IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

A Secure G-Cloud-Based Framework for Government Healthcare Services

Sanaa Sharaf[1], and Nidal F. Shilbayeh[2]

[1]Department of Computer Science, FCIT, King Abdulaziz University, Jeddah, 21589, Saudi Arabia, ssharaf@kau.edu.sa.
[2]University College in Umluj, The University of Tabuk, Umluj, Saudi Arabia, nshilbayeh@ut.edu.sa

Corresponding author: Nidal F. Shilbayeh (e-mail: nshilbayeh@ut.edu.sa).

This Project was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, under grant no. G-145-612-39. The authors, therefore, acknowledge with thanks DSR for technical and financial support.

ABSTRACT Within the literature, we have witnessed in the healthcare sector, the growing demand for and adoption of software development in the cloud environment to cope with and fulfill current and future demands in healthcare services. In this paper, we propose a flexible, secure, cost effective, and privacy-preserved cloud-based framework for the healthcare environment. We propose a secure and efficient framework for the government EHR system, in which fine-grained access control can be afforded based on multi-authority ciphertext attribute-based encryption (CP-ABE), together with a hierarchical structure, to enforce access control policies. The proposed framework will allow decision makers in the Kingdom of Saudi Arabia to develop the healthcare sector and to benefit from the existing e-government cloud computing platform "Yasser," which is responsible for delivering shared services through a highly efficient, reliable, and safe environment. This framework aims to provide health services and facilities from the government to citizens (G2C). Furthermore, multifactor applicant authentication has been identified and proofed in cooperation with two trusted authorities. Security analysis and comparisons with the related frameworks have been conducted.

INDEX TERMS Cloud Computing, Electronic Health Record, Security, Attribute-based Encryption, Ciphertext policy, Identity Proofing, Authentication, Authorization

I. INTRODUCTION

A common phenomenon in healthcare in most Arab countries is the lack of optimal utilization of human and material resources available to provide integrated healthcare to prevent diseases and treat diseases after they occur. Statistics indicate that Arab countries suffer from high rates of health problems, such as diabetes, liver disease, and parasitic diseases, such as histosomiasis and malaria. These health problems could be prevented before they occur or their complications prevented by early detection. This is due to a combination of factors: planning, operational, and technical. If we were able to overcome them, this would lead to significant progress in the level of health care. In addition, there is a weakness and lack of available hospital information systems, which is some of the most advanced software that directly serves all technical and administrative healthcare activities, ensuring that the medical institution has full control over all its activities and resources. The successes of these advanced systems do not depend on the exact selection of equipment and software for storage. Rather, their success depends on their suitability for different users—from healthcare providers, such as doctors, nurses, technicians, and even administrators—where the vision and priorities of each of these categories differ, and their information needs vary, as do the benefits of each of these systems.

The traditional health system (paper) has been replaced by an electronic health information system because the traditional system has been found to be ineffective due to a number of issues, including low storage capacity, high operating and maintenance costs, and system integration [1]. The computerized health system was then replaced by cloud computing because it relies on a more efficient infrastructure, as well as the many benefits of cloud computing in IT, such as cost, scalability, flexibility, and other features [2]. The use of cloud computing in electronic health records reduces costs in the provision of health services, maintenance costs, networks, licensing fees, and infrastructure in general, and this will therefore encourage developers to adopt the cloud in healthcare [2], [3].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2906131, IEEE Access

The rapid shift to the cloud and its use in healthcare systems has raised concerns about crucial issues of privacy and information security [4], [5]. The adoption of the cloud in IT increases the focus and concern of healthcare providers on clinical and patient-related services and reduces attention on infrastructure management [6]. The sharing of personal and health information across the Internet and various servers outside the safe environment of the healthcare institution has led to a number of problems related to privacy, security, access, and compliance issues [7], [8], [9], [10].

In the literature, there are no existing powerful frameworks that clearly address all viable schemes and interrelationships between cloud computing and healthcare technology [11], [12]. Improving the framework for healthcare in cloud computing has been studied by several researchers [13], [14], [15]. Further developments and solutions in these challenges will increase the adoption of cloud healthcare and encourage healthcare providers to move forward with cloud-based services [16].

