we as a group decided to complete this coursework first and then move on to other modules, since this requires lot of time and research. Before our meeting, we each came up with a topic for this coursework. I suggested to do something related to IoT because I found it interesting and wanted to learn more about it. Once the topic was chosen, the work was divided, and I got to do research about healthcare-based IoT clouds.

During my initial research, I found a lot of publications discussing the architecture for IoT-based clouds. It elaborated on various techniques and mechanisms for the efficient transmission of data to the cloud. It did not however elaborate much on security and privacy issues. The literature review in this paper nevertheless helped in finding some more papers related to this topic. First, I found a paper presented by Alasmari and Anwar on Security and Privacy Challenges in IoT-Based Health Cloud. After further research, I found six publications which were interesting and aligned perfectly to our topic.

Initially, I had an idea of structuring the review based on a timeline. When it was handled that way, the contents did not have a proper flow of information. Therefore, instead I structured the review according to the theme. The paper presented by Garkoti, Peddoju and Balasubramanian was the only paper in my review which specifically address the problems in transferring the medical records in clouds. Other papers provide solutions to security challenges in storing the medical records in the clouds. The review addresses the insider threats, use of multi-clouds for data security and provides architecture for secure storage of patient's medical records.

Most of the privacy and security algorithms for IoT are still in implementation stage under several assumptions. Thus, the need for more research to protect data security and privacy at all layers should be done. So, users, organizations and developers have to come under one roof and find a prominent solution for a secured IoT environment.

The online group meetings went smoothly, we met weekly twice. Since we had our own topic to review, it was easy to contribute to the assigned task. We were able to complete the coursework in two weeks which gave us plenty of time to focus on other module coursework.

## 5. REFERENCES

- Abinaya, Kumar, V. and Swathika (2015) 'Ontology Based Public Healthcare System in Internet of Things (IoT)', *Procedia Computer Science*, 50, pp. 99–102. doi: <https://doi.org/10.1016/j.procs.2015.04.067>.
- Alasmari, S. and Anwar, M. (2017) 'Security & privacy challenges in IoT-based health cloud', *Proceedings - 2016 International Conference on Computational Science and Computational Intelligence, CSCI 2016*, pp. 198–201. doi: 10.1109/CSCI.2016.0044.
- Alsubaei, F., Abuhussein, A. and Shiva, S. (2017) 'Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment', in *2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops)*, pp. 112–120. doi: 10.1109/LCN.Workshops.2017.72.
- Amaraweera, S. P. and Halgamuge, M. N. (2019) 'Internet of Things in the Healthcare Sector: Overview of Security and Privacy Issues', in Mahmood, Z. (ed.) *Security, Privacy and Trust in the IoT Environment*. Cham: Springer International Publishing, pp. 153–179. doi: 10.1007/978-3-030-18075-1\_8.
- Das, A. K. *et al.* (2018) 'Design of Secure and Lightweight Authentication Protocol for Wearable Devices Environment', *IEEE Journal of Biomedical and Health Informatics*, 22(4), pp. 1310–1322. doi: 10.1109/JBHI.2017.2753464.
- Elhoseny, M. *et al.* (2018) 'Secure Medical Data Transmission Model for IoT-Based Healthcare Systems', *IEEE Access*, 6, pp. 20596–20608. doi: 10.1109/ACCESS.2018.2817615.
- Garkoti, G., Peddoju, S. K. and Balasubramanian, R. (2014) 'Detection of Insider Attacks in Cloud Based e-Healthcare Environment', in *2014 International Conference on Information Technology*, pp. 195–200. doi: 10.1109/ICIT.2014.43.
- Gunasekhar, T. *et al.* (2015) 'Mitigation of insider attacks through multi-cloud', *International Journal of Electrical and Computer Engineering*, 5(1), pp. 136–141. doi: 10.11591/ijece.v5i1.pp136-141.
- Hathaliya, J. J. and Tanwar, S. (2020) 'An exhaustive survey on security and privacy issues in Healthcare 4.0', *Computer Communications*, 153(September 2019), pp. 311–335. doi: 10.1016/j.comcom.2020.02.018.
- He, D. *et al.* (2018) 'Privacy in the Internet of Things for Smart Healthcare', *IEEE Communications Magazine*, 56(4), pp. 38–44. doi: 10.1109/MCOM.2018.1700809.
- Kodali, R. K., Swamy, G. and Lakshmi, B. (2015) 'An implementation of IoT for healthcare', in *2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS)*, pp. 411–416. doi: 10.1109/RAICS.2015.7488451.
- Kumar, M. (2014) 'Security Issues and Privacy Concerns in the Implementation of Wireless Body Area Network', in *2014 International Conference on Information Technology*, pp. 58–62. doi: 10.1109/ICIT.2014.73.
- Liu, S. *et al.* (2016) 'A novel asymmetric three-party based authentication scheme in wearable devices environment', *Journal of Network and Computer Applications*, 60, pp. 144–154. doi: <https://doi.org/10.1016/j.jnca.2015.10.001>.
- Liu, W. *et al.* (2016) 'The yoking-proof-based authentication protocol for cloud-assisted



wearable devices', *Personal and Ubiquitous Computing*, 20(3), pp. 469–479. doi: 10.1007/s00779-016-0926-8.

