EPIC: Efficient Privacy-preserving Contact Tracing for Infection Detection

Thamer Altuwaiyan, Mohammad Hadian, and Xiaohui Liang
Department of Computer Science, University of Massachusetts, Boston
100 Morrissey Boulevard, Boston, Massachusetts, US 02125
Email: {thamerfa,mshadian,xiaohui}@cs.umb.edu

***Abstract*—The world has experienced many epidemic diseases in the past, SARS, H1N1, and Ebola are some examples of these diseases. When those diseases outbreak, they spread very quickly among people and it becomes a challenge to trace the source in order to control the disease. In this paper, we propose an efficient privacy-preserving contact tracing for infection detection (EPIC) which enables users to securely upload their data to the server and later in case of one user got infected other users can check if they have ever got in contact with the infected user in the past. The process is done privately and without disclosing any unnecessary information to the server. Our scheme uses a matching score to represent the result of the contact tracing, and uses a weight-based matching method to increase the accuracy of the score. In addition, we have developed an adaptive scanning method to optimize the power consumption of the wireless scanning process. Further, we evaluate our scheme in real experiment and show that the user's privacy is preserved, and the accuracy achieves 93% in detecting the contact tracing based on the matching score in an energy efficient way.**

I. Introduction

Outbreaks of infectious diseases such as SARS in 2002, H1N1 in 2010, Ebola in 2014, lead to health and economic disasters, as well as the global anxiety. These infectious diseases usually spread through human-to-human contact, including direct contact with bodily fluids or respiratory droplets of infected people, or with surfaces and materials contaminated with these fluids. When the outbreaks of these diseases occur, it is urgent to discover the human-to-human contact backward such that patients and people at a higher risk can be identified and then physically isolated from the public. Contact tracing is defined as finding out if a person has been physically in contact with another infected person in the past [1]. The process of contact tracing helps in diseases control, creating social networks, and building trust model among people [2], [3], [4]. For example, contact tracing methods have been introduced to control epidemic disease such as Ebola, H1N1, and SARS [5]. The contact tracing has been used to create a social network based on the frequency of the human contact. Moreover, contact tracing is used to build a trust relationship among people, which helps people to make decisions.

Contact tracing could be implemented with different technologies. First, using short-range wireless technology as WiFi and Bluetooth; with the number of these devices growing rapidly around us, each device is associated with a unique identifier which helps the process of contact tracing to match between users. Second, adapting a GPS technology which could be an effective solution to perform contact tracing. The area covered by GPS service is much bigger compared to the short-range wireless technology, and the cost of a GPS receiver is much affordable [6], [7]. Third, using data from social networks is also an approach to perform contact tracing [8], [9]. Events or specific location could indicate important information about people, who might they met or got in contact with, or even places they have been.

However, most of these contact tracing approaches face some challenges such as accuracy, privacy, and energy consumption efficiency. First, accuracy is difficult to achieve because of some technique limitations and various application needs. Most of disease infections happen indoor; however, the data collected using GPS service is lacking of indoor coverage which leads to a data loss and inaccurate information about users. Second, sharing information about the user's contact history could lead to a huge privacy issue for any user. Therefore, applying strict rules on what information can be shared and protect them is very important in the contact tracing process. Third, the cost of obtaining user's information plays a significant role in designing the contact tracing process. Scanning for nearby devices is an expensive task to perform on the user's devices and repeatedly executing this task could lead to a power consumption problem.

In this paper, we propose an efficient privacy-preserving contact tracing for infection detection (EPIC) which uses short-range wireless technologies to perform contact tracing to provide fined-grained information about human-to-human interaction information. In particular, EPIC keeps privacy of the user as a priority by applying matching techniques over encrypted content, and enhances the accuracy by using a weight-based matrix that includes data from a large number of short-range wireless devices. Our scheme uses an energy-efficient method to collect data, we use data from the accelerometer to develop the adaptive wireless network scanning strategy, which reduces the power consumption on the user's device. Our contributions can be summarized as follows:

- We propose an effective fine-grained human-to-human contact tracing scheme (EPIC) with hybrid wireless and localization technology. The EPIC scheme identifies if two users have been physically in contact with each other in the past.
- We further show that our scheme can achieve the privacy, accuracy, and the energy efficiency required to perform the contact tracing process. The privacy module protects the user's recorded contact data from unnecessary disclo-

sure, and the weight-based matrix enhances the accuracy of the result. In addition, the proposed contact tracing scheme employs the adaptive wireless scanning method for energy efficiency.

