A NOVEL PRIVACY-PRESERVING SCHEME IN IOT-BASED SOCIAL DISTANCING TECHNOLOGIES

Arwa Alrawais[1], Fatemah Alharbi[2], Moteeb Almoteri[3],
Sara A Aljwair[4] and Sara SAljwair[5]

[1,4,5] College of Computer Engineering and Sciences,
Prince Sattam Bin Abdulaziz University, Alkharj, 16278, Saudi Arabia
[2]College of Computer Science and Engineering, Taibah University,
Yanbu 46522, Saudi Arabia
[3]College of Business Administration, King Saud University,
Riyadh, 11451, Saudi Arabia

ABSTRACT

The COVID-19 pandemic has swapped the world, causing enormous cases, which led to high mortality rates across the globe. Internet of Things (IoT) based social distancing techniques and many current and emerging technologies have contributed to the fight against the spread of pandemics and reduce the number of positive cases. These technologies generate massive data, which will pose a significant threat to data owners' privacy by revealing their lifestyle and personal information since that data is stored and managed by a third party like a cloud. This paper provides a new privacy-preserving scheme based on anonymization using an improved slicing technique and implying distributed fog computing. Our implementation shows that the proposed approach ensures data privacy against a third party intending to violate it for any purpose. Furthermore, our results illustrate our scheme's efficiency and effectiveness.

KEYWORDS

Anonymization, Fog computing, IoT, Privacy, Social distancing technologies.

1. INTRODUCTION

Last year, the world fell prey to the COVID-19 pandemic and made itself prone to the negative impact. The pandemic has devastated the world with a huge number of positive cases, where the total confirmed cases reported over 124 million, including more than two million deaths [1], during one year. One of the most effective techniques to constrain this danger is social distancing, which means reducing physical contact among people. Furthermore, studies have pointed out that social distancing techniques assist in reducing the pandemic, and even single-day negligence can reciprocate the graph. This light up the opportunity in existing technologies in maintaining the social distancing between individuals. The role of these technologies is effective as it facilitates and even maintains social distancing by measuring the distances between individuals and alerts them in case, they cross the regulated distance or if a nearby individual is infected. Mobile technologies, Bluetooth, IoT devices, and other emerging technologies are used in place of social distancing.

David C. Wyld et al. (Eds): MLDS, NECO, SEMIT, IBCOM, SPPR, SCAI, CSIA, ICCSEA - 2021
pp. 237-247, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.111820

In this scenario, social distancing technologies mainly depend on sharing and collecting data by IoT devices to perform their task accurately and correctly. For instance: • Sensors measure an individual's health status to detect symptoms of COVID-19. • Wearable devices track an individual's movements then alert him to keep the imposed distance. Consequently, this enormous data collected by IoT devices will be stored and analyzed through the cloud. By its nature, this personal data is not confidential (e.g., location, identity, and medical information) [2]. However, when data is stored and analyzed, this will create a serious challenge, which can significantly exploit and affect people's privacy. The researchers in [2] defined privacy as a right of an individual to control his data by figuring out who is entitled to access his data and how they use it. When this data is used in an undisclosed manner by the cloud, such as publishing it or selling it to parties, it is considered a privacy violation. In [3], they mentioned that the impact of privacy violation, especially in publishing Location-based data, could negatively affect people in several manners, such as in employment opportunities and insurance policies. The purpose of enabling (Location-based Services) LBS is to locate places and facilitate access. When using this service in an undisclosed manner (such as monitoring movements), a whole idea of an individual will form. Cloud may sell this information to other companies, and when you apply for a job, you might get rejected because of this disclosure data. The statistics in [4] stated that 54% of adults reject downloading tracking applications for social distancing, were rejection reason of 30% of them to preserve their privacy. In this paper, we propose a novel scheme to address users' concerns about storing their data in the cloud for social distancing purposes. Applying a new approach based on anonymization using a slicing-fog privacy-preserving technique on the collected data before transferring them to the cloud. We highlight our contributions as follows: We are introducing a novel scheme called slicing-fog privacy-preserving technique by improving the slicing technique used in anonymization to protect users' privacy in social distancing technology from the cloud itself. Taking advantage of the distributed fog computing architecture to implement the proposed scheme. Demonstrate the efficient performance of implementing the proposed scheme in terms of computational time. Demonstrate how efficiently the proposed scheme preserves privacy by using two metrics: entropy and estimation error. Logically demonstrates the ability of the proposed scheme to deter three privacy threats: the identity disclosure threat, the attribute disclosure threat, and the correlation analysis attack. The paper is organized as follows. Section 2 illustrates the recent related work. In Section 3, a description of the proposed system is provided. We follow it by explaining the proposed scheme methodology, discussing the implementation, and demonstrating the results in Section 4. We draw our conclusion in Section 5.