Our contributions can be summarized as follows:

- Provides a flexible, secure, cost-effective, and privacy-preserved G-cloud-based framework for government healthcare services by:
  - Applying, using, and modifying the most recent encryption and decryption mechanisms suited for cloud-based EHR systems. The proposed scheme does not use the standard encryption system, which is not suited to the cloud environment.
  - Achieving scalability of computing resources that can be expanded and controlled according to the required health services. The EHR is able to support massive data exchanges.
  - Providing an effective solution for decision makers in the government health sector to adopt cloud-
    - based healthcare systems, especially in developing countries.
    - Providing a better authentication multifactor applicant authentication in cooperation with two trusted authorities.
    - Different domains of attributes are managed by different attribute authorities, which operate independently from each other and controlled by the central trusted authority.
- Security analysis has been conducted according to major security requirements in cloud environments.

This paper is organized as follows. Section II presents necessary background information and related works. The proposed cloud-based framework is provided in Section III. In Section IV, we provide both a security and comparison analysis. Finally, we present the conclusion and future work in Section V.

II. BACKGROUND

This section review the needed background for any proposed design based on CP-ABE for a cloud based EHR systems.

A. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptical curve cryptography (ECC) is a type of Public-Key cryptosystem based on of elliptic curve theory. ECC security relies on elliptic curve logarithm problem. Elliptic curves groups for cryptography are examined with the underlying fields of F_p (where p>3 is a prime) and F_2^m (a binary representation with 2^m elements) [26]. ECC can be used in conjunction with most public key encryption methods, such as RSA, El Gamal, and Diffie-Hellman. ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC helps to establish equivalent security with lower processing power, it is becoming widely used on compact platforms such as mobile applications and smart cards.

Definition 1 (Elliptic Curves): Let F_P is a finite field with $p > 3$ is a prime. The elliptic curve $y^2=x^3+ax+b$ over $\mathbb{Z}p$ is the set of solutions $(x,y) \in \mathbb{Z}p \times \mathbb{Z}p$ to the congruence:

- $y^2 \equiv x^3 + ax + b \pmod p$ where where $a \in \mathbb{Z}_p$, $b \in \mathbb{Z}_p$, are constants such that $4a^3 + 27b^2 \not\equiv 0 \pmod p$, together with a special point *O* called the *point at infinity*.
- If E is an elliptic curve over a field F, then the elliptic curve discrete logarithm to base $Q \in E(F)$ is the problem of finding an $n \in Z$ such that $P = nQ$ for a given $P \in E(F)$.

B. BILINEAR PAIRING

Bilinear mapping is used to construct a relationship between two or more groups with efficient pairing operation.

Definition 2 (Bilinear Pairing): let G and G_T be a cyclic group of order N; N is number of distinct prime orders P. Let g is a generator of G. Then, the bilinear mapping $e:G\times G \rightarrow G_T$ has the following properties:

- Bilinear: $\forall\ g,h \in G$, $a, b \in Z_N$, $e(g^a,h^b)=e(g,h)^{ab}$;
- Non-Degenerate: $\exists g \in G$, such that e(g,g) has order N in G_T;
- Computable: e is efficiently computable.

C. CLOUD-BASED EHR SCHEMES

In this section, we review the most important algorithms that contributed to the development of cloud-based healthcare.

In 2006, Goyal et al. [20] proposed a new idea in encryption called attribute-based encryption (ABE). In the ABE scheme, ciphertexts and users' secret keys are associated with a set of attributes. A user can decrypt a ciphertext if, and only if, there is a match between its secret key and the ciphertext. ABE has been applied and tested in many cloud-based applications.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2906131, IEEE Access

ABE is divided into two categories: ciphertext-policy ABE (CP-ABE) [21] and key-policy ABE (KP-ABE) [22]. In ciphertext-policy attribute-based encryption (CP-ABE), a user's private-key is associated with a ciphertext that specifies an access policy over user attributes. In key-policy attribute-based encryption (KP-ABE), the ciphertext is associated with attributes, and users' secret keys have access policies embedded. The PC-ABE technique has attracted the attention of many researchers in comparison with KP-ABE. CP-ABE is more flexible in the field of healthcare because the patient can specify the policy of access depending on the attributes of data users and can maintain the confidentiality of data from collusion in comparison with KP-ABE [24], [25].

