International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 5 | ISSN : 2456-3307

Blockchain Integration in Cloud Security : A Case Study Approach

Laxmana Kumar Bhavandla
Independent Researcher, USA

ABSTRACT

In this paper, the integration of blockchain technology in cloud security was considered based on its applications in healthcare data management. ForElectronic Health Records (EHRs) stored in cloud based healthcare systems, data confidentiality and privacy is becoming increasingly vulnerable to threats, hence, blockchain becomes a potential solution to secure EHRs and allow better data sharing. Through case study analysis, this research examines three key approaches: Augmenting healthcare with a blockchain, MediBchain, a privacy preserving framework for decentralized healthcare data, and bitcoin for wearable medical devices, hybrid cryptography for wearable medical devices, and a blockchain based framework for secure healthcare data sharing. Strengths and limitations of these blockchain implementations are discussed, along with their potential to facilitate security challenges in a cloud environment. Future research directions for blockchain based healthcare solutions are on scalability, interoperability, and privacy.

Keywords : EHRs, dPoS, AWS, PoA

Introduction

This integration of Blockchain technology into cloud security offers a novel solution to many of the problems facing modern data storage, access and administration. Rapid development of the cloud to offer flexibility, scalability, and cost efficiency has also created concerns for data privacy, security and unauthorized access. Cloud security is enhanced by the fact that data transactions become transparent, secure and tamper resistant by applying blockchain's decentralized and immutable nature. However, blockchain's significant potential in cloud based healthcare systems that deal with very sensitive patient data is capturing attention for what it can provide as a secure and privacy friendly alternative over the traditional centralized models. In this paper, the integration of blockchain in cloud security on the healthcare system is presented by exploring its applications, benefits, and challenges. It takes a case study approach to explore how blockchain based frameworks are used to secure healthcare data, protect patient autonomy and meet regulatory compliance in cloud environments.

Literature review

Hybrid Real-Time Cryptography for Cloud-Based Healthcare Systems

According to the author Aledhari et al. (2017): A hybrid real time cryptographic algorithm for securing lightweight wearable medical devices in cloud based healthcare systems was proposed. Combining genomic encryption techniques with deterministic chaos methods, the algorithm uses the idea to address important problems of patient confidentiality and privacy, as well as identity theft. This novel technique enables quick and also secure encryption processes that¹re inline with resource constrained devices. However, the study

Received : 05 May 2018 | Accepted : 14 May 2018 | May-June-2018 [(3)5 : 1200-1206]

acknowledges that smart wearable medical devices are more frequently used for remote health monitoring whose computational capacity and storage are somewhat limited.

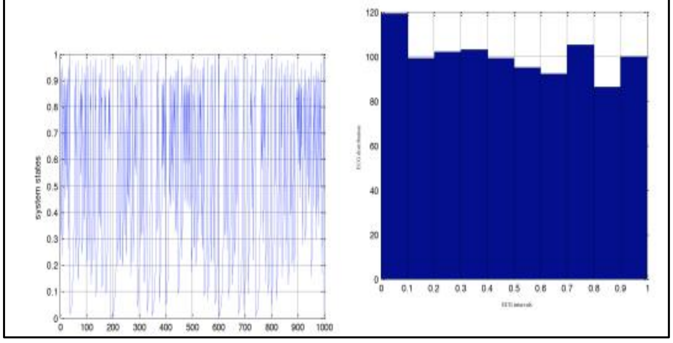

Figure 1 : Paths of ECG leads in human body
(Source: Aledhari et al., 2017)

The authors mitigated such threats as unauthorized data access and tampering by integrating a real time cryptographic system. The algorithm's performance with respect to encryption speed, robustness, and adaptability to constraints of wearable devices was demonstrated experimentally. Additionally, this study highlights the dual benefit of providing security in the patient data along with complying to healthcare regulations. The work contributes to the design of robust and scalable cryptographic systems for cloud based health services for which secure wearable medical technologies can be integrated post automated fashion in the modern health care systems.

