Toward Integrated Virtual Emotion System with AI Applicability for Secure CPS-Enabled Smart Cities: AI-Based Research Challenges and Security Issues

Hyunbum Kim and Jalel Ben-Othman

Abstract

Cyber-physical systems (CPS) basically pursue a new form of integrated interaction with humans through computation and physical capabilities covering complex, intelligent, autonomous systems. Also, artificial intelligence (AI) is considered as a promising technology that will be applicable to numerous combined next generation applications including CPS, security, and communication in smart cities. However, cyber security based on AI technologies is still in its infancy and, in particular, the differential challenges or issues should be addressed for various AI-enabled applications and systems. In this article, we introduce a new integrated virtual emotion system with AI applicability, called as I-VEmoSYS, toward secure CPS-enabled smart cities. The integrated virtual emotion system covers several subsystems such as virtual emotion barrier, virtual emotion map, and virtual emotion block. We describe their system settings, concepts, components, and operations, and also deal with AI applicability to those subsystems. Furthermore, we discuss future challenges and security issues that must be met to achieve secure advanced smart cities using the AI-enabled virtual emotion system.

Introduction

The recent advent of cyber-physical systems (CPS) motivates a new integrated system through computational and physical capabilities, particularly because it has a property of interaction with humans through various modalities [1]. Also, the Internet of Things (IoT) is able to provide numerous kinds of services for citizens and administrators in smart cities. Thus, it is expected that both CPS and IoT can allow people to have convenient and smart lives in smart cities ultimately [2, 3]. Among various research branches, the security issues for CPS and IoT should be addressed carefully so as to support secure, reliable services using CPS and IoT [4, 5].

On the other hand, emotion is unique to humans, and it definitely can distinguish humans from machines. Also, it will be highly useful if citizens can receive emotion-based services appropriately in advanced intelligent smart cities. That is, relying on an accurate emotion detection, we will surely realize successful and convenient smart life to be supported by timely emotion-based services to verified people for specific times and at proper locations. For the derivation of human emotion, there are various ways including audio and visual information, motion recognition by camera, wearable devices, body sensors, and wireless signal [6, 7]. Recently, a concept of virtual emotion was introduced by [8], which can be recognized by an IoT device through pre-installed processing units. The virtual emotion information not only can be forwarded to other entities or systems, but also can be handled as manipulatable data. Furthermore, the virtual emotion can be improved as well as expanded by combining with other promising technology such as big data and neural networks toward successful realization of smart life. Also, it is highly anticipated that if artificial intelligence (AI) [9] is applied to virtual emotion, such an AI-applicable virtual emotion will lead to an integrated virtual emotion system. However, because the research on virtual emotion is at an early stage, there are several challenges and issues such as scalability, accuracy, reliability, efficiency, and maintenance that should be addressed. In particular, because the security in virtual emotion with AI applicability is in its infancy, we should deal with the security threats and issues.

Based on the above observation and solid motivation, we aim to establish a bridgehead for secure emotion-based services with AI applicability so as to contribute to advanced smart cities by designing a secure integrated virtual emotion system. To the best of our knowledge, this is an initial work to consider the integrated virtual emotion system with novel subsystems and to deal with their security challenges and issues. Then, the main contributions of this article are summarized in the following.

- For secure CPS-enabled smart cities, we introduce an integrated virtual emotion system with AI perspective, referred as *I-VEmoSYS*. The proposed *I-VEmoSYS* is composed of two subsystems and each subsystem can be linked closely and be performed with CPS devices and intelligent applications.
- As the first subsystem, we design a virtual emotion barrier from an AI perspective, called *AI-VEmoBAR*. Also, the concepts of AI-enabled virtual emotion flow and virtual emotion map are introduced, which are referred to as *AI-VEmoFLOW* and *AI-VEmoMAP*, respectively.

Digital Object Identifier:
10.1109/MNET.011.1900299

Hyunbum Kim (corresponding author) is with the University of North Carolina at Wilmington; Jalel Ben-Othman is with the Université Paris Sud and the Université de Paris 13.

 0890-8044/20/$25.00 © 2020 IEEE

–We specify practical scenarios that are performed with AI applicability. The system settings and components are defined, and their operations are explained clearly.
–Then we suggest influential research challenges and security issues critically.

- As the second subsystem, we introduce a virtual emotion block with AI applicability, referred as *AI-VEmoBLOCK*.
  –With a definition of the virtual emotion property (*VEmoPROPERTY*), not only are the promising scenarios clarified, but also the system settings and operations are described.
  –Moreover, future research topics and security issues are discussed.

Figure 1 briefly represents an entire system view which covers two subsystems, layers, components using edge-AI enabled agents and CPS-based devices.