- We evaluate the performance of EPIC in real world experiments. We show that the accuracy of our scheme can reach 93% on performing contact tracing. We conduct the experiments in two different environments and we have designed the experiments for covering possible types of human contacts.

II. Related work

The area of using technology to perform contact tracing has been widely studied [10], [11], [12]. Al Qathrady et al. [13] introduced a systematic infection detection framework utilizing mobile communication technologies including mobile networking and encounter statistics during infection breakouts. They used an extensive WLAN campus traces of six buildings and over 34K users to perform the experiment. However, the wireless signal strength has not been considered in this study which could indicates there is a margin of around 150 meters on the encounter area. Zhang et al. [14] proposed an integrating wireless body area networks (WBANs) for body vital signs collection with mobile phones for social interaction sensing to help in epidemic control and source tracing. Unlike EPIC, this study requires users to mount sensors on their bodies which make the system harder and costly to implement. Sareen et al. [5] proposed a novel architecture based on Radio Frequency Identification Device (RFID), wearable sensor technology, and cloud computing infrastructure. The aim of their work is to prevent the spreading of the Ebola infection at the early stage of the outbreak. However, they haven't proposed enough information about the privacy issues that could be involved in their scheme, where in EPIC, we consider user's data privacy as a main goal and we proposed a privacy module that help to protect the user's information.

In addition, there were many works on how to collect and store a user's data in a privacy-preserving way. Zhang et al. [15] proposed protocols based on proximity-based mobile social networking (PMSN) to enable two users to perform profile matching without disclosing any information about their profiles. These protocols allow finer differentiation between PMSN users and can support a wide range of matching metrics at different privacy levels. Li et al. [16] introduced a privacy-preserving profile matching schemes for proximity-based mobile social networks (FindU). The user can find from a group of users the one whose profile best matches with his/her; sharing only necessary and minimal information about the private attributes of the participating users is exchanged. They proposed a novel protocol that realize each of the user privacy levels, which can also be personalized by the users. The difference between our work and previous works is that we focus on protecting data that could indicate the user's daily activities such as events and human contacts. However, previous works focus on the privacy of a user's profile information which the updates on these information is less frequent.

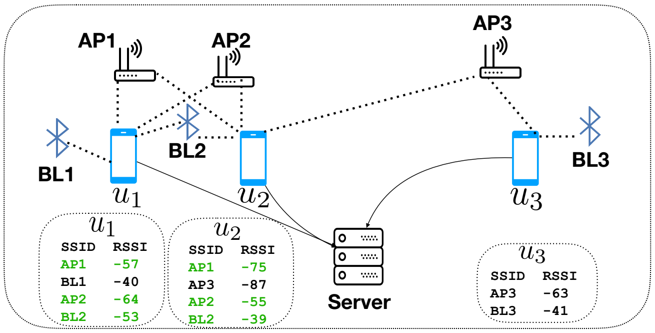


Fig. 1: System entities

III. System model

In this section, we will introduce the system entities and the design goals.

A. System entities

As shown in Fig. 1, our system model includes smartphones, wireless short-range devices such as Access Points and Bluetooth devices, and a server.

• ***Smartphones*** u_n: A study shows that people stay within arm-reach form their smartphones 48% of the time, and 82% of the time within 5 meters from their smartphones [17]. These high numbers of usage make smartphones a great tool to perform contact tracing. We are using smartphones to collect required data from each user by performing adaptive wireless scanning from time to time. As shown in Fig. 1, u_1's smartphone collects necessary raw data about nearby short-range wireless signals WiFi and Bluetooth and then encrypts these data before uploading them to the server. Specifically, the smartphone collects the following data in each network scan, a) wireless device unique identifier BSSID b) wireless Received Signal Strength Indication (RSSI) c) wireless signal type (WiFi, Bluetooth). Smartphone then uploads the encrypted data along with the timestamp for each network scan to the server.

