TollsOnly Please – Homomorphic Encryption for Toll Transponder Privacy in Internet of Vehicles

Hassan Karim, *Member, IEEE,* and Danda B. Rawat, *Senior Member, IEEE*

***Abstract*—Cities have circumvented privacy norms and deployed sensors to track vehicles via toll transponders (like E-Zpass tags). The ethical problems regarding these practices have been highlighted by various privacy advocacy groups. The industry however, has yet to implement a standard privacy protection regime to protect users' data. Further, existing risk management models do not adequately address user-controlled data sharing requirements. In this paper, we consider the challenges of protecting private data in the Internet of Vehicles (IoV) and mobile edge networks. Specifically, we present a privacy risk reduction model for electronic toll transponder data. We seek to preserve driver privacy while contributing to intelligent transportation infrastructure congestion automation schemes. We thus propose TollsOnly, a fully homomorphic encryption protocol. TollsOnly is expected to be a post-quantum privacy preservation scheme. It enables users to share specific data with smart cities via blockchain technology. TollsOnly protects driver privacy in compliance with the European General Data Protection Regulation (GDPR) and the California Consumer Privacy Act.**

***Index Terms*—IoV Privacy, Mobile Cyber Physical System, Homomorphic Encryption, Vehicle Data Privacy, Toll Data Privacy.**

I. Introduction

Companies, governments and consumers claim ownership of data generated by vehicles in Internet of Vehicles (IoV). Specifically, they claim ownership of the data sent by electronic transponders like those used in electronic toll collection (ETC) systems. Most ETC's leverage international standards such as ISO/IEC 18000-63 [3], [24] and E-Zpass, NationalPass in North America. These ETC systems are intended to make toll collection easy and reduce congestion on toll based roads. However, these transponders transmit sensitive data that could be correlated to a user and track a driver's location since they are often interrogated at more than just toll booths. For example, in New York City, it was discovered that vehicle-to-infrastructure (V2I) road side units (RSU) were distributed throughout the city and probed the toll transponders that users thought were used only at toll booths [35]. This led to demands for solutions by privacy advocates [20]. Several compounding issues have motivated this research. First, US federal law [2] made interoperability of ETC's mandatory in July 2016. As a result, several US state agencies issued requests for proposals (RFP's) including [23] [41] [42] for transponder toll systems that could collect and share data. They mandated compliance with the 6C Toll Operators Coalition (6C TOC) AVI Transponder Programming Standard [3] which explicitly provides no encryption. The European Union has mandated privacy-by-design in their GDPR [11]. The US state of California Consumer Privacy Act (CCPA) mandated that users be able to control their data [59] in IoV [52]. Thus, this research sought to find an engineering solution that reduced privacy risk, met regulatory requirements, and enabled users to control how their toll data was shared.

We leverage the Homomorphic Encryption (HE) as a privacy-preserving security solution for possible post-quantum protection. The security of prevailing encryption schemes like ECDSA [25] and RSA [54] are expected to be reduced in lieu of cryptanalysis attacks that leverage quantum computing [7].

Ideal-lattice based HE cryptography, [21], some might argue, is overkill to use since it is so computationally heavy. This argument holds some credence considering that other privacy invading techniques like cameras and license plate readers persist. However, toll tags are unique in that they carry data with them about where the driver has been. Data written to the last toll field in toll tags can be used to track a user. Further, considering that people rarely "upgrade" their toll tags, key management in a lighter crypto solution would still be an unmanaged issue. If an attacker with quantum computing was able to data mine toll tag data collected via a rogue reader, a map could be made of not just where the rogue readers exist, but where drivers had been. Thus a post-quantum solution is required.

In this paper, our technical contributions are as follows: a) we propose a novel privacy risk assessment model that can be used to validate the efficacy of privacy in the Internet of Vehicle and sharing controls in toll transponders; b) We validate the proposed model by demonstrating the extent to which risk is reduced with varying levels of encryption up to lattice-based [21] fully homomorphic encryption (FHE) [15] as implemented with the Palisade library [7], [10]. We present TollsOnly as a technique for transponder owners to anonymize transponder data with post-quantum cryptography while still contributing to the local traffic management regime; and c) Lastly, we introduce a method to enable drivers to share their data in accordance with laws like [59] enabling them to monetize their driving data. Furthermore, We developed an objective rating system with a good Risk Assessment Model for privacy of toll data (RASM), Driver Privacy Protection (DPP) and Driver Controlled Sharing capabilities (DCS), we assign an integer between 0 and 5. When an approach meets all of the criteria, the following values are achieved $RASM = 5$, $DPP = 5$, and $DCS = 5$ and 0 otherwise.

