An Autonomous Role and Consideration of Electronic Health Systems with Access Control in Developed Countries: A Review

Mohd Rafiz Salji[1], Nur Izura Udzir[2]
Faculty of Information Management, Universiti Teknologi MARA, Malaysia[1]
Faculty of Computer Science and Information Technology, Universiti Putra Malaysia[2]

***Abstract*—The electronic healthcare system (EHS) nowadays is essential to access, maintain, store, and share the electronic health records (EHR) of patients. It should provide safer, more efficient, and cost-effective healthcare. There are several challenges with EHS, notably in terms of security and privacy. Nonetheless, many approaches can be utilized to tackle it, and one of them is access control. Even though numerous access control models were presented, traditional methods of access control, such as role-based access control (RBAC), were extensively employed and are still in use today. Currently, the number of EHS equipped with access control keeps growing, and some previous works utilize RBAC only or an autonomous role. However, relying only on a role in today's advanced technology may jeopardize security and privacy. The previous work also has flaws because of using an ineffective instrument that is costly to maintain and will burden organizations, particularly in developed countries. In this paper, the background and emphasis on the challenges associated with an autonomous role in the EHS are discussed. Following that, this paper provides recommendations and analytical discussion on existing EHSs with access control mechanisms for securing and protecting EHR in developed countries. Finally, instrument information in the form of a SWOT analysis is recommended to replace the present instrument utilized by the previous work for a notion to the organizations in the developed countries to select the best environment for their future or upgrade EHS.**

***Keywords*—Access control; security; privacy; electronic healthcare system; electronic health record; developed countries**

I. Introduction

Recently, developments in information technology have made significant progress in the field of medical information. This information nowadays is managed in a system called EHS. Advanced EHS is required to manage massive volumes of EHR clearly and cost-effectively. EHR is a non-printed form that electronically stores all of a patient's medical information. EHS is now developed and administered by numerous medical institution systems that allow sharing of EHR among various healthcare practitioners and organizations, rather than by a single healthcare organization. Due to that, a sophisticated system must be put in place to secure and preserve EHR.

Many approaches have been utilized to address security and privacy protection, but the most commonly used is access control. In general, access control is important in securing systems and protecting the privacy of authorized users, especially when providing health services. Today, many types of EHS combined with access control have been proposed, however, there are still issues that impede the development of EHS with access control.

This study discusses the issue of the utilization of access control mechanisms in EHS. The current EHS [1] has been established to secure and preserve EHR in developed countries. With regards to security and privacy, the previous system was in the initial stage of discussing the plan to use some instruments to secure their system, and the EHR in this system was protected using RBAC, which uses role or job function to allow or deny access to resources. Subsequently, another previous system [2], also used the RBAC model to secure the storage server in the cloud environment. Based on these previous works [1], [2], an autonomous role was utilized in these systems. It is indisputable that this traditional access control model is still applicable today; however, the problem is that employing an autonomous role to secure systems and preserve privacy in today's advances of ICT is not acceptable and unsafe, especially in a healthcare environment, due to various drawbacks of this scheme observed by previous works. Details about RBAC are discussed in Section II. The previous work [1] also suffers from the problem of utilizing the wrong choice of instrument, since they utilize a centralized database that has been claimed to have issues such as timely, frequent errors, and costly [3], [4].

This article review's main contributions are grouped into four categories. First, based on the problems of the previous works [1], [2], this paper provides background information on the RBAC model, including a description of the model's history, followed by examining the scheme's benefits and drawbacks based on previous works, and finally, discussions on the current EHSs employing autonomous RBAC. Second, this article examines and suggests previous literature reviews related to current EHS with access control models by discovering the environment and mechanisms used by previous systems instead of relying solely on an anonymous role. The aim is as a notion or an opportunity for the clinics and hospitals in developed countries to enhance their EHS with appropriate mechanisms in a specific environment in the future. It also aids researchers in swiftly grasping each function of the mechanisms employed by prior systems. The current EHS with access control models is examined in three categories: EHS with access controls aimed at securing the system, existing systems aimed at protecting the EHR, and finally,

existing systems capable of securing the system and protecting the EHR. Third, based on previous literature reviews, this article provides an analytical discussion in terms of the issues or problems of previous works, findings, or results of the previous works, and finally, comments or suggestions based on previous works. This discussion aimed to help identify how many issues or problems were faced by previous works and group them in the same categories. This discussion also helps clinics and hospitals in developed countries in obtaining information about the problems that happen in EHS and the way to solve them and have a notion to develop or upgrade EHS. It also helps the researcher in understanding difficulties and the ideas of previous works in solving problems, and comments or suggestions can be used to find opportunities for future work. Finally, because of previous work employed the wrong instrument, this paper provides critical instrument selection information in the form of a SWOT analysis that can assist clinics and hospitals in developed countries choose an acceptable and cost-effective instrument.

The rest of this paper is organized as follows: Section II provides the background of the RBAC model, while consideration of EHS with access control is discussed in Section III. In Section IV, the SWOT analysis is presented, and finally, Section V concludes the work.

II. Role-Based Access Control (RBAC)

Role-Based Access Control (RBAC) means to allow or deny client data from being accessed by the user based on role, i.e., job function or position, however, this decision depends on organizational policy [5]. This model has been introduced for over twenty years, primarily in UNIX, and centralized computer conditions, yet this model needs standardization because every framework utilizes its restrictive elements [6]. Therefore, the National Institute of Standards and Technology (NIST) began a task in 1992 to bound together with the principles of RBAC by incorporating the current models [6]. Although RBAC has since quite a while ago existed and is viewed as traditional access control, this model is still being used and stays pertinent right up until today.

In a positive sense, there are quite a few points why RBAC has become well known and can be utilized by current systems. The advantages of RBAC are as follows:

1) Simplifies access management and user permission review [7], where it is easy to categorize roles and a group of users for each role [8] and it aids in determining which permissions are permitted for which users in a large enterprise system [9].
2) RBAC policies adhere to the need-to-know security concept and fulfil the notion of least-access privileges [10]. This model also may be well-known for managing complicated role hierarchies in organizations [11].
3) This model may not need to be concerned about users being added or deleted from the system because this architecture is ideally suited to a large organization [12].
4) It can be considered an acceptable model in a healthcare cloud, as it has key strengths such as efficient management of large-scale user permissions, enforcement of need-to-know access controls, simplified auditing for regulatory compliance, and scalability [8].