• ***Wireless Signals*** $WiFi, BL$: Short-range wireless devices are becoming very popular in crowded areas as IoT emerges. The connectivity of those devices is better in an indoor environments compared to the GPS service [18], and they usually broadcast their names SSID and unique identifier BSSID to any device nearby, which enable the user's smartphone in our case to collect the required data. The average coverage range of the WiFi is around 80 meters outdoor and 50 meters indoor, that means, the longest distance between two different users connecting to the same WiFi is around 160 meters or 100 meters in the case of indoor coverage. This distance between users is not very helpful for our case of contact tracing which require more narrowed down range between users. Thus, using data from multiple wireless devices and using weight-based matching score calculation is crucial in our scheme EPIC.

• ***Server*** S: In EPIC, we use the server for two main tasks. First, the server is responsible for storing all encrypted data received from users, those data are encrypted by the user and not disclosed to the server or any other users. Second, the server is performing the score matching calculation on the user's encrypted data. When the status of a user changed to "infected", the server will ask users to check their contact tracing matching score with the infected user. Users will send requests to find out their scores and the server then responds back with matching scores for different timestamps the regular user came in contact with the infected user. All these calculations happen without the server knowing any unnecessary information about the infected user or knowing any extra information about the user who requested the matching score.

B. Design goals

Our scheme has three design goals and they as follows:

Data Privacy. Our scheme deals with very sensitive information about users. They could include health information regarding the possibility of a user disease infection. In addition, it could disclose some of the users' behaviors and activities since it contains the user's daily contacts. Hence, protecting such information is important. All of the users' information are encrypted by the user's smartphone before uploading them to the server. Moreover, we introduce a privacy-preserving matching method which uses Homomorphic encryption to match common wireless devices between the infected user and the regular user. All operations happen without the need of the regular user to disclose other uncommon wireless information.

Accuracy. In order to increase the accuracy of the matching score, we need to collect as much information as possible about the user's surrounded wireless environment such as WiFi and Bluetooth. We design a weight-based matching score method, which uses different features such as the RSSI values, and the number of common wireless devices.

Power Efficiency. Since our scheme uses smartphones to collect data, it's necessary to use the users' device resources wisely. Performing WiFi and Bluetooth scans frequently will exhaust the user's smartphone power quickly and will not be an efficient scheme to apply. Thus, we introduce an adaptive wireless scanning method, which employs the accelerometer with the wireless scanning process so the smartphone only performs scanning when it's needed. The accelerometer allows the wireless scanning methods to know if the users is moving which could indicate that a new wireless scan is needed.

IV. Proposed scheme

In this section, we propose our scheme EPIC, which allows the server to perform an efficient privacy-preserving contact tracing to identify users who have been in contact with an infected user in the past. Consider a user u_i identified as an infected user, her data will be disclosed only to the server to calculate the matching score with other users u_n. As shown in Fig. 2, the server is able to calculate and return matching scores for any user securely. We first introduce the contact tracing process, then the concept of adaptive scanning. We further propose the weight-based matching score method, and finally introduce the privacy-preserving method.

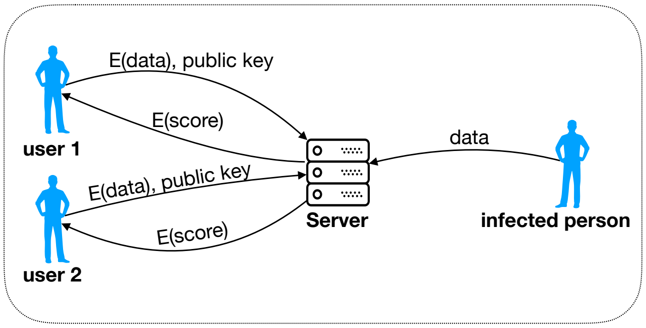


Fig. 2: Contact tracing

u_i	Infected user
u_n	Regular user
t_e	Timestamp for each wireless $scan$
m	The BSSID for each wireless device hashed with a hashing function
r_m	The RSSI value for the wireless device m
p_m	Type of each wireless signal WiFi, or Bluetooth