Authors are with the Department of Electrical Engineering and Computer Science at Howard University Washington DC, USA. Email: db.rawat@ieee.org

The remainder of this paper is organized as follows: In Section II, we describe a typical system model. Section III presents the proposed TollsOnly solution. In Section III, we present related work. Section IV presents the proposed privacy model followed by FHE in TollsOnly. We present numerical results in Section V. Finally, Section VI concludes the paper.

II. System Model

A. Typical Electronic Toll Collection (ETC) System

This research focuses on a variant of vehicle-to-infrastructures, V2I. We target transponder systems that use UHF RFID as defined by ISO 18000-63 [24] and the EPC UHF Gen2 Air Interface Protocol [17]. We concentrate on the security of the data transmitted by 6c compliant transponders [3]. The 6c standard is specifically called out in most ETC deployments in the North America today.

6c systems operate in the 902-960 MHz radio frequency range which transmits enough energy to power up transponder tags when they come within range of a reader (interrogator). That is, the power radiated towards the transponder (forward link) causes it to power up and begin broadcasting its data (Fig. 1) to any reader in range via its reverse link. Typical tags have no energy and thus are designed to be activated only within a short range (from 7 to 12 meters) from the reader. Externally powered tags are able to be read from even as far as 25 meters [19].

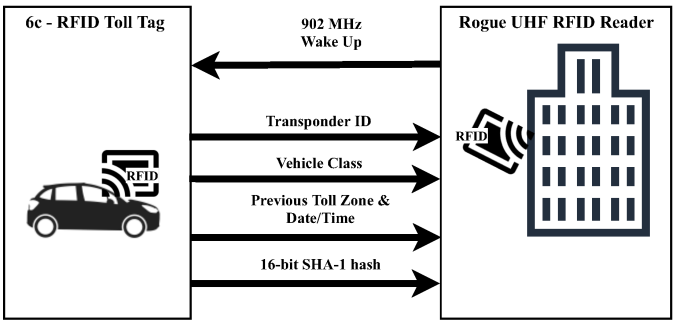

Fig. 1. Current State: Rogue tag reader steals private data

B. Sensitive Data

The data transmitted from the tag includes multiple unique pieces of data that can be used to track a vehicle and can be correlated to vehicle owner:

- Transponder ID (TID): a unique 64-bit transponder id
- 28-bit transponder serial number: comprised of 268 435 456 possible pre-defined values
- 16-bit SHA-1 hash: used to validate that vehicle description data (unique item identifier) that contains the transponder serial number is unchanged
- Previous Toll Zone and read/write date/time (PT and Time)

C. Target Problems

Fig. 1 shows the current tag reader infrastructure enables easy compromise of private toll tag data. That is, any attacker could place a UHF reader even inside a neighboring building window and send a 950 MHz (to accommodate for further distance) UHF power signal towards street traffic which would result in all toll tag data being captured. Existing risk models [28], [51] are insufficient to address risks related to toll tag collection and sharing because of the following concerns that we address in this paper:

- Transponders transmit details to any UHF reader in range, even rogue RFID readers.
- The [17] standard states that authentication is optional.
- Encryption in the 6c standard devices is explicitly not included. Thus nothing prevents any of this data from being read by any rogue actor with a reader. If encryption is enabled in any system that uses the 6c standard within the USA, it would not be interoperable, and thus violate the federal mandate. V2I readers read all data.
- UHF readers can be physically located anywhere within range
- To prevent data leakage & billing, drivers must physically hide the transponders in a RFID shielded case, like thieves [53] [8]. This method may not be practical since it requires users to remember to hide and unhide while driving.
- No known V2I deployments allow users to control with whom their data is shared and for what length of time.

