IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 2, 2021, accepted September 3, 2021, date of publication September 7, 2021,
date of current version September 15, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3110762

Privacy Preservation of User Identity in Contact Tracing for COVID-19-Like Pandemics Using Edge Computing

MOHAMMED ABDULLAH ALSAHLI[1], AHMED ALSANAD[2], MOHAMMAD MEHEDI HASSAN[1], (Senior Member, IEEE), AND ABDU GUMAEI[2,3]

[1]Department of Information Systems, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[2]STC's Artificial Intelligence Chair, Department of Information Systems, College of Computer and Information Sciences, King Saud University, Riyadh 11451, Saudi Arabia
[3]Computer Science Department, Faculty of Applied Sciences, Taiz University, Taiz 6803, Yemen

Corresponding authors: Mohammed Abdullah Alsahli (mohmmad1024@gmail.com) and Ahmed Alsanad (aasanad@ksu.edu.sa)

The authors are grateful to the Deanship of Scientific Research, King Saud University for funding through Vice Deanship of Scientific Research Chairs. The authors thank the Deanship of Scientific Research and RSSU at King Saud University for their technical support.

ABSTRACT Pandemic and infectious disease outbreaks put pressure on health authorities and require lockdowns. These outbreaks, which strain limited healthcare resources, must be swiftly controlled and monitored. A large number of healthcare authorities are currently investigating automated systems to support outbreak monitoring and control. However, current contact tracing systems face many privacy, participation, and power constraints. Furthermore, elderly or less financially able individuals often cannot participate in automated contact tracing due to not owning a smartphone. This paper proposes a new system that enables health authorities to track exposure among individuals participating in the automated system, aid health authorities in interviewing non-participating individuals, and minimize the processing required by offloading to nearby edge computing devices. The proposed system utilizes edge servers to assist health authorities in tracking users who withdraw from or are unable to use contact tracing. Edge computing devices have access to more contextual information, resulting in minimal data collection and thus enabling businesses, houses, and offices to participate in contact tracing as locations. Edge computing devices enable location-based data collection of contact tracing data using proximity-based sensors for offices, homes, and shops, thereby assisting health authorities to notify users of exposure without disclosing the identities of businesses or individuals. Moreover, the proposed system reduces the overall power for end users up to 97% by delegating contact tracing to nearby edge computing devices. In addition, the system mitigates data poisoning attacks that target individuals' smartphones, edge devices, or cloud servers by utilizing blockchain to store contacts, delegations, and identities.

INDEX TERMS Edge computing, infectious diseases, COVID-19, blockchain, pandemic contact tracing.

I. INTRODUCTION

Pandemic management overwhelms government and healthcare systems and requires them to have quick and targeted actions. The most effective method is to quarantine persons and their contacts who may have been infected by the virus [1], [2]. Health authorities and governments enforcing the quarantine of infected and exposed individuals is the most effective tool in treating infectious diseases [1]. However, individuals may not comply with health authorities' quarantine requests [1], [3]. For example, in Hong Kong, during the SARS outbreak, police found half of the quarantined individuals were missing or at large, breaking the mandated quarantine [3]. Therefore, large-scale enforcement and compliance are required to deal with COVID-19-like pandemics. In this regard, the Singapore Ministry of Health [4] employed 200 officers at the peak of the outbreak to identify all contacts of SARS cases. The purpose of such contact tracing is first to gather data on infected patients' movements and identify contacts with other people and then to follow

The associate editor coordinating the review of this manuscript and approving it for publication was Dominik Strzalka.

up with infected and exposed individuals to ensure quarantine compliance. However, this process is overwhelming for health professionals, particularly when patients cannot accurately recall all contacts whom they may have met in the incubation period of the virus [1], [2].

Pennsylvania reported a 72% success rate for manual contact tracing COVID-19 cases using patient data available in the electronic health records to communicate with infected patients [5]. However, a significant number of people were not reachable due to incorrect phone numbers or a lack of alternate means of contact [5]. Additionally, many researchers have identified issues with manual contact tracing, such as inefficient paper-based reporting systems, delays that prolong the time from contact detection to quarantining of suspected cases, and exhausted health authority resources [1], [2], [5]. Nevertheless, individuals may not participate in contact tracing process or comply with quarantine orders for a plethora of reasons, especially if they are financially or socially affected [6]. Therefore, health authorities and researchers began developing automated applications for contact tracing to report and monitor active cases and infection risks efficiently [7], [8]. The applications enabled them to collect information using different sensors to calculate infection spread and gather contacts for users. Thus, contact tracing applications began collecting users' exact locations, proximity to other users, or a combination of both [7], [9]. Accordingly, automated applications are aimed at detecting the proximity and duration of users within a given range [10]. However, collected raw data from Global Positioning System (GPS), Wi-Fi, Bluetooth Low Energy (BLE), and cellular networks need infrastructure to store and process data to trace and report contacts [7], [9], [10]. Google [11] and Apple [12] have thus published integrated Application Programmer Interfaces (APIs) into their mobile operating systems using BLE. Additionally, application developers are responsible for maintaining the infrastructure to store, process, or assist in processing. These developers build their processing and storage infrastructure according to centralized, decentralized, and hybrid architectures [5], [7]. Centralized contact tracing applications must be registered to central servers that provide temporary IDs frequently and receive user-uploaded data. Then, the central server notifies users if there is a risk of exposure. However, the central servers (assumed as trusted) have access to all data and are able to link that data to users' identities even if no exposure is detected, which raises privacy issues [6], [7]. On the other hand, decentralized contact tracing applications do not necessarily require registration, and they generate a random token string called seed utilized in a pseudorandom function to generate string tokens called chirps periodically. Then, the user's application uploads the seed to a central server that others can download to detect whether they are have been in contact with infected users. However, the end user's smartphone is required to process published seeds on a daily basis, demanding more resources and battery for redundant processing of exposure risk, which makes users reluctant to adopt decentralized applications [6], [7]. Finally, hybrid contact tracing applications keep the generation of temporary identity locally and offload the exposure risk analysis to central servers, thereby reducing the required processing on local smartphones [6], [7].

However, a malicious or compromised server in all architectures is able to perform many data poisoning attacks or user identification attacks by colluding with other malicious entities. In addition, malicious users may not only delete or alter uploaded data for any reason [13] but also carry out de-anonymization attacks to link users' identities to their contact tracing information [14]. Hence, attackers may be able to utilize rely, delayed replay, or poisoning attacks to compromise the whole system or a given user [7], [14]. Researchers have consequently proposed the utilization of blockchain, which is a collection of data blocks linked using cryptographic hashes to ensure that data is immutable and tamper-proof [9], [13], [15]. Additionally, the immutability of blockchain has ensured trust of shared data on decentralized applications [13], [15].

Blockchain-based data sharing has many privacy-preserving applications, especially in medical data sharing [13], [15], [16]. Thus, blockchain has mainly two variations regarding permission to append data: public permissionless blockchain and authorized permissioned blockchain [13]. On the one hand, permissionless blockchain has privacy issues, as all data blocks are shared in a distributed environment, and access is permitted to anyone [13], [16]. In addition, users are required to develop a consensus of the distributed blockchain ledger, which increases the resources required to maintain a valid blockchain [17]. On the other hand, permissioned blockchain ensures data blocks are added only from authorized users [16]. Moreover, the central authority is able to reverse updates or delete blocks without public transparency, thus requiring users' complete trust in the authority [16]. The combination of both blockchain variations is hence required to minimize the aforementioned issues [16]. Furthermore, the combination of blockchain and public-key cryptography ensures that only the user with the private key can share data blocks for that anonymous identity. Also, it enables verification of that data blocks using the user's public key [17].

Blockchain-based Public Key Infrastructure (PKI) is the utilization of public-key cryptography to sign data blocks, ensuring that all data in the blockchain is from the certificate owner [18]. Thus, it reduces the processing required for data validation for a data block without consensus with others [18]. Also, the complete sequence of data blocks can be validated using blockchain, ensuring data integrity and availability. Many researchers [13] have used blockchain as a scalable and secure data exchange, especially with 5G and edge computing. Combining blockchain with edge computing offers low latency and context-aware processing, which is suitable for medical applications [13], [19]–[21].

Edge computing is the utilization of computational and network resources in mobile and edge devices for offloading

processing from centralized or cloud servers on a larger scale [19]–[22]. Edge devices are more context-aware, which improves the accuracy of data collection on edge devices. Accordingly, offloading computing to edge computing enables applications to reduce the overall required resources and enables real-time applications [22]–[24]. The integration of edge computing and blockchain provides verifiable data storage that is scalable on different architectures [19]–[21]. In addition, edge computing technologies are utilized to secure privacy in medical applications [21].

At any automated or technical rate, not all people have access to smart or modern phones that can participate in automated contact tracing [25]. The Pew Research Center has published the results of a survey of smartphone ownership [25]. This survey indicates that 11% of adults in the US do not have smartphones; this percentage is higher among low-income individuals (19%) and people 65+ years old (29%), who are more vulnerable to pandemics. A solution is thus required to assist health authorities in their efforts to perform contact tracing of possible and indirect infections [7]. Additionally, health authorities are not considered in the design of the most automated contact tracing applications. Furthermore, neighbors separated by a physical wall may be classified as contacts in automated contact tracing [26], [27]. Besides, contact tracing may ignore indirect ways in which viruses can spread. Ultimately, contact tracing enables health authorities to help patients and users at an individual level [26], [27].

The abovementioned challenges and limitations of existing work in contact tracing motivated the solution—an automated system—proposed in this paper, in addition to our observation of contact tracing using mobile phone not being an accurate estimate of person-to-person proximation, as detailed in Section V. Additionally, promising technologies such as edge computing and blockchain offer innovative solutions and introduce limitations that motivated the proposed system to carefully mitigate them while benefiting from the technologies.