2. RELATED WORK

In this section, we mainly summarize the recent and significant privacy-preserving approaches in the research communities. In [3], the authors defined the security and privacy preserving of data collected by the social distancing technologies as a challenging problem. Several proposed mechanisms are presented to preserve the location, identity, and health information in other works. Authors in [5], [6] proposed a scheme in privacy-preserving of LBS by using lightweight cryptography. In another works [2], [7], the authors investigated the privacy-preserving approaches in IoT and discussed the pros and cons of each technique besides mentioning the future issues and open problems. In [8], the authors addressed the role of IoT technology in the COVID-19 pandemic setting aside its contributions to social distancing while clarifying their concerns in terms of security and privacy issues and mentioned that one of the biggest challenges facing the IoT technology is the data collected requires big storage centers. Similarly, researchers in [9] have proposed an approach that demonstrated the effectiveness of IoT in monitoring patients of COVID-19 remotely and studying their cases. In [10], the researchers conducted the first privacy study on 41 official contact tracing applications. They discovered the privacy and security concerns in some applications, where it is possible to access the application's fingerprint and track some users. As another study in [11] also analyzed 48 COVID-19 applications to assess their privacy elements, focusing on three criteria: data retention, right to opt-out, and compliance and polling many participants. In another work in [4], the authors described three scenarios that contact tracing applications and highlight the actors that threaten privacy and cause sensitive data to leak in these applications. These applications include application developers who may perform some malicious activities such as selling data to a third party and suggest several privacy guidelines, which could apply to any contact tracing application. The researchers in [12] proposed an application that measures distance and gives a real-time alert if social distancing violates. To preserve the user's privacy, the researchers suggested that it does not request any personal information at the time of registration, except for email and the account identification assigned to each user residing on the server side. The work in [13] presented a new initiative by designing an open-source application that combines two tasks based on alerting users if they breach the social distancing as well as tracking the contacts via Bluetooth Low Energy (BLE). The application warns the users if an infection appears, considering the security and privacy concerns by storing the timestamp and deleting the data after 28 days of collecting it. While researchers in [14] pointed out that Ultra-wideband (UWB) technology is capable of effectively collecting the location data and measuring the distance more accurately than BLE and Wi-Fi, with consuming significantly lower power. Relatively fewer efforts in social distancing techniques focus on privacy preservation and not considering all the privacy challenging issues. Even if they conceal the identity, the accumulated storage of data in the cloud poses a danger when analyzing this data, especially location tracking data. It may lead to disclosing the identity or lifestyle. In this paper, we attempt to fill this gap.

3. PROPOSED SYSTEM STRUCTURE

The proposed system structure consists of three layers: IoT layer, fog computing layer, and cloud computing layer, as Fig. 1. It begins with the IoT devices (representing the lowest layer). IoT devices are connected via the Internet to collect data such as location or measure a user's health. The collected information intends to provide services that benefit the end-user, such as alert the user in case of violating the imposed distance or in case there are infected people around him. Due to limited storage capacity in IoT devices, the data is stored and processed by the cloud (representing the top layer). The IoT layer and cloud layer connected through fog computing (representing the middle layer), which is distributed computing that brings storage and computing closer to end-users (the IoT layer). Fog computing aims to improve response time and performance by reducing the overload on the cloud, where it intermediates the layer between the IoT layer and cloud. Our proposed scheme could be placed in the fog computing layer for the purpose of protecting the privacy of end-users from the cloud. This is due to several reasons:

- Fog computing has features that address cloud limitations, as we mentioned earlier.
- It is less subject able to violations [15]; therefore, we can consider it as a secure environment.
- Unlike the cloud, it is not provided from an external source. The data is stored in a distributed manner, not centralized as in the cloud [16], which reduces the surface of privacy violation.
- Finally, the most significant incentive in fog computing ability is to apply policies on data before it is sent to the cloud [17].