TABLE I: Notations

A. Contact tracing

To better explain the details of the scheme, we put all notations in Table I. Let us assume that the user u_i has been identified as an infected user, the user then must disclose all information to the server so the server can use them later to calculate matching scores. The data uploaded to the server by the infected user u_i is represented as follows, u_i=\{$scan_{i,1}$, $scan_{i,2}$, ..., $scan_{i,w}$\} where $scan$=\{t_e, [$m_{i,1}, r_{m_{i,1}}, p_{m_{i,1}}$],..., [$m_{i,j}, r_{m_{i,1}}, p_{m_{i,1}}$]\}.

All other regular users u_n will be notified to check their matching scores, which indicate if user u_n has been in contact with the infected user u_i in the past. Each regular user u_n sends a tracing contact matching score request which includes her public key. The server first matches between timestamps t_e of the regular user u_n=\{$scan_{n,1}$, $scan_{n,2}$, ..., $scan_{n,w}$\} with the infected user u_i, this matching is done in plain text since t_e is always disclosed to the server. It is important to note that we consider two timestamps as matched if the difference between them is 15 seconds or less. The server then has to match between common wireless devices using the privacy-preserving method (described in section IV. D). This process will assure that matching is done without the need to expose uncommon wireless devices unnecessarily. After that, the server receives RSSI values for common wireless devices and calculates the matching score (described in section IV. C). The server then returns an array of scores and timestamps where score is below our threshold.

B. Adaptive wireless scanning

As mentioned earlier, scanning for nearby wireless devices is an expensive task to perform on the user's device, thus we introduce an adaptive wireless scanning method which optimizes the power consumption. Since the data collected from the wireless scanning process indicates the nearby wireless devices, we then only need to scan again if the user has been moving for a while. For that reason, we integrate our scanning method with the user's smartphone accelerometer. Smartphones will only perform a new scan if the user moves continuously for more than ten seconds. Also, if the user is staying still for more than two minutes, we perform a new scan to refresh the collected information. In order to make the matching between an stationary user and a moving user possible, the smartphone will send the last scanning results if the stationary user did not move for more than ten seconds. This will assure that when the user stays still in a place such as sitting in an office, the phone is not constantly performing any new wireless scans. All scan results are encrypted the uploaded to the server periodically (once a day).

C. *Weight-based matching score*

In order to calculate the matching score between two users, they must have scanned at least three common wireless devices with the same timestamp in the past. In most cases, having data from one or two common wireless devices will not result in an accurate information about whether the two users are close enough from each other. Fig. 3 illustrates two cases where the first one (left) has only two wireless devices, and since we are using the difference in the RSSI values between the two user, it will be hard to decide if u_1 is close to u_2. However, in the second case (Right) in Fig. 3, it's clear that $AP3$ helps us on identifying that u_1 actually not close to u_2 since the difference in RSSI values between the two users significantly increased.

Our weight-based matching calculation depends on two main features, they are described as follows:

1) RSSI difference RD: The RSSI is a function that help to determine the distance between the transmission power and the receiver, it's calculated as follows:

$$RSSI(dBm) = 10nlog10d + A \tag{1}$$

where n is the signal decay exponent, d is the distance between transmitter and receiver, and A is the received signal strength at a distance of 1 meter from the transmitter. In our weight-based matching calculations, we use the difference in RSSI values between the two scans for the same wireless devices as one of the features. Suppose two users u_1 and u_2 scanned the same WiFi signal and their RSSI values are $-36dBm$ and $-38dBm$ continuously, the difference here in this case is $|2|$. However, if the RSSI values were $-76dBm$ and $-78dBm$, the difference is $|2|$ but in our proposed scheme we need to differentiate between these values since the difference between $-36dBm$ and $-38dBm$ tells us more accurate information compared to the difference between $-76dBm$ and $-78dBm$. For that reason, we decided to assign a larger weight on small RSSI values when calculating the matching score, which is described as follows:

$$RD = \sqrt[\alpha]{(median(|rssi_1|, |rssi_2|))(||rssi_1| - |rssi_2||)} \tag{2}$$

