I.J. Wireless and Microwave Technologies, **2021, 3, 22-29**
Published Online June 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2021.03.04

Supporting Audio Privacy-aware Services in Emerging IoT Environment

Naushin Nower
Institute of Information Technology, University of Dhaka, Bangladesh
Email: naushin@iit.du.ac.bd

Received: 20 April 2021; Revised: 11 May 2021; Accepted: 25 May 2021; Published: 08 June 2021

Abstract: The increasing exploration of smart space voice assistants and audio monitoring IoT devices leads to significant trust and privacy concerns. Among them, some of the data are sensitive and a user may not aware of when and where audio recordings are sent for processing. This provides burning questions- how do users gain knowledge of, and control the amount of data captured in the physical world. Moreover, the sending and processing of these sensitive data to the far cloud do not provide an efficient solution for sensitive data which causes serious privacy and security concerns. In this paper, a new architecture for providing audio transparency and privacy in the IoT-rich environment is proposed. The proposed privacy enforcement module is used to operate within a nearby fog node, which situated close to the data sources and enforces privacy according to the data owner's desire. To show the effectiveness of the proposed architecture, a well-known privacy threat framework is investigated.

Index Terms: Audio privacy, IoT, PSOLA, Privacy architecture, Privacy threats analysis.

1. Introduction

Rapid advances in communication and sensing technologies lead to the widespread deployment of IoT devices in a wide range of places (including public and private) and as a result, it generates an enormous amount of data with significant value. After data generation, processing, and exploring these collected IoT data will increase the risk of a privacy breach. It is found that 33% of the collected data from IoT sensors are sensitive and thus an obvious target for opponents [1]. The data is considered to be sensitive when it includes personal identifiable information and any data format for example text, image, audio, and video data can contain personal identifiable information [2]. Various privacy-preserving techniques have been developed to protect user data privacy. Most of the existing privacy-preserving solutions are focused on preserve location privacy and some methods are developed for image and video privacy. None of the developed methods considers privacy preservation on audio data. However, recently smart home IoT devices are increasing adding audio recording and monitoring features to a numerous household devices including smart speakers, virtual assistant AI devices, security systems, thermostats, doorbells, voice control devices (TV, vacuum cleaner), and many more [3]. All of the voice control devices are equipped with recorders and microphones which significantly increases privacy concerns. As a result, it is an urgent need to develop a method to ensure audio privacy.

Nowadays, a huge number of sensors or intelligent devices have been integrated into people's daily life which generates massive sensing data from smart homes to the smart office. This work is motivated by a vision of a world in which IoT audio sensors and actuators are widely deployed and frequently encountered by users as they go about their daily lives. Consider the following scenario:

Jony is a freelance contractor. This afternoon, like many others, he is hot-desking in a city local to his current clients to conduct face-to-face meetings. The smart office space he has hired offers a variety of context-aware services that automatically adapt to the people that are currently present in the space. For example, the office provides services to capture meetings (audio and video recording) and provides voice control for heating, lights, and control meeting capture services. Jony's meeting with Joe is about to begin; soon as Joe enters the office building, his device automatically informs him about the sensing available at the location and his current preferences and options. In this case, Jony and Joe are meeting for informal catchup, and Joe decides to activate his "private meeting mode" to obscure his face and voice from potential recordings conducted by the voice control or meeting capture services. Jony also provides his choice to ensure his privacy.

The reporter is taking an interview with a rape case victim or survivor of sexual assaulter or a person injured with domestic violence. In most cases, victims are often still in shock and trauma and unaware of the pitfalls of speaking and the victim does not want to disclose her identity in this situation. When this news is broadcasted the victim's face is blurred to hide his/her identity but the voice is on air without any change. As a result of her voice, her identity can be

easily disclosed. If victims can obscure his/her voice their privacy can be preserved. Using audio privacy mode, the user can control her privacy by producing a synthesized voice so that identity can be concealed.

These scenarios highlight the ubiquity of IoT technology and the range of data that may be collected from potential users. Besides these example cases, there are many situations/cases to collect personal data that increase potential privacy issues. While the IoT privacy landscape is complex, the main concept is to ensure user's privacy by controlling their data. That means the user should decide whether he/she discloses their data or not. Providing privacy controls for owner's data and protecting sensitive IoT data is a great challenge especially for audio data since there is no such work to protect audio data.