4. PROPOSED PRIVACY PRESERVATION APPROACH

The building block of the proposed scheme is data generated by IoT devices, so it is imperative to understand its nature. Firstly, the data formed in a table of rows (records) and columns (attributes). A single record is a set of attributes that describe a single user. Secondly, in terms of privacy, these attributes are classified into three categories [18]:

- Identifiers (ID): they are unique attributes that identify the individual. For instance, name and national identity.
- Quasi-Identifiers (QI): they are attributes that identify an individual when combining two or more attributes. For instance, gender, age, and address.
- Sensitive Attribute (SA): these are the sensitive attributes of the individual, which should not be revealed. For instance, medical data, historical location, and current location.

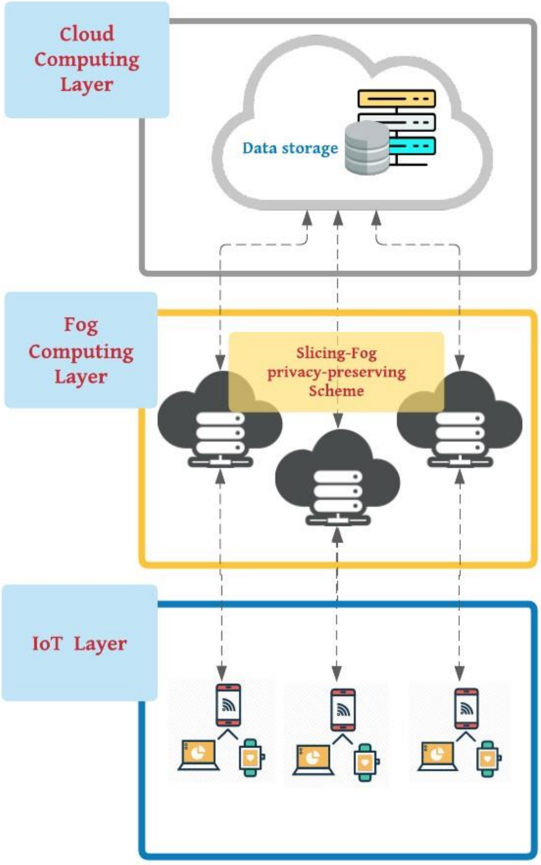

Figure 1. Proposed System Structure

According to [3], the general principle of privacy preserving is defined as the sensitive data available for public access, which must be kept private, such as data stored in the cloud. Where it may lose its privacy, if it is not well preserved or published by the cloud. To achieve this principle, there are many mechanisms to protect the privacy. Based on our observation and study in the field, we find that the slicing technique is an effective and efficient approach to maintaining user data collected for the social distancing purpose. The essential of the slicing technique is to remove the correlation between the attributes of a single user record, which is obtained in several steps.

To illustrate the details of the steps of the proposed privacy-preserving scheme, we assumed data resulting from social distancing processes then performed the steps of the proposed scheme on it by the example shown in Tab. 1.

Step 1: Apply Vertical Partition: the table is partitioned into columns and each column contains a set of attributes as shown in Tab. 2. This partition is according to the correlation of (QI) attributes where the correlation is intense between (QI) attributes in each column to have better utilization. As for the Sensitive Attribute (SA) must be in one column to remove their correlation with the other attributes. Before doing the vertical partition, we have added a primary step in our scheme. Wherein the fog layer will replace the identifier attribute with fog-ID.

Step 2: Apply Horizontal Partition: records are divided into buckets based on a certain duration as shown in Tab. 3, (where) and each bucket contains a set of records.

Step 3: Apply Permutation: last step and most important one in the slicing technique is the random permutation between the values of the columns in each bucket shown in Tab. 4. This step aims to break the correlation between these columns, especially the sensitive attribute columns, as we mentioned earlier in the first step.