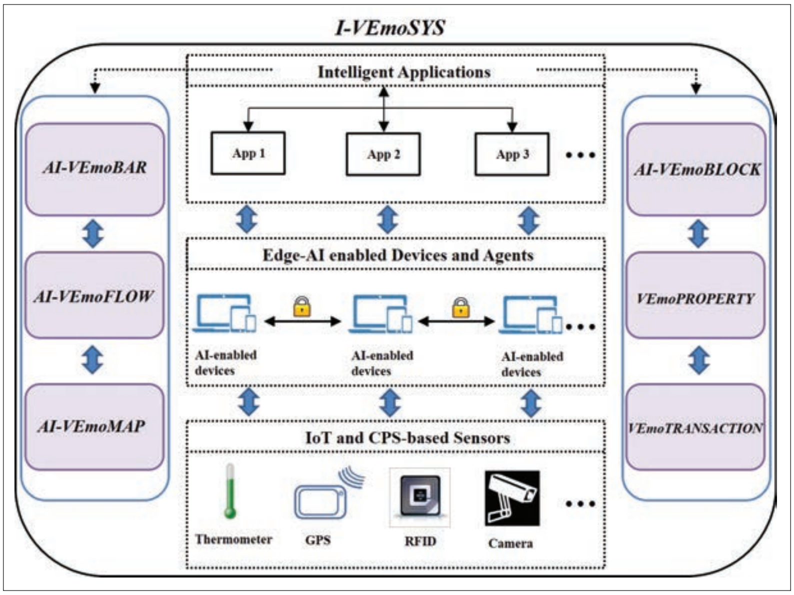

FIGURE 1. A description of the proposed integrated virtual emotion system from the AI perspective.

AI-Enabled VEmoBAR and VEmoMAP

In this section, we introduce the proposed AI-enabled virtual emotion barrier, flow, and map to provide secure emotion-based services to citizens in advanced smart cities.

Assumption and System Settings

Here we explain the assumption and settings to activate the proposed system:

- Basically, we consider human emotion detection by wireless signal, and its reflection and feature extraction because the scheme using wireless signal has clear advantages for better coverage, angles, and implementation requirements than other approaches using cameras [10].
- Given that they are equipped with wireless signal and pre-installed derivation procedures, heterogeneous edge-AI-enabled IoT and CPS devices are able to detect human emotion using wireless signal and its reflection. Also, the detected information is periodically stored for processing within edge-AI-enabled devices.
- For emotion categorization, the proposed system recognizes at least five different types of human emotion including joy, pleasure, neutrality, sadness, and anger.
- The detected emotion information can be processed as private data and/or anonymous data. Thus, a citizen has a right to give permission to the proposed system for the use of recognized emotion information with anonymity. Also, according to the permission level for emotion detection in both public and private areas, the system can give a benefit to the allowed person. Then it is possible for the permitted data to be manipulated for specific purposes in various emotion-based applications.
- With permission given by a citizen, the manipulatable emotion information can be shared within *I-VEmoSYS* and be sent to other entities in smart cities.

Architecture and Operation with AI Applicability

In intelligent smart cities, if we can detect human emotion correctly at a specific location and for a specific time, such information is very useful to provide emotion-based services to citizens. As essential parts of *I-VEmoSYS*, we introduce the concepts of AI-enabled subsystems, called *AI-VEmoBAR*, *AI-VEmoFLOW*, and f*AI-VEmoMAP*. Figure 2 shows the first subsystem view for *AI-VEmoBAR*, *AI-VEmoFLOW*, and *AI-VEmoMAP*, which depicts how to detect and derive virtual emotion through AI-enabled devices and agents. When IoT and CPS devices equipped with wireless transmitters in the virtual emotion barrier detect human emotion, AI can be used to efficiently construct *AI-VEmoBAR* in the given area. Because we may have an extensive area to monitor for numerous anonymous people, and the areas of interest for virtual emotion can be changed dynamically, it is necessary to deliberate on the applicability of AI when *AI-VEmoBAR* is created with those requirements and expectations. Also, it is possible to apply monitoring and drawing *AI-VEmoMAP* and *AI-VEmoFLOW* when meaningful virtual emotion information fitting with various intelligent applications is extracted from a continuously accumulated big amount of virtual emotion information and data through the constructed *AI-VEmoBAR*.

Operation of AI-VEmoBAR: Fundamentally, the barrier can be constructed for emotion detection at both private and public areas supported by IoT and CPS devices [8]. In particular, if the system is able to detect a person or a specific group with serious emotions such as extreme rage, fury, anger, and fear and monitor or track specific areas with those possible emergent events continuously, the integrated system can provide fast and smart emotion-based services for the purpose of public safety and citizen protection from potential threat and panic. To detect a specific emotion type, our system deliberates on *AI-VEmoBAR*. When a detection request for a specific emotion type occurs in the system, *AI-VEmoBAR* can be generated temporarily or continuously between two specific endpoints where *AI-VEmoBAR* is composed of various IoT and CPS devices with heterogeneity including on-body sensors, smart home appliances and devices, smart drones, building sensors, wireless devices in public transportation, and so on. Once the target emotion type of people passing