The major objective of this research is to develop a architecture that will provide audio-privacy aware IoT service. Since, now-a-days, many of the IoT devices are equipped with recording and microphone services, as a the risk of audio privacy is increasing. Existing literature focus on the privacy from video, location and other IoT services without considering audio privacy. The reason is that previously voice controlled devices and IoT devices with recording capabilities were not widely used. But recently voice-controlled devices in smart are widely used which increases audio privacy concerns also.

This paper aims to offer a solution that diminishes audio privacy risks associated with data processing and sharing sensitive data considering the owner's privacy concerns. Moreover, the processing of sensitive data is done in the nearby fog node to reduce the change of privacy attracts by the third party. In the propose solution, a software module called privacy-preserving module (PPM) is proposed in this paper to protect the owner's audio data privacy within a single fog node. PPM enforces the owner's privacy by enforcing a privacy policy to the recorded data according to the owner's choice. The PPM mechanism relies on creating and disseminating of virtual machine-based execution engine, which protects owner's private data and their metadata according to the owner's privacy policies via data protection operations.

The rest of the paper is organized as follows. Section 2 provides background information on fog computing and data privacy. Section 3 gives an overview of the proposed solution. Section 4 discusses the privacy threat analysis of the proposed architecture. Finally, Section 5 concludes the paper.

2. Background

In this section, the importance of fog computing in the field of IoT and the existing privacy approaches are highlighted.

2.1 Fog Computing

IoT brings connectivity to every home, vehicle, and workplace with smart, Internet-connected devices. As most of the appliances, TV, light, door, freeze, and many other devices in the home and office become potentially connected and voice controlled, thus it also produces a sheer amount of input data from different sources. In a traditional IoT system, the data from different sources are pushed up to the centralized cloud, where data is processed, analyzed and then the decision is made. However, a cloud-based IoT system is not efficient because of the latency problem (since the cloud is not situated nearby), and also sensitive data needs quick action without delay [4]. Besides these, in cloud-based processing, the sensitive data needs to traverse all levels of the network which provides serious security and privacy concerns. To solve this problem the concept of fog node is introduced in [5] in which fog aims to process data closer to the things compared to that of cloud and thus analyzes sensitive data at the edge of the network. Thus, fog node analyzes the sensitive data at the network edge in milliseconds based on the policy, close to where it is generated instead of sending vast amounts of IoT data to the cloud. It also selects data to the cloud for historical analysis after applying the privacy policies on the data. In brief, the fog computing has the following properties which mainly make fog computing suitable for IoT applications: (a) low propagation delay and location awareness, (b) widespread geographical distribution, (c) mobility, (d) a very large number of nodes, (e) predominant role of wireless access, (f) strong presence of streaming and real-time applications, and (g) heterogeneity [5]. Considering all these advantages, for real-time sensitive data analytics, fog computing can be considered as a prominent technology. [6]. It provides a faster response than the cloud by distributing the processing at the edge of the network. Motivated from the above factors, in this paper, a fog-based audio privacy architecture is proposed which easily can be incorporated with the other privacy-preserving solutions (video or text, etc).

2.2 Existing Privacy Preserving Approaches

The increasing and invisible deployment of IoT devices that collect, process, and disseminate personal data give rise to privacy concerns that have attracted considerable research attention. Many of the existing research focuses on developing different privacy-protecting tools and some research concentrate on people's privacy expectations from IoT sensors, privacy concerns, and reasons for privacy concerns mitigations. In [7], a privacy-sensitive information diluting mechanism (PSIUM) mechanism is proposed to ensure the user's location privacy by providing multiple location information, where none of the location information contains true location. Another approach proposed in [8] offers anonymous communication facilities by using a special store and forward network that contains a special mix node. In the technique, the hostile observer cannot trace the source and destination because of the mixed node network. In this

approach, *n*-equal length packets are created and forwarded to the mix node as input. Mix node reorders them by some predefined metric in such as a way that linkability between the incoming and outgoing message cannot be detected. Another location preserving method is Mist [9] which is a communication infrastructure that aims to preserve privacy in a pervasive computing environment. This method aims to separate user location from his/her identity and thus users can access services without revealing their location privacy. The Mist uses hierarchy of specialized routers that form an overlay network to protect location privacy. All of these previously proposed privacy-preserving methods are very limited in terms of providing control to the user. In these methods, there is no option for the user to control their privacy that means users are unable to express their privacy preferences.