The proposed scheme structure is shown in Fig. 2. In this paper, we rely on IoT-based social distancing techniques. We assumed some attributes of the data collected from IoT devices when implementing social distancing techniques. We considered location, health status, and time as sensitive attributes, and the rest are quasi-identifiers attributes. Essentially, the data is sent to fog for temporary storage to perform real-time social distancing operations. Then, the fog implements the proposed scheme on the collected data (i.e., collected by the end of the day) before sending it to the cloud for permanent storage. Considering that the data will return to its natural form when it retrieves from cloud to fog, as needed. Finally, we achieved the purpose of the proposed scheme so that the sliced data stored in the cloud does not reveal the identity of users to the cloud, as shown in Tab. 5. Additionally, if the cloud event is exposed to an attack or the cloud is intended to publish the database.

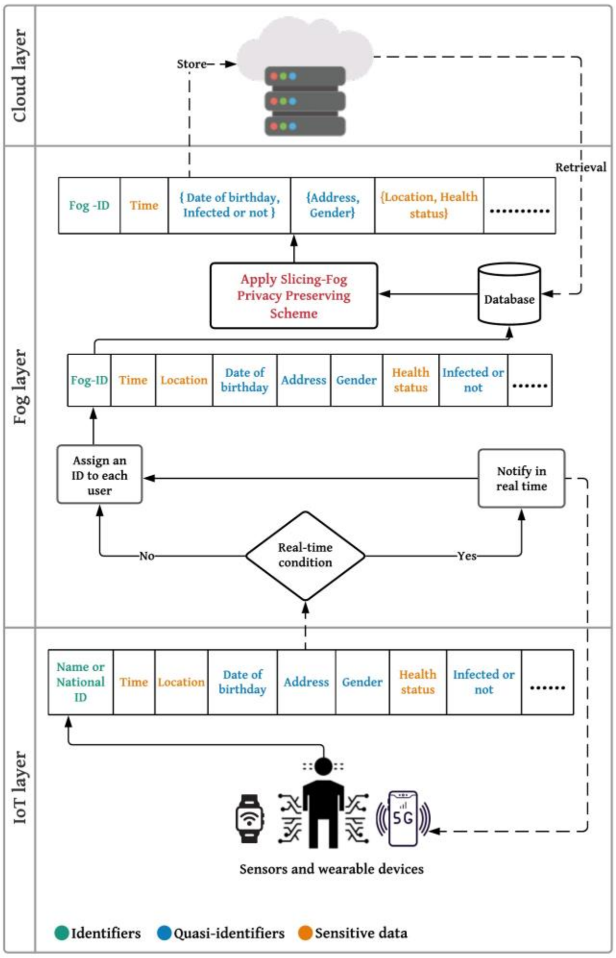

Figure 2. Proposed Privacy-Preserving Scheme.

5. Implementation And Result

In this section, we describe our implementation setup and discuss our scheme evaluation to validate its effectiveness

5.1. Experimental Setup

For performance evaluation purposes, a PC fulfilled our experimental setup requirements. The PC is equipped with Intel® Core™ i7-7700 CPU @ 3.60GHz 3.60 GHz and 16 GB RAM running 64-bit Windows 10 20H2 operating system. We implement our scheme in C# Window Forms language utilizing .NET Framework 4.8. In our implementation, we utilize a set of data collected from 5000 users.

Table 1. Original table of collected data from IoT devices

National ID	Time	Location	Date of birth	Address	Gender	Health status	Infected or not
1087658432	15:02	24.1635° N, 47.3339° E	30-2-1990	Riyadh-11564	female	Healthy	not
1117239099	15:05	26.1415° N, 43.7321° E	13-6-1991	Riyadh-11564	male	Healthy	Infected
1000326722	15:08	24.1532° N, 47.2718° E	5-2-2001	Kharj-16244	male	asthma	Infected
1219876278	15:10	26.3592° N, 43.9818° E	30-7-1990	Qassem-51431	male	Healthy	Infected
1768987657	15:13	26.3072° N, 50.1783° E	19-2-1999	Khobar-34424	female	asthma	not
1032457890	15:17	26.3223° N, 50.2168° E	26-6-1995	Khobar-34424	male	Blood pressure	not
1167975421	15:17	24.7311° N, 46.6701° E	7-2-1988	Riyadh-11564	male	diabetes	Infected
112568900	15:18	24.6951° N, 46.6806° E	9-11-1997	Riyadh-11564	female	asthma	not