III. Related Works

Privacy issues related to RFID based ETC have been well researched for decades. Only a few attempted to provide a comprehensive solution. In this section, we present related state-of-the-art approaches. One of the earliest works on RFID security [57] presents a clear category of security risks of RFID without mathematical model to assess privacy risks and did not offer a solution for user-sharing controls. In [17] the authors provide a security risk & control methodology for the risk of rogue tag readers and data leakage. Work in [29] provided a security risk & controls methodology for vehicle tracking issues. The work in [51] stated that the threat levels are relative to the proximity of a reader since RFID tags are powered by energy from the reader. Although [48] offered no risk assessment model to protect driver privacy using a somewhat homomorphic encryption commitment process. The work in [6], [48] were earliest uses cases of homomorphic encryption for V2X data where GPS data from toll data. However, the design favored the Toll controller and not the driver since the physical location of the data reader provides location of the vehicle. Thus, encrypting the GPS data in the target problem was a step in the right direction but it was not enough. Further the on-board unit they proposed still left the traceable data readable. Similarly, the work in [38] focused on preserving the privacy of toll collection locations not driver privacy. The encryption mechanism, zero knowledge proof was relative to sharing traveled segments.

In [14] toll privacy was addressed from a legal perspective. Their solution, public disclosure, addresses only the notification aspect which is in alignment with our baseline assumption of $\Omega = 3$, i.e. driver is informed of data sharing. In [26] a wide breadth of vehicle data sharing concerns was explored. The paper however only presented a blockchain-based data sharing idea. It did not provide a mathematical model or details of user-controlled data sharing, encrypting user data, or risk management.

Although the work in [27] presented a thorough distributed storage and decentralized information sharing platform, it failed to give user control of the sharing. The work in [31] presented a expiry mechanism for IoT end-to-end encryption. The [49] paper presents a method to share V2X data in general using blockchain. It addressed security controls including encryption, but it did not address privacy of toll data, nor did it present a risk reduction model. The blockchain sharing mechanism did decentralize control of the data, but it failed to put the user in control of sharing. The work in [62] presented driver privacy protection, however, it has an inherent weakness since it was designed specifically to enable the authority to trace the real identity of the toll tag and the driver. In [36], a light security and privacy framework was discussed but their solution focused on removing vulnerabilities and not directly preserving data privacy. Work in [22] proposed an innovative scoring mechanism to provide access to Industrial IoT data that is saved on a blockchain. The paper [32] approached privacy in smart devices, including toll tags, from an economic perspective. It did not offer a risk assessment. Authors of [58] presented a method to leverage homomorphic proxy-reencryption with a detailed crypto model to protect user privacy. Table IV summarizes the state-of-art review and compares the proposed TollsOnly approach in the scale of 0 to 5 for RASM, DPP and DSC.

IV. The Proposal Solution and Description

Step 1. Assess: We first define a model for current risks to gauge adherence to privacy norms, laws, and to understand what controls are required. The current risk models are not sufficient to meet TollsOnly privacy needs so we propose our own.

Step 2. Preserve: To solve the issue of toll data confidentiality, we propose TollsOnly, a tool that leverages HE to encrypt specific toll data elements and provide privacy.

Step 3. Share: TollsOnly can share some data to law-enforcement (as required by various laws), and place all data in a monetized digital twin (e.g., [37]) of the toll tag on blockchain to enable timed access to toll tag data. Table I summarizes the controls implemented with the TollsOnly solution.

The proposed privacy preserving solution and sharing model are illustrated in Fig. 2 and detailed in Sections IV-B and IV-C.

A. Privacy Risk Assessment

1) Risk Assessment Model: We approach this as a security engineering problem with a design goal of reducing risk levels.

TABLE I
Controls for Target Sensitive Transponder Data

Toll Tag Data	Proposed Protection
Transponder ID (TID)	Encrypt, store on digital twin (DT) on block chain, enable monetize timed access, securely compare to Law Enforcement Target (LETarget) with in-fog HE, share on Law Enforcement Blockchain (LEBlock)
28-bit transponder serial number	Encrypt, store on DT enable monetize timed access, securely compare to LETarget with HE, share on LEBlock
16-bit SHA-1 hash	Recompute with based on new encrypted TID. Store on DT
Previous Toll Zone and read/write date/time (PT and Time)	Encrypt, UPDATE DT and monetize