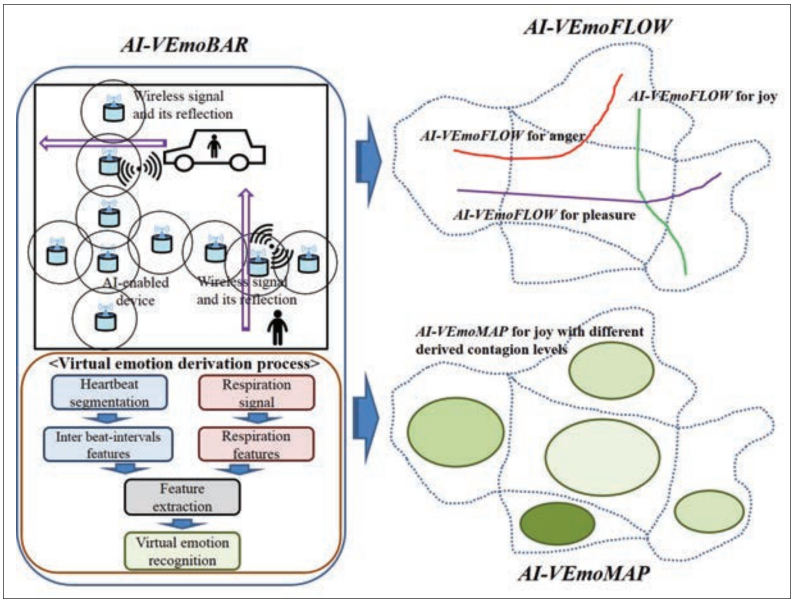

FIGURE 2. A brief description of *AI-VEmoBAR*, *AI-VEmoFLOW*, and *AI-VEmoMAP* as the first subsystem.

through the region of interest (RoI) is detected, the emotion information is sent to the requesters among distributed peers in the system or AI agents depending on the request level, the detection information priority or emergency level, and application objective. It is highly expected that many requests for specific emotion type detection from system users or peers will exist, and those numerous requests will be saved to the system if it is necessary and/or various number of entities or devices are related to those requests. Also, it is noted that the detection accuracy by wireless signal also depends on the distance between the IoT device and the target person, so we cannot select IoT devices simply to construct *AI-VEmoBAR* in RoI. Since *AI-VEmoBAR* consists of heterogeneous devices with a possibility of limited resources, maximizing a system lifetime with high accuracy should be one of critical issues in an *AI-VEmoBAR* system. To handle those issues, we can apply AI technology to the system. For example, according to system requirements and requests, an AI-enabled system will find an optimal schedule to maximize a system lifetime as well as to construct *AI-VEmoBAR* with possible high detection accuracy within a specific RoI during a requested emotion monitoring period. From initial construction in a dynamically changing environment with moving people, mobile devices, participating system configurations, or component changes, the AI agent based on machine learning will not only accumulate the system status information for each time period automatically but also maintain the system reliably without any serious faults or errors. Thus, it follows that *AI-VEmoBAR* with an AI agent will be implemented continuously, and the objective of the system will be satisfied successfully by the AI agent.

Operation of AI-VEmoFLOW: For specific emotion type, *AI-VEmoFLOW* can be derived from the already constructed *AI-VEmoBAR*. Intrinsically, *AI-VEmoFLOW* can be defined as the flow of virtual emotion information that is detected by the built *AI-VEmoBAR* within the given region. Also, *AI-VEmoFLOW* may have different flow levels or flow values. Suppose that users in the system wish to derive the flow of serious anger at a specific level during a target time period for security purposes such as crime prevention. The AI agent in the system will check which *AI-VEmoBAR* detected the requested emotion type and will also verify which devices within *AI-VEmoBAR* had recognized the emotion at the requested emotion level during the given time period so as to extract from a large amount of the accumulated emotion information from those identified devices in *AI-VEmoBAR*. Using the extracted virtual emotion information, it is possible to generate a flow of anger in the system. On the other hand, if other users in the system would like to get the flow of pleasure for the specific time period, the AI agent will first identify *AI-VEmoBAR*, which detected the virtual emotion type of pleasure within the requested region. After the AI agent verifies the devices in the found *AI-VEmoBAR* and collects their virtual emotion information, it will create the flow of pleasure within a specific bounded area. If we can create *AI-VEmoFLOW*, it should be very useful to support emotion-based services. Specifically, it can be utilized for security and patrol applications. For example, let us suppose that there is a big event held in a public park, and the system should detect a serious emotion to protect citizens from any terror threat. If the system is able to detect a specific emotion flow such as anger, it allows us to reinforce the specific region for public safety and patrol by monitoring or tracking the serious emotion flow and the expected region at a high level through an AI agent. On the other hand, the concept of *AI-VEmoFLOW* can be applied to intelligent transportation systems. Because it is anticipated that smart cars and public buses communicate with roadside units (RSUs) in smart cities [11], those RSUs can possibly recognize the emotion of humans with serious anger levels in smart cars and to accumulate the detected information continuously and forward it to the system. Then, through those RSUs and the detected information, we can generate *AI-VEmoFLOW* and track cars or objects, covering people with serious levels of anger.