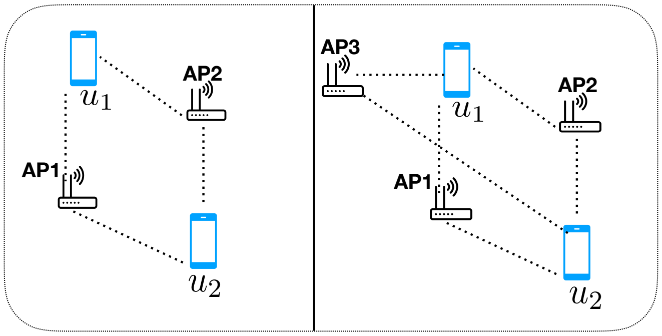


Fig. 3: Wireless scanning

After applying Equation (2), the RSSI difference RD from the previous example changed to 32.2 for the first scenario, and 56.5 for the second, in the case of $\alpha = 1.3$.

2) Number of wireless devices matched θ: As mentioned earlier, the minimum number of wireless devices we use to calculate the matching score is three devices, however, the more wireless devices detected the more accurate the result is. Thus, we use the number of wireless devices as a weight to calculate our final matching score as shown in equation 3.

3) Calculating the matching score MS: Our proposed scheme sends back to the user an array of matching scores MS where each score is equal or less than our predefined threshold. This array indicates the timestamps and the score for each timestamp, lower score shows that we are more confident that the regular user was in contact with the infected user.

$$MS_{te} = \frac{MAX_3(RD)}{\ln(\theta - 1)} \tag{3}$$

The above equation generates a single matching score for a specific timestamp t_e where RD is the RSSI difference and θ is the total number of common wireless devices. We focused only on the average of the top three largest values of RD because these are the values that indicate the greatest distance between the two users.

D. *Privacy*

EPIC aims to achieve a high level of privacy on the user's information so the server and the user will not be able to know unnecessary information. By following privacy steps described below, our scheme will achieve the privacy level needed, these steps are explained as follows:

- After a user u_i has been identified as an infected user, the server will receive a matching score request from a regular user u_n, this request includes the public key for the user u_n. The first step the server does is to match between scans based on timestamps in u_i and u_n. Those timestamps are stored in the server in plain text.
- The second step after matching scans is to identify if the two users have scanned similar wireless devices m. The server already has all information about the infected user u_i in plain text, however, the server has no information about the regular user, since her data are encrypted in the server. Our privacy method allows the regular user to reveal only the necessary information to the server, which

	$m_{i,2}$	$m_{i,3}$
$m_{n,1}$	$E((m_{n,1} - m_{i,2}) * d_{1,2})$	$E((m_{n,1} - m_{i,3}) * d_{1,3})$
$m_{n,2}$	$E((m_{n,2} - m_{i,2}) * d_{2,2})$	$E((m_{n,2} - m_{i,3}) * d_{2,3})$
$m_{n,4}$	$E((m_{n,4} - m_{i,2}) * d_{4,2})$	$E((m_{n,4} - m_{i,3}) * d_{4,3})$

TABLE II: Encrypted matrix

are in this case the matched (common) wireless devices. The server uses the user's public key received from u_n to encrypt each m_i where $m_i \in u_i$. The server then returns a matrix which has the encrypted subtraction result of all pairs of m_i and m_n using Homomorphic encryption [19] multiplied by a random value d added by the server to prevent u_n from knowing unnecessary information related to u_i. As shown in table II, a sample of the matrix where $\{m_{i,2}, m_{i,3}\} \in u_i$ and $\{m_{n,1}, m_{n,2}, m_{n,4}\} \in u_n$.