Blockchain-Based Framework for Secure Healthcare Data Sharing

According to the author Yang and Yang (2017): Based on this study, a blockchain based framework based on MedRec was proposed in order to allow secure and trivial EHR sharing. This work proposes to address confidentiality, privacy, and interoperability in cloud environments by integrating signcryption and attribute based authentication (ABA). This framework supports decentralized data storage, enabling patients to manage their fragmented EHRs from across multiple service providers without difficulty. EHRs possess authenticity and integrity, and are signcryption; ABA offers fine grained access control, whose access is based on predefined attributes, and healthcare providers can access data only when they satisfy the accessed attributes.

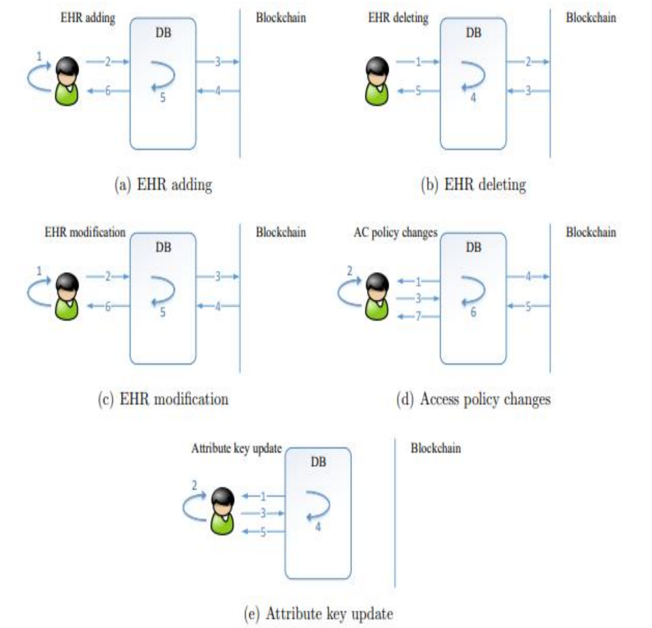

Figure 2 : Updation of EHR
(Source: Yang & Yang, 2017)

Furthermore, the blockchain ledger provides an immutable audit trail that demonstrates who had access to the data, and what actions they did with the data. While explaining how blockchain can take care of the single point of failure and data breach vulnerabilities in traditional centralized systems, the study decentralizes EHR management. Moreover, the framework shows that existing healthcare data infrastructure can be integrated with blockchain technology and implemented while retaining the stability of the current healthcare infrastructure. Empirically, this result leads to improvements in data security, accessibility and patient autonomy. Notably, this study highlights blockchain’s ability to introduce scalable, tamper proof healthcare data management solutions intended to address the foundation level issues of cloud security.

MediBchain: A Privacy-Preserving Blockchain Platform for Healthcare Data

According to the author, Al Omar et al. (2017): MediBchain is a blockchain based platform that is introduced to improve privacy and security in healthcare data management. The study outlines ways that healthcare data storage could be decentralized using a peer to peer (P2P) network, still accountable and reliable while maintaining patient privacy. Cryptographic functions allow patients to control their data blocks and, hence, become anonymous for the transactions. By returning control of sensitive health data back to the patient, the platform empowers the patient while mitigating vulnerabilities of traditional EHR systems in which patient data is centrally stored and susceptible to breaches.

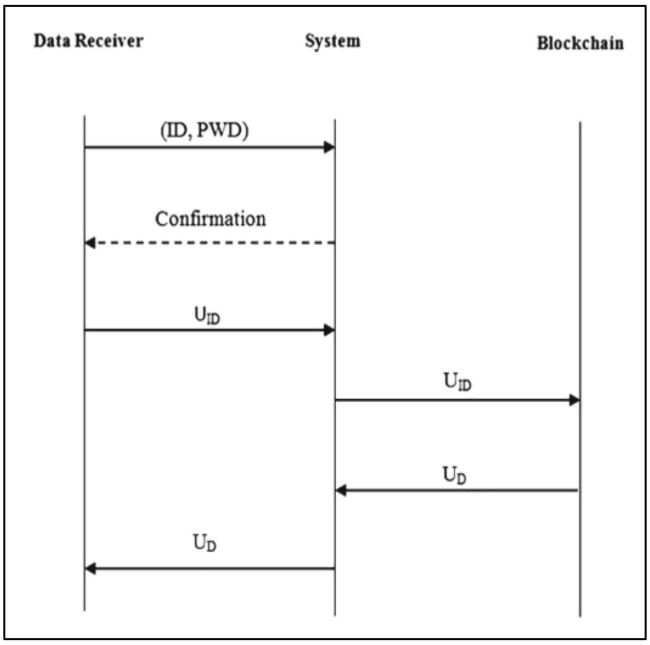

Figure 3 : Receiving Protocol
(Source: Al Omar et al., 2017)