Table 2. Step 1 replace all identifier attribute with fog-id and apply vertical partition

Fog-ID	Time	{Date of birth, Infected or not}	{Address, Gender}	{Location, Health status}
333	15:02	{30-2-1990, Not}	{Riyadh-11564, Female}	{24.1635° N, 47.3339° E, Healthy}
549	15:05	{13-6-1991, Infected}	{Riyadh-11564, Male}	{26.1415° N, 43.7321° E, Healthy}
278	15:08	{5-2-2001, Infected}	{Kharj-16244, Male}	{24.1532° N, 47.2718° E, Asthma}
999	15:10	{30-7-1990, Infected}	{Qassem-51431, Male}	{26.3592° N, 43.9818° E, Healthy}
123	15:13	{19-2-1999, Not}	{Khobar-34424, Female}	{26.3072° N, 50.1783° E, Asthma}
345	15:17	{26-6-1995, Not}	{Khobar-34424, Male}	{26.3223° N, 50.2168° E, Blood pressure}
789	15:17	{7-2-1988, Infected}	{Riyadh-11564, Male}	{24.7311° N, 46.6701° E, Diabetes}
267	15:18	{9-11-1997, Not}	{Riyadh-11564, Female}	{24.6951° N, 46.6806° E, Asthma}

Table 3. Step 2 applying horizontal partition at specific span of time, in this scenario period = 10 minutes

Fog-ID	Time	{Date of birth, Infected or not}	{Address, Gender}	{Location, Health status}
333	15:02	{30-2-1990, Not}	{Riyadh-11564, Female}	{24.1635° N, 47.3339° E, Healthy}
549	15:05	{13-6-1991, Infected}	{Riyadh-11564, Male}	{26.1415° N, 43.7321° E, Healthy}
278	15:08	{5-2-2001, Infected}	{Kharj-16244, Male}	{24.1532° N, 47.2718° E, Asthma}
999	15:10	{30-7-1990, Infected}	{Qassem-51431, Male}	{26.3592° N, 43.9818° E, Healthy}
123	15:13	{19-2-1999, Not}	{Khobar-34424, Female}	{26.3072° N, 50.1783° E, Asthma}
345	15:17	{26-6-1995, Not}	{Khobar-34424, Male}	{26.3223° N, 50.2168° E, Blood pressure}
789	15:17	{7-2-1988, Infected}	{Riyadh-11564, Male}	{24.7311° N, 46.6701° E, Diabetes}
267	15:18	{9-11-1997, Not}	{Riyadh-11564, Female}	{24.6951° N, 46.6806° E, Asthma}

Table 4. Step 3 applying random permutation in each bucket to ensure removing the correlation between the attributes of a single record

Fog-ID	Time	{Date of birth, Infected or not}	{Address, Gender}	{Location, Health status}
333	15:02	{30-7-1990, Infected}	{Kharj-16244, Male}	{26.1415° N, 43.7321° E, Healthy}
549	15:05	{5-2-2001, Infected}	{Qassem-51431, Male}	{24.1635° N, 47.3339° E, Healthy}
278	15:08	{30-2-1990, Not}	{Riyadh-11564, Female}	{26.3592° N, 43.9818° E, Healthy}
999	15:10	{13-6-1991, Infected}	{Riyadh-11564, Male}	{24.1532° N, 47.2718° E, Asthma}
123	15:13	{26-6-1995, Not}	{Riyadh-11564, Male}	{24.7311° N, 46.6701° E, Diabetes}
345	15:17	{9-11-1997, Not}	{Khobar-34424, Female}	{24.6951° N, 46.6806° E, Asthma}
789	15:17	{19-2-1999, Not}	{Riyadh-11564, Female}	{26.3072° N, 50.1783° E, Asthma}
267	15:18	{7-2-1988, Infected}	{Riyadh-11564, Male}	{26.3223° N, 50.2168° E, Blood pressure}