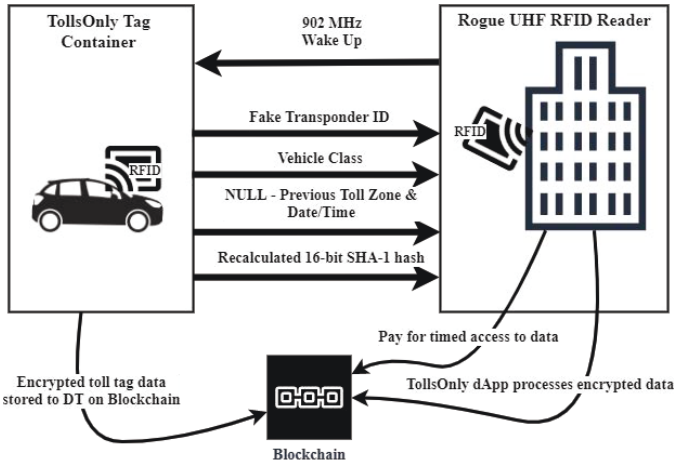

Fig. 2. Proposed: TollsOnly privatize() function saves FHE encrypted toll tag data to a digital twin on blockchain. A POCI buyer uses TollsOnly dApp to pay for access to data, and to retrieve the data using ephemeral Shared Key

We thus define the target risk as the probability, R, of a privacy breach in which the plain text tag data can be viewed by an honest-but-curious (HBC) attacker who has access to read memory or transmitted data anywhere along the transmission path. We leverage [28] as the standard information security risk equation in (1):

$$R = Impact \times Probability \times Threat \tag{1}$$

For the sake of this research, we consider the scenario where tag reader equipment is permanently deployed as infrastructure without being at legitimate toll ways, as is the case in various locations in NYC [20]. We assign a value of 1 to threat for this scenario. That is, in the context of tags, a threat exists, in which case $threat = 1$ as indicated in [51], or does not (i.e. no tag readers within range), $threat = 0$. We also assign 100% to probability in the target use case resulting in (2):

$$R = PrivacyImpact \times 100\% \times 1 \tag{2}$$

2) Privacy Impact: Considering that current European law and California law imposes heavy fines on companies that

fail to prevent privacy breaches and that fail to prevent users from being able to control their personal data, we propose that Privacy Impact, I, is a function of data type, τ; impact if privacy was breached, B; and impact if data was not shareable, Ω. To scale the resulting impact, we divide the whole result by the maximum values of each τ',B',Ω' as formally defined in (3).

$$\begin{aligned} I(\tau, \mathrm{B}, \Omega) &= \tau \times (\mathrm{B} + \Omega) \\ &= \frac{\tau \times (\mathrm{B} + \Omega)}{\tau' \times (\mathrm{B'} + \Omega')} \end{aligned} \tag{3}$$

Data Type, Breach, and Sharing Requirements: Data Type, τ, is assigned a value of $\tau = 0$ if the data contains no private data at all. We assign a value of $\tau = 1$ if the data contains location details or can be correlated to location details. $\tau = 2$ if that piece of data directly reveals identity, is correlatable to identity, or is itself raw personal biometric data that could be used to digitally represent a user, like EEG signatures. τ is formally defined in (4).

$$\tau \in \mathbb{Z} \,|\, 0 \leq \tau \leq 2 \tag{4}$$

We describe the impact of privacy breach, B, in Table II.

TABLE II
PRIVACY BREACH IMPACT

Breach Impact	Description	Example
$\mathrm{B} = 0$	No impact if breached, i.e. data is not sensitive	Transponder model number posted online
$\mathrm{B} = 1$	If data were breached, low likelihood of it correlating back to a specific driver or tracking a driver's patterns	single data point car weight posted online
$\mathrm{B} = 2$	A targeted effort with significant resources may be able to correlate some piece of data back to a subset of drivers or able to be used to track a subset of drivers driving patterns	Transponder ID, car color, Previous Toll Zone and read/write date/time posted online
$\mathrm{B} = 3$	Driver data and patterns may be discerned by an honest-but-curious admin.	GPS data, Transponder customer name stored in city database
$\mathrm{B} = 4$	Not Private. All is plaintext and might be seen and shared by anyone that stumbled upon it.	Transponder ID, Previous Toll Zone and read/write date/time, GPS data, Transponder customer Name, billing info stored in an insecure AWS container.