Richer forms of privacy control of personal location data were explored by Myles et al. [10] who provided a framework that enabled users to express complex rules governing location disclosure. However, enforcing these rules required all location-based applications to use a common service that restricted access to individual user-location records. The authors in [11] have presented a system, that provides image privacy from unrestricted services. Their proposed system is known as DARKLY, which presents a privacy-preserving layer to protect images from the sensitive perceptual sensors such as a camera. This system transforms images by extracting features in a privacy-preserving way before they are available to an application. The user can use a filter to obscure faces according to the privacy choice of the user. After this, the obscured image would be available to the requested application. Another approach called PlaceAvoider is also used to preserve privacy in taking life logs in sensitive places [12]. The user can choose the place not to take pictures or to apply different actions based on a location or the context of an image. A probabilistic algorithm is used to determine whether the location or the image is sensitive or not. However, these approaches provide privacy and user control on the captured image only.

Most recent works on privacy concentrate on large-scale IoT systems, where scalability issue arises for the central control model to handle a large volume of sensitive data which also causes transmission delay. As a result, fog/edge-based privacy architecture is explored to preserve privacy and faster response in many recent works. For example, to protect a massive volume of IoT-sensitive data, a fog computing-based solution named policy enforcement fog module is proposed to enforce privacy policy locally for the IoT applications [2]. In their proposed fog-based architecture, sensitive data which require real-time processing are processed and enforced policy in the fog node by considering the data owner's privacy policy. For non-real-time processing, the data is processed and privacy is enforced remotely. For remote enforcement, active data bundles which are containers with a payload of sensitive data, metadata, and a virtual machine is used to enforce privacy policy to the remote fog or cloud node. The paper [2] proposes a general architecture to preserve privacy in the fog node but it does not provide any details of how it preserves privacy for image, audio, video, or other data formats. Besides this, a system is proposed to offer privacy-aware live videos as an IoT service in the fog node [13]. To make the video safe from the privacy point of view, a denatured video stream is produced. A denatured video stream is one whose content has been analyzed to identify potential privacy leaks and has been modified to eliminate those leaks. Their privacy-aware IoT architecture for live video analytics uses privacy preservation on live video streams to apply personalized policies to blur faces. However, while [13] provides a comprehensive approach for video analytics, they did not consider the privacy of audio. All of the existing solutions provide privacy from image, video, and location services without providing privacy from audio services. We believe that our architecture provides a solution for audio privacy – supporting both awareness and control of data capture. Moreover, the architecture is designed in such a way it can be incorporated with any fog-based privacy solution.

3. Framework

Voice assistant and IoT devices with audio monitoring features are increasingly added in the smart space. A wide range of household devices include audio and recording features such as smart speakers, televisions, thermostats, security systems, TV, and doorbells. As a result, devices equipped with microphones and recording devices are significantly raises privacy concerns [14]. In this section, a system is described that offers privacy-aware live audio as an IoT service. The main goal is to process audio in such a way that is protected from the privacy viewpoint. A protected audio stream is one whose content is masked so that speaker identification is disguised from the audio and as a result speaker identity cannot be revealed from the audio. The proposed solution contains a software module named a privacy-preserving module (PPM) in the fog node. PPM protects the sensitive audio data by enforcing privacy policy even the main processing is done on the remote cloud node. The main advantage of the PPM is that it is placed in the nearby fog node, which assures that privacy-preserving policy is applied to the audio sources before it discloses to the external network. The overall architecture of the proposed system is shown in Fig. 1.