Table 5. Shows the efficiency of the scheme, as all users' data do not refer to a specific induvial comparing with original table

Fog-ID	Time	{Date of birth, Infected or not}	{Address, Gender}	{Location, Health status}
333	15:02	{30-7-1990, Infected}	{Kharj-16244, Male}	{26.1415° N, 43.7321° E, Healthy}
549	15:05	{5-2-2001, Infected}	{Qassem-51431, Male}	{24.1635° N, 47.3339° E, Healthy}
278	15:08	{30-2-1990, Not}	{Riyadh-11564, Female}	{26.3592° N, 43.9818° E, Healthy}
999	15:10	{13-6-1991, Infected}	{Riyadh-11564, Male}	{24.1532° N, 47.2718° E, Asthma}
123	15:13	{26-6-1995, Not}	{Riyadh-11564, Male}	{24.7311° N, 46.6701° E, Diabetes}
345	15:17	{9-11-1997, Not}	{Khobar-34424, Female}	{24.6951° N, 46.6806° E, Asthma}
789	15:17	{19-2-1999, Not}	{Riyadh-11564, Female}	{26.3072° N, 50.1783° E, Asthma}
267	15:18	{7-2-1988, Infected}	{Riyadh-11564, Male}	{26.3223° N, 50.2168° E, Blood pressure}

5.2. Result

In our evaluation, we focus on three factors: the performance factor, the privacy factor, and the logical factor.

5.2.1. Performance Factor

The proposed scheme performance is evaluated by measuring the computing time of implementing the scheme on users' data. The computing time greatly affects real-time analysis. Our evaluation result is illustrated in Fig. 3. The computation time of implementing the proposed scheme is measured in milliseconds (*ms*) on various inputs of data. The results show the efficient performance of the scheme, as it consumes a reasonable period when the number of data is increased. This shows that the scheme is lightweight on the device. Therefore, our scheme does not consume resources, consequently power.

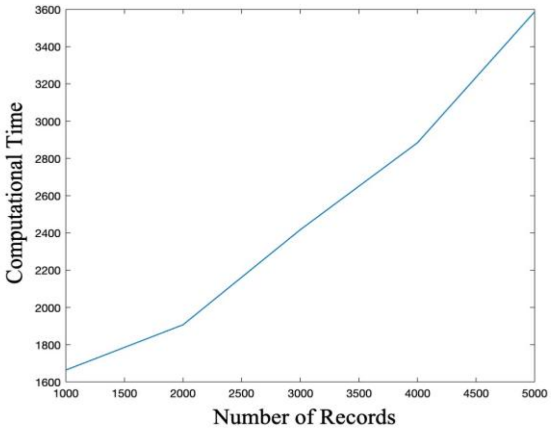

Figure 3. Computational Time

5.2.2. Privacy Factor

It is worth mentioning that our privacy-preserving scheme is based on the principle of anonymization by slicing technique but in a novel way. To evaluate the privacy efficiency of our proposed scheme, we have used entropy and estimation error as a privacy metric. The entropy metric represents the amount of accurate and correct information about a specific user that cloud provider deduces from the collected data. The equation below defined the entropy [19]:

$$\mathrm{E} = -\sum_{\mathrm{i}=0}^{\mathrm{n}} \mathrm{P_i} * \mathrm{Log_2}(\mathrm{P_i}) \quad (1)$$

Where n is the number of data sent and Pi is the probability of that data i belongs to a specific user. Therefore, in our scheme the data is collected in the cloud is sliced and does not identify a specific user. Consequently, the entropy is at the maximum, which is the one making the highest level of privacy-preserving.

Estimation error means the rate of the attacker or the violator falling in fault. The attacker must not be able to detect the correct user data, by increasing the value of the estimation error [19]. To achieve this goal in the proposed scheme, when permutations are made between a larger set of data in each bucket, especially the data of columns, which contain sensitive attributes, greater than the estimation error rate of the attacker. Its value and relationship to the entropy metric is illustrated in the following equation:

$$EE = (E) * 100\% \quad (2)$$

Where E is the Entropy value. As we mentioned that the maximum entropy value in the proposed scheme is 1, and when that value is offset in the error estimation equation, the result becomes 100%. This indicates the maximum rate of the attacker and even the cloud provider could be wrong in detecting the correct user data.