Mahajan, A. and Sharma, S. (2015) 'The Malicious Insiders Threat in the Cloud', *International Journal of Engineering Research and General Science*, 3(2), pp. 246–256. Available at: [www.ijergs.org](http://www.ijergs.org).

Manogaran, G. *et al.* (2018) 'A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system', *Future Generation Computer Systems*, 82, pp. 375–387. doi: <https://doi.org/10.1016/j.future.2017.10.045>.

S, J. and Philip, M. (2016) 'Rfid based security platform for internet of things in health care environment', in *2016 Online International Conference on Green Engineering and Technologies (IC-GET)*, pp. 1–3. doi: 10.1109/GET.2016.7916693.

Sadki, S. and Bakkali, H. El (2014) 'PPAMH: A novel privacy-preserving approach for mobile healthcare', in *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*, pp. 209–214. doi: 10.1109/ICITST.2014.7038807.

Sathya, D. and Kumar, P. G. (2017) 'Secured remote health monitoring system', *Healthcare Technology Letters*, 4(6), pp. 228–232. doi: 10.1049/htl.2017.0033.

Srinivas, J. *et al.* (2020) 'Cloud Centric Authentication for Wearable Healthcare Monitoring System', *IEEE Transactions on Dependable and Secure Computing*, 17(5), pp. 942–956. doi: 10.1109/TDSC.2018.2828306.

Strielkina, A. *et al.* (2018) 'Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment', in *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, pp. 67–73. doi: 10.1109/DESSERT.2018.8409101.

V.R., B. and S., M. (2014) 'Enhanced security for multi-cloud storage using cryptographic data splitting with dynamic approach', in *2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies*, pp. 1190–1194. doi: 10.1109/ICACCCT.2014.7019286.

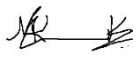


Vedaraj, M. and Ezhumalai, P. (2021) 'HERDE-MSNB: a predictive security architecture for IoT health cloud system', *Journal of Ambient Intelligence and Humanized Computing*, 12(7), pp. 7333–7342. doi: 10.1007/s12652-020-02408-x.

Yang, L., Zheng, Q. and Fan, X. (2017) 'RSPP: A reliable, searchable and privacy-preserving e-healthcare system for cloud-assisted body area networks', in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, pp. 1–9. doi: 10.1109/INFOCOM.2017.8056954.

Zhang, K. *et al.* (2015) 'Security and privacy for mobile healthcare networks: from a quality of protection perspective', *IEEE Wireless Communications*, 22(4), pp. 104–112. doi: 10.1109/MWC.2015.7224734.

Zhou, J. *et al.* (2015) 'TR-MABE: White-box traceable and revocable multi-authority attribute-based encryption and its applications to multi-level privacy-preserving e-healthcare cloud computing systems', in *2015 IEEE Conference on Computer Communications (INFOCOM)*, pp. 2398–2406. doi: 10.1109/INFOCOM.2015.7218628.

## A Contribution Share Agreement

Student Name	Student ID	Contribution (%)	Signature
Kiran Kumar Mohanraj	20054954	33.33	
Abdulaziz Saud Alahmed	19037366	33.33	
Abdulaziz Alaskar	19037894	33.33	

## B Alignment with CyBOK

The cyber security body of knowledge aims to inform and underpin education and professional training for the cyber security sector. The knowledge base of CyBOK is divided into various categories. This paper aligns with most of the categories provided. Namely, human, organisational and regulatory aspects, attacks and defences, system security, and infrastructure security. According to this knowledge base, the network security knowledge area under the wider advanced network security topics discusses IoT security. The first part of the review mostly aligns with adversarial behaviours and security operations, where IoT architectures were proposed to overcome the security flaws in the existing models. The review of IoT-based health clouds aligns with the authentication, authorisation and accountability (AAA) and privacy and online rights knowledge areas, with various privacy mechanisms proposed to ensure integrity and privacy of the patient's medical records.