Operation of AI-VEmoMAP: When we need to create *AI-VEmoMAP* to perform the emotion-based objectives, we can utilize a large amount of data obtained from *AI-VEmoBAR* and *AI-VEmoFLOW*. With the accumulated big data of virtual emotion for specific regions and at specific times, we can apply deep learning and machine learning technology of AI in order to extract and derive meaningful emotion information fitting with the current request and application objective. Using those processes, it is possible to generate visualized *AI-VEmoMAP* for each emotion type to cover a requested region for a specific time duration. If the system through the AI agent can create *AI-VEmoMAP*, it must be useful for various objectives covering business purposes, public safety, and so on. For example, if the system is able to build *AI-VEmoMAP* for the emotion type of joy or pleasure, the institutions in the system can access *AI-VEmoMAP*, which allows them to do efficient or concentrated advertisement of possible goods and products to anonymous citizens within the region, which is represented as a high level of joy or pleasure in *AI-VEmoMAP*. Moreover, *AI-VE-*

moMAP should contribute to the applications to protect citizens and to prevent potential criminal or accidents. For instance, *AI-VEmoMAP* can be applied to the application in public transportation such as public subways, trains, and buses. Similarly, the system should recognize an emergent or serious emotion type including anger or fury. By monitoring the area through the generated *AI-VEmoMAP*, our system can provide public safety to people who use public transportation in CPS-enabled smart cities. On the other hand, we may deliberate on the applicability of group emotion and emotion contagion in the proposed system. It has been known that an individual emotion may affect group emotion and behavior through emotion contagion [12]. Using the accumulated information of *AI-VEmoBAR* and *AI-VEmoFLOW*, an AI agent creates *AI-VEmoMAP*, which depicts a group emotion for a specific region during the given time period.

Research Challenges and Security Issues

Now we discuss the future research challenges and security issues that originate from the proposed system.

Research and Security Issue 1: If virtual emotion is detected by *AI-VEmoBAR*, the virtual emotion information with required anonymity can be shared with other edge-AI agents, and then the information can be utilized for generating or updating *AI-VEmoFLOW* and *AI-VEmoMAP*. Also, if a user is willing to share more of its own virtual emotion information for a specific location and duration, the user may get more benefit or incentive from both *AI-VEmoFLOW* and *AI-VEmoMAP*. However, when the information is sent to the system to be shared with other edge-AI agents or users, the detected information may have security threats including forgery and counterfeit by malicious attackers and penetrators. Thus, we should detect those threats and guarantee that the virtual emotion information is original with an integrity after the information is sent from source user or AI-agent. Also, those detection and prevention strategies need to be developed with a fast process and light complexity. Moreover, due to the CPS's complex property, there may be various attack types generated by a malicious AI-agent. Thus, it is highly necessary to consider how to recognize, detect, and solve those complex attack threats by utilizing AI-based security solutions and techniques to implement *AI-VEmoBAR*, *AI-VEmoFLOW*, and *AI-VEmoMAP* securely.

Research and Security Issue 2: Basically, the virtual emotion information in *AI-VEmoFLOW* and *AI-VEmoMAP* can originate from the detected information with anonymity by *AI-VEmoBAR* in a public area such as public transportation or a public building. Also, our system can allow users to contribute their own virtual emotion information to the system. That is, users in a private area have opportunities to contribute to *AI-VEmoFLOW* and *AI-VEmoMAP* by sending their own virtual emotion information anonymously. Then, from the system, they can receive incentives including access to *AI-VEmoFLOW* and *AI-VEmoMAP*, and business or shopping offers from institutions or companies that participate in the system. Because the system should guarantee the anonymity of the virtual emotion provider, we have additional issues to be handled. For example, selfish virtual emotion providers may send wrong emotion information, or they may pretend that the fake emotion information is the original emotion information. Hence, the issuing of provider identification with anonymity should be considered important. Also, an AI-based identification scheme and secure access control should be developed to support the system's reliability and confidence to users.

Research and Security Issue 3: When we form *AI-VEmoBAR* to derive human emotion, it is possible to apply sleep-wakeup scheduling alternately in order to maximize the lifetime because some devices may have low energy resources. Also, the participating devices or system architectures can be changed very frequently because a large number of AI-edge devices can be joined to the system or be left. Due to such a complex system property consisting of a large number of heterogeneous CPS, there may be zero-day threats for unknown misbehavior from compromised devices by penetrators. To handle those issues, an AI-based scheduling scheme can be used for efficient system maintenance. It is strictly required that such AI-based scheduling and implementation schemes should also detect malfunctioning devices or nodes compromised by attackers. Thus, we should first devise fast and accurate machine-learning-based solutions that are able to detect compromised devices and malfunctioning nodes continuously in the built *AI-VEmoBAR* and to predict future misbehavior or malfunction by malicious attackers. Besides, for zero-day threats, AI-based solutions using cypertext analysis should be developed.