B is formally defined in (5).

$$\mathrm{B} \in \mathbb{Z} \,|\, 0 \leq \mathrm{B} \leq 4 \tag{5}$$

The Impact of a solution's inability to enable users to share their data, Ω, is summarized in Table III.

Ω is formally defined in (6).

$$\Omega \in \mathbb{Z} \,|\, 0 \leq \Omega \leq 4 \tag{6}$$

TABLE III
USER SHAREABILITY REQUIREMENTS

Shareability Impact	Description
$\Omega = 0$	User can control with whom and for how long data can be shared.
$\Omega = 1$	User can control with whom OR for how long data can be shared, but not both.
$\Omega = 2$	User can only control who can access the data but not for how long
$\Omega = 3$	User is informed of data sharing but the only option to prevent breach is to not use the toll tag
$\Omega = 4$	User has no control or knowledge of data sharing

3) Privacy Controls: We strive to reduce the impact of privacy breach and non-shareability to 0. Our privacy model (11), is thus a function of τ, ρ, and Ω as well as Data Transition Types, λ (7), User Control, υ(8), and Control Type, $\varkappa$ (9) where each are formerly described herein.

Data Transition Types: Data Transition Types, λ, represent the transition state of the data. This is important because different measures might be used at different states to protect the data. Although we are focused on the data-in-compute case, we define all three for completeness. We assign a value of $\lambda = 1$ if the data is stored, $\lambda = 2$ if data is in transit, i.e. being communicated over some transmission media, like the UHF frequency, or $\lambda = 3$ for data-in-compute, (7).

$$\lambda \in \mathbb{Z} \mid 1 \leq \lambda \leq 3 \tag{7}$$

User Controls: User controls, υ, represent the controllability factor required by a growing number of governments. We assign $\upsilon = 0$ if the user has no control of what data is shared. We assign $\upsilon = 1$ if the user can control which data points get shared but without any other restrictions. $\upsilon = 4$ is assigned if the user can control which data points, with whom it is shared, and for how long the data is shared. A value of $\upsilon = 5$ is assigned if the user can also assign an expiration on the data, assuming the start time to be when the data is shared. We thus give (8) as the formal definition for υ

$$\upsilon \in \mathbb{Z} \mid 0 \leq \upsilon \leq 5 \tag{8}$$

Encryption Control: Encryption Control Type, $\varkappa$, represents the strength of protection being provided. The lowest level, $\kappa = 0$, indicates that the data is raw or just encoded, as in the current state of toll tags. $\varkappa$=1 suggests that the data is protected by some simple cipher, like a Caesar cipher which is marginally better than simple encoding, but easily crackable. $\kappa = 2$ is assigned for a linear algorithm like DES [40]. $\kappa = 3$ is assigned to logarithmic algorithms like Elgamal [13] or an elliptical curve cipher (ECC), like [25], or partially homomorphic like Pallier [45]. $\kappa = 4$ is assigned if somewhat homomorphic encryption (SWHE) is employed. $\kappa = 5$ would indicate that FHE with lattice is employed. We formally describe $\varkappa$ in (9)

$$\kappa \in \mathbb{Z} \mid 0 \leq \kappa \leq 5 \tag{9}$$

Complete Privacy Controls: We thus formally express privacy controls in (10)

$$\rho\left(\tau,\lambda,\upsilon,\kappa\right)=\tau\times\lambda\left(\upsilon+\kappa\right) \tag{10}$$

And when summed with our original risk model, we derive the resulting residual risk R_r after applying the privacy controls, as expressed in (11):

$$R_r=\frac{\tau\times\left(\mathrm{B}+\Omega\right)}{\tau'\times\left(\mathrm{B}'+\Omega'\right)}-\tau\times\lambda\left(\upsilon+\kappa\right) \tag{11}$$

B. Privacy Preservation

Now that we have established the need for strong quantum safe crypto to effectively preserve toll tag owners' privacy, in this section, we describe a TollsOnly prototype that would reduce the risk of privacy breach.