III. THE PROPOSED GCLOUD-BASED FRAMEWORK

A cloud-based theoretical framework has been developed for the improvement of electronic health services in Saudi Arabia. The proposed framework will allow decision makers to develop the health sector and to benefit from the services provided by other sectors in the kingdom, such as the electronic services system called "Absher," which is used by the Ministry of the Interior to ensure the personal identity of the beneficiaries [27], [28], and the e-government cloud computing platform "Yasser," [17] which is responsible for delivering shared services through a highly efficient, reliable, and safe environment.

The proposed framework uses cloud computing to develop health services provided by the Ministry of Health to citizens. This framework aims to provide health services and facilities from the government to citizens (G2C) in the kingdom.

Figure 1 show the proposed cloud-based framework, which consists of four fundamental entities. These entities interact with one another directly and indirectly to perform their tasks in the cloud-based EHR framework.

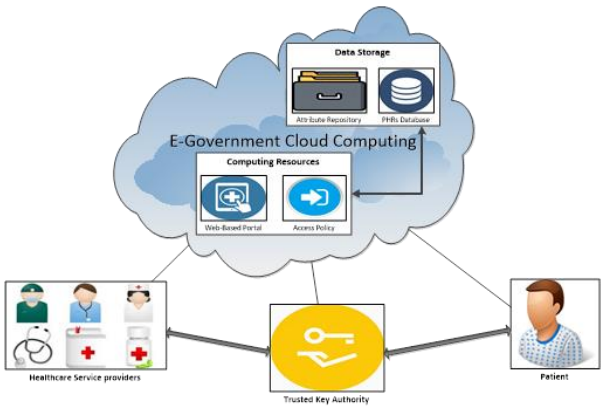

FIGURE 1. The Proposed G-Cloud-Based Framework

A. The System Entities

The system entities are described as follows:

I. The Patient

The patient is the main entity in our proposed framework. The patient has the following main tasks:

- A new patient must apply for an authentication request to the trusted authority to get his or her identification number (ID), and then he or she will be able to use the system services.
- Creates the patient history record (PHR) and stores it at the cloud server.
- Ensures the PHR is fully secured and protected by defining an (attribute-based) access policy that can be used for encrypting the data before it is distributed.

II. Healthcare Providers

Healthcare providers are individuals who provide healthcare services of all kinds in an organized manner to all members of a community. The healthcare providers could include the following members: health practitioners and specialists, physicians, nurses, pharmacists, surgeons, medical technicians, laboratory workers, and other employees. Each of these members must have access to some part of the patient records for specific purposes.

Each healthcare provider must complete the following tasks:

- Apply for an identification number (ID) from the trusted authority to be able to access specific parts of the patient's record.
- Apply a request for the secret key attached with the appropriate parameters.
- Be able to decrypt, modify, and encrypt the same document with the same key.

III. Trusted Authority

The trusted authority (TU), such as the Ministry of Health or any government sector, is responsible for the following functions:

- Authenticate all participants who interact with the system.
- Generate keys for healthcare providers and publish public parameters required by cryptographic operations.

IV. The E-Government Cloud-Based EHR

The e-government cloud-based EHR is the backbone of our proposed framework. In the Kingdom of Saudi Arabia, the e-government program (Yesser) has been established, and one of its initiatives and products is government cloud computing [26]. This government cloud computing provides beneficiaries with efficient, secure, and reliable infrastructure, platform, and software, all as services. Thus, the Ministry of Health can utilize this service and move

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2906131, IEEE Access

forward to adopt the EHR system in Saudi Arabia, satisfying the vision of 2030.

The proposed e-government cloud-based EHR consists of the following cloud services:

- The first service consists of two fundamental parts: data repository and computing resources. The first service is responsible for storing the encrypted EHRs that are accessible only by the authenticated healthcare providers through an access policy based on healthcare provider attributes.
- The second service is responsible for generating the access policies, providing efficient keys management, and performing other required computing processes.
- The third service is hosting the web-based portal. The developed web-based portal should be a secure online website that can be accessed by the stockholders from anywhere, with 24-hour a day access, through Internet connection, and can be accessed by any device.

*1. **Patient and Service Providers Identity Proofing***

When applicants access the portal for the first time, i.e., patients and service providers, they must be registered from the trusted health authority to be able to interact with the system. Through the web portal in the e-government cloud, the applicants can send, update, and receive health information from the cloud's central database with limited access, depending on the end user's privileges.