Even though RBAC offers advantages, this model likewise experiences a few limitations. The following are RBAC drawbacks:

1) This model is incompatible with an open system in which the user is almost likely unknown, and the system recognizes a user solely by roles without knowing the identity and purpose of access —[13].
2) Previous works [14], [15] have highlighted that RBAC can lead to privacy disclosure, especially sensitive attributes to unauthorized and untrusted users because of the insufficient and inefficient of this model.
3) RBAC is less flexible and responsive because of its static role. As a result, RBAC cannot define granular control over users in certain roles in accessing certain individual objects, which is generally not sufficient for organizations with complex organizational structures, such as collaborative E-healthcare environments [9], [16], [17].
4) In a healthcare environment, installing an emergency access mechanism on a static role can pose a high security threat [18], for example, if unauthorized users can have illegal access rights under RBAC, they can easily compromise health records using the emergency access control window because there are no additional control variables to authenticate attacker access.
5) Although a previous study [12] has shown that RBAC is suitable for large organizations, however, RBAC is experiencing a role explosion or lack of scalability due to the increasing number of different roles. Furthermore, maintaining all these roles to provide appropriate access rights can be a difficult task [19]. Therefore, RBAC is not advised to be used in cloud computing or in a large system due to the lack of scalability [20], [21], [4].

In light of the previous passages, the aim of featuring the advantages and the drawbacks is to indicate the performance of this model. Despite the fact that the relevance of using RBAC until now was highlighted, nonetheless, this model also has many limitations. Therefore, proposing access control with an autonomous role, in the current context, i.e., in a collaborative system, is extremely hazardous.

Currently, several EHSs utilizing an autonomous role have been proposed. First, previous work [1] proposes a notion of early implementation of the EHS design model in the clinics and hospitals in developed countries, so that they do not miss out on the benefits of building this system rather than paper-based. A typical hospital workflow was defined and utilized in the design process. This study offers a prototype of an EHR web-based system that secures and protects privacy by utilizing RBAC. However, relying solely on RBAC without supporting other features may cause a security and privacy risk. This system also suffers weaknesses when using RBAC, such as static in nature and inflexibility [9], [16], [18], [17], which pose a difficulty if the user needs to treat patients during an emergency situation. A centralized database is an instrument

used in this system to allow access, maintain and store EHR. However, this instrument is not suitable to be utilized in developed countries since it contradicts the goals of generating cost-effective EHS. Next, Li et al. [22] also propose EHS with RBAC model to protect cloud-based outsourced EHRs. They claimed that this model provides an efficient and secure RBAC strategy for securing EHR stored on a storage server, even if the storage server is administered by an untrustworthy third party. This system offers a distinct and more efficient form of fine-grained access control that does not rely on attribute-based encryption (ABE). Only users with roles that adhere to the access policy are permitted to decapsulate. However, in the current circumstances, adopting an autonomous role may put the system in danger.

To summarize, employing an autonomous role to secure and maintain privacy in an internal, external, or collaborative system setting is not viable in today's tough environment. It is agreed that RBAC is still relevant nowadays since it has numerous benefits, however, this model needs support or a hybrid with other features. In the next section, the recommended current EHSs with access control utilizing with or without roles to secure and preserve the EHR is highlighted.

III. Consideration of EHS with Access Control Model

This section provides information on current EHSs with access control as a reference or notion for organizations in developed countries to developing efficient and effective EHS. The main aim is to highlight and compare the environment and mechanisms applied in the previous works. This section is divided into three sections: 1) The EHS with access control approaches seeks to secure the system, 2) The EHS with access control mechanisms intends to protect the EHR, and 3) The EHS with access control models to secure and protect EHR. This section also provides an analytical discussion of all collections of previous works in terms of the problems or issues, finding or results, and comments or suggestions.

A. Security

There are eight EHSs with access control in a cloud environment, and in this section, these systems are discussed.

First, in the cloud-fog computing environment, a searchable personal health records (PHR) framework with fine-grained access control was proposed. PHR is also EHR, however, PHR is controlled, shared, or maintained by patients themselves to support their personal care [23]. This framework was proposed to address the need for local information for a terminal device and the weaknesses of cloud computing [24]. To provide a keyword search function and fine-grained access control, the proposed framework integrates attribute-based encryption (ABE) technology and search encryption (SE) technology. When the keyword index and trapdoor match are successful, the cloud server provider only delivers relevant search results to the user, resulting in a more accurate search. Experiments with simulations demonstrate that the proposed method works well in a cloud-fog scenario. However, the keyword sets are obtained from the actual encrypted file on the cloud, introducing the prospect of a chosen-ciphertext attack. Besides, a novel, fine-grained, and flexible PHRs data access control system for cloud computing based on encryption was proposed to address the problem of repeated processes in data encryption [2]. The scheme consists of the symmetric key and the ABE layer. The system supports multi-privilege access control for PHRs from multiple patients in the ABE layer. To resolve the problem of repetitive processes, the scheme combines data encryption from different patients, where data is under a single access policy, to reduce encryption and decryption costs. Through implementation and simulation, the proposed scheme shows efficient in terms of time. Moreover, the proposed scheme proved that it was secured based on the security of the CP-ABE scheme. This system ensures data privacy, but, due to computational complexity and scalability concerns, it is unsuitable for health records. Next, the previous work [25] also utilized a CP-ABE based access control for a smart medical system with policy-hiding capabilities that is secure and efficient to overcome the problem of Zhang et al. [26] approach that fails to offer efficient large data storage with leakage resistance. The access control uses hidden access policies to satisfy the medical user's attribute values. A comparison of performance analysis reveals that the suggested system is more efficient than the current scheme. A Secure Healthcare Framework (SecHS) in the cloud using CP-ABE was proposed to provide secure access to health and medical information [27]. Patient data is encrypted under a symmetric encryption scheme and the access policy in CP-ABE is embedded with the ciphertext. The proposed framework was compared with current CP-ABE frameworks, and it demonstrates that SecHS offers greater features for data security. Next, the User Usage Based Encryption (UUBE) diversified access control framework, which usually builds on the searchable encryption technique to secure outsourced data was proposed [28]. In this method, the owner or patient will outsource data to the cloud data center. Data will be encrypted with a multiuser setting and will be stored in the form of ciphertext and finally stored in the database. To search PHR, the user needs to be authenticated by their category of user and institution. After receiving a request from a user, the data center computes the matching encrypted keyword search and returns the relevant outcome. Usage-based encryption is designed for user access and revoke after a specified time. This approach ensures a high level of security for data sharing. If there is misconduct in data access and various attacks by the revocation of the user, the suggested approach proved efficient. However, granular data access cannot be achieved using standard CP-ABE techniques, instead, a multi message CP-ABE is required. Subsequently, to secure cloud storage, a novel system using a hybrid encryption algorithm using Improved Key Scheme of RSA (IKGSR) and Blowfish was proposed [10]. To efficiently retrieve the encrypted data, steganography-based access control was utilized for key sharing via substring indexing and keyword search mechanisms. The findings clearly show that the proposed technique delivers superior security while also retrieving data more efficiently. An expressive and efficient access control method with attribute/user revocation based on the ordered binary decision diagram (OBDD) access structure was proposed to overcome the previous CP-ABE schemes relying on access structures that are either restrictive or cumbersome, resulting in less expressive and efficient [29]. The proposed work establishes attribute groups, which are made up of users who have specific attributes. Each attribute group has its own group key. Version numbers are assigned to user secret keys and ciphertexts to avoid cooperation between