1) FHE Model: We build our model on Gentry's FHE model [15] to gain multiple HE operations. We incorporate features found in CaseGHX [7], to take advantage of fast additive operations with symmetric encryption schemes that use multiple algorithms. TollsOnly is comprised of several algorithms. The FHE stack includes genKey(), a function that generates a single-use symmetric shared key (sk). We used shared secrets/shared keys since we did not want to rely on a centralized trust authority and with only a single key, greater efficiency exists over ones that needed to handle multiple key exchanges. genKey() is called twice: (1) to produce the actual key to perform the encryption, and (2) to produce a secret bootstrapping key (bk) that will be used during timed access to the data for FHE key refresh. BK will also be used for computations by 3rd parties who wish to access the private data. This process is described further in (IV-C).

The next algorithm is the encrypt function, $fheEncrypt()$, that encrypts arbitrary values like $x_1, x_2, ...,$ etc., using sk deriving ciphertext $\{x'_1, x'_2, ..., x'_n\}$ such that when $fheEncrypt(sk, (x_1, x_2, x_3, x_4, x_5))$ is ran, all x's are the results of a FHE operation. We encrypt with CaseGHX using these steps:

1) Encoding the toll tag data in bulk as vectors, V, of length $n = 2^{12}$ (chosen based on CaseGHX recommended parameters) with our $k = 4$-bit entries producing $V_i \in 0, 2^4 - 1$. We chose 4-bit entries to take advantage of the smaller cipher expansion factor.
2) We then transform these vectors, V, into polynomial messages, $m(V) = \sum_{i=0}^{n-1} V_i \times V^i$
3) We then encrypt these messages using our fheEncrypt() function to produce Ring Learning With Errors (RLWE) ciphers, $\sigma \equiv (a(V); b(V))$, as indicated in 12

$$fheEncrypt(sk; m(V)) \rightarrow \sigma \tag{12}$$

TollsOnly also implements an evaluation function, fheEval(), which evaluates Boolean multiplication functions while processing ciphertext. Legitimate city planners would have a blockchain app that used the fheEval() function to unpack the RLWE ciphers, though it could also be built into RSU's or their cloud counterparts. fheEval() produces Learning With Errors (LWE) ciphers, σ_L, for each message m(V): $c_i = \sigma_L(V_i)$.

The blockchain app would use $fheEval$ to process our multiplication function MultiF() with fheEval(sk, x1', x2', x3', x4', x5', MultiF()) which generates the encrypted results of computation, MultiF(x1, x2, x3, x4, x5).

2) Device Specifications: TollsOnly is a powered container that holds the toll tag. It does not have the limitation of non-powered RFID tags, and thus can easily perform the computations in a reasonable amount of time. TollsOnly regularly updates its local database of known toll locations from public information using existing toll API services like those used by Waze, Waymo, Here, etc. When TollsOnly detects that it is within range of a legitimate toll, it proxies the conversation with the reader, responding with all the same data that the tag would send in an unencrypted format. The data is proxied as-is rather than just cloned and transmitted to avoid being flagged as a fake and have the transponder blacklisted. At any other location, TollsOnly transmits fake data, storing the encrypted version of the toll tag data on the blockchain.

3) Infrastructure Changes: Modifications to infrastructure are required to support the TollsOnly protocol to retrieve valid data if the user desires to do so. Otherwise, the anonymized data sent will suffice for traffic counting. It is theorized that two fog-based features could be implemented: homomorphic encryption for enhanced watch-list validation for law enforcement, and a blockchain-based data sharing platform for maintaining a single-use digital twin. This paper presents details of the digital twin use case.

4) Data I/O: TollsOnly uses as its inputs, the sensitive transponder fields described in Table I. It outputs 3 datasets. Dataset (a) is the encrypted data sent to the UHF reader. Dataset (b) is the blockchain locator for the decrypted dataset version of the dataset, to enable direct access as an alternative to using [12] POCI-based method. Dataset (c) is encrypted dataset placed on the blockchain as a digital twin.

5) Palisade Library: We initially used the Palisade framework because it leveraged quantum-safe lattice operations. As was demonstrated by [21] [18] [55], lattice-based encryption is provably quantum safe as indicated in the referenced articles. We preferred a quantum-safe model, over traditional crypto solutions, because it offered privacy protection for the foreseeable future, even when quantum-computers become a prevalent threat. Another reason we used the palisade framework was that we were able to extend and adapt the lattice cryptography library to protect V2X data with fewer computations and theoretically less compute resources than other frameworks. Specifically, Palisade provided functions to ensure FHE-level privacy and sharing for toll tag data using Proxy Re-Encryption like those implemented in [4], [16], [30], [43], [50], [62].