5.2.3. Logical Factor

After measuring the effectiveness of the approach in preserving privacy, we can logically demonstrate the validity of the approach in deterring privacy threats.

- The identity disclosure threat: giving a fog-id to each user instead of his name and identification, is a deterrent against the threat of identity disclosure.
- The attribute disclosure threat: this threat discloses the user identity and sensitive data, through combining data from more than one attribute. In the proposed scheme, the process of data permutation in each bucket is to remove the correlation between the sensitive attributes. Thus, the information about any user can not be identified when combining two or more attributes.
- Correlation Analysis Attack: the attacker collects and tracks the user’s history of location data, health status, or other serial data.

Then it analyzes it to predict the new data [19]. To deter this type of attack, the main principle of the slicing technique is to remove the correlation between each user’s attributes by permutations within the bucket. Furthermore, the approach provides proper preservation of the utility. For instance, when conducting statistics that usually executed in social distancing such as the number of infected people of ages between 30 and 35 years, it will give correct results. Due to sliced data, which is divided vertically, according to the most associated attribute as mentioned previously. Finally, the implementation of this proposed approach is not limited to social distancing techniques rather, it can be implemented on various IoT applications.

6. CONCLUSION

Social distancing has greatly contributed for limiting the spread of pandemics in recent years. While the benefits associated with implementing social distancing technology are numerous, privacy issues have been raised. Consequently, we have proposed a new scheme to preserve the privacy based on improving the slicing technique and imply fog computing. This approach has enhanced the level of privacy in social distancing techniques. In our future work, we plan to apply our scheme in more complex environment where privacy preserving is demanded.

ACKNOWLEDGMENT

This project was supported by the Deanship of Scientific Research at Prince Sattam Bin Abdulaziz University under the research project No.2019/01/10411.

REFERENCES

[1] "World Health Organization: Who coronavirus (covid-19) dashboard." https://covid19.who.int (accessed Mar. 28, 2020).

[2] A. A. A. Sen, F. A. Eassa, K. Jambi and M. Yamin, "Preserving Privacy in Internet of Things: A Survey," International Journal of Information Technology, vol. 10, no. 2, pp. 189-200, 2018.

[3] C. T. Nguyen, Y.M. Saputra. N. V. Huynh, N.T. Nguyen and T. V. Khoa et al., "A comprehensive survey of enabling and emerging technologies for social distancing—part ii: Emerging technologies and open issues," IEEE Access, vol. 8, pp. 154209–154236, 2020.

[4] M. Shukla, R. MA, S. Lodha, G. Shroff and R. Raskar, "Privacy guidelines for contact tracing applications," arXiv preprint arXiv: 2004.13328, 2020.

[5] H. Shen, M. Zhang, H. Wang, F. Guo and W. Susilo, "A Lightweight Privacy-Preserving Fair Meeting Location Determination Scheme," IEEE Internet of Things Journal, vol. 7, no. 4, pp. 3083-3093, 2020.

[6] Y. Pu, J. Luo, Y. Wang, C. Hu and Y. Huo et al., "Privacy preserving scheme for location based services using cryptographic approach," in Proceedings of PAC, Washington, DC, USA, pp. 125–126, 2018.

[7] A. Alrawais, A. Alhothaily, C. Hu and X. Cheng, "Fog computing for the internet of things: Security and privacy issues," IEEE Internet Computing, vol. 21, no. 2, pp. 34–42, 2017.

[8] M. Kamal, A. Aljohani and E. Alanazi, "IoT meets covid-19: Status, challenges, and opportunities," arXiv preprint arXiv: 2007.12268, 2020.

[9] S. Jaafari, A. Alhasani, E. Alghosn, R. Alfahhad and S. M. Almutairi, "Certain investigations on IoT system for Covid-19," in Proceedings of ICCIT-1441, Tabuk, Saudi Arabia, pp. 1–4. IEEE, 2020.

[10] H. Wen, Q. Zhao, Z. Lin, D. Xuan and N. Shroff, "A study of the privacy of covid-19 contact tracing apps," in Proceedings of SecureComm:2020, Washington, DC, USA, pp. 297–317. Springer, 2020.