revoked and non-revoked users. When a user's attribute is revoked, a new attribute group key is produced and disseminated to all group members except the revoked user. When there is a change in the attribute group key following an attribute/user revocation, the version number is incremented. The proposed approach was analyzed regarding security and efficiency, and shows that it is secure, expressive, and efficient. Finally, due to the inflexibility of the RBAC, a cloud-based EHR architecture to implement ABAC that employs extensible access control markup language (XACML) was presented [30]. The proposed approach has two stages, after conducting access control on patient records, encryption and digital signatures are applied as an additional security precaution utilizing XML encryption and XML digital signatures to provide more flexible and fine-grained control and minimize the chances of revealing patient private records. A comparison of the security criteria to those utilized in other relevant research was applied and found that the suggested technique was more secure than previous methods. However, encryption in XML requests and responses, on the other hand, is highly expensive for data sharing. Requests and responses are explicitly communicated between legal parties in the first phase and are thus vulnerable to attack.

Subsequently, the previous discussion of EHS with access control models aimed to secure the system is summarized in the form of a comparative analysis. The explanation is shown in Table I.

B. Privacy

In this section, eight EHSs with access control models that seek to protect EHR are discussed.

First, a privacy-aware relationship semantics–based extensible access control markup language (XACML) access control model was proposed that uses XACML to execute hybrid relationship and ABAC in the hybrid cloud [4]. To enhance multipurpose EHR utilization, the proposed approach offers fine-grained relation-based access control (Rel BAC) with an anonymization technique called Anatomy as it provides quality data utilization. The proposed model delivers and maintains efficient privacy vs utility trade-off. The proposed model was explicitly validated to assess its efficacy regarding privacy-aware electronic health data access and multi-functional usage. The experimental findings demonstrate that access policies based on relationships and EHR anonymization may perform well in terms of access policy response time, and space storage in the proposed model. Next, due to the patient's reluctance to share sensitive data, organizations rely on cloud solutions that employ machine learning models. This article offers a Euclidean L3P-based Multi-Objective Successive Approximation (EMSA) algorithm, efficient measure of privacy in a cloud [31]. Each EHR is divided into common and privacy-related attributes. Privacy-related attributes, such as sensitive information, are subjected to a cryptographic mechanism to produce a key for storage in a cloud environment. Role-based encryption keys are provided here as the fundamental foundation for the storage of sensitive data in cloud environments. In terms of performance, the proposed EMSA was compared with Bat, PUBAT, TPNGS, WOA, and CIC-WOA algorithms based on performance metrics, such as fitness, privacy, and utility. According to the simulation, the suggested EMSA model has greater privacy values.

A new framework for access control was proposed that protects the privacy of PHR data while a patient is in an emergency [32]. The system proposed uses smart contracts that may limit PHR access permissions in a state of emergency. The smart contract also enables the PHR owner to assign the rules to an employee (a certified medical practitioner) who has the authorization to access the actual data from the PHR, considering the time restriction. The system suggested provides historical audit records that store the history of transactions in an emergency. The proposed framework, based on the experiment, is improved regarding accessibility, privacy, emergency access control, and data auditing in health care systems. A PHR-based blockchain model was proposed to solve the limitation of the blockchain [33]. The proposed model is constructed to provide a tamper-resistant feature utilizing blockchain technology. To protect privacy, proxy re-encryption, and other cryptographic methods are applied. A comprehensive safety analysis reveals that the proposed model can protect the privacy and tamper resistance. The performance study reveals superior overall performance in the proposed model compared to the current literature approach. This work extended [34] by analyzing the system on a variety of user counts and PHR data sizes in a real-world situation.

Permission to access the EHR requires agreement from the patient (data owner), and additional access authorization to be granted by the patient to the healthcare professional is required. A newly built Health Information System (HIS) access decisions flow, guaranteed by RBAC, incorporating patient-centered control was designed [35]. Colored Petri-Networks (CPN) is used as a mimic for RBAC to demonstrate security policy conflicts or restrictions during the access control authorization process. To provide explicit permission for a patient to access their data in a non-offensive access flow, a discretionary access control (DAC) feature was added. Mutual exclusive was designed to consider patient needs for them to permit healthcare providers to access EHR data. Additional information was added to the permission Access Control matrix to ensure privacy is protected and subject to DAC. When compared to prior CPN simulations, a minor modification is proposed to integrate RBAC-aware systems with no significant drawbacks. Subsequently, a novel healthcare access control model named Solution de Gestion Automatisée du Consentement / automated consent management solution (SGAC) was proposed to manage patient consent for accessing their EHR [36]. Because patient preferences and rules may conflict, the SGAC provides a mechanism to handle this issue based on priority, specificity, and modality. Four sorts of characteristics were examined to safeguard patient privacy while providing effective care in life-threatening situations: accessibility, availability, contextuality, and rule effectivity. The verification of SGAC access control rules utilizing two first-order logic model controls, Alloy, and ProB, based on distinct technologies. The results show that SGAC performs better than XACML and that ProB outperforms Alloy by two orders of magnitude thanks to its programmable approach to constraint solving. A formal specification of the system based on the legislation that defines it was proposed to improve the confidence level of the patient towards the system in privacy preservation [37]. This work concentrated on the control and access features

TABLE I. EHS WITH ACCESS CONTROL MODELS IN THE CLOUD ENVIRONMENT AIMS TO SECURE THE SYSTEM

No	Ref.	Mechanism										
		ABE	CP-ABE	UUBE	SE	Sym metric	IKGSR	Blowfish	Stega-nography	OBDD	ABAC	XACML
1.	Sun, 2018	/			/							
2.	Li, 2018		/			/						
3.	Rana, 2020		/									
4.	Satar, 2021		/									
5.	Suresh, 2019			/								
6.	Chinnasamy, 2021						/	/	/			
7.	Edemacu, 2020									/		
8.	Seol, 2018										/	/

of patients' health information. The method used relies on the correct-by-construction Event-B to prove the control and access properties of the system. Finally, traditional approaches like k-anonymity and its derivations frequently overgeneralize, resulting in lower data accuracy. To address this problem, the Semantic Linkage K-Anonymity (SLKA) method was offered, which allows for continuing record linkages [38]. This work demonstrates how SLKA strikes a balance between privacy and utility preservation by detecting risky combinations hidden in data releases.

Subsequently, the previous discussion of EHSs with access control aims to protect privacy is summarized in the form of comparative analysis. The explanation is shown in Table II.

C. Security and Privacy

In this section, information about recent works on EHSs with access control to secure the system and protect EHR is highlighted.