The following is the usual sequence completed by the applicant for proofing his or her identity, as shown in Figure 2:

1. The applicant requests a digital service from the Ministry of Health (trusted health authority) through an enrollment process.
2. The trusted health authority (THA) directs the applicant's request to the Ministry of Interior (trusted interior authority) for identity proofing to see if he or she can apply for the requested service.
3. The trusted interior authority (TIA) checks to see if the applicant's identity has not been confirmed for other e-government services, and then he or she is directed to go to a trusted national identity office (TNIO) for in-person proofing (multifactor identity proofing is checked under the highest identity assurance level (IAL3)). Otherwise, they will receive a confirmation and personal identification number (PIN).
4. The TNIO informs the TIO about the success and acceptance of the identity proofing.
5. The TIO sends the confirmation and PIN to both the THA and the applicant for future use.

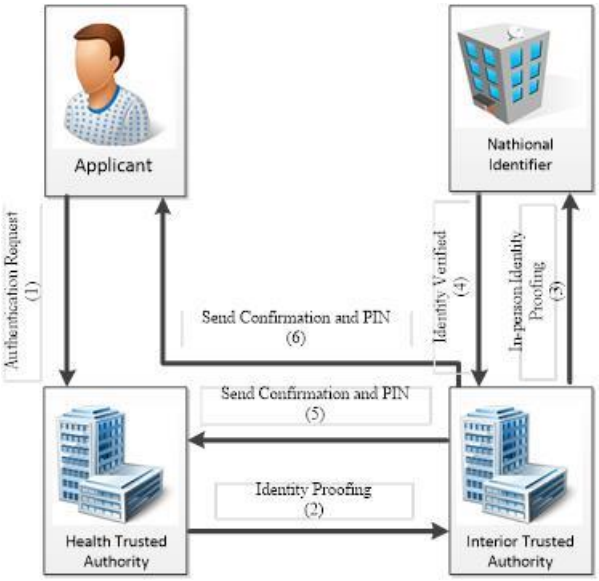

FIGURE 2. Identity Proofing Sequence

*2. **The Proposed Access Control***

Figure 3 demonstrates the basic access hierarchy for cloud-based government EHR. The hierarchy begins with the patient uploading his or her EHR to the cloud associated with the access policies for every service provider, according to their domains and types. The THA encrypts the patient's EHR, attached with the defined policies, and distributes different decryption keys to the corresponding service providers. When the healthcare service provider retrieves an encrypted EHR, the service provider can decrypt the file if, and only if, there is a match between the access structure of the encrypted file and the attributes associated with his or her decryption key.

I. Data Distribution

Due to the fact that the EHR database is very large and contains several users with different access privileges, it is not acceptable for the trusted central authority to encrypt the EHR separately for each user. It is more efficient to encrypt the EHR only once and distribute the encryption among many attribute authorities (AAs), according to their functionalities.

II. Access Structure of EHRs

The proposed access structure categorizes the users of the EHR into different domains based on their functionalities. There are many different users in the healthcare domain, such as primary care providers, nurses, specialists, pharmacists, medical doctors, and doctors of osteopathic medicine, who focus on family practice, internal medicine, or pediatrics. Each user holds some attributes defined in attribute set *S*. Only those users whose attributes satisfy the access structure defined in the ciphertext are able to decrypt the patient's record successfully.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2906131, IEEE Access

Figure 3 illustrates the proposed hierarchical multi-authority CP-ABE access structure framework. In our scheme, we adopt both the CP-ABE [21], [23] and the hierarchical framework [18], [19]. The access control framework is designed in a hierarchical way, which contains the government authority (GA) and multiple attribute authorities (AAs) from independent domains. The GA is the root of the access structure policy.