Through the proposed system, this paper primarily aims to solve the dependency on central resources, data pointing, or fake data injection attacks to contact tracing information by malicious users or compromised devices. In addition to that, minimize the risk of de-anonymization attacks by reducing the exchanged information by utilizing edge computing devices and authenticating devices using blockchain-based PKI. Additionally, assisting health authorities in the contact tracing process of users who cannot participate in automated contact tracing and enforce quarantine orders for infected individuals. Moreover, the required processing, broadcasting, and scanning for end users is large, which may affect participation in contact tracing [28]. To the best of our knowledge, the proposed system is able to ensure users' privacy in edge computing environments and assist health authorities to monitor outbreaks and ensure quarantine enforcement.

The contributions of this paper are the following:

1) Preserving users' identities in a contact-tracking application by delegating contact tracing to edge computing devices, thus reducing the number of broadcasts from users' devices.
2) Assisting health authorities in tracking users who withdraw from contact tracing applications by enabling homes', offices', and businesses' edge devices to collect contact tracing data to assist health authorities in the interview process, especially for users who do not participate in automated contact tracing. Authorities in the interview process, especially for users that did not participate in the automated contact tracing.
3) Reducing the power required for smartphones by offloading tracking and processing contact tracing to nearby edge devices.
4) Securing against data poisoning attacks by using blockchain-based PKI for verification of data exchanges and publishing data to public ledgers.

The remainder of this paper is structured as follows. Related and existing solutions for contact tracing, as well as the gap that motivated the proposal of this paper's system, are discussed in Section II, and the details of the system itself are presented in Section III. Thereafter, Section IV describes the setup used for the experiments and testing of the system, and the data and observations from the experiments show the benefits of the proposed system in Section V. Then, Section VI contains a discussion about the proposed system, data analysis, observations, and security analysis. Finally, system limitations and future directions are explained in Section VII.

II. RELATED WORKS

Promising technologies have offered solutions to different sets of challenges to control and monitor the spread of COVID-19. Hence, He *et al.* [29], Mbunge *et al.* [30], Nguyen *et al.* [17], Ahmed *et al.* [22] and Mbunge [31] have discussed the opportunities of emerging and promising technologies that offer innovative solutions to control the spread of COVID-19-like pandemics. Table 1 summarizes the promising technologies along with their general application and limitations to combat COVID-19-like pandemics. In this study, both edge computing and blockchain technologies are employed in the proposed solution.

A. EDGE COMPUTING

Edge computing improves performance by reducing latency and context awareness. By bringing efficient computing and data processing at network edge low latency sensing and processing in higher throughput. Most research on edge computing considers the offloading to edge computing devices. Debe *et al.* [32] designed a decentralized blockchain-oriented solution to deploy a reputation-based trust model for Internet of Things (IoT)-edge applications. The authors used smart contracts for client registration,

TABLE 1. Promising technologies to combat COVID-19 like pandemics [17], [29]–[31].

Technology	applications for COVID-19-like pandemics	Limitation
Artificial intelligence	• infection case analysis and prediction • early diagnosis of suspected infections • classification of risk of infection • screening for possible infection	• lack of data sharing and quality used in the learning process • privacy concerns for data collection and utilization as well as for users' consent
Big data	• analysis and assistance in large-scale data sharing and collection • enabler for artificial intelligence applications • integration of different data sources for better decision making (transportation, health records, contact tracing patterns, traffic, etc.) • real-time monitoring of conspiracies and false information on social media	• serious privacy concerns for large-scale data collection for a given user • well-established processing and communication infrastructure needed (has a higher cost of operation) • strong security and access control required
Edge computing	• low latency processing of raw data and artificial intelligence models • accurate data sensing and automated contact tracing by utilizing context awareness • higher bandwidth for raw sensors' data collection • real-time analysis and selective data uploads	• limited computing resources, and cloud computing required to store and process big data • higher development costs, as edge devices are heterogeneous
Blockchain	• cases' data authentication and validation in distributed systems • trusted, tamper-proof data structure to share case data across countries and domains • secure data from poisoning attacks and assurance of data integrity	• increased overhead processing required on public ledgers • immutable data structure that may conflict with data deletion requests

the processing devices' reputation, and credibility. However, the authors introduced non-autonomous device registration and management overhead that may not scale well on large deployments. Bhat *et al.* [33] created a comprehensive overview of different research challenges of edge computing along with security issues and current mitigations. They also identified the challenges, impact, and risks associated with integrating blockchain into edge computing. The authors identified the required processing and storage capacities for public blockchain; for instance, bitcoin only processes seven transactions per second. In addition to vulnerabilities and security threats of 51% of attacks and double-spend attacks. Moreover, the total consumption of energy is high for edge devices in a public blockchain. However, Bhat *et al.* [33] also demonstrated that permissioned blockchains significantly reduce the requirements for processing and storage. Accordingly, the authors have proposed the integration of blockchain into edge computing in the future. Ernest and Shiguang [20] proposed a privacy enhancement scheme using randomly generated public keys based on the elliptic curve cryptosystem to ensure user anonymity and message integrity. In addition, to ensure that messages are tamper-proof, the authors used blockchain by including the prior message hash with the next message. Buda *et al.* [23] proposed an edge computing-based scheme to enable a lightweight blockchain in decentralized vehicular environments. The proposed solution employed a fuzzy logic-based edge node selection approach using different factors that reduced the communication overhead. Akkaoui *et al.* [21] presented a hybrid, edge blockchain-based, distributed health-data-sharing framework to overcome the computational and storage requirements of scaling blockchain and to ensure secure and transparent medical data sharing, fulfilling the healthcare requirements using less computing and storage resources. Furthermore, the authors proposed the integration of artificial intelligence into edge computing and blockchain. Ali *et al.* [24] identified security risks and mitigations to ensure trustworthy edge computing environments. In addition, they highlighted the features of low latency, cost effectiveness, and context awareness for adopting edge computing that benefit many use cases, such as location-based services and distributed content and caching. Moreover, Ali *et al.* [24] pointed out the inherent risks in cloud computing and the additional security risks that could be mitigated using different approaches, mainly by using a hierarchical architecture to ensure security compliance. Zhou *et al.* [34] outlined the key concepts and future directions for IoT 2.0, and they detailed many enabling technologies for modern applications. Edge computing is a key enabling technology that reduces latency, thus significantly enabling many real-time applications. Adámek *et al.* [35] demonstrated the benefit of using edge computing to reduce the total power consumption of data processing. In addition, the authors demonstrated an average of 43% reduction in

power consumption by optimizing the frequency scaling of core clocks on NVIDIA A100 GPU. Sun *et al.* [36] optimized the energy efficiency of the wireless edge computing network model by proposing an energy-efficient task offloading method optimized by differential evolution. Furthermore, the authors have indicated a future improvement to resolve slight fluctuations that result from randomness differential evolution optimization. Silva *et al.* [37] proposed a queuing model to evaluate the performance of health monitoring in the context of IoHT. The evaluation included IoT sensors and edge, fog, and cloud components while estimating metrics such as mean response time, the utilization level, and message drop rate. The authors showed a significant benefit of increasing low latency processing, which reduced the arrival rate of messages and thus enabled efficient data collection.

B. BLOCKCHIAN

Blockchain technology has contributed improvements and innovations in data management in healthcare. Various published research papers have examined the potential of blockchain technology in contact tracing and medical data exchange. Ricci *et al.* [9] conducted an in-depth analysis of the utilization of blockchain in contact tracing efforts regarding COVID-19 infections. The authors identified the following general challenges that contact tracing blockchain solutions face: permissionless lower throughput, public data publishing nature and privacy of permissionless throughput, and susceptibility to Paparazzi attacks [14]. Accordingly, Ricci *et al.* [9] proposed the utilization of self-sovereign identity systems with blockchain technology that might enable private and secure systems. Hasan *et al.* [38] proposed decentralized, immutable, and tamper-proof COVID-19 contact tracing using Ethereum blockchain smart contracts. Their solution is customizable to the different requirements of various infectious diseases. However, the proposed solution requires the registration of oracles to central systems and only collects proof of location, which impose privacy issues of location-based data registration. Furthermore, Ali *et al.* [39] presented a comprehensive study of blockchain benefits, challenges, and functionalities in government, financial, manufacturing, and healthcare sectors. The authors categorized each dimension of their study, with the most important being the aspects of privacy and usability of data using blockchain in the healthcare sector. Accordingly, Ali *et al.* [39] summarized the beneficial impact of blockchain in healthcare by ensuring data sharing, quality, and integrity. However, there are challenges in utilizing blockchain in healthcare. They include interoperability with existing systems, adoption, and scalability challenges, with emphasis on the power consumption issues of using blockchain. Madine *et al.* [40] proposed a decentralized, integrated, blockchain-based, peer-to-peer file storage system to share medical data. The proposed system trusted reputations-based re-encryption proxies to ensure that data is encrypted to intended users. However, data is stored on-chain, which prevents data deletion for any reason; registration is centralized; and there is assumed trust in proxy re-encrypted oracles. Hasan *et al.* [41] proposed a blockchain-based solution to track and verify both COVID-19 tests taken and immunity passports. The proposed solution integrates proxy re-encryption schemes with peer-to-peer file storage to share users' medical information, identity, and travel information. However, the system is only usable by government agencies that require immunity for users to travel. Malamas *et al.* [42] proposed hierarchical blockchain fine-grained access control to medical data. The proposed architecture enables design policy enforcement auditing and transaction verifiability. However, the authors outlined the scalability limitation and the security balance with using the proof-of-stack public blockchain consensus algorithm. Xiang *et al.* [43] presented a permissioned, blockchain-based identity management and user authentication healthcare system, which has a lightweight computation requirement that can be applied to terminal devices. However, the presented work assumes the trust of central medical servers in addition to using public leaders, which introduces consensus overhead computing. Shala *et al.* [44] proposed a decentralized, blockchain-based trust evaluation system using a lightweight and trust-based consensus protocol. However, the proposal introduces overhead in the consensus computation that increases the total power required by the system.

