**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The traditional health system (paper) has been replaced by an electronic health information system because the traditional system has been found to be ineffective due to a number of issues, including low storage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].

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 privacypreserved G-cloud-based framework for government♣ healthcare services by: o 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. o 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. o Providing an effective solution for decision makers in the government health sector to adopt cloud- based healthcare systems, especially inϖ developing countries. Providing a better authentication multifactorϖ applicant authentication in cooperation with two trusted authorities. Different domains of attributes are managed byϖ 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.