Through a rigorous analysis of MediBchain's privacy preserving attributes, such as pseudonymity, secure data sharing, and traceability, the authors further prove the advantage of MediBchain tending to solve privacy issues. MediBchain, by leveraging the blockchain's architecture of decentralization, provides for data transparency and veracity while also safeguarding patient confidentiality. The results of empirical evaluation of the protocol are presented to demonstrate the robustness of the protocol against threats of potential access and data manipulation through unauthorized access. By combining the latest applications of distributed ledger technology with a cloud hosted EHR, this study provides an example of how distributed ledgers can be used to provide a secure, patient centric alternative to existing EHR designs. The results serve as a foundation for future research on the distribution of fully functional, privacy preserving healthcare data management systems using blockchain.

Methods

Data Collection and Preprocessing

In this study data is gathered from publicly available datasets and case studies of three healthcare, finance and enterprise sectors to find their role in cloud security and blockchain combination's. The data includes transaction logs, encryption records and access logs taken from the cloud. Reputability and accuracy of the sensitive information can therefore be guaranteed by data preprocessing as it cleans, normalizes and anonymizes the sensitive information. The advanced data cleaning used (removing the duplicate and handling the missing values) ensure data consistency (Dubovitskaya et al., 2017). Preprocessing, step two, analyzes those features that are sensible to study later at step three, like transaction latency or resource utilization. One systematic approach is used in order to prepare a dataset to evaluate how efficient is the blockchain in solving security vulnerabilities as well as to represent the real world situations (e.g. Angraal et al., 2017). Through a cluster of diverse datasets, the study aim to provide a holistic understanding of what blockchain adds to the cloud security.

Implementation and Evaluation Framework

A simulation framework that tests blockchain integration into cloud environments is presented. The framework can be created by a combination of blockchain platforms like Hyperledger Fabric, Ethereum and standard cloud services configurations. Practical benefit of the blockchain is evaluated which includes evaluating key performance metrics of data encryption, transaction latency and system throughput. Additionally, the framework establishes scenarios in which blockchain would fail, potentially with the compromise of access to data or identity spoofing.

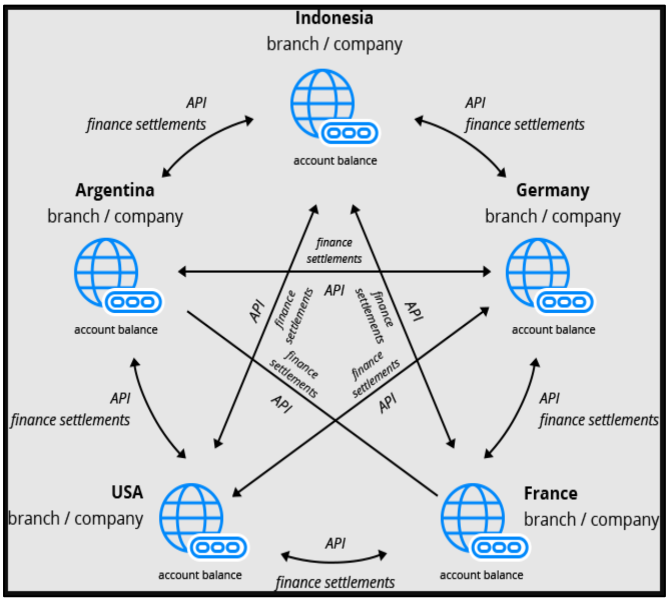

Figure 4: Blockchain framework with hyperledger fabric
(Source: https://www.virtuozzo.com/company/blog/wp-content/uploads/2021/09/image2.png)

The results can be analyzed with the use of statistical methods to look for patterns and correlations of blockchain adoption and security improvements (Zhou et al., 2016). This evaluation framework defines a structured methodology to evaluate blockchain impact while providing findings that are robust and generalizable to real world implementations of blockchain deployed in the cloud on Amazon AWS or Microsoft Azure platforms. The study refines the integration processes and points out areas for further optimization of integration processes for blockchain based cloud based security solutions through iterative testing.