C. CONTACT TRACING

Contact tracing applications employ different data and processing architectures. Many researchers and application developers have utilized proximity, location, or a combination of both. The collected data requires processing to calculate the risk of infection [7], [17], [18], but different processing architectures have varying privacy or data collection constraints. Processing architectures can be categorized mainly into centralized, decentralized, or hybrid architectures. Accordingly, the related work examined processing architecture and collected data in those areas.

Contact tracing applications utilize different types of data to calculate the risk of infection. First, location-based data (e.g., from GPS, Wi-Fi, and cellular networks) refers to the absolute location of the user at a given time [7], [9]. However, location-based data needs a substantial central server that can process thousands of data points to calculate the risk of infections. In addition, its accuracy is low, especially in cities and close spaces [7], [9]. Second, proximity-based data is able to calculate contacts on a device-to-device basis [7], [9], [11], [12]. In addition, the user's absolute location is not disclosed, and only contacts are shared with other users or central servers. However, proximity sensors go beyond physical objects by registering neighbors separated by walls as close contacts. Utilizing a combination of both location and proximity data ensures accurate risk estimation [7], [9]. Thus, BLE [11], [12] was standardized for contact tracing, as announced by Google [11] and Apple [12], and many contact tracing applications are now using the APIs provided by the two companies for Android and IOS mobile

operating systems. However, many applications are relying on those APIs with different configurations of where the processing for notification and risk calculation.

These are the centralized, decentralized, and hybrid architectures, detailed in depth in the work of Ahmed *et al.* [7]. Central servers' role determines the architecture and precisely users registration, processing infection risk, and push notifications regardless of utilized data types and structures. In a centralized architecture, the user registers their information on central servers to gain the ability to participate in automated contact tracing. Moreover, it is the most commonly used architecture due to the low cost of development and more information, especially for government-developed applications [45]. Tawakkalna [46], TraceTogether [47], CovidSafe [48], among many others [45], use a centralized architecture. However, this type of architecture has a single point of failure and faces privacy issues, as central servers are able to link users' identities and their contact tracing regardless of infection [7], [45]. In contrast, a decentralized architecture enables users to participate in contact tracing without registering on central servers; this ensures the privacy of their identities. However, users must share data with other users at scale; therefore, central servers only facilitate the exchange of contact tracing information between users. SwissCoviD [14], CovidWatch [49], COVID Safe Paths [50] are examples of systems using a decentralized architecture [7], [45]. However, users' devices have ample overhead storage and processing capacity to identify their risk of infections by downloading and process infected users' data from central servers on a daily basis [7], [45]. A hybrid architecture combines both centralized and decentralized architectures: it ensures privacy using decentralization and employs centralized servers for the processing of infection risk and notification. EpiOne [51], ConTra CORONA [52], and DESIRE [53] make use of a hybrid architecture [7]. However, on all architectures, central servers have access to shared data and play a significant role in the exchange. Thus, a malicious or compromised central server could perform user de-anonymization attacks [7]. Additionally, for users, closer computing resources exist that are not employed in the contact tracing processing architecture.

Furthermore, researchers have proposed the utilization of edge computing devices in close proximity to the user ensure privacy and eliminate the requirement for a central server [13], [54]. Whaiduzzaman *et al.* [54] presented a contact tracing framework that utilizes edge computing devices and preserves privacy by limiting the collected data and ensuring differential privacy by clustering analysis results. Vangipuram *et al.* [55] presented a framework to ensure data integrity originating from Internet of Medical Things sensors to cloud servers' processing and storage resources using edge computing gateways. Zhang *et al.* [13] utilized the edge resource in contact processing to push status only to central servers, thereby reducing the amount of uploaded data and ensuring privacy. In addition, users were able to check the risk of exposure at locations they visited using public blockchain. Similarly, Xu *et al.* [56] proposed blockchain-enabled privacy-preserving contact tracing (BeepTrace) that employs two public blockchains. Desensitize location blockchain authorizes only geo solvers to calculate the risk of infections and then pushes data to a notification blockchain that is accessed by users.

Table 2 compares our proposed solution with related work. The proposed solution ensures the privacy of a user's identity by utilizing edge computing and blockchain, and it considers elderly or low-income individuals who do not have access to contact tracing applications. In addition, the proposed solution reduces overall power consumption by utilizing a secure private delegation of contact tracing to edge devices.

III. PROPOSED METHODOLOGY

The overall system relies on a permission blockchain that contains many contacts, where each user has a ledger of blocks sorted by time intervals. Additionally, blockchains can be used to serve users on different settings using time intervals. Users can also utilize edge devices and delegate collections of contact tracing data in both home and office environments to edge servers. Figure 1 illustrates the overall system view and shows that edge servers are closer to users who are provided with many multimedia and networking services. Furthermore, internet service providers are the largest providers of edge servers for other service providers [57]. Figure 2 presents an overview of how user contacts and data are collected on the overall system. Edge devices actively participate in the contact tracing system to help reduce the amount of processing on users' smartphones. Each user broadcasts a two-part message, as depicted in Figure 3. First, the identity block with a timestamped block signs the same identity block for the user to verify both blocks. The identity block is used to defend against disk operating system attacks and poisoning attacks, and it requires an identity provider (government agency, or hospitals, a private company registered on the public ledger). Additionally, the user can generate an anonymous root identity block on a public ledger. When the user remains in a location within the edge device's coverage, they send a sync message stating the location, as shown in Figure 4. An edge server sends an additional public key to the user to verify the edge server's identity and owner. Then, the user's device sends a delegation message that includes the identity block, the delegation block, and the private key of that block. The delegation block should be shared with other devices that broadcast in the edge server's coverage, thereby reducing the number of broadcasting users. Each broadcast heard at the edge server shares an encounter list based on distance and direction, in addition to every user's delegation block in that area. This will reduce the messages that need to be sent and increase the accuracy of contact tracing, as edge servers have more power and better wireless sensors. An identity provider generates a root identity for employees and staff that can be used to generate identity blocks and then generates temp identities that can be changed

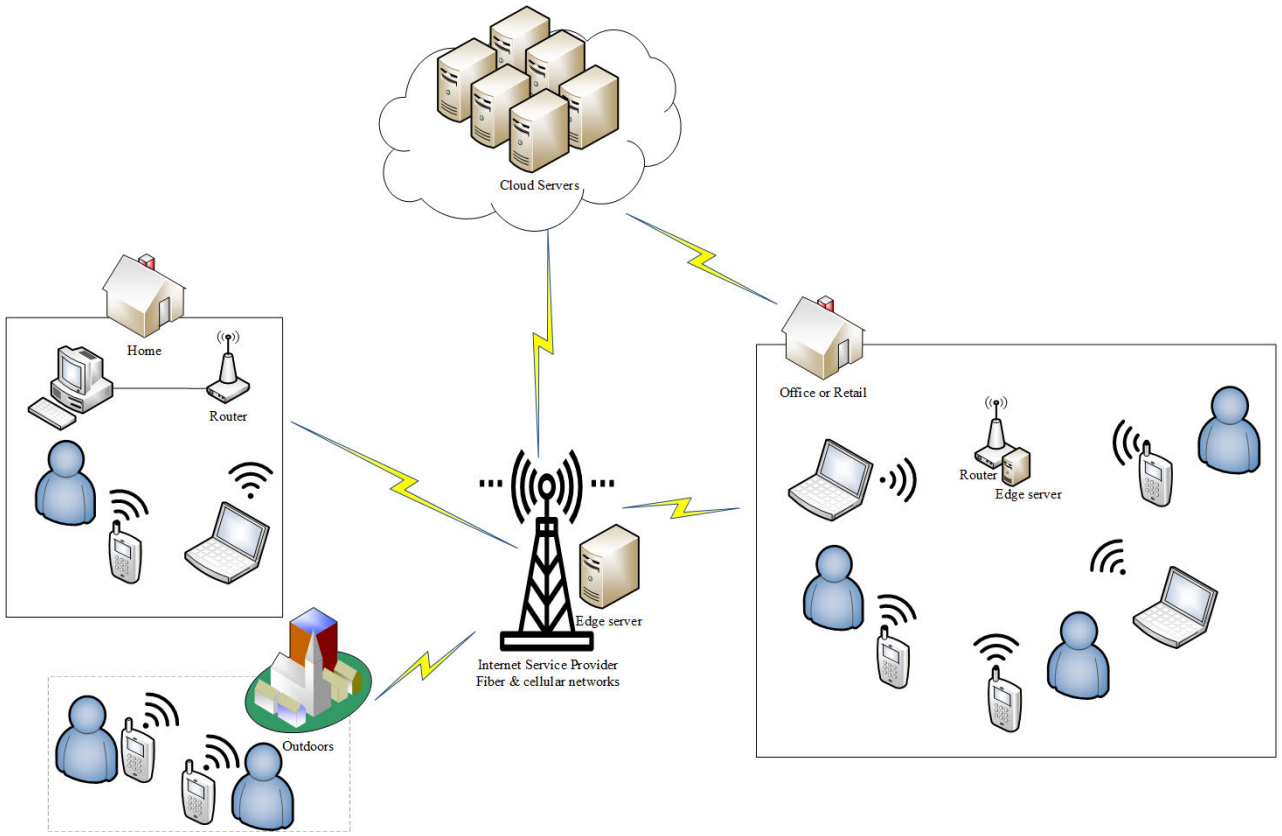

FIGURE 1. System overall overview.