A secure sharing architecture based on MA-ABE with anonymous authentication outsourcing was proposed to protect the patients' privacy and guarantee that patients may control their PHRs [39]. Before outsourcing, all PHRs are protected using MA-ABE, which overcomes the key hosting problem and achieves fine-grained access control to PHRs. Furthermore, anonymous authentication between the cloud and the user is recommended in order to secure data integrity on the cloud without revealing the user's identity during authentication. The proposed authentication is based on a novel attribute-based online-offline signature. In comparison to previous studies, the suggested approach not only retains encrypted PHRs resistant to collusion assaults and not forged throughout the sharing time, but it also accomplishes privacy preservation, which improves patients' control over their PHRs. Next, some health institutions in the Republic of South Africa have problems protecting HIV patient data because they still use traditional approaches, e.g., paper-based. This work aims to build a cloud-based access control model to share in nine (9) provinces in the South African Republic [40]. This study is based on the acceptance and use of the RBAC model for permission access based on job function, the Access Control List (ACL) contained a list of access control entries (ACE) to identify trustees and specify access privileges, and Motive Based Access Control (MBAC) models related to data object and motives of seeking them. However, this framework proposes a static model which is not suitable for emergency conditions. Subsequently, CP-ABE also was employed in the proposed scheme to enhance the retrieval capabilities of data based on disease and to solve the inefficiency of RBAC [41]. The proposed scheme can retrieve encrypted EHR based on a specific disease. Furthermore, the scheme ensures user access control and the anonymity of the user or data owner during data retrieval. Moreover, the scheme is resistant to collusion between unauthorized retrievers to access the data. Based on the results of the analysis, the suggested method accomplishes data confidentiality, user anonymity, and collusion resistance. A unique privacy-preserving access control (PPAC) method for electronic health records (EHR) was proposed based on the attribute-based signcryption (ABSC) scheme and the cuckoo filter [42] to solve the issue of security and privacy in sharing EHR. The ciphertext-policy attribute-based signcryption (CP-ABSC) is proposed to ensure fine-grained access control of the EHR data, utilize a cuckoo filter to hide the access policy, and preserve the privacy of EHR owners. Security analysis reveals that the proposed scheme is provably secure. In addition, the performance study reveals that, compared to previous schemes, the suggested scheme achieves low communication and calculation costs, while maintaining the privacy of its owner. However, hiding the AC policy may result in a loss of efficiency. A multi-layer access control (MLAC) model was proposed for building a secure and privacy-preserving EHR system that allows patients to exchange data with stakeholders [43]. In this article, a dual-layer access control model called pseudo-role attribute-based access control (PR-ABAC) was utilized that incorporates attributes with roles for secure sharing of EHR across many contributors. To protect the integrity of patient data, the proposed system also employs the notion of provenance. PASH, a privacy-aware s-health access control system, was introduced based on a large universe CP-ABE with partially concealed access restrictions to solve the problems of conventional CP-ABE [41]. In PASH, access policy attribute values are concealed in encrypted s-health records (SHRs), and only attribute names are exposed. In reality, attribute values contain far more sensitive data than general attribute names.

TABLE II. EHS WITH ACCESS CONTROL MODELS AIMS TO PROTECT PRIVACY

No.	Ref.	Environment		Mechanism									
		Cloud	Blockchain	XACML	ABAC	Rel BAC	Anatomy	EMSA algorithm	CPN	RBAC	SGAC	Event-B	SLKA
1.	Kanwal, 2019	/		/	/	/	/						
2.	Sathya, 2021	/						/					
3.	Rajput, 2021		/										
4.	Thwin, 2019		/										
5.	Junior, 2020								/	/			
6.	Huynh, 2019										/		
7.	Rivera, 2020											/	
8.	Lu, 2018												/

PASH, in particular, implements an efficient SHR decryption test that requires a limited number of bilinear pairings. The attribute universe can be exponentially huge, whereas public parameters are modest and constant in size. According to security analysis, PASH is completely secure in the standard model. PASH is more efficient and expressive than prior systems, based on performance comparisons and experimental data. However, this system lacks revocation. A sensitive and energetic access control (SEAC) was proposed for managing cloud-hosted EHRs and enabling fine-grained access control even in the critical environment to solve problems of the security of the prior system that have threatened the patient's privacy [44]. The system suggested guarantees that data from a patient are confidential where only authorized users may be permitted to modify or review particular data from the patient. Before submitting to cloud storage, each EHR data is encrypted by the managing authority. The requesting user can receive rights that change permission dynamically based on authentication and context attributes. The security analysis shows that the SEAC mechanism is secure and prevents unwanted access. The findings indicate outstanding compatibility and performance with various configurations and settings. However, keyword searches on encrypted data are not possible using the encryption methods employed. The encryption technique employs bilinear mapping, which has a high computational cost and is impractical for lightweight applications. A hybrid framework called MediTrust was proposed which combines two systems, namely RBAC and ABE, and operates in a semantic database, guaranteeing that patient data are accessible to various access controls [19]. On the provider side, patient data is encrypted before it is outsourced to the cloud server. After download, it is decrypted again at the user. The patient's general PHR and medical reports are stored separately on another cloud server. CAPTCHA provides the second stage of security control, particularly for security checks, which allows users to connect to MediTrust. The third step of safety control additionally provides for sharing one key with the registered cell phone number of the user and sharing another key with the user's e-mail id. In MediTrust, the PHR must be decrypted with the combination of the two keys. Furthermore, Amazon AWS EC2 CA was used to validate ABE policies and access control security mechanisms for privacy preservation on PHR. The results of performance evaluations demonstrate that regarding time complexity and computational overhead, the proposed MediTrust is superior than the prior projects.

A system was proposed by using a technique known as channelling integrated with a smart contract logic script within the network to ensure interoperability of EHR and access control only through the authorization of the patient [45]. The goal of this approach is to provide the entire privacy, integrity, and access control of distributed EHR. Simulated findings show that the proposed solution uses the blockchain to provide absolute transparency and perfect privacy inside a distributed network of sharing EHRs in the medical setting. Next, a blockchain-based architecture was proposed to secure, interoperable and efficient access to patients' medical records, while protecting the privacy of sensitive data of patients [46]. The proposed framework, named Ancile, uses smart contracts on an Ethereum-based blockchain for enhanced access control, and data obfuscation, as well as advanced cryptographic methods for additional security. However, this work uses six different forms of smart contracts for a proxy re-encryption approach that may incur high computational costs. Finally, Smart Contract-based Attribute-based Searchable Encryption (SC-ABSE) was proposed to solve the issue of security, privacy, and searchability in PHR [47]. This work bridges the gap between PHRs and blockchain technology by downloading extensive medical data into the IPFS and building a compulsory cryptography authorization and access control system for outsourced encrypted medical data. This system expands CP-ABE and searchable symmetric encryption (SSE), as well as using smart contract technologies, to accomplish the following: 1) efficient and secure fine-grained access control of outsourced encrypted data, 2) confidentiality of data by eliminating trusted private key generators, and 3) multi keyword searchable mechanism. The rigorous security indistinguishability analysis, based on decisional bilinear Diffie–Hellman hardness assumptions (DBDH) and dismulti-keywordhm (DL) issues, reveals that SC-ABSE is secure against the chosen-keyword attack (CKA) and keyword secrecy (KS) in the standard model. User collusion assaults are prevented, and data tamper-proof resistance is assured. Furthermore, security validation is validated by simulating a formal verification scenario with Automated Validation of Internet Security Protocols and

Applications (AVISPA), revealing that SC-ABSE is immune to man-in-the-middle (MIM) and replay attacks. Simulation findings demonstrate that SC-ABSE has high performance and low latency and that network life are ultimately increased in comparison with conventional medical systems.