- After the user u_n receives the matrix, she decrypts all results and returns a binary array corresponded to the decryption result where 0 indicates that two wireless devices are matched and vice versa. The user u_n will also send RSSI values for matched wireless devices in plain text. By applying this privacy-preserving method, the user u_n disclosed to the server only the common wireless information with the infected user u_i, and kept other uncommon wireless device information secret. In the meantime, the server only disclosed the information about the common wireless devices to the regular user u_n, while all other uncommon wireless information are kept secret.

V. EVALUATION

In this section, we evaluate the performance of EPIC in real world experiments. We have built an Android application to run it on our testing smartphones (Samsung S3), we have also asked ten students to carry the smartphones while our application is running. We conducted all of our experiments in two different environments. First, we picked the science building in our school campus where it contains four floors, each floor equipped with at least ten access points and we have also placed ten Bluetooth devices in each floor in random spots within the users' path. Second, we conducted experiments in an apartment complex building next to our school, this building contains nine floors and more than 150 apartments. All data collected from the scanning process are stored locally in the smartphone's memory card, and manually uploaded to the server where we perform the contact tracing calculations later.

A. Data collection

As shown in Fig. 4 (a, b, c), we have designed three scenarios where two users come in contact with each other in different ways. First, in Fig. 4(a), two users start from two points far from each other such that they have no common wireless devices in the scan process. The two users then walk to a target spot which is in this case a restroom located in the same floor. They stay together in a range of about three meters for two minutes before they walk back to the original starting spot. The second scenario in Fig. 4(b) shows the two users start also from far away points; however, the target this time is to flip spots between users, they both take same path such that they cross each other in a middle point. Finally, in the third scenario the two users walk together within about three meters range for half of the path as shown in Fig. 4(c). Table III shows a real sample of our data collection file where two users have scanned similar wireless devices at the same time.

Timestamp	u_1 $rssi$	m	Type	u_2 $rssi$
1509240563.03	-64	D8:84:66:4C:D1:00	WiFi	-85
1509240563.03	-69	D8:84:66:4E:E4:F0	WiFi	-79
1509240563.03	-59	D8:84:66:4E:F0:04	BL	-91

TABLE III: Data collection sample

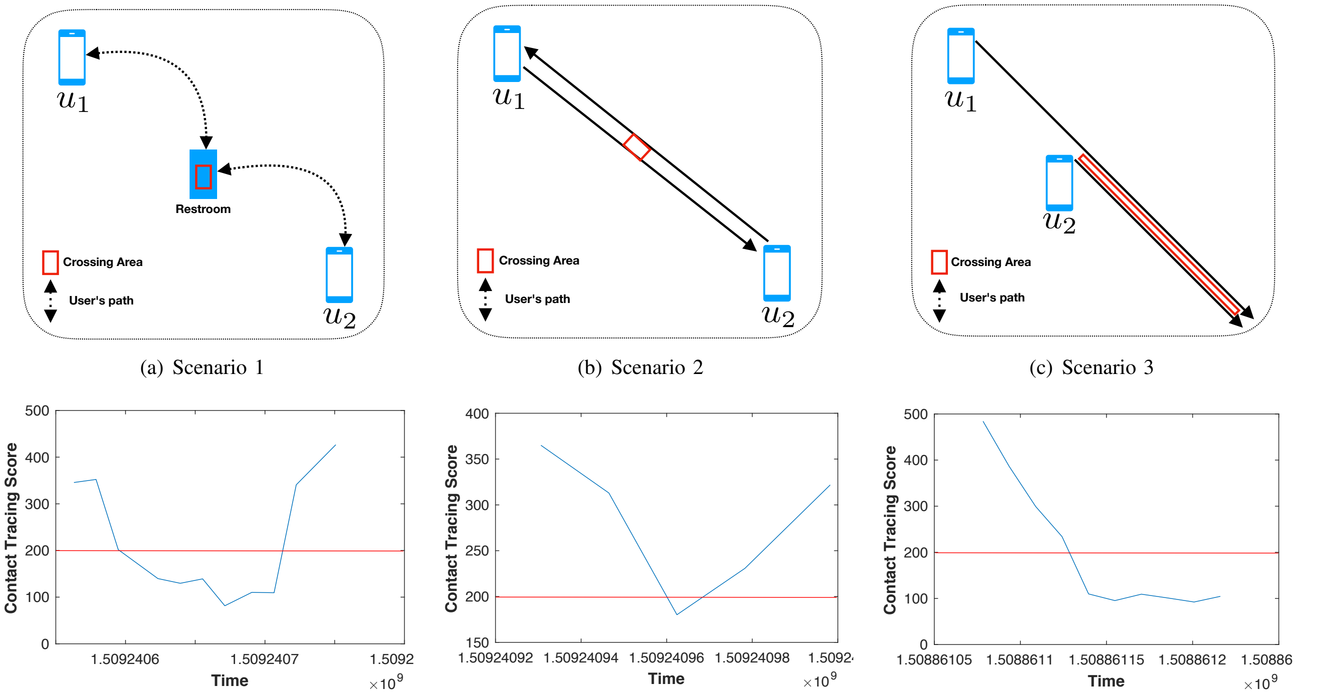
We divided the ten students into five pairs, each pair conducted 18 experiments; that is six experiments for each scenario. Those experiments have been conducted in the two environments, where all samples cover most of the real life scenarios such as users crossing each other on the Line of Sight (LOS) from the APs, or in a narrowed hallway, and not on LOS where APs located behind walls. We have collected total of 90 samples divided equally between the two environments. It is important to mention that for each experiment, we assigned one person to manually log the time where the two users physically meet each other within about three meters distance.