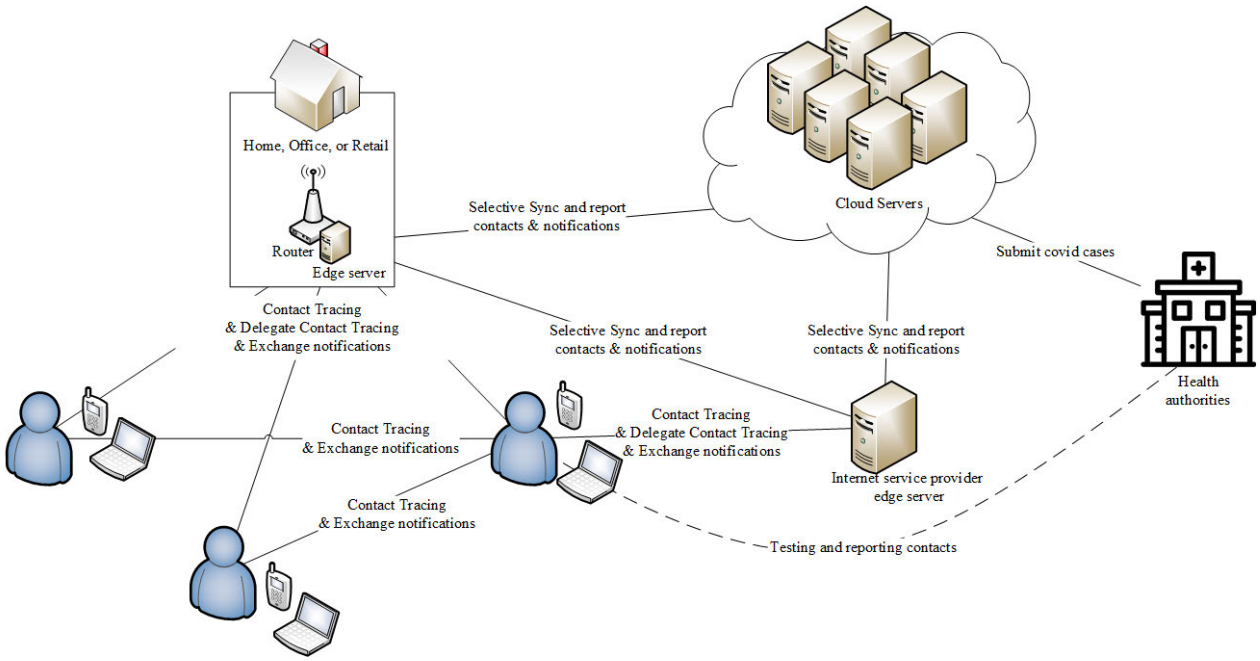

FIGURE 2. Contact tracing and exposure notification overview.

on different intervals, as depicted in Figure 5. This process enables the user's device to verify the employee's contacts. The health authorities identify the business and users affected by contacts even if the user has utilized services with indirect contacts for a given business or an employee in a given time frame. Additionally, a user can use a business identity while working, thus showing more information to health authorities to identify businesses that are heavily affected

TABLE 2. Comparison of contact tracing application and our proposed solution.

Applcaiotn/Reasearch	Processing archiatcure	Utlize Edge computing	Delegation to Edge computing	Blockchain Variant
Tawakkalna [46]	Centrlized	No	No	N/A
SwissCoviD [14]	Decentrlized	No	No	N/A
CovidWatch [49]	Decentrlized	No	No	N/A
Xu et al. [56]	Decentrlized	No	No	Public
Whaiduzzaman et al. [54]	Centrlized	Yes	No	N/A
Zhang et al. [13]	Hybrid	Yes	No	Public
Vangipuram et al. [55]	Centrlized	Yes	No	Public
Poposed solution	Hybrid	Yes	Yes	Public & Private

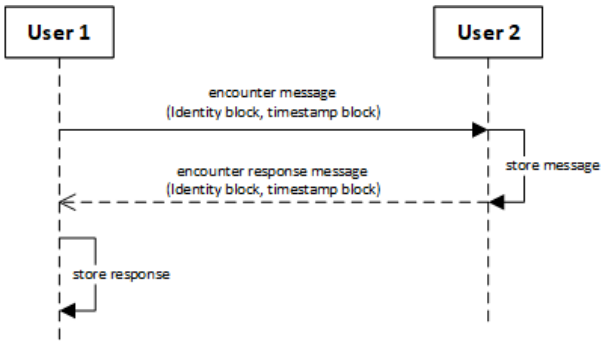

FIGURE 3. Encounter process with other users and edge servers.

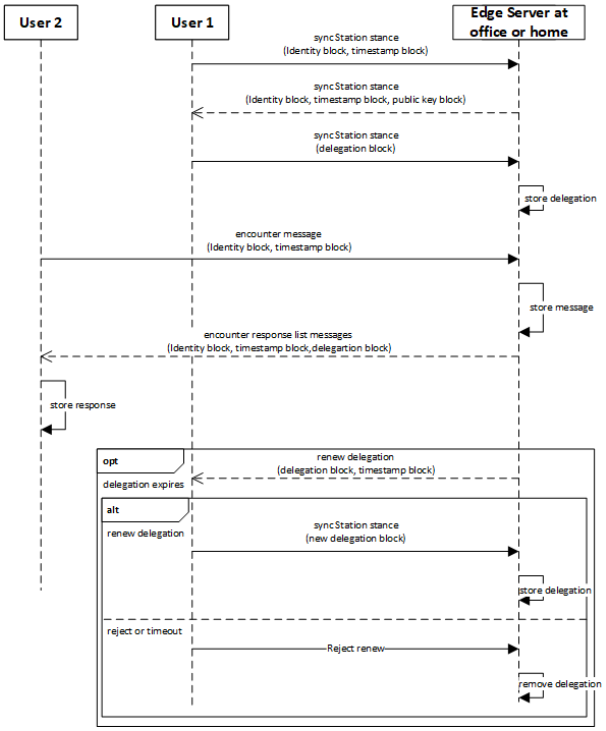

FIGURE 4. Delegation process for encounter processing.

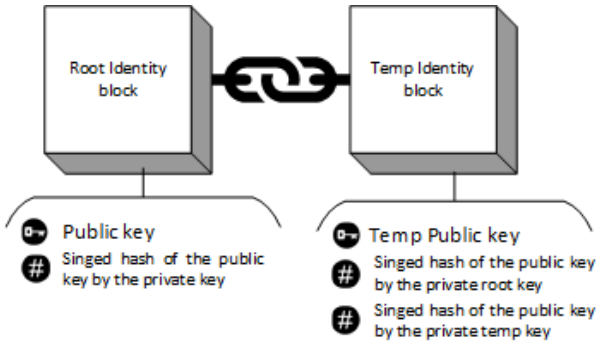

FIGURE 5. Direct identity block.

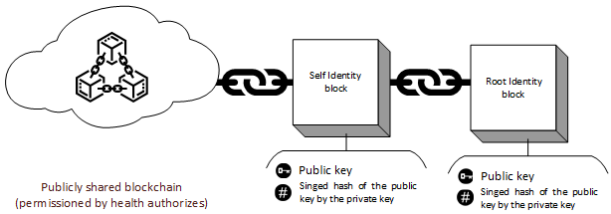

FIGURE 6. Self-generated root identity block.

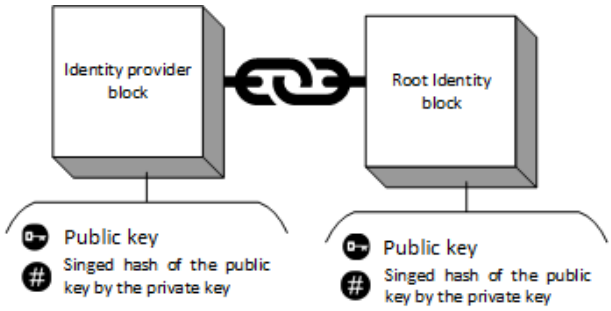

FIGURE 7. Identity provider generated root identity block.

by an outbreak rather than continuing to interview infected patients to know which businesses are affected. The identity block can be employed to generate temporary identity blocks that are used in contact tracing contacts. Figures 6 and 7 display the approaches of generating the identity block by self-generation on a public ledger and by an identity provider, respectively. Additionally, Figures 9 and 8 present the details of the data recorded in the blocks for delegation and time blocks.

IV. EXPERIMENTAL SETUP

The evaluation of the current contact tracing implementation setup took place on a Raspberry pi 4 model B using

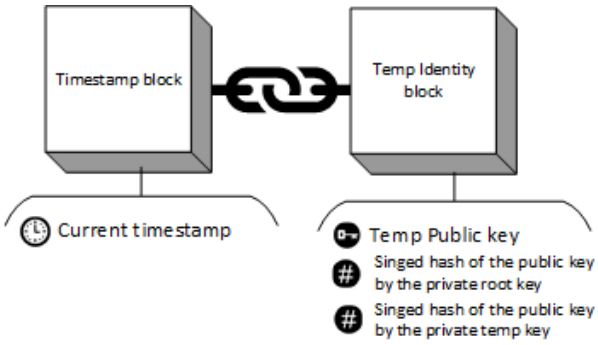

FIGURE 8. Time block.