AI-Enabled VEMoBlock

In this section, we present another subsystem of *I-VEmoSYS*, which can be implemented using the concept of blockchain [13].

Assumption and System Setting

We explain the assumption and setting that are considered in the proposed system.

- The system is composed of heterogeneous IoT and CPS devices, which include an edge-enabled AI agent, and should have the sensing and reflection processing capability using wireless signal and pre-installed derivation procedures to derive virtual emotion. Also, AI algorithms based on deep learning can be implemented by an edge-enabled AI agent. And, the derived virtual emotion information is periodically stored for processing.
- For emotion categorization, the proposed system recognizes at least five different types of human emotion, including joy, pleasure, neutrality, sadness, and anger.
- Depending on requested emotion type, duration, and specific location, the worth of virtual emotion information may have different values or benefits.
- Each person can generate an initial account for her/his own virtual emotion property, which is not public. Also, each person has a right to deny system access for virtual emotion sharing.
- The proposed system covers both concepts of public blockchain and private blockchain.

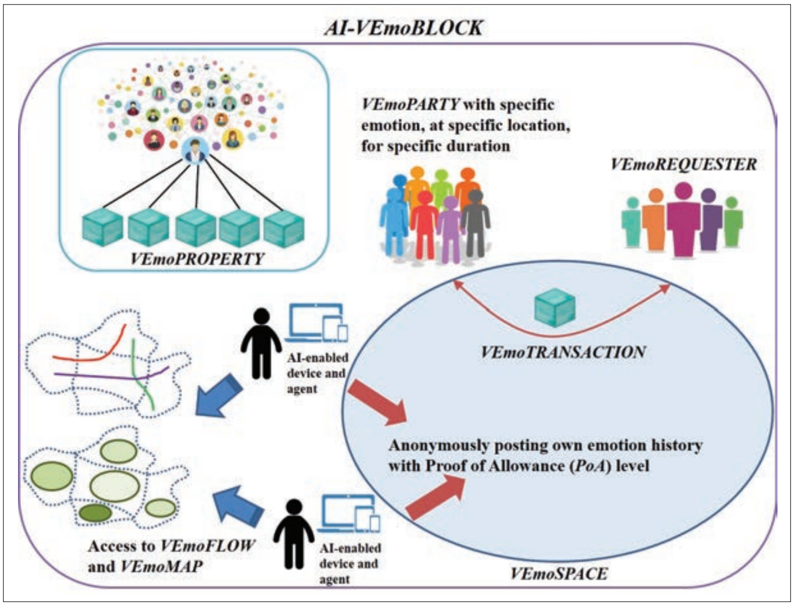

FIGURE 3. A brief description of the proposed *AI-VEmoBLOCK*, including *VEmoPRORPERTY*, *VEmoSPACE*, *VEmoPARTY*, *VEmoREQUESTER*, and *VEmoTRANSACTION* as the second subsystem.

Architecture and Operation with Applicability of AI

Here, we explain how to operate the second subsystem based on blockchain with AI applicability. Figure 3 depicts the second subsystem view for *AI-VEmoBLOCK*, which is composed of *VEmoSPACE*, *VEmoPARTY*, *VEmoREQUESTER*, and *VEmoTRANSACTION*. For the relationship between two subsystems, those two subsystems are connected closely within integrated *I-VEmoSYS*. Basically, both subsystems can be operated with common sensors, devices, and AI agents. For example, virtual emotion detection information through IoT and CPS-based sensors can be handled by edge-AI enabled devices and agents. Then the processed and classified information by AI agents with anonymity can be utilized at various intelligent applications such as emotion-fitting online shopping, intelligent medical services using emotion information, and secure surveillance systems. Then both subsystems are linked with those intelligent applications. Thus, the first subsystem can be operated with those intelligent applications by allowing those applications to access the constructed *AI-VEmoBAR*, *AI-VEmoFLOW*, *AI-VEmoMAP*. Also, the second system can support intelligent applications by allowing users in the second subsystem to access those applications so that users can contribute or get benefits when they want to receive emotion-based services.

Creation of *VEmoPROPERTY*: In future smart cities, it is highly expected that the data information of each person is very important for numerous services, applications. Because the developing speed of advanced technology and the increasing number of various IoT and other devices based on the devised technology are growing extraordinarily, the complete prevention of leaking personal information that is earned in a public area by various IoT devices such as surveillance cameras and motion capture devices might consequently be impossible as time goes by. Rather than the drain on personal information in public areas such as public roads, public buildings, and public transportation, it would be better if each person is willing to share their own virtual emotion information with anonymity. Because emotion is a unique feature of humans distinguishable from machines, the emotion information should be valuable or private property among different data types for proper services in future advancedß smart cities.

