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

Mohd Rafiz Salji¹, Nur Izura Udzir²
Faculty of Information Management, Universiti Teknologi MARA, Malaysia¹
Faculty of Computer Science and Information Technology, Universiti Putra Malaysia²

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 of health records (EHR) of patients. It should provide safer, more efficient, and cost-effective healthcare. 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 the 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 fulfill 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, introduc-
ing 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 compu-
tational 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 En-
cryption (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 mutliuser 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 stan-
dard 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 effectiveness. 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
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>
<thead>
<tr>
<th>No</th>
<th>Ref.</th>
<th>Mechanism</th>
<th>ABE</th>
<th>CP-ABE</th>
<th>UUBE</th>
<th>SE</th>
<th>Symmetric</th>
<th>IKGSR</th>
<th>Blowfish</th>
<th>Steganography</th>
<th>OBDD</th>
<th>ABAC</th>
<th>XACML</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Sun, 2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Li, 2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Rana, 2020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Satar, 2021</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Suresh, 2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Chinnasamy, 2021</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Edemacu, 2020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Serl, 2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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-keyword (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

---

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

<table>
<thead>
<tr>
<th>No.</th>
<th>Ref.</th>
<th>Environment</th>
<th>Mechanism</th>
<th>XACML</th>
<th>ABAC</th>
<th>Rel BAC</th>
<th>Anatomy</th>
<th>EMSA algorithm</th>
<th>CPN</th>
<th>RBAC</th>
<th>SGAC</th>
<th>Event-B</th>
<th>SLKA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Kanwal, 2019</td>
<td>Cloud</td>
<td>XACML</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Sathya, 2021</td>
<td>Blockchain</td>
<td>ABAC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Rajput, 2021</td>
<td></td>
<td>Rel BAC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Huynh, 2019</td>
<td></td>
<td>Anatomy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Rivera, 2020</td>
<td></td>
<td>EMSA algorithm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Lü, 2018</td>
<td></td>
<td>CPN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td></td>
<td></td>
<td>RBAC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td></td>
<td></td>
<td>SGAC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td></td>
<td></td>
<td>Event-B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td></td>
<td></td>
<td>SLKA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 authority 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].
TABLE III. EHS WITH ACCESS CONTROL MODELS AIMS TO SECURE THE SYSTEM AND PROTECT PRIVACY

<table>
<thead>
<tr>
<th>No.</th>
<th>Ref.</th>
<th>Environment</th>
<th>Mechanism</th>
<th>CP-ABE</th>
<th>ABSC</th>
<th>Cuckoo filter</th>
<th>PR-ABAC</th>
<th>ABE</th>
<th>SSE</th>
<th>AC</th>
<th>Channeling integrated</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Zhang, 2020</td>
<td>Cloud</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>2.</td>
<td>Azeez, 2015</td>
<td>Cloud</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>4.</td>
<td>Ming, 2018</td>
<td>Cloud</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>5.</td>
<td>Chenthara, 2019</td>
<td>Cloud</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>7.</td>
<td>Riaid, 2019</td>
<td>Cloud</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>8.</td>
<td>Tembhare, 2019</td>
<td>Cloud</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>10.</td>
<td>Dagher, 2018</td>
<td>Cloud</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>11.</td>
<td>Huisser, 2021</td>
<td>Cloud</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
<td>/</td>
</tr>
</tbody>
</table>

- **Strengths**
  - 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].
  - 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].
  - 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].
  - It does not require hardware and software updates as it is managed by the cloud provider [55].

- **Weaknesses**
  - Concerns raised regarding the integrity, privacy, and security of services for users and their data [54].
  - 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