B. Accuracy evaluation

After data collection process finished, we uploaded all collected data to the server to calculate the contact tracing score for the three scenarios. To identify the right value of the matching score threshold, we have used half of the samples to conduct a threshold assessment. We chose 200 as the value of the threshold where α = 1.3, any score below or equal 200 considered as a positive human contact for a specific timestamp. Figure 4 (d, e, f) shows our tracing score results for representative data samples of the three scenarios; it is important to note that we only calculate score when the number of common wireless devices θ is equal or above 3. As shown in Fig. 4(d), the matching score falls under the threshold 200 for almost two minutes, that because the two users are met in the restroom and stayed with each other for two minutes before they walked back to their original spot. Moreover, in Fig. 4(e), it is clear that the score falls under 200 only once. This is consistent with scenario (2) where the two users only crossed each other for a very short period of time. Finally, the matching score in Fig. 4(f) falls under the threshold 200 in middle of the chart until the end, which represents exactly the design of scenario (3) where the two users met in a middle spot and walk with each other until the end. From our extensive experiments and analysis, our scheme was able to calculate the contact tracing score and correctly detect the contact with an accuracy 93%. This is calculated as the number of the timestamps where the contact/no-contact cases were correctly detected divided by the number of total timestamps.

VI. CONCLUSION

In this paper, we proposed an efficient privacy-preserving contact tracing for infection detection (EPIC) scheme which



(a) Scenario 1

(b) Scenario 2

(c) Scenario 3

(d) Scenario 1 - Result

(e) Scenario 2 - Result

(f) Scenario 3 - Result

Fig. 4: Experiments and Results

allows the server to perform a contact tracing process in a privacy-preserving way. EPIC uses a weight-based method to calculate the matching score using different features such as the RSSI values and the number of common wireless devices. An adaptive wireless scanning is employed to collect information from different short-range wireless devices such as WiFi and Bluetooth. Our experimented results show the EPIC is accurate, privacy-preserving, and energy efficient. In our future work, we will explore more features to be added as weight to improve the accuracy of our contact tracing matching score. We will also enhance our experiment by expanding it to different environments and involve more users.

Acknowledgements

This work is supported by University of Massachusetts Boston Healey Research Grant Program and Shaqra University in Saudi Arabia.

References

[1] W. H. Organization *et al.*, “Contact tracing during an outbreak of ebola virus disease,” 2014.