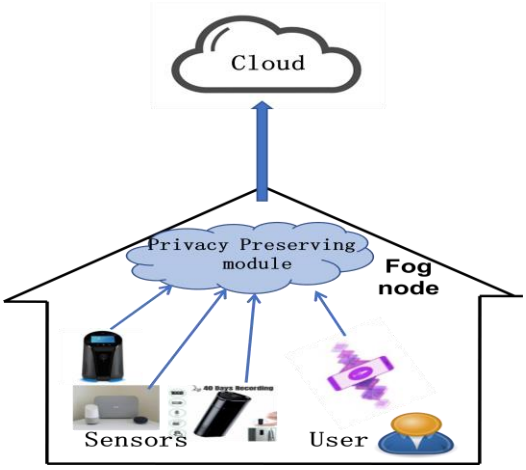

Fig.1. Architecture of a Privacy Preserving Fog Module

Consider, a smart home equipped with a microphone and other recording devices. These devices are considered sensors that capture audio and send the captured audio to the fog node (as a gateway). The PPM is implemented in the fog node and performs privacy preservation according to the user's concern. The user provides his/her privacy-preserving module via a mobile client application. A user contains a mobile client application that provides immediate notification when the data capture started. The mobile client application provides the privacy-preserving options to the user which are 1) null disclose, 2) partial disclose and 3) full disclose and the user selects the option he/she desires.

Null disclose indicates total obscure of his/her speech so that identity cannot be revealed. In this case, PPM performs the speech-to-text conversion and removes the personal identifiable information from the text, and sends the text file to the cloud. To do that, speech-to-text conversion is used using DeepMind's Wavenet [15] and tensor flow. From the speech signal, Mel frequency cepstrum coefficients (MFCC) are extracted and a deep convolution neural network is applied on the extracted MFCC. The architecture for producing speech to text is given in Fig. 2.

In the **partial disclose** mode the synthesized speech signal is produced so that, from the speech, speaker identity cannot be revealed. In this case, the mobile client application sends the user's sample speech to the PPM and PPM obscures that user's speech. The mobile client application takes the sample voice of the owner and then sends this sample voice to fog node to produce synthesized speech.

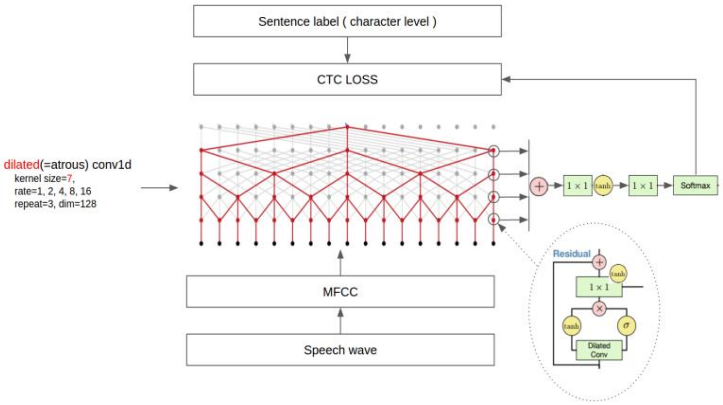

Fig.2. Speech to text conversion architecture using DeepMind's Wavenet []

In the **partial disclose mode**, the aim is to preserve the speaker's privacy by hiding the identity, which can be achieved by synthesized speech production. To do that, PSOLA (Pitch Synchronous Overlap and Add) [16] as a speech synthesis technique is implemented in the privacy-preserving module. It manipulates the pitch and duration of the speech signal to preserve the speaker's identity without affecting the speech. PSOLA decomposes the signals into smaller segments and then, modifies these segments by repeating some speech segments. This modifies the duration of the signal, and then, smaller segments are recombined through overlapping and adding. Finally, the resulting signal is re-sampled to change the pitch. Thus, a speech signal with the same spectrum as the original but with a different fundamental frequency is produced. Modified fundamental frequency and duration disguise the identity of the original speaker. PSOLA works directly on the signal waveform without any sort of model, therefore, does not lose any detail of the speech signal and can also perform in real-time.

In the null disclose and partial disclose mode, for each time a virtual machine (VM) is created and after processing VM is destructed. As a result, if a same person's voice is obscure once and he/she enters the room again, a new VM is created thus it is quit impossible to link with the previous VM.

In the full disclose mode, the original speech signal goes to the fog node without any policy enforcement as a user wants no privacy policy enforcement.

However, to provide extreme privacy (null disclose mode), the PPM can convert text from the speech so that the speaker's identity can never be revealed. Thus, PPM takes audio stream from the microphone and performs privacy mediation according to the user's preference. **Full disclose** mode provides the option to disclose everything for those who want no privacy.