Furthermore, extending from cloud computing, edge (or fog) computing is considered as a promising paradigm that allows a large amount of data and resources to users or peers in the system [14]. AI technology at the edge devices of the IoT environment can be applied to derive meaningful sensory data rather than massive redundant data from the CPS environment. In particular, the personal emotion information should become indispensable and sensitive to perform human-emotion-based services including individual private service and public services. Hence, such valuable emotion information or derived emotion knowledge should be considered personal property. Here, we define personal virtual emotion information as *VEmoPROPERTY*, which can be used to receive specific services continuously in our system. Also, it is noted that *VEmoPROPERTY* is not open to the public and is considered as private property. Besides, *VEmoPROPERTY* as a kind of virtual money or tokens can be utilized at the Virtual Emotion Information Sharing Space which is defined as *VEmoSPACE*, similar to an online trade market or sharing space. Instead of proof of work (*PoW*) [15], each person can apply proof of allowance (*PoA*) to the system so that the incentive (or benefit) in *VEmoSPACE* will be different depending on the specific location, meaningful quality information, the period shared for emotion information. With a feature of property, it follows that the amount of *VEmoPROPERTY* for every person can be increased or decreased in the system.

Operation of AI-VEmoBLOCK: Recently, an open decentralized technology with ledger entity, called blockchain, motivated various research branches in both academic and industry [15] because the technology can support promising properties such as decentralization, transparency, and trust against tamper prevention. To make the virtual emotion information tradable in a distributed manner, we may borrow the concept of blockchain and apply it to our AI-based emotion system. Hence, it is now named *AI-VEmoBLOCK*. Basically, *AI-VEmoBLOCK* consists of several entities as follows. In *VEmoSPACE*, the emotion party (called *VEmoPARTY*) can express its own willingness with anonymity to participate in shared emotion information with PoA after deciding the amount of sharing emotion information with emotion information specification including sharing time period, sharing emotion type, and so on. Then the AI-agent can post the information of the *VEmoPARTY* to *VEmoSPACE*. When an emotion requester, referred to as *VEmoREQUESTER*, wants to take or earn the emotion history of other users, the *VEmoTRANSACTION* can be done between *VEmoPARTY* and *VEmoREQUESTER* using paid sharing with *VEmoPROPERTY*. It follows that the emotion verifier has several options. The first option is that the *VEmoREQUESTER* can open some portion of its own emotion history through PoA with the data amount that the *VEmoREQUESTER* would like to get. Then the AI-agent can post the shared portion of *VEmoRE-*

Component	Activities and roles	Research challenges and issues
AI-VEmoBAR	–Detection of virtual emotion during specific time period –Categorization of detected virtual emotion information –Scheduling construction of barrier –Forwarding information to necessary other edge-AI agents	–Anonymity of detected virtual emotion information –Threats of forgery, counterfeit of virtual emotion information –Efficient scheduling for dynamical construction of barrier –Integrity of transmitted emotion information
AI-VEmoFLOW	–Create different emotion flow levels –Provide the requested emotion flow to users –Maintenance and update of flow levels –Linked access to other emotion-based applications	–Secure access control to the system –Secure verification of users in the system –Zero-day threats for unknown misbehavior –Prevention of fake emotion from compromised devices
AI-VEmoMAP	–Generate various emotion regions for each emotion type –Visualization of emotion regions during specific time –Maintenance of each emotion during specific duration –Connects the map to other systems	–Secure access control to the system –Secure verification of users in the system –Zero-day threats for unknown misbehavior –Prevention of fake emotion from compromised devices
AI-VEmoBLOCK	–Integrated paid sharing allowance in the system –Public blockchain with different access levels –Private blockchain with private access –Matching or pricing standard for emotion value	–Efficient and scalable consensus with proof of allowance –Support secure consensus public blockchain –Support secure consensus private blockchain –Threats of forgery, counterfeit of pricing emotion value
VEmoSPACE	–Provide online space for emotion-based services –Allow request, transaction, necessary emotion information search within the space –Guarantee dynamic user changes, emotion information eligibility	–Identification of accessing users –Secure access control with possible anonymity –Efficient space maintenance for users and emotion information updates
VEmoPROPERTY	–Pricing of emotion information –Allow users to receive services using it	–Strict, fair pricing schemes –Reliability to be received for guaranteed services using it
VEmoPARTY	–Share own emotion information and history with anonymity –Participate in *VEmoTRANSACTION* as information provider for paid sharing	–Detection of selfish *VEmoPARTY* –Low computation overhead to prevent impersonation attack
VEmoREQUESTER	–Request specific emotion type at specific region –Participate in *VEmoTRANSACTION* as information requesters for paid sharing	–Prevention of fake request –Improved privacy of *VEmoREQUESTER*
VEmoTRANSACTION	–Paid sharing between *VEmoREQUESTER* and *VEmoPARTY* –Connects incentives to *VEmoPROPERTY* with anonymity	–Efficient transaction history maintenance and access allowance with anonymity –Improved reliability of transaction history

TABLE 1. Description and summary of key components.