Subsequently, the previous discussion of EHS with access control models aim to secure the system and protect privacy are summarized in the form of a comparative analysis. The explanation is shown in Table III.

Finally, all previous literature will be discussed in the form of an analytical discussion. The discussion is depicted in Table IV.

IV. SWOT Analysis of Instruments Considerable in Developed Countries

In view of past work [1], an affordable EHS was developed and it was targeted to be utilized by the organizations in the developed countries. The instrument used to maintain and store EHR is by using a centralized database system. However, this storage is timely, frequent error, and costly [3], [4] to use and maintain, and it is against the aims of creating an affordable EHS in developed countries. As indicated in the preceding sections, blockchain system and cloud computing were the dominant instruments to be used for accessing, maintaining, and storing EHR. These instruments can also be used as one of the solutions for securing and protecting privacy. However, organizations in developed countries should have the knowledge to choose the right instruments for their new or upgraded EHS. Therefore, information about blockchain systems and cloud computing is provided in this paper in the form of strength, weakness, opportunity, and threat (SWOT) analysis to allow organizations doing instrument selection either to use only one or hybrid instruments. This analysis is essential planning that can take enormous amounts of information inside these four domains and sort out them into explicit concerns [48], [49]. Because of its successful and simple forms of analysis, hospitals may use this method, and it is ideal for use in strategic planning in healthcare systems or medical advances.

First, the Blockchain is discussed in the form of a SWOT analysis. The description of the analysis is discussed as follows and summarized in the form of a list in Table V.

1) Strengths
   Benefits were classified into two groups: patient-related benefits and organizational-related benefits.

   For patient-related benefits, they include the followings:
   a) Users may only register their identity on the blockchain network once so they do not need to re-register their identification for the future [50].
   b) Allows healthcare professionals to embrace the concept of a shared database capable of producing sharable individualized healthcare plans for patients [50].
   c) The traceability feature enables tracking of the patient since every Bitcoin transaction is logged with a timestamp that is validated and maintained by all computer nodes participating in the blockchain network [50].
   d) Enable effective patient monitoring, especially for critically sick patients, because this technology assists physicians in making appropriate medical-related treatment decisions. To do this, patients' wearable gadgets such as smartwatches, smartphones, and smart glasses must be linked to the healthcare blockchain network [50].
   e) Improve privacy protection for citizens and governments by giving individuals more control over their personal data. They can use blockchain technology to control who has access to their data, for what purpose, and for how long [51].

   The organizational-related benefits are:
   a) To enable the secure sharing of patient information between healthcare organizations [50].
   b) To make clinical trial management easier because the study contains extremely sensitive patient-related information [50].
   c) The traceability function is crucial in controlling the pharmaceutical supply chain. In particular, can identify the origin of data, which can help pharmaceutical firms track the supply of products [50].
   d) Ability to manage medical insurance [50].
   e) Decentralized authority allows for the reduction of time, errors, and costs in the performance of processes, with the goal of building and updating a predictive model that supports medical care and risk management [3].
   f) The cryptographic system, the immutability of the data transmitted throughout the network, and the decentralized autho rity all contribute to increased confidence in the system [3].
   g) Every member can confirm the activities that happen in the organization as they have a duplicate of the entire blockchain on their gadget and this makes the process transparent [3].
   h) In Bitcoin, it is possible to identify any alteration to transaction records after they have been verified by solving a cryptographic problem [51].
2) Weaknesses
   a) A verified transaction might be reversed after a government or group of persons in control of a blockchain [51].
   b) With the possibility for additional records to be produced natively on chain via smart contracts, legal admissibility must be considered. Laws and regulations regulating the admission and weight to be given to such evidence vary by jurisdiction, making it difficult to generalize how such evidence could be regarded by courts [51].

TABLE III. EHS WITH ACCESS CONTROL MODELS AIMS TO SECURE THE SYSTEM AND PROTECT PRIVACY

No.	Ref.	Environment		Mechanism										
		Cloud	Block Chain	MA- ABE	RBAC	MBAC	CP-ABE	ABSC	Cuckoo filter	PR- ABAC	ABE	SSE	AC	Channeling integrated
1.	Zhang, 2020	/		/										
2.	Azeez, 2018	/				/								
3.	Zarezadeh, 2020	/					/							
4.	Ming, 2018	/						/	/					
5.	Chenthara, 2019	/								/				
6.	Zhang, 2018	/					/							
7.	Riad, 2019	/												
8.	Tembhare, 2019	/			/						/			
9.	Nortey, 2019		/										/	/
10.	Dagher, 2018		/											
11.	Hussien, 2021		/				/					/		

c) Blockchain records are intended to be immutable rather than changeable. This highlights the larger issue of how to remove or dispose of records from blockchain, which is also an issue to address when adopting data retention regulations or correcting mistakes in the record [51].
d) The topic of how to maintain blockchain records, in the long run, remains unanswered [51].

3) Opportunities
a) As more companies see the advantages of blockchain-based recordkeeping, they will need a trusted adviser to assist them [51].
b) Through its usage, information professionals may reinvent their methods. For example, the UK National Archives is investigating smart contracts, to automatically execute data publishing [51].

4) Threats
a) The sharing of whole copies of the blockchain under a model in which sensitive data on a single patient is shared would raise several issues related to privacy regulations, especially if entities other than public healthcare corporations participated in the network [52].
b) Scalability has become a major challenge for public blockchain applications, such as linking wearable devices because there is no control over the number of people joining the network [50].
c) Vulnerable to cyber-attacks where the attacker gains control of the blockchain network, which can lead to disaster if the attacker disrupts, stops or even reverses previously verified transactions within the network [50].
d) The high energy consumption has been noted since it pertains to the usage of the blockchain (public blockchain) based on proof of work, which is a mining process that uses a lot of electricity and it has gotten worse as more users have joined it and the number of transactions made per second has risen [50].
e) Absence of guidelines given by legitimate experts for blockchain advances [50].
f) Interoperability was considered as one of the significant difficulties for blockchain innovation reception in medical services because of the absence of trust between medical care organizations [50].
g) Lack of adequate technical skills and capabilities while carrying out blockchain advancements might prompt tragic results [50].
h) Data centers require a high cost of financing to maintain and require a large quantity of electricity [52].
i) One of the challenges is to train stakeholders on how to use this complex new system [52].

