BIOGRAPHICAL SKETCH

Sherif Abdelfattah is currently a Graduate Research Assistant in the Department of Electrical and Computer Engineering, Tennessee Tech. University, USA since August 2019 and pursuing his Ph.D. degree in the same department. He works under the supervision of Dr. Mohamed Mahmoud. He received his BS and MS in Electronics and Communications Engineering from Arab Academy for Science, Technology and Maritime Transport (AASTMT), Alexandria, Egypt in 2012 and 2016, respectively. His research interests include several topics in the area of security and privacy in smart healthcare systems, privacy-preserving machine learning, cryptography and network security, and cloud-based systems security. He has more than four years of academic and teaching experience in different topics. He is an active reviewer in Top IEEE journals/conferences.

EDUCATION

Doctor of Philosophy, Engineering, Tennessee Technological University, December 2022 (expected), Cookeville, Tennessee

Master of Science, Electronics and Communications Engineering, Arab Academy for Science, Technology and Maritime Transport, Alexandria, Egypt, 2016

Bachelor of Science, Electronics and Communications Engineering, Arab Academy for Science, Technology and Maritime Transport, Alexandria, Egypt, 2012

College of Engineering

TENNESSEE TECH

The Department of

Electrical and Computer Engineering

Announces the Dissertation Defense of

Sherif Abdelfattah

In Partial

Fulfillment of the Requirements

For the degree of

Doctor of Philosophy in Engineering

August 8, 2022

2:00 p.m.

Tennessee Tech University

Join Zoom Meeting

https://tntech.zoom.us/j/8978016564?pwd=U4qxot7-6zTq1rT6QgYMv3xZiEyx6l.1

FIELD OF STUDY

Security and Privacy Preservation

DISSERTATION TOPIC

Efficient and Privacy-Preserving Data Search and Medical Diagnosis for Cloud-Based E-Health Systems

EXAMINING COMMITTEE

Mohamed Mahmoud, Committee Chair
Associate Professor, Electrical and Computer Engineering

Allen MacKenzie
Chair & Professor, Electrical and Computer Engineering

Tarek Elfouly
Associate Professor, Electrical and Computer Engineering

Sheikh Ghafoor
Professor, Computer Science

Akond Rahman
Assistant Professor, Computer Science

AN ABSTRACT OF A DISSERTATION

Despite the benefits of the advanced health care systems, it is vulnerable to security and privacy attacks. **Firstly**, several schemes have been proposed to enable cloud servers to search encrypted medical data to preserve patients' privacy. However, the existing schemes use inefficient Attribute-Based Encryption (ABE) approaches for access control. Also, servers cannot learn whether a doctor can achieve the access policy of a document and this check is done by doctors, so unrelated documents are outsourced. Moreover, the existing schemes only support single data-owner setting where a doctor needs to share a key with each patient. To address these limitations, we develop an efficient ABE approach. Patients use it to encrypt the symmetric key (that encrypted a document) so that only authorized doctors can obtain the key and decrypt the document. Our analysis indicates that our scheme can preserve privacy, and our experimental results demonstrate the efficiency of our scheme compared to the existing schemes. Also, the number of keys in the system are significantly reduced. **Secondly**, the existing searchable encryption schemes are inefficient because they are designed for a single-data-owner setting. Moreover, they are not secure against different security attacks, and do not allow doctors to customize their search to avoid downloading irrelevant documents. In this dissertation, we develop an efficient search scheme over encrypted data for multi-data-owner setting. The cloud server obtains noisy similarity scores and doctors de-noise them to download the most relevant documents. Our scheme enables doctors to customize their search. Our formal proof and analysis indicate that our scheme can preserve privacy and is secure against different security attacks, and the results of extensive experiments demonstrate the efficiency of our scheme compared to the existing works. **Thirdly**, support vector machine (SVM) models are widely used for medical diagnosis due to their high accuracy. Few schemes have been proposed for privacy-preserving cloud-based medical diagnosis systems using SVM. Some of these works do not protect the model's intellectual property and other works do not hide the classification result from the server. Also, they suffer from high computation/communication overhead. Thus, an efficient and privacy-preserving cloud-based medical diagnostic scheme using multi-class SVM is proposed in this dissertation. Extensive analysis is conducted and the results demonstrate that the proposed scheme is secure and can preserve privacy, and the results of our experiments indicate that our scheme requires less communication/computation overhead compared to the existing schemes. **Lastly**, several schemes have been proposed for privacy preserving cloud-based medical diagnosis using decision tree ensemble models. However, these schemes are inefficient, and none of them can simultaneously protect the model's intellectual property and preserve the privacy of the patients' data and diagnosis results. Also, they do not provide inherent access control for the outsourced model. In this dissertation, we develop a lightweight and privacy-preserving cloud-based medical diagnosis scheme using ensemble models with high accuracy and acceptable overhead. Using our scheme, the model owner controls the authorized patients who can use the model. Also, the patient must make a micro-payment to pay for the diagnosis service. Our analysis indicates that our scheme can protect the model's intellectual property and preserve the privacy of the patients' medical data and the diagnosis results. Our experimental results demonstrate that our scheme is more efficient comparing to the existing schemes.