QUESTER with anonymity to *VEmoSPACE*. The second option is to pay the emotion information of *VEmoPARTY* using its own *VEmoPROPERTY*. It follows that after *VEmoREQUESTER* presents its own requesting conditions and requirements for target emotion information, the AI agent is able to forward the request to *VEmoSPACE* as well as to search for possible matching emotion information of *VEmoPARTY*. The emotion information could have different values originally according to the shared time period and location, and the amount of paid *VEmoPROPERTY* might be various. The matching or pricing standard can also be decided between *VEmoREQUESTER* and *VEmoPARTY*, or there may be a given standard for emotion value pricing in *VEmoSPACE* initially. Then, based on the pricing standard, the emotion information sharing transaction, referred to as *VEmoTRANSACTION*, can be completed. Moreover, if *VEmoREQUESTER* requests the emotion information of multiple parties, the group information of *VEmoPARTY* can be shared and taken by *VEmoREQUESTER*.

On the other hand, our *AI-VEmoBLOCK* deliberates on public blocks and private blocks. For a public block, after *VEmoREQUESTER*'s request and the paid amount of *VEmoPROPERTY*, a user can access *AI-VEmoFLOW* and *AI-VEmoMAP* with different access levels that were generated at previous subsystems. Thus, such an access record is stored as public block. For a private block, it represents the process between *VEmoREQUESTER* and *VEmoPARTY* allowing private access into *VEmoSPACE* and its *VEmoTRANSACTION*. Therefore, the process information is also considered as a private block.

Research Challenges and Security Issues

Now, we deal with critical research challenges and security issues for the proposed systems.

Research and Security Issue 1: It has been known that there are two types of blockchain: public blockchain and private blockchain. While any person is able to read, write, and access a public blockchain system, a private blockchain may require permissions, and then only a few or multiple members can access the private blockchain system. Depending on the system requirements or application goals, two different blockchain systems can be applied to our *AI-VEmoBLOCK*, respectively. However, we may have additional critical issues. On one hand, if we consider public blockchain for *AI-VEmoBLOCK*, it will cause a large amount of complexity including resource and computing time due to the mining work to reach consensus. On the other hand, if we consider applying the concept of private blockchan to *AI-VEmoBLOCK*, we have clear advantages of less required resources, faster computing time, and better scalability for consensus when compared to *AI-VEmoBLOCK* based on public blockchain. However, an exisiting consensus scheme is not appropriate for PoA within *AI-VEmoBLOCK*. Hence, the issue of efficient, scalable consensus schemes fitting with PoA for both public blockchain and private blockchain should be investigated.

Research and Security Issue 2: When the *AI-VEmoBLOCK* is implemented, the AI agent for every edge device can manage several processes or issues for storing detected emotion information, posting the shared portion of *VEmoREQUESTER*, sustaining *VEmoTRANSACTION*, maintaining private *VEmoPROPERTY*, and so on. In the system, the virtual emotion information and each *VEmoPROPERTY* can be attacked by malicious attackers. Then the compromised AI-enabled edge devices by malicious attackers will cause serious security problems so that those penetrators may tamper with the virtual emotion information and *VEmoPROPERTY*. Also, some critical identities or information for *VEmoTRANSACTION* within the compromised devices can be derived or tampered with by malicious attackers. Hence, if the system has the compromised AI-edge devices, the compromised information should be detected as well as the integrity and confidentiality of information covering *VEmoPROPERTY*, and *VEmoTRANSACTION* should be sustained continuously.

Furthermore, we have to handle secure access control such that an AI-enabled edge device can access *VEmoSPACE* with anonymity. In particular, because anyone can access *VEmoSPACE* if we apply public blockchain, the secure access control with an AI-based efficient permission scheme should be considered toward secure, sustainable, efficient *AI-VEmoBLOCK* implementation.

Research and Security Issue 3: When *VEmoPARTY* uploads its own virtual emotion information in an encrypted manner to *VEmoSPACE* after deciding the amount of sharing emotion information, the integrity of the original virtual emotion information should be ensured because the information can be hijacked with forgery by malicious attackers. Also, the privacy of *VEmoPARTY* should be protected with complete anonymity and the *VEmoPARTY* of virtual emotion information should be authenticated with low computation overhead to prevent impersonation attack. Furthermore, the system should detect the selfish *VEmoPARTY* or the suspect edge device if those selfish devices within *VEmoPARTY* pretend that their own virtual emotions are more valuable to increase the rewarding or incentive value when it is uploaded to *VEmoSPACE* for paid sharing. Therefore, we not only have to verify those selfish devices but also need to predict future selfish devices' misbehaviors by considering how to utilize AI-based and machine-learning-based techniques to solve those new critical issues in the proposed *AI-VEmoBLOCK* system.