4. Privacy Threats Analysis of the Proposed Architecture

In this paper, a privacy-preserving architecture for audio data is presented. To evaluate the architecture we investigate whether the proposed architecture can defend the general privacy threats. The privacy threats are an effort to obtain user's personal data/private data without taking user's concerns and execute malicious action on the collected data. From the analysis and research different privacy threats are identify that can provide potential risk on user's private data. Among them a framework called "LINDDUN" for identifying possible privacy threats [17] is widely used and covered all the existing privacy threats. LINDDUN is a short form of L—linkability, I—identifiability, N—non-repudiation, D—Detectability, D— information Disclosure, U—consent Unawareness, and N— Noncompliance [17]. These seven threats are assumed to have same severity level in this model. This framework provides a systematic way to identify, prioritize and, mitigate privacy threats. It consists of six steps where the first three steps identify privacy threats in a system and the last three steps focus on solution techniques. The first three steps are i) Define the Data Flow Diagram (DFD) of the system ii) Mapping the privacy threats to the DFD elements iii) Identify the threat scenarios. The LINDDUN framework is a counterpart of the security threat analysis model named STRIDE, which concentrates on security violation. In this section, the LINDDUN privacy threats are investigated for the proposed architecture.

The LINDDUN privacy threats, in general, can be defined as follows: (a) Linkability is the ability to determine whether two or more items of interest from different sources can be linked to a single source. It means different information (from the entity, data flow, and during data processing) can be linked to the same subject even without knowing the identity of the subject. (b) Identifiability indicates that the identity of a subject can be revealed from the data. It is the ability to identify a subject within a set of subjects. (c) Non-repudiation is a threat that can be utilized against a subject. (for example, the opponent wants to prove that a user gives her consent to use her data but she did not provide her consent actually) (d) Detectability is the threat that can detect an item of interest and can make a target of that item (e) Information disclosure threat exposes subject's data to unauthorized third parties (f) Consent unawareness threat means that the subject is unaware about the consequence of data sharing. (g) Noncompliance threat indicates that although a subject provides her privacy policy, there is no guarantee that it will be maintained. These threats can violate privacy thus we need to investigate how our architecture can defend these privacy threats. To do that we follow the first three steps of the LINDDUN model.

i) Define the DFD of our architecture

The DFD is a graphical representation of the data flows within the system. It shows how data is entered into the system, how it is processed, where it is stored, and finally how it leaves the system. The DFD describes the system using four basic building blocks i) Entity (User), ii) Data flow (communication), iii) Processes (the process of functionality) and, iv) Data store (database, file). In our architecture, data is not stored thus we do not have a Data store block. The DFD based on a high-level system description of our architecture is shown in Fig. 3.

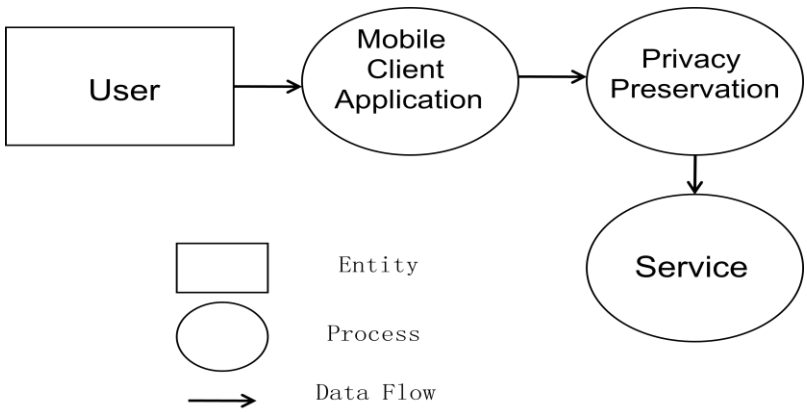

Fig.3. Data Flow Diagram (DFD) of the proposed architecture

ii) Mapping privacy threats to the DFD elements

This step is used to map the privacy threats associated with each DFD element. According to the LINDDUN mapping guideline [17], the privacy threats associated with each DFD element are shown in the following Table 1. The intersection marked with 'X' indicates a possible privacy threat to the DFD element of the system. Linkability, Identifiability, Non-repudiation, and Consent unawareness threat can be associated with the Entity elements. The possible threats that are related to the Process and Data flow are Linkability, Identifiability, Detectability, Information Disclosure, and Noncompliance.