[11] T. Sharma, T. Wang and M. Bashir, "Advocating for users' privacy protections: A case study of Covid-19 apps," in Proceedings of MobileHCI'20, New York, NY, USA, pp. 1–4, 2020.

[12] A. Ksentini and B. Brik, "An edge-based social distancing detection service to mitigate Covid-19 propagation," IEEE Internet of Things Magazine, vol. 3, no. 3, pp. 35–39, 2020.

[13] Y. C. Ho, Y. H. Chen, S. H. Hung, C. H. Huang and P. Po et al., "Social distancing 2.0 with privacy-preserving contact tracing to avoid a second wave of Covid-19," arXiv preprint arXiv: 2006.16611, 2020.

[14] F. S. CA and S. A. Kabeer, "Smart access card system to mitigate the covid-19 outbreak," in Proceedings of ICCAKM, Dubai, UAE, pp. 168–173. IEEE, 2021.

[15] V. Puri, S. Sachdeva and P. Kaur, "Data anonymization for privacy protection in fog-enhanced smart homes," in Proceedings of ICSC, Noida, India, pp. 201– 205. IEEE, 2020.

[16] P. Bellavista, J. Berrocal, A. Corradi, S. K. Das and L. Foschini et al., "A survey on fog computing for the internet of things," Pervasive and mobile computing, vol. 52, pp. 71–99, 2019.

[17] A. A. A. Sen and M. Yamin, "Advantages of using fog in IoT applications," International Journal of Information Technology, vol. 13, no. 3, pp. 829–837, 2021.

[18] A. Kumar and M. Gyanchandani, "A comparative survey on privacy preservation and privacy measuring techniques in data publishing," in Proceedings of ICICCS, Madurai, India, pp. 1902–1906. IEEE, 2018.

[19] S. S. Albouq, A. A. A. Sen, A. Namoun, N. M. Bahbouh, and A. B. Alkhodre et al., “A double obfuscation approach for protecting the privacy of IoT location based applications,” IEEE Access, vol. 8, pp. 129415–129431, 2020.

AUTHORS

Arwa Alrawais received the M.S. degree in computer science and the Ph.D. degree from the Department of Computer Science, The George Washington University, Washington, DC, USA, in 2011 and 2017, respectively. She holds a patent in system and method for remote authentication with dynamic usernames. Her current research interests include network security, wireless and mobile security, and algorithm design and analysis. She serves as a Professional Reviewer for several conferences and journals of the IEEE and ACM.

Fatemah Alharbi is an assistant professor in the Computer Science department at Taibah University, Yanbu, Saudi Arabia. She received her Ph.D. from University of California, Riverside, in 2020. Her research interests are on system and network security, including vulnerability discovery, Internet of Thing (IoT), applied cryptography, applied program analysis, system building, and measurement of real-world security problems.

MoteebAlmoteri received the B.Sc. degree in computer science (information assurance emphasis) from the University of Findlay, OH, USA, in 2010, the M.Sc. degree in information security and assurance from Robert Morris University, PA, USA, in 2012, and the Ph.D. degree in computer science from the Florida Institute of Technology, FL, USA, in 2017. He has been an Assistant Professor with the Department of MIS, Business Administration College, King Saud University, since February 2018, and the Chairman of the MIS Department, King Saud University, since January 2019. His research interests include cloud security, security shared responsibility, information security strategies, information security management, cyber security GRC, and computer vision.

Sara AAljwair received the B.S. degree in Information System from the Department of Information System in 2019 and the M.S. degree in Engineering of Cybersecurity from the Department of Computer Engineering in 2021, The Prince Sattam bin Abdulaziz University, Al-kharj, KSA. Her current research interests include the security and privacy of the Internet of things, algorithm design and analysis.

Sara SAljwair received the B.S. degree in Information System from the Department of Information System in 2017 and The M.S. degree in engineering of cybersecurity from the Department of Computer Engineering, The Prince Sattam bin Abdulaziz University, Al-kharj, KSA, in 2021. Her current research interests include security and privacy in the Internet of Things applications and algorithm design and analysis.