On the other hand, reasonable policies for estimating virtual emotion information should be discussed because the value of virtual emotion information can be different and be affected by various factors such as shared emotion information period, location, shared emotion type, and number of *VEmoREQUESTER*s. For example, when there are a large number of competing *VEmoREQUESTER*s seeking specific emotion information type, the information value within *VEmoPARTY* can be increased. Then *VEmoREQUESTER* who suggests the best value can obtain the requested information, and the incentive value will be distributed immediately as *VEmoPROPERTY* to users who provide the satisfied emotion information.

Concluding Remarks

In this article, we introduce an integrated virtual emotion system, *I-VEmoSYS*, from an AI perspective. As its conceptual subsystems, we propose two different subsystems. On one hand, as the first subsystem, we introduce promising AI-enabled *AI-VEmoBAR*, *AI-VEmoFLOW*, and *AI-VEmoMAP*, respectively. Then, we describe how they are operated in the system, and deal with their critical security challenges and issues. On the other hand, we propose the creation of *VEmoPROPERTY* and designed a *AI-VEmoBLOCK* as the second subsystem. Then we suggest their security issues and discuss possible solutions toward secure CPS-enabled advanced smart cities. As future works, we plan to develop and implement the proposed model in practical settings and scenarios based on the contributed conceptual components, activities, and roles.

References

[1] R. Baheti and H. Gill, "Cyber-Physical Systems," *The Impact of Control Technology*, 2011, pp. 161–66.

[2] L. Zhao *et al.*, "Optimal Edge Resource Allocation in IoT-Based Smart Cities," *IEEE Network*, vol. 33, 2019, pp. 30–35.

[3] H. Ko and S. Pack, "Neighbor-Aware Energy-Efficient Monitoring System for Energy Harvesting Internet of Things," *IEEE Internet of Things J.*, vol.6, 2019, pp. 5745–52.

[4] R. Chow, "The Last Mile for IoT Privacy," *IEEE Security and Privacy*, vol. 15, 2017, pp. 73–76.

[5] Z. Hong *et al.*, "Attacker Location Evaluation-Based Fake Source Scheduling for Source Location Privacy in Cyber-Physical Systems," *IEEE Trans. Info. Forensics and Security*, vol .14, 2019, pp. 1337–50.

[6] Z. Zeng *et al.*, "A Survey of Affect Recognition Methods: Audio, Visual, and Spontaneous Expressions," *IEEE Trans. Machine Intelligence*, vol. 31, 2009, pp. 39–58.

[7] M. Zhao, F. Adib, and D. Katabi, "Emotion Recognition Using Wireless Signals," *Proc. ACM MobiCom*, 2016, pp. 95–108.

[8] H. Kim *et al.*, "A Framework for IoT-Enabled Virtual Emotion Detection in Advanced Smart Cities," *IEEE Network*, 2019.

[9] M. Frutos-Pascual and B. G. Zapirain, "Review of the Use of AI Techniques in Serious Games: Decision Making and Machine Learning," *IEEE Trans. Computational Intelligence and AI in Games*, vol. 9, 2017, pp. 133–52.

[10] W. Wang *et al.*, "Device-Free Human Activity Recognition Using Commercial WiFi Devices," *IEEE JSAC*, vol. 35, 2017, pp. 1118–31.

[11] H. Binol *et al.*, "Time Optimal Multi-UAV Path Planning for Gathering ITS Data from Roadside Units," *Proc. IEEE VTC-Fall*, 2018.

[12] S. G. Barsade, "The Ripple Effect: Emotional Contagion and Its Influence on Group Behavior," *Administrative Science Quarterly*, vol. 47, 2002, pp. 644–75.

[13] G. Zyskind, O. Nathan and A. S. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," *IEEE Security and Privacy Wksps.*, 2015, pp. 180–84.

[14] G. Jia *et al.*, "Edge Computing-Based Intelligent Manhole Cover Management System for Smart Cities," *IEEE Internet of Things J.*, 2018, pp. 1648–56.

[15] Z. Li *et al.*, "Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things," *IEEE Trans. Industrial Informatics*, vol. 14, 2018, pp. 3690–700.

Biographies

Hyunbum Kim (kimh@uncw.edu) received his Ph.D. degree in computer science from the University of Texas at Dallas in 2013. He is currently an assistant professor in the Department of Computer Science at the University of North Carolina at Wilmington. His research interests include algorithm design and performance analysis in various areas including the Internet of Things, intelligent computing, virtual emotion systems, unmanned aerial vehicles, smart cities, next generation systems, and cyber security.

Jalel Ben-Othman (jbo@l2s.centralesupelec.fr) received his Ph.D. degree from the University of Versailles, France, in 1998. He is a full professor at the University of Paris 13. His research interests are in the areas of wireless ad hoc and sensor networks, broadband wireless networks, the Internet of Things, and security in wireless networks in general and wireless sensor and ad hoc networks in particular. His work appears in highly respected international journals and conferences.