[2] J. Manweiler, R. Scudellari, and L. P. Cox, “Smile: encounter-based trust for mobile social services,” in *Proceedings of the 16th ACM conference on Computer and communications security*, 2009.

[3] X. Ni, J. Luo, B. Zhang, J. Teng, X. Bai, B. Liu, and D. Xuan, “A mobile phone-based physical-social location proof system for mobile social network service,” *Security and Communication Networks*, 2016.

[4] A. Mohaien, D. F. Kune, E. Y. Vasserman, M. Kim, and Y. Kim, “Secure encounter-based mobile social networks: Requirements, designs, and tradeoffs,” *IEEE Transactions on Dependable and Secure Computing*, 2013.

[5] S. Sareen, S. K. Sood, and S. K. Gupta, “Iot-based cloud framework to control ebola virus outbreak,” *Journal of Ambient Intelligence and Humanized Computing*, 2016.

[6] J. A. Sacks, E. Zehe, C. Redick, A. Bah, K. Cowger, M. Camara, A. Diallo, A. N. I. Gigo, R. S. Dhillon, and A. Liu, “Introduction of mobile health tools to support ebola surveillance and contact tracing in guinea,” *Global Health: Science and Practice*, 2015.

[7] J. Manweiler, R. Scudellari, Z. Cancio, and L. P. Cox, “We saw each other on the subway: secure, anonymous proximity-based missed connections,” in *Proceedings of the 10th workshop on Mobile Computing Systems and Applications*. ACM, 2009.

[8] K. Zhang, X. Liang, J. Ni, K. Yang, and X. Shen, “Exploiting social network to enhance human-to-human infection analysis without privacy leakage,” *IEEE Transactions on Dependable and Secure Computing*, 2016.

[9] D. Liben-Nowell and J. Kleinberg, “The link-prediction problem for social networks,” *journal of the Association for Information Science and Technology*, 2007.

[10] A. Prasad, X. Liang, and D. Kotz, “SPICE: Secure Proximity-based Infrastructure for Close Encounters,” in *Proceedings of the ACM Workshop on Mobile Crowdsensing Systems and Applications (CrowdSense)*. ACM, 2017.

[11] S. M. Firestone, R. M. Christley, M. P. Ward, and N. K. Dhand, “Adding the spatial dimension to the social network analysis of an epidemic: investigation of the 2007 outbreak of equine influenza in australia,” *Preventive veterinary medicine*.

[12] U. Kumar, G. Thakur, and A. Helmy, “Protect: proximity-based trust-advisor using encounters for mobile societies,” in *Proceedings of the 6th International Wireless Communications and Mobile Computing Conference*. ACM, 2010.

[13] M. Al Qathrady, A. Helmy, and K. Almuzaini, “Infection tracing in smart hospitals,” in *2016 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications.*

[14] Z. Zhang, H. Wang, X. Lin, H. Fang, and D. Xuan, “Effective epidemic control and source tracing through mobile social sensing over wbans,” in *IEEE INFOCOM, 2013 Proceedings IEEE*, 2013.

[15] R. Zhang, J. Zhang, Y. Zhang, J. Sun, and G. Yan, “Privacy-preserving profile matching for proximity-based mobile social networking,” *IEEE Journal on Selected Areas in Communications*, 2013.

[16] M. Li, S. Yu, N. Cao, and W. Lou, “Privacy-preserving distributed profile matching in proximity-based mobile social networks,” *IEEE Transactions on Wireless Communications*, 2013.

[17] A. K. Dey, K. Wac, D. Ferreira, K. Tassini, J.-H. Hong, and J. Ramos, “Getting closer: an empirical investigation of the proximity of user to their smart phones,” in *Proceedings of the 13th international conference on Ubiquitous computing*. ACM, 2011.

[18] P. A. Zandbergen, “Accuracy of iphone locations: A comparison of assisted gps, wifi and cellular positioning,” *Transactions in GIS*, 2009.

[19] M. Naehrig, K. Lauter, and V. Vaikuntanathan, “Can homomorphic encryption be practical?” in *Proceedings of the 3rd ACM workshop on Cloud computing security workshop*, 2011.