Next, this paper describes the SWOT analysis of cloud computing. A detailed list of cloud analysis is indicated in Table VI.

1) Strengths
a) It has been recognized that cloud computing reduces the price of IT infrastructure, and the lower cost of IT infrastructure will open the road for certain businesses to embrace the technology [53].
b) Cloud computing allows companies to concentrate their efforts on their core competencies while also providing them with a scalability scenario, both in terms of services and infrastructure, that becomes “unlimited” [54].
c) Cloud resources can be anything: database services, virtual servers or machines, full service processes, or complex setups of distributed computing systems such as clusters [54].
d) It does not require hardware and software updates as it is managed by the cloud provider [55].

2) Weaknesses
a) Concerns raised regarding the integrity, privacy, and security of services for users and their data [54].
b) Raises legal difficulties such as trademark infringement, security concerns, and the sharing of proprietary data resources [54].

c) There is a lack of consistency in service legal agreement (SLA) terminology. Performance and availability are essential SLA goals, but additional variables like security, data (ownership, location, access, and portability), dispute mediation, disaster recovery, and exit strategy negotiation are also crucial [54].

3) Opportunities
   a) Assist developed countries in reaping the advantages of cloud without the large upfront costs that have hindered previous attempts [54].
   b) Many innovative services are produced in the cloud, such as educational applications for African or developed country schools [54].
   c) Many vendors provide affordable cloud computing services [56].
   d) Cloud computing research is still in its initial phases, particularly in the health industry [56].
   e) The network, server, and security issues associated with locally installed, outdated systems are eliminated by adopting cloud computing [57].
4) Threats
   a) Problem in terms of data security, IT audit policies [54].
   b) Raises privacy problems since the service provider may access the data on the cloud at any moment, notwithstanding their own encryption claim. They may inadvertently or purposefully change or destroy data [54].
   c) The problem is with the legal ownership of the data. Many Terms of Service agreements do not address ownership issues [54].
   d) Lack of trust in cloud services [55].

V. Conclusion

This paper discusses the EHS with access control to secure and preserve EHR. The issue addressed in this paper is about the EHS with the RBAC model. In general, RBAC is a prevalent model in access control, and it may still be used in current EHS research, despite the fact that it is considered a conventional access control model. The problem highlighted in this paper is that using EHS with RBAC only to secure and preserve an EHR may cause a huge risk to the system. Therefore, several of the current studies on EHS utilizing access control have been suggested and examined their mechanisms and environment for a notion to the organizations in developed countries to develop their EHS instead of using an autonomous role. Analytical discussion in the form of a table has also been provided to identify the issues or problems, findings or results, and comments or suggestions related to previous works. Finally, due to problems with the instrument used by the previous work, information on instrument selection was provided in the form of a SWOT analysis as it is hoped that this information can be useful for organizations in developed countries in obtaining ideas for building their new or upgraded EHS in the right environment.

In the future, further developments need to be considered. First, many different types of access control models were employed, such as trust, purpose, and attributes. Therefore, this is an opportunity for researchers to develop EHS with a variety of access control models instead of an anonymous role to secure the system and protect privacy. Second, instead of developing EHS in a blockchain and cloud environment, maybe developing EHS in another environment needs to be considered for example mobile or IoT environment.

TABLE IV. ANALYSIS OF THE PREVIOUS LITERATURE

No.	Ref.	Problems / Issues										Findings / Results	Comments / Suggestions
		Data Access	Data Sharing	Patient Consent	Patient Control	Emergency Cases	Data Protection	Security Issues	CP-ABE Problems	Lack of RBAC	Other Problems		
1.	Sun, 2018										/	a) Proven secured b) Proposed model works well	a) The keyword sets = Possibility of a chosen -ciphertext attack b) Confidential guaranteed.
2.	Li, 2018										/	a) Implementation and simulation = Efficient (time) b) Proved secured	Impractical for health records = Computational complexity and scalability issues
3.	Rana, 2020										/	a) Protocol secured b) Efficient than the prior	-
4.	Satar, 2021	/										Secured compared to prior	-
5.	Suresh, 2019										/	a) Ensure secure data sharing b) Approach proved efficient	a) Granular data access cannot be achieved using standard CP-ABE b) Not suitable for single attribute's authority.
6.	Chinnasamy, 2021										/	a) Secure b) Retrieve data efficiently	-
7.	Edemacu, 2020								/			Analysis = Secure, expressive, and efficient	-
8.	Seol, 2018									/		a) Develop a prototype b) Secure than the prior	a) Encryption = Costly. b) Requests and responses = Exposed to attack.
9.	Kanwal, 2019		/									Access policies based on relationships and EHR anonymization performs well.	Access control rules and access control were improved
10.	Sathya, 2021						/					Has greater privacy value	-
11.	Rajput, 2021					/						Accessibility, privacy, emergency AC and data auditing improved	-
12.	Thwin, 2019										/	a) Protect the privacy and tamper resistance b) Superior than prior	Extends this work to fit with the real scenario.
13.	Junior, 2020			/								Minor modification of CPN was proposed	No experimental analysis
14.	Huynh, 2019			/								a) SGAC performs better b) ProB outperforms Alloy	-
15.	Rivera, 2020										/	a) Assure access to and control over the system b) Confidence utilize the system	-

No.	Ref.	Problems / Issues										Findings / Results	Comments / Suggestions
		Data Access	Data Sharing	Patient Consent	Patient Control	Emergency Cases	Data Protection	Security Issues	CP-ABE Problems	Lack of RBAC	Other Problems		
16.	Lu, 2018										/	No experimental analysis	-
17.	Zhang, 2020		/		/							Comparison = Accomplishes privacy preservation	-
18.	Azeez, 2018		/									Show preliminary framework	Static
19.	Zarezadeh, 2020										/	Accomplishes data confidentiality, user anonymity, and collusion resistance.	-
20.	Ming, 2018		/									a) Security analysis = Secure b) Performance = Low cost, while maintaining the privacy	Hiding the AC policy may sacrifice efficiency.
21.	Chenthara, 2019		/									No experimental analysis	-
22.	Zhang, 2018								/			a) Security analysis = Secure b) Performance = Efficient and expressive than prior	Lack of revocation
23.	Riad, 2019							/				a) Security analysis = Secure and prevents unwanted access. b) Outstanding compatibility and performance.	Encryption schemes = Has a huge computational cost and inefficient for lightweight applications.
24.	Tembhare, 2019	/										Performance = Superior than prior	-
25.	Nortey, 2019							/				Transparency and privacy	No experimental analysis
26.	Dagher, 2018				/	/	/					No experimental analysis	High computational cost
27.	Hussien, 2021						/	/				a) Proved secured b) AVISPA = Immune to man-in-the-middle-attack and replay attack c) High performance	-