<table>
<thead>
<tr>
<th>No.</th>
<th>Ref.</th>
<th>Problems / Issues</th>
<th>Findings / Results</th>
<th>Comments / Suggestions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Sun, 2018</td>
<td>Data Access, Data Sharing</td>
<td>a) Proven secured, b) Proposed model works well</td>
<td>a) The keyword sets = Possibility of a chosen ciphertext attack, b) Confidential guaranteed.</td>
</tr>
<tr>
<td>2.</td>
<td>Li, 2018</td>
<td>Data Access, Data Sharing</td>
<td>a) Implementation and simulation = Efficient (time), b) Proved secured</td>
<td>Impractical for health records = Computational complexity and scalability issues</td>
</tr>
<tr>
<td>3.</td>
<td>Rana, 2020</td>
<td>Data Access, Data Sharing</td>
<td>a) Protocol secured, b) Efficient than the prior</td>
<td>-</td>
</tr>
<tr>
<td>4.</td>
<td>Satar, 2021</td>
<td>Data Access, Data Sharing</td>
<td>Secured compared to prior</td>
<td>-</td>
</tr>
<tr>
<td>5.</td>
<td>Suresh, 2019</td>
<td>Data Access, Data Sharing</td>
<td>a) Ensure secure data sharing, b) Approach proved efficient</td>
<td>a) Granular data access cannot be achieved using standard CP-ABE, b) Not suitable for single attribute’s authority.</td>
</tr>
<tr>
<td>6.</td>
<td>Chinnasamy, 2021</td>
<td>Data Access, Data Sharing</td>
<td>a) Secure, b) Retrieve data efficiently</td>
<td>-</td>
</tr>
<tr>
<td>7.</td>
<td>Edemacu, 2020</td>
<td>Data Access, Data Sharing</td>
<td>Analysis = Secure, expressive, and efficient</td>
<td>-</td>
</tr>
<tr>
<td>8.</td>
<td>Seol, 2018</td>
<td>Data Access, Data Sharing</td>
<td>a) Develop a prototype, b) Secure than the prior</td>
<td>a) Encryption = Costly, b) Requests and responses = Exposed to attack.</td>
</tr>
<tr>
<td>9.</td>
<td>Kanwal, 2019</td>
<td>Data Access, Data Sharing</td>
<td>Access policies based on relationships and EHR anonymization performs well.</td>
<td>Access control rules and access control were improved</td>
</tr>
<tr>
<td>10.</td>
<td>Sathya, 2021</td>
<td>Data Access, Data Sharing</td>
<td>Has greater privacy value</td>
<td>-</td>
</tr>
<tr>
<td>11.</td>
<td>Rajput, 2021</td>
<td>Data Access, Data Sharing</td>
<td>Accessibility, privacy, emergency AC and data auditing improved</td>
<td>-</td>
</tr>
<tr>
<td>12.</td>
<td>Thwin, 2019</td>
<td>Data Access, Data Sharing</td>
<td>a) Protect the privacy and tamper resistance, b) Superior than prior</td>
<td>Extends this work to fit with the real scenario.</td>
</tr>
<tr>
<td>13.</td>
<td>Junior, 2020</td>
<td>Data Access, Data Sharing</td>
<td>Minor modification of CPN was proposed</td>
<td>No experimental analysis</td>
</tr>
<tr>
<td>14.</td>
<td>Hayth, 2019</td>
<td>Data Access, Data Sharing</td>
<td>a) SGAC performs better, b) ProB outperforms Alloy</td>
<td>-</td>
</tr>
<tr>
<td>15.</td>
<td>Rivera, 2020</td>
<td>Data Access, Data Sharing</td>
<td>a) Assure access to and control over the system, b) Confidence utilize the system</td>
<td>-</td>
</tr>
<tr>
<td>No.</td>
<td>Ref.</td>
<td>Problems / Issues</td>
<td>Findings / Results</td>
<td>Comments / Suggestions</td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
<td>-------------------</td>
<td>--------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>16.</td>
<td>Lu, 2018</td>
<td>Data Access</td>
<td>No experimental analysis</td>
<td>-</td>
</tr>
<tr>
<td>17.</td>
<td>Zhang, 2020</td>
<td>Data Sharing</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>18.</td>
<td>Accrue, 2018</td>
<td>Patient Consent</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>19.</td>
<td>Ezzeldeen, 2018</td>
<td>Patient Control</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Note: The table above lists various issues related to data access, sharing, patient consent, and control in the context of security and privacy in healthcare. Each row represents a different study or paper, with columns for references, problems/issues, findings/results, and comments/suggestions. The notes on the right side of the table provide additional context for each entry.
### TABLE V. SWOT OF BLOCKCHAIN TECHNOLOGY

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

### TABLE VI. SWOT OF CLOUD COMPUTING

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Reduce price</td>
<td>- Integrity, privacy, and security issues.</td>
</tr>
<tr>
<td>- Scalability</td>
<td>- Legal issues</td>
</tr>
<tr>
<td>- Multi-purpose</td>
<td>- SLA inconsistency</td>
</tr>
<tr>
<td>- Updated by the cloud provider</td>
<td>Opportunities</td>
</tr>
<tr>
<td></td>
<td>- Data security and audit</td>
</tr>
<tr>
<td></td>
<td>- Privacy problem</td>
</tr>
<tr>
<td></td>
<td>- Data legal ownership</td>
</tr>
<tr>
<td></td>
<td>- Trust issues</td>
</tr>
<tr>
<td></td>
<td>- Professional reinvention</td>
</tr>
<tr>
<td></td>
<td>- Produce innovative services</td>
</tr>
<tr>
<td></td>
<td>- Services affordable</td>
</tr>
<tr>
<td></td>
<td>- Research</td>
</tr>
<tr>
<td></td>
<td>- Equipment and installation are removed</td>
</tr>
<tr>
<td>Threats</td>
<td>- Data security and audit</td>
</tr>
<tr>
<td>- Integrity, privacy, and security issues.</td>
<td>- Legal issues</td>
</tr>
<tr>
<td>- SLA inconsistency</td>
<td>- Privacy problem</td>
</tr>
<tr>
<td>- Data legal ownership</td>
<td>- Trust issues</td>
</tr>
</tbody>
</table>

### REFERENCES