Table 1. Mapping threats to the DFD element

	L	**I**	**N**	**D**	**D**	**U**	**N**
Entity	X	X	X			X	
Process …	X	X		X	X		X
Data Flow	X	X		X	X		X

iii) Identify threats scenarios

In this step, each of the 'X' in Table 1 is analyzed to resolve whether the threat exists with that element or not. To do that LINDDUN provides a group of privacy threat tree patterns for each of the 'X'. The threat tree for the linkability of a process is shown in Fig. 4 as an example. Linkability of a process means that data can be accessed during processing and different action in the process can be linked to the same user. Due to the space limitation, the total fourteen threat trees (the total number of 'X' in Table 1) are not provided here.

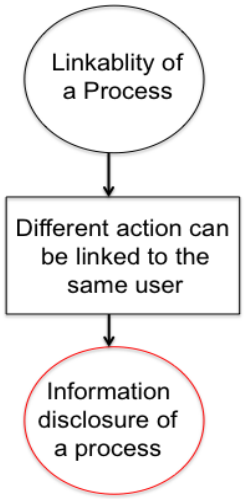

Fig.4. Threat tree for the linkability of a process [17]

5. Protecting Privacy by Using Proposed Architecture

The user's information can be linked and identity can be revealed from the user's data. Thus linkability and identifiability threats can be associated with the user (entity). An entity can be linked and identifiable if untrusted communication is used for login. In our architecture, the user's own mobile phone is used for login and a nearby fog node with a privacy-preserving module is used for data processing. The user gives his/her consent using a trusted mobile client app thus entity's information cannot linkable and identifiable. The architecture provides awareness by using mobile client applications so that a user can start his/her desired privacy service before providing his/her data. The user can only access his/her phone and can give his/her voice sample to do further processing. As a result, the user gives his/her consent with awareness thus non-repudiation threat is resolved.

The process and data flow have Linkability, Identifiability, Detectability, Information Disclosure, and Noncompliance privacy threats. To overcome the above threats, the fog node in our proposed architecture acts as a gateway where the privacy-preserving module (could be VM) performs privacy mediation before the data goes to the third-party services. The PPM performs the privacy preservation frame-by-frame basis in real-time. It takes a frame as an input and generates the output (processed frame) without storing the data. The PPM sends the processed data to the cloud for the use of third-party software. Thus only the mediated data without identity information is available to the

third party service. Furthermore, once a person's data is processed, the VM running for a person will be stopped and no longer exists in the system. Even if the same person enters the room again, a new VM is created for him. Thus linkability is not possible. Furthermore, data inside the fog node (with PPM) cannot be accessed by the others thus detectability, information disclosure threat associated with a process is resolved. The same is true for data flow also as data flow is protected within a trusted fog node, which resides in a local gateway. The PPM VM performs the mediation according to the privacy requirements of the user as a result noncompliance threat is also mitigated.

6. Conclusions

As IoT devices increasingly adopt microphones and other voice assistant devices, there is a growing need for practical privacy defenses. In this paper, an audio privacy-aware architecture is proposed in the emerging IoT environment to provide user awareness, control, and privacy. In the proposed architecture a privacy-preserving module is implemented which is based on the PSOLA technique. PSOLA is a very well-known speech processing technique and it can process the pitch and duration of the speech in real-time. The user can control his/her privacy using the proposed solution. The proposed solution can be easily incorporated with other privacy architecture that provides privacy from video services and other services. Moreover, the module is implemented in the fog node which also ensures sensitive data protection from the outer network. In this research, a privacy-aware audio architecture is proposed and investigated how it can handle different privacy threats. In future, it is planned to evaluate performance of the proposed architecture in real life.

References

[1] Vormetric Data Security, “Trends in Encryption and Data Security,” (Slides). Cloud, Big Data and IoT Edition, Vormetric Data Threat Report, San Jose, CA, 2016.

[2] Al-Hasnawi, Abduljaleel, and Leszek Lilien. "Pushing Data Privacy Control to the Edge in IoT using Policy Enforcement Fog Module," Companion Proceedings of the10th International Conference on Utility and Cloud Computing, pp. 145-150, 2017.