TABLE V. SWOT OF BLOCKCHAIN TECHNOLOGY

Strengths	Weaknesses
Patient-related: - Register once - Shared database - Traceability - Patient monitoring - Privacy protection Organizational-related: - Secure sharing - Clinical trials - Pharmaceutical supply chain - Manage medical insurance - Reduce time, error, cost - Confidence - Transparent - Alteration detection	- Controlled by the top management - Legal admissibility - Disposition records - Maintain records
Opportunities	Threats
- Trusted advisor - Professional reinvention	- Sharing sensitive data - Scalability - Cyber-attack - High-energy consumption - Absence of guidelines - Inter-operability - Technical skills - Financial cost - Training

TABLE VI. SWOT OF CLOUD COMPUTING

Strengths	Weaknesses
- Reduce price - Scalability - Multi-purpose - Updated by the cloud provider	- Integrity, privacy, and security issues. - Legal issues - SLA inconsistency
Opportunities	Threats
- Assist developed countries - Produce innovative services - Services affordable - Research - Equipment and installation are removed	- Data security and audit - Privacy problem - Data legal ownership - Trust issues

REFERENCES

[1] O. E. Adetoyi and O. A. Raji, "Electronic health record design for inclusion in sub-Saharan Africa medical record informatics," *Scientific African*, vol. 7, p. e00304, 2020.

[2] W. Li, B. M. Liu, D. Liu, R. P. Liu, P. Wang, S. Luo, and W. Ni, "Unified fine-grained access control for personal health records in cloud computing," *IEEE Journal of Biomedical and Health Informatics*, vol. 23, no. 3, pp. 1278–1289, 2018.

[3] A. Fusco, G. Dicuonzo, V. Dell'Atti, and M. Tatullo, "Blockchain in healthcare: Insights on covid-19," *International Journal of Environmental Research and Public Health*, vol. 17, no. 19, p. 7167, 2020.

[4] T. Kanwal, A. A. Jabbar, A. Anjum, S. U. Malik, A. Khan, N. Ahmad, U. Manzoor, M. N. Shahzad, and M. A. Balubaid, "Privacy-aware relationship semantics–based XACML access control model for electronic health records in hybrid cloud," *International Journal of Distributed Sensor Networks*, vol. 15, no. 6, p. 1550147719846050, 2019.

[5] R. Sandhu, D. Ferraiolo, R. Kuhn *et al.*, "The NIST model for role-based access control: towards a unified standard," in *ACM Workshop on Role-based Access Control*, vol. 10, no. 344287.344301, 2000.

[6] H. A. Weber, "Role-based access control: the NIST solution," *SANS Institute InfoSec Reading Room*, 2003.

[7] S. Alshehri and R. K. Raj, "Secure access control for health information sharing systems," in *2013 IEEE International Conference on Healthcare Informatics*. IEEE, 2013, pp. 277–286.

[8] A. Small and D. Wainwright, "Privacy and security of electronic patient records–tailoring multimethodology to explore the socio-political problems associated with role based access control systems," *European Journal of Operational Research*, vol. 265, no. 1, pp. 344–360, 2018.

[9] H. Chi, E. L. Jones, and L. Zhao, "Implementation of a security access control model for inter-organizational healthcare information systems," in *2008 IEEE Asia-Pacific Services Computing Conference*. IEEE, 2008, pp. 692–696.

[10] P. Chinnasamy and P. Deepalakshmi, "HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–19, 2021.

[11] A. El Kettani, S. Housban, Z. Serhier, and M. B. Othmani, "Confidentiality in electronic health records systems: A review," *Journal of Medical and Surgical Research*, vol. 5, pp. 551–554, 2018.

[12] R. Gopalan, A. Antón, and J. Doyle, "UCONLEGAL: a usage control model for HIPAA," in *Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium*, 2012, pp. 227–236.

[13] A. Lazouski, F. Martinelli, and P. Mori, "Usage control in computer security: A survey," *Computer Science Review*, vol. 4, no. 2, pp. 81–99, 2010.

[14] M. R. Salji, N. I. Udzir, M. I. H. Ninggal, N. F. M. Sani, and H. Ibrahim, "Trust, purpose, and role-based access control model for privacy protection," in *International Symposium on ICT Management and Administration (ISICTMA2019)*, 2019, p. 69.

[15] ——, "Trust-based access control model with quantification method for protecting sensitive attributes," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 2, 2022. [Online]. Available: http://dx.doi.org/10.14569/IJACSA.2022.0130282

[16] S. Dixit, K. P. Joshi, and S. G. Choi, "Multi authority access control in a cloud EHR system with MA-ABE," in *2019 IEEE International Conference on Edge Computing (EDGE)*. IEEE, 2019, pp. 107–109.

[17] T. Tsegaye and S. Flowerday, "A Clark-Wilson and ANSI role-based access control model," *Information & Computer Security*, 2020.

[18] L. O. Nweke, P. Yeng, S. Wolthusen, and B. Yang, "Understanding attribute-based access control for modelling and analysing healthcare professionals' security practices," 2020.

[19] A. Tembhare, S. S. Chakkaravarthy, D. Sangeetha, V. Vaidehi, and M. V. Rathnam, "Role-based policy to maintain privacy of patient health records in cloud," *The Journal of Supercomputing*, vol. 75, no. 9, pp. 5866–5881, 2019.

[20] O. Alabi, "A review on information security of cloud based electronic health record," *Available at SSRN 3834180*, 2021.

[21] Y. Cheng, J. Park, and R. Sandhu, "Attribute-aware relationship-based access control for online social networks," in *IFIP Annual Conference on Data and Applications Security and Privacy*. Springer, 2014, pp. 292–306.

[22] W. Li, W. Ni, D. Liu, R. P. Liu, P. Wang, and S. Luo, "Fine-grained access control for personal health records in cloud computing," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*. IEEE, 2017, pp. 1–5.

[23] M. Price, P. Bellwood, N. Kitson, I. Davies, J. Weber, and F. Lau, "Conditions potentially sensitive to a personal health record (phr) intervention, a systematic review," *BMC medical informatics and decision making*, vol. 15, no. 1, pp. 1–12, 2015.

[24] J. Sun, X. Wang, S. Wang, and L. Ren, "A searchable personal health records framework with fine-grained access control in cloud-fog computing," *PloS one*, vol. 13, no. 11, p. e0207543, 2018.

[25] S. Rana and D. Mishra, "Efficient and secure attribute based access control architecture for smart healthcare," *Journal of Medical Systems*, vol. 44, no. 5, pp. 1–11, 2020.

[26] Y. Zhang, M. Yang, D. Zheng, P. Lang, A. Wu, and C. Chen, "Efficient and secure big data storage system with leakage resilience in cloud computing," *Soft Computing*, vol. 22, no. 23, pp. 7763–7772, 2018.