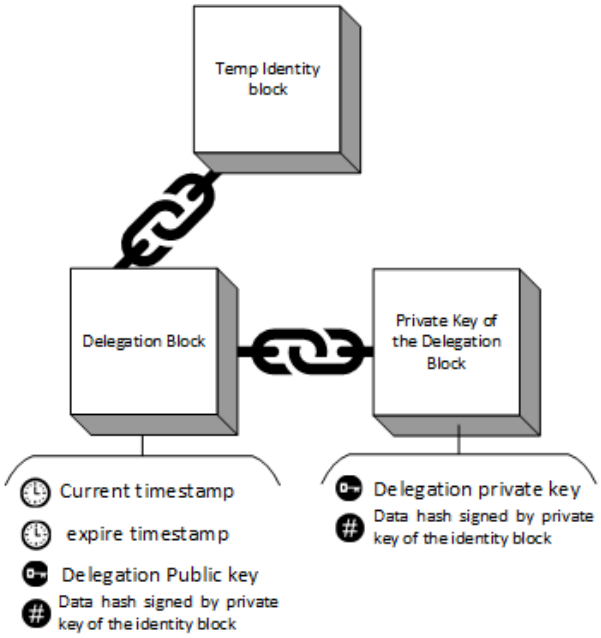

FIGURE 9. Delegation block.

Dka *et al.* [58]. We followed Google's and Apple's API recommendations for broadcasting and scanning to mainly have a rolling window of 10 to 20 min for temporary keys and broadcasting intervals between 200 and 270 ms long [11], [12]. Additionally, the two APIs represent the primary implementation of Bluetooth contact tracing on end users' devices [7], [11], [12], and each application must have its own implementation of key generation and notification management. Accordingly, two smartphones and six different Raspberry pi versions (2, 3B, and zero W) were used to broadcast in the range of Raspberry pi 4 model B. Then, all data was gathered using an Intel i5 computer connected using wired Ethernet cables to ensure that only wireless resources were used by each device in the experiment, as illustrated in Figure 10. Before each experiment for recording the consumed power and the number of broadcasts, a full central processing unit (CPU) workload was executed to calibrate all measurement devices fill heat capacity to average working

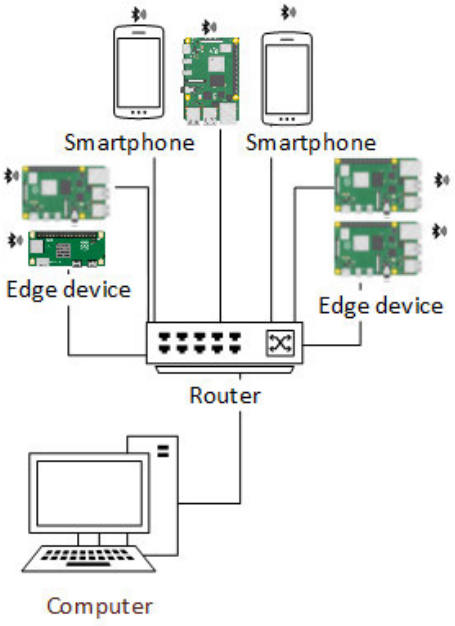

FIGURE 10. Overview of experimental setup.

temperatures ensure all experiments are performed at the same CPU and wireless processing conditions (affects power consumption and performance [59]). Regarding the number of broadcasts given, the number of users was simulated when hardware resources showed no limitation of running contact tracing implementation of Google's and Apple's [11], [12] at a large scale. Additionally, the total power consumed was measured using MakerHawk's USB power meter to collect the total current used during any part of the experiments. Additionally, the number of users to be supported by a single board computer such as the Raspberry pi 4 model B and similar in CPU and memory architecture to modern smartphones [60]. Accordingly, increasing user privacy by reducing the amount of information broadcasted from their phones and devices. Hence, the total power and the number of broadcasts confirm the privacy benefits of a reduced number of broadcasts and a reduction in the amount of power needed for the proposed solution.

V. EXPERIMENTS

Contact tracing can take place in a home, an office, or a coffee shop. Thus in our proposed system, users can delegate the contact tracing to the edge devices nearby to perform contact tracing with other peoples' smartphones, and health authorities can trace the indirect exposure on shipments and services during the time frame of an affected user (contact tracing the location). Figure 11 and Table 3 simulate the contact tracing of different intervals and delegation ratios of a particular user during the day.

The experiments required exposure notification in each scenario to show the average patterns in users' movement for contact tracing; the results have not yet been published.

TABLE 3. Number of broadcasts for each user during 24 hours in different intervals.

		broadcast interval								
		50	150	250	350	450	550	650	750	850
delegation ratio %	0.0	1,728,000	576,000	345,600	246,857	192,000	157,091	132,923	115,200	101,647
	0.1	1,536,000	512,000	307,200	219,429	170,667	139,636	118,154	102,400	90,353
	0.2	1,344,000	448,000	268,800	192,000	149,333	122,182	103,385	89,600	79,059
	0.3	1,152,000	384,000	230,400	164,571	128,000	104,727	88,615	76,800	67,765
	0.4	960,000	320,000	192,000	137,143	106,667	87,273	73,846	64,000	56,471
	0.6	768,000	256,000	153,600	109,714	85,333	69,818	59,077	51,200	45,176
	0.7	576,000	192,000	115,200	82,286	64,000	52,364	44,308	38,400	33,882
	0.8	384,000	128,000	76,800	54,857	42,667	34,909	29,538	25,600	22,588
	0.9	192,000	64,000	38,400	27,429	21,333	17,455	14,769	12,800	11,294

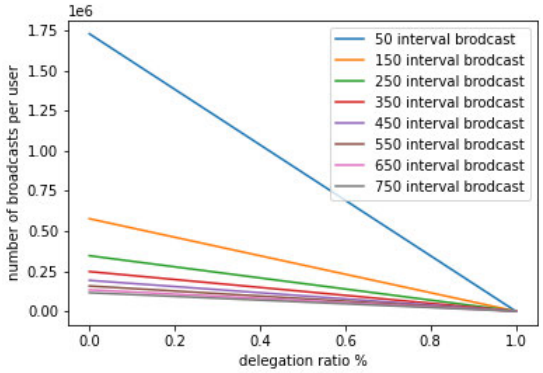

FIGURE 11. The number of broadcasts in different interval and delegation ratios.

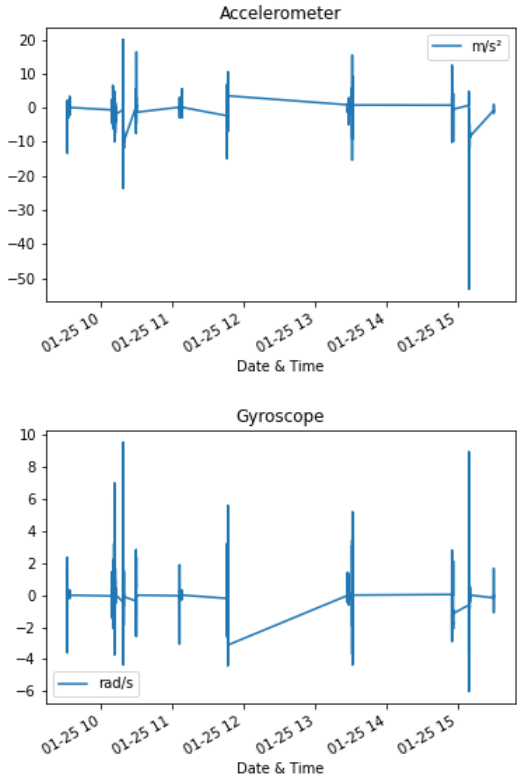

FIGURE 12. Accelerometer and Gyroscope sensors values for an office employee inside offices.

However, each advertisement has flags and universally unique identifiers, which are seven bytes. Additionally, the proposed advertisement increases in size by 70%. Instead of the full hash, the last 20 bytes or less can be shared. However, the delegation process limits the required communication between users. Most users spent most of their time at home or in the office, where available edge devices could reduce computation and communication. Additionally, users spend approximately 70% (around 16 h of sleep and work) of the day at home or in the office. Accordingly, users who change position and location should broadcast their exposure rather than broadcast on a fixed or home environment. Combining the users' smartphone motion sensors to broadcasting contact tracing information where if motion is detected, the smartphone will terminate the delegation of nearby edge devices and start broadcasting information. Once the smartphone is stationary, the smartphone is delegated to near-edge devices, as shown in Figure 4. In the experiment to investigate workers' movements in an IT office environment, where employees has different meetings with customers and colleagues, an employee installed an app to capture accelerometer and gyroscope sensor change events (device movement events), as shown in Figures 12 and 13.

The employee's smartphone moved in only 3% of the working hours, which indicates the following:

1) The employee did not take their phone to stand-up and quick one-on-one meetings.
2) The smartphone was kept on a disk while charging, which rendered contact tracing useless.

However, the proposed solution will enable health authorities to contact trace users with smartphones and delegated users (i.e., employees in offices or users at their homes), even if users do not use their phones in stores, offices, and homes. Additionally, low-energy Bluetooth broadcasts that required power are negligible compared with the processing power required for exposure notification encryption and randomization. Figure 14 illustrates the power required to run the

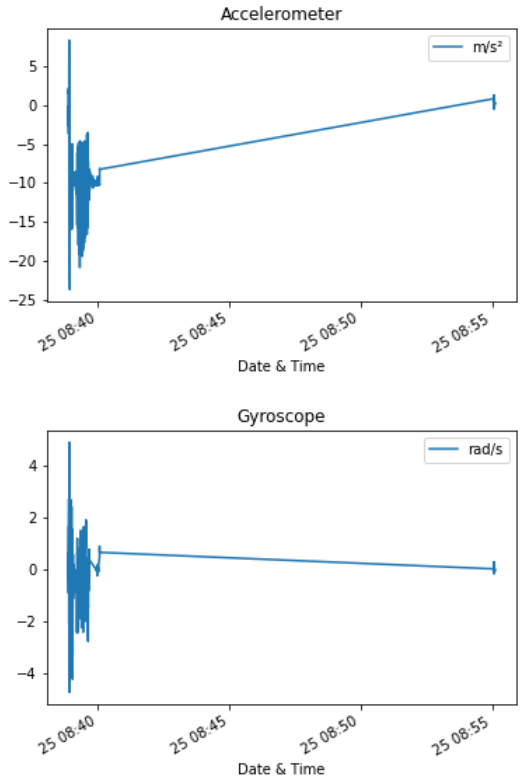

FIGURE 13. Accelerometer and Gyroscope sensors values for an office employee driving to work.