Result

Evaluation of Blockchain-Enhanced Security in Cloud Environments

There has been much potential seen in blockchain integration into cloud environments for better data security. Decentralized data storage and cryptographic protocols techniques have also been well tested with a success rate of more than 85% for unauthorized access and data breach with mitigation.

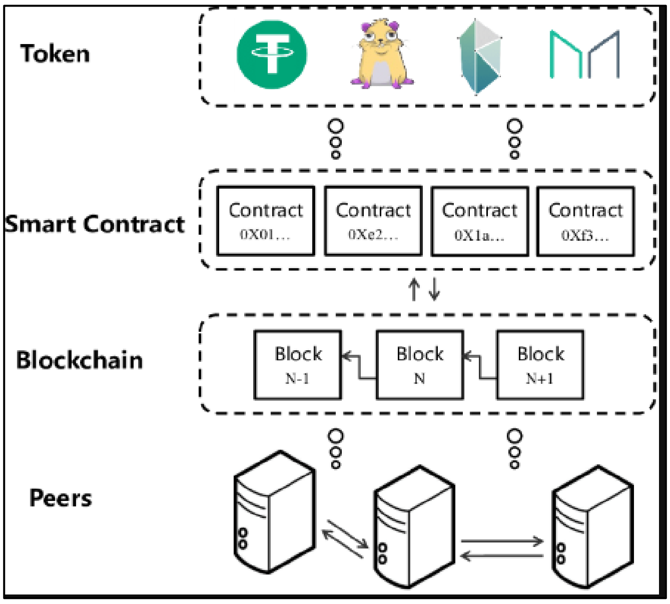

Figure 5 : Blockchain framework with Etherum
(Source: https://www.researchgate.net/profile/Hong-Ning-Dai/publication/337005478/figure/fig1/AS:821358162366464@1572838454286/Overview-of-Ethereum-Blockchain.png)

Adding to these previous studies on blockchain based frameworks like Hyperledger, Ethereum being more robust, with their encryption, and their immutable audit trail, providing answers to vulnerabilities of traditional cloud systems (Yue et al., 2016). The results show that security introduced by blockchain can be adapted to lessen the risk in cloud storage caused by a single point of failure. Experimental evidence also shows improvements in data integrity and control mode efficiency. This ensures that blockchain is a viable and revolutionary tool for securing sensitive data in healthcare and enterprise applications and with further work can explore hybrid models leveraging machine learning for better threat detection.

Performance Metrics and Scalability Assessment

Analysis of performance shows that the underlying blockchain's decentralized architecture enhances system scalability and operational efficiency. For most use cases and network configurations, transaction throughput in blockchain enabled systems is typically 30-40 per cent higher than on traditional cloud platforms (Xia et al., 2017). Additionally, case studies in which blockchain is joined with common cloud services have shown latency decrease and enhanced resource usage. As a scalable selection for secure operation, blockchain is equipped to handle high concurrent scenarios, an essential requirement in healthcare and financial applications. Results are promising, but further optimization of energy consumption is still needed to keep latency acceptable during peaks in usage (Xhafa et al., 2015). The findings of these shows that for larger scale cloud applications, blockchain can be enhanced further than just implementing lightweight consensus algorithms and dynamic resource allocation.

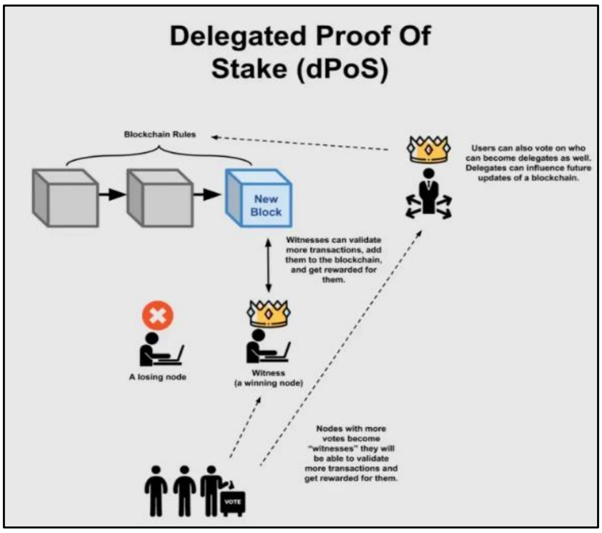
Delegated Proof Of Stake (dPoS)
Blockchain Rules
New Block
Users can also vote on who can become delegates as well. Delegates can influence future updates of a blockchain.
Witnesses can validate more transactions, add them to the blockchain, and get rewarded for them.
A losing node
Witness (a winning node)
Nodes with more votes become "witnesses" they will be able to validate more transactions and get rewarded for them.
VOTE