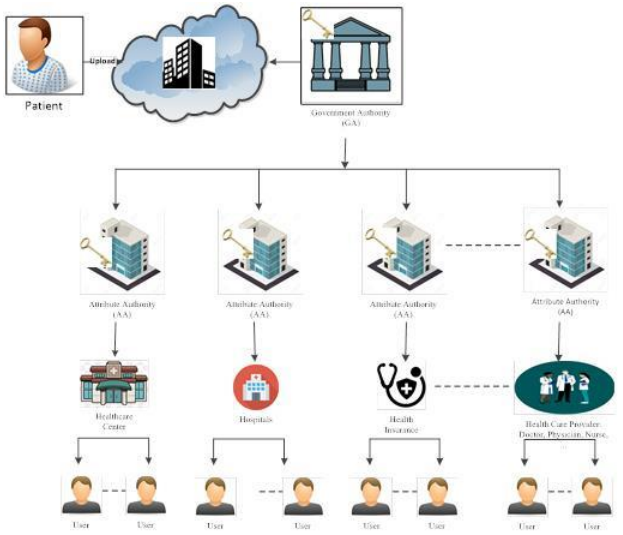

FIGURE 3. The Hierarchical Multi-Attribute Authority CP-ABE Access Structure Framework

The main advantages of using the proposed access structure is achieving lightweight key management when the number of users is large and mitigating and reducing the workload of the GA responsibility to encrypt the EHR, generate decryption keys, and distribute them to the authorized users.

The proposed scheme consists of the following five algorithms:

[1] Setup (K). The system setup algorithm takes a security parameter, K, as input. It outputs the public key (PK) and the master key (MK).

[2] CreateAttributeAuthority (PK, AA). This algorithm is executed by the GA (central authority) with the AA request as input. It outputs a functional identifier, A_{id}, for the AA with a set of attributes, S_{id}, and a secret authority key, SKA_{id}. The Ministry of Health categorizes the AAs according to their functionalities and then assigns the attributes for users of these functionalities.

[3] AttributeKeyGenerator (PK, SKA_{id}, S_{id}). This algorithm is executed by the A_{id} domain authority. It takes as input the PK and the domain authority's secret key, SKA_{id}, and the set of attributes, S_{id}. It outputs the attribute secret keys for the user SKU_j.

[4] Encrypt (PK, M, P, PKU). The encrypt algorithm takes as input the PK, a message (M), an access policy (P), and the set of public user keys (PKUs) corresponding to all the attributes in P. It outputs the ciphertext message CT.

[5] Decrypt (PK, CT, P, SKU_j, SKA). The decrypt algorithm takes as input the PK, a ciphertext message CT, the same access P used in encryption, the secret user key, SKU_j, and the set of secret attribute keys, SKA. The CT message will be decrypted if the attributes are sufficient to satisfy the P; otherwise the output will be null.

IV. ANALYSIS OF THE PROPOSED FRAMEWORK

A. *SECURITY ANALYSIS*

The proposed hierarchical multi-attribute authority CP-ABE framework in the EHR cloud environment satisfies the following security requirements:

❖ **Data privacy**

The proposed framework protects users' privacy. The EHR's privacy is satisfied when the user uploads the message encrypted with the access policy privileges settled by the user's own policy and is protected by authority attribute domains.

❖ **Fine-grained access control**

The proposed framework is designed in a way that after successful identity authentication, different applicants will have different access privileges according to the attribute key generator and the access policy used by the user. The proposed framework is based on CP-ABE [21] and uses a central authority with multiple authority attribute domains that impose different access privileges for different types of applicants in order to achieve fine-grained access control. This means that all the attributes must be matched with the user access policy structure to be able to access the required information.

❖ **Efficiency**

The computational overhead completed by the government or the central authority can be reduced greatly by assigning tasks to the attribute domain authorities. The proposed scheme enforces attribute domain authorities to generate and distribute keys to the entities. In general, applying multiple attribute domain authorities can efficiently distribute the computational overhead over multiple domain authorities because each authority will be not overloaded.

❖ **Scalability**

Migrating and adopting the patients' records from the in-house servers existing in any healthcare centers to the cloud has many advantages in comparison with traditional client-servers systems. Scalability is one advantage of such migration. The cloud-based EHR system requires less IT

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2906131, IEEE Access

resources, reducing operating costs, improving accessibility and collaboration, ensuring simpler implementation, delivering new services, and ensuring better scalability. Our proposed scheme improves the scalability of the system but limits the impressibility of the access policy because it only supports conjunctive policy across multiple AAs.

B. Comparison and Performance Analysis

Standard coding techniques that rely on the use of keys in encryption and decryption are not well suited for use in cloud-based applications, especially those related to healthcare systems.