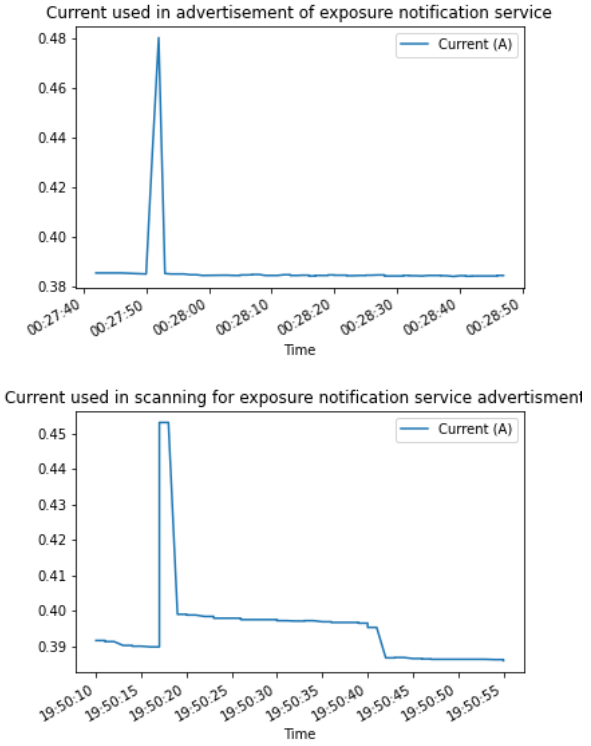

FIGURE 14. Power usage during scanning and advertisements for exposure notification using the work of Huebler [61].

exposure notification on a Raspberry pi 4 (similar architrave to modern smartphones with greater control for running applications and processes). Therefore, the proposed delegation of contact tracing reduces the overall required scanning and processing power, while assisting health authorities in tracing contacts for users who do not use exposure notification applications. Additionally, the accumulative power consumed by a large number of users participating in the exposure notification is significantly higher than that of the proposed solution, as Figure 15 shows.

VI. DISCUSSION

The proposed contact tracing system reduces the number of broadcasts from users' phones and coordinates that process to nearby edge devices. Therefore, it reduces the risk of a malicious actor following a user from home to work by using the triangulation of broadcasts. Since the user delegates the contact tracing to edge devices, physical triangulation attacks are abstracted and eliminated. Furthermore, reducing the amount of data shared to cloud servers minimizes privacy attacks on contact tracing users. user contacts who are not participating in contact tracing applications (users with no smartphones, such as elderly and poor people) by using business and home edge devices as contacts. Apart from notifying customers who utilize delivery services affect employees using that business permissioned ledger and edge devices to trace contacts and services. In this solution, contact tracing (exposure notification) is not limited to users' smartphones but includes places where fixed-position edge servers participate in the exposure notification. Additionally, delegating the processing and contact tracing to edge computing devices reduces the power and communication needs for the users of the contact tracing application. Finally, malicious actors trying to inject fake information or collect data from other users need to attack a larger surface of distributed edge devices, and public (public identities) or private (contact tracing ledger and private identities) ledgers add integrity checks to remove fake data.

A. INCLUSIVE COVERAGE

Suppose that there are four individuals: Alice, Bob, Ted, and John. Both Alice and Ted have a smartphone and are willing to utilize contact tracing applications. Bob also has a smartphone and is unwilling to participate in the contact tracing application. Last but not least, John is 70 years old and does not have a smartphone. Alice visits the pharmacy on Sunday at 9 AM and exchanges contact tracing data with the edge devices in the pharmacy. Alice then tests positive, and health authorities are assessing possible infection to others and notifying the pharmacy edge devices. Then, Ted receives a notification of possible infection due to his visit to the pharmacy at the same time as Alice. Thus, when John and Bob visit the pharmacy at 9 AM, they will not be able to receive an automated notification; however, the

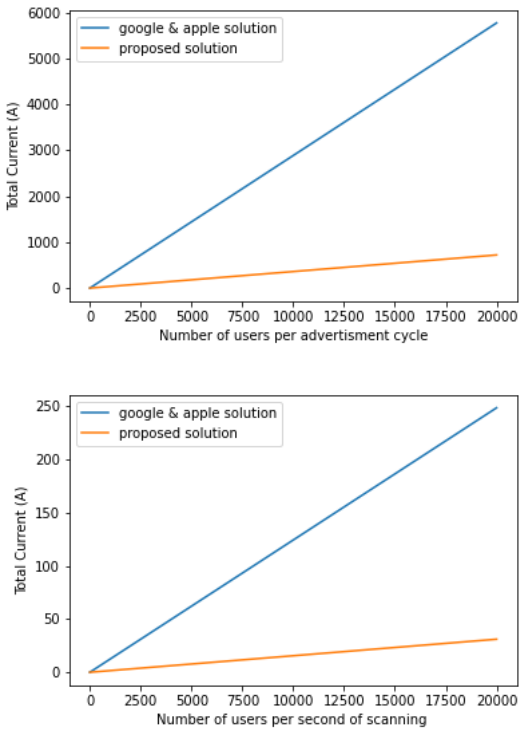

FIGURE 15. Total power used for several participating users in the exposure notification.

pharmacy administration and health authorities could notify customers at that time. Accordingly, when John visits the supermarket later that week and then later on tests positive. Hence, health authorities interview John, identify his visit to the supermarket, and notify the relevant edge devices of possible infection spread. Moreover, even though Bob is evading all lockdown measures and refuses to test for infection, Internet service providers are able to indicate the violation of lockdown measures and the possibility for Bob being within range of spreading events. At any rate, health authorities are able to collect more information and send more notifications while preserving the privacy of other users.

B. SECURITY ANALYSIS

When creating a new identity using an identity provider, the Identity Provider *IDP* generates a random pair of public E_r and private D_r keys and then creates two data blocks attached to the identity provider permission blockchain. The first block contains the private key D_r and is only sent to the user, along with a second data block containing the random public key E_r, hash signed random public key by the identity provider, private key $Sign(IDP_d, Hash(E_r))$, and private key block signed by the random private key $Sign(D_r, Hash(E_r)$. Accordingly, the temp identity (D_t and E_t) is generated using the root identity as an identity provider and carries out the same process of creating the root identity; however, the private key of the generated temporary key Dt is not shared. The delegation block consequently contains the delegation keys (D_d and E_d), which are created by following similar steps to those for generating a temporary identity block. Additionally, an expiration timestamp is added to the data block that points to the temporary block.

1) SECURITY PROPERTIES

All generated key pairs use the Rivest, Shamir, and Adleman (RSA) algorithm, whereby an attacker can factor the prime numbers of the public key. This requires an exponential amount of time and computing resources to figure out the private key in any generated keys [62]. Moreover, all shared data blocks have references to private blocks and are signed by the private keys of the identity providers to ensure user identity. Therefore, each temporary data block is signed by the private key to verify that the user owns the private key. Additionally, timestamp blocks are signed using the private key to mitigate replay attacks. Every data block in the system is signed by the private key of that block (i.e., temporary keys using temporary blocks, and the same for the delegation blocks). The signed hashes of the prior data blocks (i.e., blockchain) make the shared data immutable, thereby ensuring data integrity. Furthermore, users who are not using the private identity providers must submit a self-generated RSA key pair to a publicly shared blockchain permitted by health authorities in which the user is required to submit proof of time elapsed [63].

2) THREAT ANALYSIS

The proposed solution aims to protect against data poisoning, where an attacker can submit a list of contacts as exposure for notification services. The attacker may do this by injecting fake data or replaying captured data. An attacker can also generate a root identity; however, they cannot append data to the edge and cloud servers of possible exposure. Both the edge and cloud servers will verify the contacts, as each contact is a temporary key pair signed by a root identity block. An attacker cannot factor D_t or D_r in a non-exponential time in addition to edge and cloud servers to verify signature using public keys in the shared temporary and root identity block using Et and Er. Another attack involves identifying the user from an advertisement by locating the user physically (either using radio directional findings or listening near the home environment). In the proposed system, users delegate the exposure notification to the edge devices of homes and businesses, reducing the number of messages from their devices. For example, User A goes to work, and Attacker C tries to identify A's movements and routines. In existing exposure notifications [11], [12], User A's smartphone advertises the exposure notification process even inside their home. However, Attacker C can know if User A is inside their home by finding an existing advertisement from A's home or following the advertisement with a similar distance to A's smartphone, thus revealing A's relative location. In this proposed solution, User A's smartphone device will not advertise

inside their home or car, reducing the risk of exposing their location.

VII. CONCLUSION

In this paper, we proposed a system that preserves users' identities in a contact-tracking application, assisting health authorities with users who withdraw from contact tracing. Additionally, the proposed system is able to reduce the total power required by offloading contact tracing to nearby edge servers. Moreover, it secures against data poisoning by using blockchain to validate data exchanges in contact tracing. Preserving a user's privacy while delegating to nearby edge computing devices reduces both computing and power needs and enables authorities to notify active users of exposure to others who not actively participating in the exposure notification. In this paper, the proposed system enables health authorities to track users who do not actively participate in contact tracing and assist active users with exposure notifications. The security analysis described user identity attacks and how our system mitigates them. The security analysis also demonstrated the privacy of the delegation process and protection against exposure notification data poisoning attacks. Future improvement to the proposed work include decentralized notification management that is effective in controlling the spread of COVID-19-like pandemics. In addition, the system should be able to automatically (requiring no interview by health authorities) track people who purposefully avoid contact tracing apps. Additionally, health authorities will need to enforce the installation of apps or devices to ensure that individuals do not violate lockdowns or manipulate contact tracing data to show compliance, especially if there is a high risk of violating lockdown. These cases can be overcome by using wireless sensing [64] to cross validate contact tracing data and notify users and authorities of such issues. Additionally, denial-of-service and Sybil attacks against small edge computing devices and individual smart phones must be mitigated to ensure the availability of the exposure notification system to all users.