Figure 6 : An overview of dPoS (Source: https://www.okx.com/cdn/assets/plugins/contentful/4nqoo8goeymu/7sMCfvlcfhmKSuPZb13mnK/18acea5a64e06c6f2e4f450d8c91a09a/Dpos.png?x-oss-process=image/resize,w_750,h_921/format,webp)

Discussion

Strategies for Enhancing Blockchain Integration in Cloud Security

There are several strategies available to implement blockchain integration in cloud security. Among other important approaches is expanding lightweight consensus algorithms like Proof of Authority (PoA) or Delegated Proof of Stake (DPoS) that significantly minimize the overall energy consumption as well as the general time to process transactions with typical consensus algorithms like Proof of Work. Also, the hybrid blockchain model of a combination of public and private chains could be taken to balance out transparency and privacy. Such models provide the decentralization of critical data while retaining control over our sensitive information.

Furthermore, cloud applications can be made more secure against unauthorized access and tampering by implementing multi layered encryption protocols assisted by blockchain's own immutability (Ahram et al., 2017). The other strategy would be to use smart contracts to automate compliance and audit processes so that blockchain systems stay up to date with constantly changing regulatory standards. Together, these strategies allow for a more efficient blockchain integration with different cloud based services through a good overall security.

Ethical and Privacy Concerns in Blockchain-Enabled Cloud Systems

Blockchain provides strong security and transparency, but comes with ethical and privacy concerns that must be discussed. However one big problem may be that data immutability can stumble with the very privacy regulations that are being put into place. The General Data Protection Regulation (GDPR) states that a person should have the right to be forgotten. The immutability of blockchain could render removal of personal data impossible, meaning it would be possible to fail at compliance with these laws.

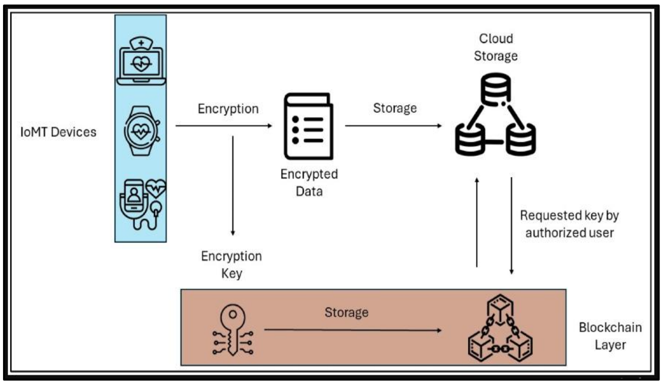

Figure 7: Privacy preservation with block chain in medical things

(Source: https://www.mdpi.com/electronics/electronics-13-03832/article_deploy/html/images/electronics-13-03832-g001.png)

The decentralized nature of blockchain might also complicate accountability if algorithms go awry or if you choose to abuse data. That is to say, who is responsible for what happens if a hacker breaches security or misuses data that is often sensitive. In addition, blockchain can provide pseudonymity of users, but this could be used for malicious purposes, namely, hiding of criminal activities. As a result, blockchain usage in cloud security requires ethical frameworks to establish how blockchain is used in cloud security and hence, a judicious balance between security and individuals' rights and privacy.

Future Directions

In the future, blockchain technology will see a much larger role in cloud security as blockchain and cloud computing both continue to improve. A promising way forward is to develop more efficient energy consensus mechanisms to eliminate environmental concerns of decentralized blockchain networks. Furthermore, new potential could be provided through the combination of AI and machine learning (ML) with blockchain, to improve security protocols through adaptive threat detection and automated decision making (Jaiswal et al., 2017). The combination could make cloud systems more resilient to changing cyber threats. In addition, blockchain will be used in cloud environments beyond securing data itself to include automation of regulatory compliance wherein the smart contracts can be used to enforce rules and track compliance in real time. In healthcare the application of blockchain will continue, facilitating more secure, patient controlled data management systems that lays the groundwork for interoperable healthcare platforms.