- Symmetric-key encryption. These techniques are effective in many applications but are more complicated in healthcare applications as they require additional mechanisms to implement access control. This is especially true when healthcare providers all use a shared key to encrypt and decrypt, so if this shared key is hacked, the whole healthcare system will be compromised.
- Public-key encryption. These techniques are not considered to be practical because they require an expensive infrastructure for the public key to maintain the distribution and management of public keys.

In 2006, Goyal et al. [20] proposed a new idea in encryption called attribute-based encryption (ABE) which generalizes the functional role of identities and keys. In the ABE scheme, ciphertexts and users' secret keys are associated with a set of attributes. A user can decrypt a ciphertext if, and only if, there is a match between its secret key and the ciphertext. The problem with the ABE-based encryption scheme is that data encryption needs to use the public key for each licensed user and needs to use attributes to control the user's access to the system. So, ABE cryptographic credentials are issued by trusted attribute authority, which is in possession of a global master key for key generation.

In 2010, Wang et al. [30] proposed a Hierarchal attribute-based encryption (HABE) scheme by combining the hierarchical identity-based encryption system and the ciphertext-policy attribute-based encryption (CP-ABE) system. , and then making a performance-expressivity tradeoff, finally applying proxy re-encryption and lazy re-encryption to their scheme.

In 2007, Bethencourt et al. [21] Ciphertext-policy attribute-based encryption (CP-ABE), as one of the most promising encryption systems in this field, allows the encryption of data by specifying an access control policy over attributes, so that only users with a set of attributes satisfying this policy can decrypt the corresponding data.

In 2013, Li et al. [22] proposed an expressive decentralizing KP-ABE scheme. The ciphertext size does not rely on the number of attribute used in ciphertext. User's keys are attached with access structures and ciphertext is associated with attributes. A user is able to decrypt, if ciphertext's attributes is the authorized set of the access structure.

In 2013, Li et al. [29] enhanced a Multi-authority Attribute base encryption (MA-ABE) scheme to handle efficient and on-demand user revocation, and prove its security. The proposed MA-ABE scheme utilized ABE to encrypt and access not only the patient data but also various users from public domain with different professional roles, qualifications and affiliations.

In 2012, Alshehri et al. [25] proposed a cloud-based EHR system, which consists of the cloud-based data storage and computing resources, healthcare providers, and attribute authority (AA). In this scheme, one single AA is responsible for key management, including generation, distribution, and revocation in the EHR system. The proposed scheme considered a CP-ABE scheme and organized EHR to the labeled hierarchical data structure to provide flexibility, scalability, and fine-grained access control.

Comparing various security requirements of the proposed framework with existing frameworks is shown in table 1.

Our proposed framework is based on CP-ABE which is more secure and more efficient in comparison with other existing frameworks. It uses multiple authority attribute domains that impose different access privileges for different types of applicants in order to achieve fine-grained access control. This means that all the attributes must be matched with the user access policy structure to be able to access the required information. It is uses multi-factor authentication and controlled by the government trusted authority. The proposed scheme is suited for G-based cloud EHR systems and gets advantages from the facilities and the infrastructure provided by the government. We believe that our framework contribute in using a modified version of the PC-ABE scheme with multi-attribute and multi-factor proofing authentication.

V. CONCLUSION AND FUTURE WORKS

In this paper, we proposed a secure cloud-based EHR framework that guarantees the security and privacy of medical data stored in the cloud, relying on hierarchical multi-authority CP-ABE to enforce access control policies. The proposed framework provides a high level of integration, interoperability, and sharing of EHRs among healthcare providers, patients, and practitioners. In the framework, the attribute domain authority manages a different attribute domain and operates independently. In addition, no

computational overhead is completed by the government authority, and multi-factor applicant authentication have been identified and proofed.

The proposed scheme can be adopted by any government that has a cloud computing infrastructure and provides treatment services to the majority of citizen patients. Future work includes implementing and evaluating the proposed scheme in a real-world environment.