ACKNOWLEDGMENT

The authors would like to thank the Deanship of Scientific Research and RSSU at King Saud University for their technical support.

REFERENCES

[1] A. Wilder-Smith and D. O. Freedman, "Isolation, quarantine, social distancing and community containment: Pivotal role for old-style public health measures in the novel coronavirus (2019-nCoV) outbreak," *J. Travel Med.*, vol. 27, no. 2, p. taaa020, Mar. 2020.

[2] B. Nussbaumer-Streit, V. Mayr, A. I. Dobrescu, A. Chapman, E. Persad, I. Klerings, G. Wagner, U. Siebert, D. Ledinger, C. Zachariah, and G. Gartlehner, "Quarantine alone or in combination with other public health measures to control COVID-19: A rapid review," *Cochrane Database Syst. Rev.*, no. 9, 2020, Art. no. CD013574. Accessed: Sep. 7, 2021, doi: 10.1002/14651858.CD013574.pub2.

[3] A. Mandavilli, "SARS epidemic unmasks age-old quarantine conundrum," *Nature Med.*, vol. 9, no. 5, p. 487, 2003.

[4] P. L. Ooi, S. Lim, and S. K. Chew, "Use of quarantine in the control of SARS in Singapore," *Amer. J. Infection Control*, vol. 33, no. 5, pp. 252–257, Jun. 2005.

[5] V. Jahmunah, V. K. Sudarshan, S. L. Oh, R. Gururajan, R. Gururajan, X. Zhou, X. Tao, O. Faust, E. J. Ciaccio, K. H. Ng, and U. R. Acharya, "Future IoT tools for COVID-19 contact tracing and prediction: A review of the state-of-the-science," *Int. J. Imag. Syst. Technol.*, vol. 31, no. 2, pp. 455–471, Jun. 2021.

[6] S. Hobson, M. Hind, A. Mojsilovic, and K. R. Varshney, "Trust and transparency in contact tracing applications," 2020, *arXiv:2006.11356*. [Online]. Available: http://arxiv.org/abs/2006.11356

[7] N. Ahmed, R. A. Michelin, W. Xue, S. Ruj, R. Malaney, S. S. Kanhere, A. Seneviratne, W. Hu, H. Janicke, and S. K. Jha, "A survey of COVID-19 contact tracing apps," *IEEE Access*, vol. 8, pp. 134577–134601, 2020.

[8] R. Sun, W. Wang, M. Xue, G. Tyson, S. Camtepe, and D. C. Ranasinghe, "An empirical assessment of global COVID-19 contact tracing applications," in *Proc. IEEE/ACM 43rd Int. Conf. Softw. Eng. (ICSE)*, May 2021, pp. 1085–1097.

[9] L. Ricci, D. D. F. Maesa, A. Favenza, and E. Ferro, "Blockchains for COVID-19 contact tracing and vaccine support: A systematic review," *IEEE Access*, vol. 9, pp. 37936–37950, 2021.

[10] L. Maccari and V. Cagno, "Do we need a contact tracing app?" *Comput. Commun.*, vol. 166, pp. 9–18, Jan. 2021.

[11] *Google and Apple Jointly Created the Exposure Notifications System*. Accessed: Oct. 31, 2020. [Online]. Available: https://www.google.com/covid19/exposurenotifications/

[12] *Privacy-Preserving Contact Tracing*. Accessed: Oct. 31, 2020. [Online]. Available: https://covid19.apple.com/contacttracing

[13] C. Zhang, C. Xu, K. Sharif, and L. Zhu, "Privacy-preserving contact tracing in 5G-integrated and blockchain-based medical applications," *Comput. Standards Interfaces*, vol. 77, Aug. 2021, Art. no. 103520.

[14] S. Vaudenay, "Analysis of DP3T: Between scylla and charybdis," *IACR Cryptol. ePrint Arch.*, vol. 2020, p. 399, Apr. 2020. [Online]. Available: https://eprint.iacr.org/2020/399

[15] T. M. Hewa, Y. Hu, M. Liyanage, S. S. Kanhare, and M. Ylianttila, "Survey on blockchain-based smart contracts: Technical aspects and future research," *IEEE Access*, vol. 9, pp. 87643–87662, 2021.

[16] A. K. Pandey, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal, R. Kumar, and R. A. Khan, "Key issues in healthcare data integrity: Analysis and recommendations," *IEEE Access*, vol. 8, pp. 40612–40628, 2020.

[17] C. T. Nguyen, Y. M. Saputra, N. Van Huynh, N.-T. Nguyen, T. V. Khoa, B. M. Tuan, D. N. Nguyen, D. T. Hoang, T. X. Vu, E. Dutkiewicz, S. Chatzinotas, and B. Ottersten, "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.

[18] C. Brunner, F. Knirsch, A. Unterweger, and D. Engel, "A comparison of blockchain-based PKI implementations," in *Proc. 6th Int. Conf. Inf. Syst. Secur. Privacy*, 2020, pp. 333–340.

[19] I. V. Pustokhina, D. A. Pustokhin, D. Gupta, A. Khanna, K. Shankar, and G. N. Nguyen, "An effective training scheme for deep neural network in edge computing enabled internet of medical things (IoMT) systems," *IEEE Access*, vol. 8, pp. 107112–107123, 2020.

[20] B. Ernest and J. Shiguang, "Privacy enhancement scheme (PES) in a blockchain-edge computing environment," *IEEE Access*, vol. 8, pp. 25863–25876, 2020.

[21] R. Akkaoui, X. Hei, and W. Cheng, "EdgeMediChain: A hybrid edge blockchain-based framework for health data exchange," *IEEE Access*, vol. 8, pp. 113467–113486, 2020.

[22] E. Ahmed, A. Ahmed, I. Yaqoob, J. Shuja, A. Gani, M. Imran, and M. Shoaib, "Bringing computation closer toward the user network: Is edge computing the solution?" *IEEE Commun. Mag.*, vol. 55, no. 11, pp. 138–144, Nov. 2017.

[23] S. Buda, C. Wu, W. Bao, S. Guleng, J. Zhang, K.-L.-A. Yau, and Y. Ji, "Empowering blockchain in vehicular environments with decentralized edges," *IEEE Access*, vol. 8, pp. 202032–202041, 2020.

[24] B. Ali, M. A. Gregory, and S. Li, "Multi-access edge computing architecture, data security and privacy: A review," *IEEE Access*, vol. 9, pp. 18706–18721, 2021.

[25] *Demographics of Mobile Device Ownership and Adoption in the United States*. Accessed: Jul. 17, 2021. [Online]. Available: https://www.pewresearch.org/internet/fact-sheet/mobile/

[26] Q. Tang, "Privacy-preserving contact tracing: Current solutions and open questions," 2020, *arXiv:2004.06818*. [Online]. Available: http://arxiv.org/abs/2004.06818