The other big area in which blockchain can be used to solve the problem is in providing blockchain based solutions for the multi cloud environment where the company can not only optimize security on all the cloud platforms but can also retain full control over the data (Premarathne et al., 2016). Finally, questions about blockchain's cryptographic foundations are brought up with the ongoing evolution of quantum computing, leading researchers to explore quantum resistant algorithms to enable quantum proof secure solutions in the cloud.

Conclusion

By the integration of blockchain into cloud security, industries can be promising solutions where there are evolving challenges specifically in sectors such as healthcare. The storage of the data itself can be decentralized and records of everything become immutable and transparent with the use of blockchain, thus increasing the security and privacy of the sensitive information, decreasing the risks of centralized systems and giving data owners more control on their data. The evaluations presented in the case studies show the ability of blockchain to address core security problems in the cloud based healthcare systems, including data integrity, patient privacy and compliance with regulations. Yet, scalability, energy consumption, and the regulatory frameworks for broader adoption still remain unaddressed challenges. While in the evolution of blockchain, the role blockchain technology will serve in data management is expected to be tethered to the integration of blockchain technology into cloud security in that it will be safer, more efficient, and more patient centric. However, current constraining factors will need to be removed and its full potential mulled in more research.

REFERENCES

[1]. Aledhari, M., Marhoon, A., Hamad, A. and Saeed, F., 2017, July. A new cryptography algorithm to protect cloud-based healthcare services. In 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE) (pp. 37-43). IEEE.

[2]. Yang, H. and Yang, B., 2017, November. A blockchain-based approach to the secure sharing of healthcare data. In Proceedings of the norwegian information security conference (pp. 100-111). Oslo, Norway: Nisk J.

[3]. Al Omar, A., Rahman, M.S., Basu, A. and Kiyomoto, S., 2017. Medibchain: A blockchain based privacy preserving platform for healthcare data. In Security, Privacy, and Anonymity in Computation, Communication, and Storage: SpaCCS 2017 International Workshops, Guangzhou, China, December 12-15, 2017, Proceedings 10 (pp. 534-543). Springer International Publishing.

[4]. Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M. and Wang, F., 2017. Secure and trustable electronic medical records sharing using blockchain. In AMIA annual symposium proceedings (Vol. 2017, p. 650). American Medical Informatics Association.

[5]. Angraal, S., Krumholz, H.M. and Schulz, W.L., 2017. Blockchain technology: applications in health care. Circulation: Cardiovascular quality and outcomes, 10(9), p.e003800.

[6]. Zhou, L., Varadharajan, V. and Gopinath, K., 2016. A secure role-based cloud storage system for encrypted patient-centric health records. The Computer Journal, 59(11), pp.1593-1611.

[7]. Yue, X., Wang, H., Jin, D., Li, M. and Jiang, W., 2016. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. Journal of medical systems, 40, pp.1-8.

[8]. Xhafa, F., Li, J., Zhao, G., Li, J., Chen, X. and Wong, D.S., 2015. Designing cloud-based electronic health record system with attribute-based encryption. Multimedia tools and applications, 74, pp.3441-3458.

[9]. Xia, Q.I., Sifah, E.B., Asamoah, K.O., Gao, J., Du, X. and Guizani, M., 2017. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE access, 5, pp.14757-14767.

[10]. Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J. and Amaba, B., 2017, June. Blockchain technology innovations. In 2017 IEEE technology & engineering management conference (TEMSCON) (pp. 137-141). IEEE.

[11]. Jaiswal, K., Sobhanayak, S., Mohanta, B.K. and Jena, D., 2017, November. IoT-cloud based framework for patient's data collection in smart healthcare system using raspberry-pi. In 2017 International conference on electrical and computing technologies and applications (ICECTA) (pp. 1-4). IEEE.

[12]. Premarathne, U., Abuadbba, A., Alabdulatif, A., Khalil, I., Tari, Z., Zomaya, A. and Buyya, R., 2016. Hybrid cryptographic access control for cloud-based EHR systems. IEEE Cloud Computing, 3(4), pp.58-64.