TABLE 1

Comparing the proposed framework with the existing schemes

Scheme	ABE [20]	HABE [30]	MA-ABE [29]	EHR PC-ABE [25]	PC-ABE [21]	KP-ABE [22]	Symmetric/ public key	Proposed Framework
Multiple Authentication	No	No	No	No	No	No	No	Yes
Cloud Based	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Fine-grained access control	No	No	No	Yes	Yes	Yes	No	Yes
Data privacy	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Efficiency	Average	Average	Average	High	High	Average	Low	High
Scalability	No	No	No	Yes	Yes	No	No	Yes
Data Confidentiality	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
collusion resistant	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Multi/Single AA	Single	Single	Multi	Single	Single	Single	Single	Multi

ACKNOWLEDGMENT

This Project was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, under grant no. G-145-612-39. The authors, therefore, acknowledge with thanks DSR for technical and financial support.

REFERENCES

[1] Masrom, Maslin, and Ailar Rahimli. "A Review of Cloud Computing Technology Solution for Healthcare System." *Research Journal of Applied Sciences, Engineering and Technology* 8, no. 20 (2014): 2150–2155.

[2] HUCÍKOVÁ, Anežka, and Ankica Babic. "Cloud Computing in Healthcare: A Space of Opportunities and Challenges." *Transforming Healthcare with the Internet of Things* (2016): 122.

[3] Yang, Haibo, and Mary Tate. "A descriptive literature review and classification of cloud computing research." *CAIS* 31 (2012): 2.

[4] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." *Future Generation computer systems* 28, no. 3 (2012): 583–592.

[5] Nigam, Vaibhav Kamal, and Shubham Bhatia. "Impact of Cloud Computing on Health Care." (2016).

[6] "How to Improve Healthcare with Cloud Computing", *By Hitachi Data Systems*, white paper, (2012).

[7] Mehraeen, Esmaeil, Marjan Ghazisaeedi, Jebraeil Farzi, and Saghar Mirshekari. "Security Challenges in Healthcare Cloud Computing: A Systematic Review." *Global Journal of Health Science* 9, no. 3 (2016): 157.

[8] Sun, Dawei, Guiran Chang, Lina Sun, and Xingwei Wang. "Surveying and analyzing security, privacy and trust issues in cloud computing environments." *Procedia Engineering* 15 (2011): 2852–2856.

[9] Khan, Nabeel, and Adil Al-Yasiri. "Identifying cloud security threats to strengthen cloud computing adoption framework." *Procedia Computer Science* 94 (2016): 485–490.

[10] Hamlen, Kevin, Murat Kantarcioglu, Latifur Khan, and Bhavani Thuraisingham. "Security issues for cloud computing." *Optimizing Information Security and Advancing Privacy Assurance: New Technologies: New Technologies* 150 (2012).

[11] Omachonu, Vincent K., and Norman G. Einspruch. "Innovation in healthcare delivery systems: a conceptual framework." *The Innovation Journal: The Public Sector Innovation Journal* 15, no. 1 (2010): 1–20.

[12] Reddy, B. Eswara, TV Suresh Kumar, and Gandikota Ramu. "An efficient cloud framework for health care monitoring system." In *Cloud and Services Computing (ISCOS), 2012 International Symposium on*, pp. 113-117. IEEE, 2012.

[13] Parekh, Maulik, and B. Saleena. "Designing a cloud based framework for healthcare system and applying clustering techniques for region wise diagnosis." *Procedia Computer Science* 50 (2015): 537–542.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2906131, IEEE Access

[14] Botta, Alessio, Walter De Donato, Valerio Persico, and Antonio Pescapé. "Integration of cloud computing and internet of things: a survey." *Future Generation Computer Systems* 56 (2016): 684–700.

[15] Stergiou, Christos, Kostas E. Psannis, Byung-Gyu Kim, and Brij Gupta. "Secure integration of IoT and cloud computing." *Future Generation Computer Systems* 78,(2018):964–975.

[16] Zhiwei Yu, Chaokun Wang, Clark Thomborson, Jianmin Wang, Shiguo Lian and Athanasios V. Vasilakos, A novel watermarking method for software protection in the cloud, SOFTWARE – PRACTICE AND EXPERIENCE, **42**:409–430, 2012.

[17] https://www.yesser.gov.sa/en/Pages/default.aspx

[18] Huang, Jie, Mohamed Sharaf, and Chin-Tser Huang. "A hierarchical framework for secure and scalable ehr sharing and access control in multi-cloud." In *Parallel Processing Workshops (ICPPW), 2012 41st International Conference on*, pp. 279–287. IEEE, 2012.