[27] S. Abuhammad, O. F. Khabour, and K. H. Alzoubi, "COVID-19 contact-tracing technology: Acceptability and ethical issues of use," *Patient Preference Adherence*, vol. 14, p. 1639, Sep. 2020.
[28] V. Garousi, D. Cutting, and M. Felderer, "Mining user reviews of COVID contact-tracing apps: An exploratory analysis of nine European apps," 2020, *arXiv:2012.13589*. [Online]. Available: http://arxiv.org/abs/2012.13589
[29] W. He, Z. Zhang, and W. Li, "Information technology solutions, challenges, and suggestions for tackling the COVID-19 pandemic," *Int. J. Inf. Manage.*, vol. 57, Apr. 2021, Art. no. 102287.
[30] E. Mbunge, B. Akinnuwesi, S. G. Fashoto, A. S. Metfula, and P. Mashwama, "A critical review of emerging technologies for tackling COVID-19 pandemic," *Hum. Behav. Emerg. Technol.*, vol. 3, no. 1, pp. 25–39, 2021.
[31] E. Mbunge, "Integrating emerging technologies into COVID-19 contact tracing: Opportunities, challenges and pitfalls," *Diabetes Metabolic Syndrome, Clin. Res. Rev.*, vol. 14, no. 6, pp. 1631–1636, 2020.
[32] M. Debe, K. Salah, M. H. U. Rehman, and D. Svetinovic, "IoT public fog nodes reputation system: A decentralized solution using ethereum blockchain," *IEEE Access*, vol. 7, pp. 178082–178093, 2019.
[33] S. A. Bhat, I. B. Sofi, and C.-Y. Chi, "Edge computing and its convergence with blockchain in 5G and beyond: Security, challenges, and opportunities," *IEEE Access*, vol. 8, pp. 205340–205373, 2020.
[34] I. Zhou, I. Makhdoom, N. Shariati, M. A. Raza, R. Keshavarz, J. Lipman, M. Abolhasan, and A. Jamalipour, "Internet of Things 2.0: Concepts, applications, and future directions," *IEEE Access*, vol. 9, pp. 70961–71012, 2021.
[35] K. Adámek, J. Novotnỳ, J. Thiyagalingam, and W. Armour, "Efficiency near the edge: Increasing the energy efficiency of FFTs on GPUs for real-time edge computing," *IEEE Access*, vol. 9, pp. 18167–18182, 2021.
[36] Y. Sun, C. Song, S. Yu, Y. Liu, H. Pan, and P. Zeng, "Energy-efficient task offloading based on differential evolution in edge computing system with energy harvesting," *IEEE Access*, vol. 9, pp. 16383–16391, 2021.
[37] F. A. Silva, T. A. Nguyen, I. Fé, C. Brito, D. Min, and J.-W. Lee, "Performance evaluation of an Internet of Healthcare Things for medical monitoring using M/M/c/K queuing models," *IEEE Access*, vol. 9, pp. 55271–55283, 2021.
[38] H. R. Hasan, K. Salah, R. Jayaraman, I. Yaqoob, M. Omar, and S. Ellahham, "COVID-19 contact tracing using blockchain," *IEEE Access*, vol. 9, pp. 62956–62971, 2021.
[39] O. Ali, A. Jaradat, A. Kulakli, and A. Abuhalimeh, "A comparative study: Blockchain technology utilization benefits, challenges and functionalities," *IEEE Access*, vol. 9, pp. 12730–12749, 2021.
[40] M. M. Madine, A. A. Battah, I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi, S. Pesic, and S. Ellahham, "Blockchain for giving patients control over their medical records," *IEEE Access*, vol. 8, pp. 193102–193115, 2020.
[41] H. R. Hasan, K. Salah, R. Jayaraman, J. Arshad, I. Yaqoob, M. Omar, and S. Ellahham, "Blockchain-based solution for COVID-19 digital medical passports and immunity certificates," *IEEE Access*, vol. 8, pp. 222093–222108, 2020.
[42] V. Malamas, P. Kotzanikolaou, T. K. Dasaklis, and M. Burmester, "A hierarchical multi blockchain for fine grained access to medical data," *IEEE Access*, vol. 8, pp. 134393–134412, 2020.
[43] X. Xiang, M. Wang, and W. Fan, "A permissioned blockchain-based identity management and user authentication scheme for E-health systems," *IEEE Access*, vol. 8, pp. 171771–171783, 2020.
[44] B. Shala, U. Trick, A. Lehmann, B. Ghita, and S. Shiaeles, "Blockchain and trust for secure, end-user-based and decentralized IoT service provision," *IEEE Access*, vol. 8, pp. 119961–119979, 2020.
[45] B. Sowmiya, V. S. Abhijith, S. Sudersan, R. S. J. Sundar, M. Thangavel, and P. Varalakshmi, "A survey on security and privacy issues in contact tracing application of COVID-19," *Social Netw. Comput. Sci.*, vol. 2, no. 3, pp. 1–11, May 2021.
[46] I. Hidayat-ur Rehman, A. Ahmad, M. Ahmed, and A. Alam, "Mobile applications to fight against COVID-19 pandemic: The case of Saudi Arabia," *TEM J.*, vol. 10, pp. 69–77, Feb. 2021, doi: 10.18421/TEM101-09.
[47] H. Stevens and M. B. Haines, "TraceTogether: Pandemic response, democracy, and technology," *East Asian Sci., Technol. Soc., Int. J.*, vol. 14, no. 3, pp. 523–532, Sep. 2020.
[48] W. David, "COVIDSafe, Australia's digital contact tracing app: The legal issues," *SSRN Electron. J.*, vol. 12, no. 10, pp. 1–13, 2020, doi: 10.2139/ssrn.3591622.
[49] A. U. Morgan, M. Balachandran, D. Do, D. Lam, A. Parambath, K. H. Chaiyachati, N. M. Bonalumi, S. C. Day, K. C. Lee, and D. A. Asch, "Remote monitoring of patients with COVID-19: Design, implementation, and outcomes of the first 3,000 patients in COVID watch," *NEJM Catalyst Innov. Care Del.*, vol. 1, no. 4, pp. 1–12, 2020.
[50] *COVID Safe Paths*. Accessed: Jul. 17, 2021. [Online]. Available: https://github.com/Path-Check/safeplaces-dct-app
[51] N. Trieu, K. Shehata, P. Saxena, R. Shokri, and D. Song, "Epione: Lightweight contact tracing with strong privacy," 2020, *arXiv:2004.13293*. [Online]. Available: http://arxiv.org/abs/2004.13293
[52] W. Beskorovajnov, F. Dörre, G. Hartung, A. Koch, J. Müller-Quade, and T. Strufe, "Contra corona: Contact tracing against the coronavirus by bridging the centralized–decentralized divide for stronger privacy," 2020. [Online]. Available: https://eprint.iacr.org/2020/505
[53] C. Castelluccia, N. Bielova, A. Boutet, M. Cunche, C. Lauradoux, D. Le Métayer, and V. Roca, "DESIRE: A third way for a European exposure notification system leveraging the best of centralized and decentralized systems," 2020, *arXiv:2008.01621*. [Online]. Available: http://arxiv.org/abs/2008.01621
[54] M. Whaiduzzaman, M. R. Hossain, A. R. Shovon, S. Roy, A. Laszka, R. Buyya, and A. Barros, "A privacy-preserving mobile and fog computing framework to trace and prevent COVID-19 community transmission," *IEEE J. Biomed. Health Informat.*, vol. 24, no. 12, pp. 3564–3575, Dec. 2020.
[55] S. L. T. Vangipuram, S. P. Mohanty, and E. Kougianos, "CoviChain: A blockchain based framework for nonrepudiable contact tracing in healthcare cyber-physical systems during pandemic outbreaks," *Social Netw. Comput. Sci.*, vol. 2, no. 5, pp. 1–16, Sep. 2021.
[56] H. Xu, L. Zhang, O. Onireti, Y. Fang, W. J. Buchanan, and M. A. Imran, "BeepTrace: Blockchain-enabled privacy-preserving contact tracing for COVID-19 pandemic and beyond," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3915–3929, Mar. 2021.
[57] Z. Wang, L. Gao, T. Wang, and J. Luo, "Monetizing edge service in mobile internet ecosystem," *IEEE Trans. Mobile Comput.*, early access, Sep. 21, 2020, doi: 10.1109/TMC.2020.3025286.
[58] *Diagnosis Key Analysis*. Accessed: Jan. 12, 2021. [Online]. Available: https://github.com/micb25/dka
[59] A. M. Haywood, J. Sherbeck, P. Phelan, G. Varsamopoulos, and S. K. S. Gupta, "The relationship among CPU utilization, temperature, and thermal power for waste heat utilization," *Energy Convers. Manage.*, vol. 95, pp. 297–303, May 2015.
[60] J. C. Diehl, P. Oyibo, T. Agbana, S. Jujjavarapu, G.-Y. Van, G. Vdovin, and W. Oyibo, "Schistoscope: Smartphone versus raspberry Pi based low-cost diagnostic device for urinary schistosomiasis," in *Proc. IEEE Global Humanitarian Technol. Conf. (GHTC)*, Oct. 2020, pp. 1–8.
[61] M. Huebler. *Exposure Notification BLE Simulator*. Accessed: Jan. 28, 2021. [Online]. Available: https://github.com/mh-/exposure-notification-ble-python
[62] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.
[63] Hyperledger. *Hyperledger Sawtooth*. Accessed: Feb. 14, 2021. [Online]. Available: https://github.com/hyperledger/sawtooth-core
[64] X. Wang and L. Zhang, "Light weight passive human motion detection with WiFi," in *Proc. 6th Int. Conf. Intell. Comput. Signal Process. (ICSP)*, Apr. 2021, pp. 1310–1315.

MOHAMMED ABDULLAH ALSAHLI received the B.S. and M.S. degrees in information systems from King Saud University, Riyadh, Saudi Arabia, in 2014 and 2017, respectively, where he is currently pursuing the Ph.D. degree in information systems. In 2014, he joined Saudi e-Government Program in the digital transformation initiatives. His research interests include edge computing, cloud computing, data privacy, data standardization, AI, and big data.

AHMED ALSANAD received the Ph.D. degree in computer science from De Montfort University, U.K., in 2013. He is currently an Associate Professor with the Information System Department and the Chair Member of pervasive and mobile computing with CCIS, King Saud University, Riyadh, Saudi Arabia. He has authored or coauthored more than 12 publications, including refereed IEEE/ACM/ Springer journals, conference papers, and book chapters. His research interests include cloud computing, health informatics, ERP, and CRM.

MOHAMMAD MEHEDI HASSAN (Senior Member, IEEE) received the Ph.D. degree in computer engineering from Kyung Hee University, South Korea, in 2011. He is currently a Professor with the Department of Information Systems, College of Computer and Information Sciences, King Saud University (KSU), Riyadh, Saudi Arabia. He has authored or coauthored more than 260 publications, including refereed journals (more than 218 SCI/ISI-indexed journal articles, more than four ESI highly cited articles, and one hot article), conference papers, books, and book chapters. His research interests include cloud/edge computing, the Internet of Things, artificial intelligence, body sensor networks, big data, mobile computing, cyber security, smart computing, 5G/6G networks, and social networks. He was a recipient of several awards, including the Best Conference Paper Award from CloudComp Conference, in 2014; the Excellence in Research Award from CCIS, KSU, in 2015 and 2016; the Best Journal Paper Award from the IEEE Systems Journal, in 2018; the Distinguished Research Award from CCIS, KSU, in 2020; and the Best Conference Paper Award from the IEEE International Conference on Sustainable Technologies for Industry 4.0, in 2020. He is listed as one of the top 2% scientists of the world in the networking and telecommunication field.

ABDU GUMAEI received the Ph.D. degree in computer science from King Saud University, Riyadh, Saudi Arabia, in 2019. He was a Lecturer with the Department of Computer Science, Taiz University, Yemen, and taught many courses, such as programming languages. He is currently an Assistant Professor with the College of Computer and Information Sciences, King Saud University. He has authored or coauthored more than 30 journal and conference papers in well-reputed international journals. He received a patent from the United States Patent and Trademark Office, in 2013. His research interests include software engineering, image processing, computer vision, machine learning, networks, and the Internet of Things.