[3] Mitev, Richard, Anna Pazii, Markus Miettinen, William Enck, and Ahmad-Reza Sadeghi. "LeakyPick: IoT Audio Spy Detector." In Annual Computer Security Applications Conference, pp. 694-705, 2020.

[4] Hossan, Sakhawat, and Naushin Nower. "Fog-based dynamic traffic light control system for improving public transport," Public Transport, vol. 12, no. 2, pp. 431-454, 2020.

[5] Bonomi, Flavio. "Connected vehicles, the internet of things, and fog computing," In The eighth ACM international workshop on vehicular inter-networking (VANET), Las Vegas, USA, pp. 13-15, 2011.

[6] Stojmenovic, Ivan. "Fog computing: A cloud to the ground support for smart things and machine-to-machine networks," In IEEE Australasian telecommunication networks and applications conference (ATNAC), pp. 117-122, 2014.

[7] H. S. Cheng, D. Zhang, J. G. Tan, “Protection of Privacy in Pervasive Computing Environments,” International Conference on Information Technology: Coding and Computing, pp. 242-247, 2005.

[8] A. R. Beresford, F. Stajano, “Location Privacy in Pervasive Computing,” Pervasive Computing, IEEE, Vol. 2(1), pp. 46-55, 2003.

[9] R. Campbell, J. Al-Muhtadi, P. Naldurg, G. Sampemane, M. D. Mickunas, “Towards Security and Privacy for Pervasive Computing,” Proceedings of International Symposium on Software Security, 2002.

[10] G. Myles, A. Friday, and N. Davies, “Preserving Privacy in Environments with Location-based Applications,” IEEE Pervasive Computing, vol. 2, no. 1, pp. 56–64, 2003.

[11] Suman Jana, Arvind Narayanan, Vitaly Shmatikov, "A Scanner Darkly: Protecting user Privacy from Perceptual Applications, " 2013 IEEE Symposium on Security and Privacy, (SP), pp. 349–363, 2013.

[12] Robert Templeman, Mohammed Korayem, David Crandall, Apu Kapadia, "Placeavoider: Steering First-Person Cameras Away from Sensitive Spaces," in: Network and Distributed System Security Symposium, NDSS, 2014.

[13] Wang, Junjue, Brandon Amos, Anupam Das, Padmanabhan Pillai, Norman Sadeh, and Mahadev Satyanarayanan. "A scalable and privacy-aware IoT service for live video analytics," In Proceedings of the 8th ACM on Multimedia Systems Conference, pp. 38-49. 2017.

[14] Zheng, Serena, Noah Apthorpe, Marshini Chetty, and Nick Feamster. "User perceptions of smart home IoT privacy," Proceedings of the ACM on Human-Computer Interaction (CSCW), pp 1-20, 2018.

[15] Oord, Aaron van den, Sander Dieleman, Heiga Zen, Karen Simonyan, Oriol Vinyals, Alex Graves, Nal Kalchbrenner, Andrew Senior, and Koray Kavukcuoglu, "Wavenet: A generative model for raw audio," arXiv preprint arXiv:1609.03499, 2016.

[16] Kortekaas, Reinier WL, and Armin Kohlrausch. "Psychoacoustical evaluation of the pitch-synchronous overlap-and-add speech-waveform manipulation technique using single-formant stimuli," The Journal of the Acoustical Society of America 101, no. 4 pp. 2202-2213, 1997.

[17] Deng, Mina, Kim Wuyts, Riccardo Scandariato, Bart Preneel, and Wouter Joosen. "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements," Requirements Engineering, vol. 16, no. 1, 3-32, 2011.

Authors' Profile

Naushin Nower received her B.Sc and MS degrees in Computer science and Engineering from the University of Dhaka, Bangladesh, in 2007 and 2009, respectively. She received her Ph.D degree from Japan Advanced Institute of Science and Technology in 2015. She is the faculty member of Institute of Information Technology ,University of Dhaka, Dhaka 1000, Bangladesh. Her research interests include IoT, Cyber-physical System, Intelligent traffic control systems and reversible logic.

How to cite this paper: Naushin Nower, " Supporting Audio Privacy-aware Services in Emerging IoT Environment", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.11, No.3, pp. 22-29, 2021.DOI: 10.5815/ijwmt.2021.03.04