[19] Huang, Qinlong, Yixian Yang, and Mansuo Shen. "Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing." *Future Generation Computer Systems*72 (2017): 239–249.

[20] Goyal, Vipul, Omkant Pandey, Amit Sahai, and Brent Waters. "Attribute-based encryption for fine-grained access control of encrypted data." In *Proceedings of the 13th ACM conference on Computer and communications security*, pp. 89–98. Acm, 2006.

[21] Bethencourt, John, Amit Sahai, and Brent Waters. "Ciphertext-policy attribute-based encryption." In *Security and Privacy, 2007. SP'07. IEEE Symposium on*, pp. 321–334. IEEE, 2007.

[22] Li, Qinyi, Hu Xiong, Fengli Zhang, and Shengke Zeng. "An expressive decentralizing kp-abe scheme with constant-size ciphertext." *IJ Network Security* 15, no. 3 (2013): 161–170.

[23] Li, Qi, Jianfeng Ma, Rui Li, Ximeng Liu, Jinbo Xiong, and Danwei Chen. "Secure, efficient and revocable multi-authority access control system in cloud storage." *Computers & Security* 59 (2016): 45–59.

[24] Sekhar, B. Raja, B. Sunil Kumar, L. Swathi Reddy, and V. Poorna Chandar. "CP-ABE based encryption for secured cloud storage access." *International Journal of Scientific & Engineering Research* 3, no. 9 (2012): 1–5.

[25] Alshehri, Suhair, Stanisław Radziszowski, and Rajendra K. Raj. "Designing a secure cloud-based ehr system using ciphertext-policy attribute-based encryption." In *Proceedings of the Data Management in the Cloud Workshop, Washington, DC, USA*. 2012.

[26] Hankerson, Darrel, and Alfred Menezes. *Elliptic curve cryptography*. Springer US, 2011.

[27] Boneh, Dan, and Matt Franklin. "Identity-based encryption from the Weil pairing." In *Annual international cryptology conference*, pp. 213-229. Springer, Berlin, Heidelberg, 2001.

[28] Sahai, Amit, and Brent Waters. "Fuzzy identity-based encryption." In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 457-473. Springer, Berlin, Heidelberg, 2005.

[29] Li, Ming, et al. "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption." *IEEE transactions on parallel and distributed systems* 24.1 (2013): 131-143.

[30] Wang, Guojun, Qin Liu, and Jie Wu. "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services." In *Proceedings of the 17th ACM conference on Computer and communications security*, pp. 735-737. ACM, 2010.

Sanaa Sharaf received the BSc. With first honor degree in Computer Science from King Abdulaziz University, Jeddah, Saudi Arabia, and MSc with Distinction from University of Bradford, UK in Information Security in 2006. Sanaa finished her Ph.D. in Grid Computing from the University of Leeds, UK in 2012. In 1998, she joined the Computer Science Department, King Abdulaziz University, as a Teacher Assistant. She is currently an Assistant Professor in the Computer Science Department, Faculty of Computing and Information Technology, KAU. Her main areas of research interest are Information and System Security, Grid/Cloud Computing and High-Performance Computing. Since 2013 she started some administrative assignments includes: Supervisor of Information System department - Sulaymniah branch, FCIT vice-dean in both Faisliyah branch and University of Jeddah and now she is the High-Performance Computing Center deputy director for Academic Affairs, King Abdulaziz University, Jeddah, Saudi Arabia.

Nidal Shilbayeh received the BSc degree in computer science from Yarmouk University, Irbid, Jordan in 1988, the MS degree in computer science from Montclair State University, New Jersey, USA in 1992, and the PhD in computer science from Rajasthan University, Rajasthan, India in 1997. He is a Professor at the University of Tabuk. He was the Vice Dean at university of Tabuk, Saudi Arabia; He was the Vice Dean of Graduate Studies and Scientific Research at Middle East University, Amman, Jordan. He supervised many graduate students for the MS and PhD degrees. His research interests include Security (Biometrics, Identification, Privacy, Authentication, and Cryptography), Information Security (e-payment, e-voting, and e-government), Face Recognition, Digit Recognition, Watermarking, Embedding, Nose System, Neural Network, Image Processing, and Pattern Recognition.