[27] S. D. M. Satar, M. A. Mohamed, M. Hussin, Z. M. Hanapi, and S. D. M. Satar, "Cloud-based secure healthcare framework by using enhanced ciphertext policy attribute-based encryption scheme," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 6, 2021. [Online]. Available: http://dx.doi.org/10.14569/IJACSA.2021.0120643

[28] D. Suresh and M. L. Florence, "Securing personal health record system in cloud using user usage based encryption," *Journal of medical systems*, vol. 43, no. 6, pp. 1–11, 2019.

[29] K. Edemacu, B. Jang, and J. W. Kim, "Efficient and expressive access control with revocation for privacy of PHR based on OBDD access structure," *IEEE Access*, vol. 8, pp. 18 546–18 557, 2020.

[30] K. Seol, Y.-G. Kim, E. Lee, Y.-D. Seo, and D.-K. Baik, "Privacy-preserving attribute-based access control model for XML-based electronic health record system," *IEEE Access*, vol. 6, pp. 9114–9128, 2018.

[31] A. Sathya and S. K. S. Raja, "Privacy preservation-based access control intelligence for cloud data storage in smart healthcare infrastructure," *Wireless Personal Communications*, vol. 118, no. 4, pp. 3595–3614, 2021.

[32] A. R. Rajput, Q. Li, and M. T. Ahvanooey, "A blockchain-based secret-data sharing framework for personal health records in emergency condition," in *Healthcare*, vol. 9, no. 2. Multidisciplinary Digital Publishing Institute, 2021, p. 206.

[33] T. T. Thwin and S. Vasupongayya, "Blockchain-based access control model to preserve privacy for personal health record systems," *Security and Communication Networks*, vol. 2019, 2019.

[34] ——, "Performance analysis of blockchain-based access control model for personal health record system with architectural modelling and simulation," *International Journal of Networked and Distributed Computing*, vol. 8, no. 3, pp. 139–151, 2020.

[35] M. A. de Carvalho Junior and P. Bandiera-Paiva, "Strengthen electronic health records system (EHR-S) access-control to cope with GDPR explicit consent," *Journal of Medical Systems*, vol. 44, no. 10, pp. 1–7, 2020.

[36] N. Huynh, M. Frappier, H. Pooda, A. Mammar, and R. Laleau, "SGAC : a multi-layered access control model with conflict resolution strategy," *The Computer Journal*, vol. 62, no. 12, pp. 1707–1733, 2019.

[37] V. Rivera, "Formal verification of access control model for my health record system," in *2020 25th International Conference on Engineering of Complex Computer Systems (ICECCS)*. IEEE, 2020, pp. 21–30.

[38] L. Zhang, Y. Ye, and Y. Mu, "Multiauthority access control with anonymous authentication for personal health record," *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 156–167, 2020.

[39] N. A. Azeez and C. Van der Vyver, "Access control model for e-health in a cloud-based environment for HIV patients in South Africa," in *2018 IST-Africa Week Conference (IST-Africa)*. IEEE, 2018, pp. Page–1.

[40] M. Zarezadeh, M. Ashouri-Talouki, and M. Siavashi, "Attribute-based access control for cloud-based electronic health record (EHR) systems," *The ISC International Journal of Information Security*, vol. 12, no. 2, pp. 129–140, 2020.

[41] Y. Ming and T. Zhang, "Efficient privacy-preserving access control scheme in electronic health records system," *Sensors*, vol. 18, no. 10, p. 3520, 2018.

[42] S. Chenthara, K. Ahmed, and F. Whittaker, "Privacy-preserving data sharing using multi-layer access control model in electronic health environment," *EAI Endorsed Transactions on Scalable Information Systems*, vol. 6, no. 22, 2019.

[43] K. Riad, R. Hamza, and H. Yan, "Sensitive and energetic IoT access control for managing cloud electronic health records," *IEEE Access*, vol. 7, pp. 86 384–86 393, 2019.

[44] R. N. Nortey, L. Yue, P. R. Agdedanu, and M. Adjeisah, "Privacy module for distributed electronic health records (EHRs) using the blockchain," in *2019 IEEE 4th International Conference on Big Data Analytics (ICBDA)*. IEEE, 2019, pp. 369–374.

[45] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustainable cities and society*, vol. 39, pp. 283–297, 2018.

[46] Y. Lu, R. O. Sinnott, K. Verspoor, and U. Parampalli, "Privacy-preserving access control in electronic health record linkage," in *2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*. IEEE, 2018, pp. 1079–1090.

[47] H. M. Hussien, S. M. Yasin, N. I. Udzir, and M. I. H. Ninggal, "Blockchain-based access control scheme for secure shared personal health records over decentralised storage," *Sensors*, vol. 21, no. 7, p. 2462, 2021.

[48] B. Phadermrod, R. M. Crowder, and G. B. Wills, "Importance-performance analysis based SWOT analysis," *International Journal of Information Management*, vol. 44, pp. 194–203, 2019.

[49] S. Walston, *Strategic Healthcare Management: Planning and Execution, Second Edition*, ser. AUPHA/HAP Book. Health Administration Press, 2018. [Online]. Available: https://books.google.com.my/books?id=-DocxQEACAAJ

[50] I. Abu-Elezz, A. Hassan, A. Nazeemudeen, M. Househ, and A. Abd-Alrazaq, "The benefits and threats of blockchain technology in healthcare: A scoping review," *International Journal of Medical Informatics*, p. 104246, 2020.

[51] V. L. Lemieux, "Blockchain recordkeeping: A SWOT analysis," *Information Management*, vol. 51, no. 6, pp. 20–27, 2017.

[52] S. Alla, L. Soltanisehat, U. Tatar, and O. Keskin, "Blockchain technology in electronic healthcare systems," in *Proceedings of the 2018 IISE Annual Conference*, 2018, pp. 1–6.

[53] O. M. S. H. Ali and A. Shrestha, "Analysis of the total cost of ownership for cloud computing technology adoption: A case study of regional municipal government sector," no. 56, 2017. [Online]. Available: https://aisel.aisnet.org/acis2017/56

[54] M. M. Seke, "Be mindful of the move: A SWOT analysis of cloud computing towards the democratization of technology," *i-manager's Journal on Cloud Computing*, vol. 5, no. 1, p. 26, 2018.

[55] J. Singh, "Study on challenges, opportunities and predictions in cloud computing," *International Journal of Modern Education and Computer Science*, vol. 9, no. 3, p. 17, 2017.

[56] S. J. Putra, M. N. Gunawan, D. P. Sari, S. Ratnawati, Y. Sugiarti *et al.*, "A cloud computing based for clinical information system," 2020.

[57] M.-H. Kuo, A. Kushniruk, and E. Borycki, "Can cloud computing benefit health services? : A SWOT analysis," in *User Centred Networked Health Care*. IOS Press, 2011, pp. 379–383.