Palisade made it possible, theoretically, to implement any scheme, including CaseGHX. It handled the encoding leaving the higher-level lattice-crypto mathematical building blocks alone at the lattice-ops layer. For simulations, TollsOnly leveraged the NTL with GMP libraries for the low-level generic mathematical operations, such as multi-precision arithmetic implementations.

Data encoding: Before encrypting, most of the FHE schemes require that the data be encoded to meet specific formats. Fortunately, toll tag data are only 64-bit integers for transponder ID or 96-bit text strings for other fields. One change the authors recommends to the 6c standard is the use of the BLAKE2 algorithm [5] since it is presumably quantum resistant and runs faster than others with a 16-bit input at 0.53 cycles / byte [9]. We opted not to use Blake2 in TollsOnly as doing so doesn't increase driver privacy.

Security parameters: Although the primary scheme we finally opted to leverage was the CaseGHX scheme [7], in our early experimentation, we found that modulus attributes based on recommendations in [47] produced very fast results. For comparison, CaseGHX used 2 basic parameters that included other features, $n = 2^{12}$ and $k = 4$. Whereas Palisade recommended parameters included: randomly generated prime Plain modulus, 496 for the coefficient modulus and $mod = x^{(2^9)}+1$ for the poly modulus.

6) TollsOnly Algorithms: The TollsOnly driver Algorithm 1 takes as input, raw tag data which is read from the toll tag when TollsOnly is powered up (i.e. car starts). As output the TollsOnly driver Algorithm produces different sets of output, depending on if the UHF Reader location is legit:

1) If the UHF reader is in a rogue location (i.e. not where a known toll is), output is thus:
   a) Randomized anonymous data sent to reader with blockchain link to access real data
   b) FHE encrypted toll tag data written to blockchain.
   c) Single-use Secret Key
2) If the UHF reader is detected at a known toll site, send raw toll tag data.

In Algorithm 1 we don't show the steps that TollsOnly takes to handle UHF channel startup with the reader i.e. Power Up, Synch Clock, Carrier signal for return data, i.e. Pilot tone, CRC, 16-bit random number/RN16.

Algorithm 1: TollsOnly Driver

Input : dataRaw

```
readerLegit ← 0
while listenForUHF do
    if TollsOnly Detects UHF 902-928Mhz then
        gps.location ← detectLocation()
        isReaderLegit(gps.location)
    end
    if Toll site is legit then
        send(UnalteredProxyresponses)
    else
        /* UHF Reader must be rogue, so
           Privatize                          */
        ptd ← privatize(dataRaw, gps.location)
        send(Randomized Tag ID) when Receive(Query
         TAG ID)
        send(Randomized Serial number) when
         Receive(QuerySerialNumber)
        send(fake sha-1 Hash) when Receive(sha-1
         Hash)
        send( NULL ) when Receive(PrevToll and
         Time)
        send
         (EncryptedUserMemory + blockchainlink)
         when Receive(Query User Memory)
        if Receive(Write toll location to user memory)
         then
            Write (gps.location) to DB of rogue reader
             locations
            /* Write nothing to user
               memory on tag.                 */
        end
    end
end
```

In Algorithm 2, the privatization function, $privatize()$, uses $fheEncrypt()$ to produce both the fully homomorphic encrypted ciphertext, and the anonymized data that is sent to the rogue UHF reader.

C. Sharing Via Blockchain Model

To reduce the shareability impact to the lowest amount possible, TollsOnly provides the user with greater control than in status quo. In the base state, the driver is at best informed (via the legalese when registering for the toll tag) of data sharing but the only option the driver has is to not use the toll tag. Toll tag devices don't have any type of on-off switch so there is no concept of "turning off the tag". Although it may seem trivial to hide the device, it is not. Unless the user hides the tag in a radio frequency resistant Faraday cage [44], [46], then the tag can still be read [39], [60]. Plus, some toll tags are merely adhesive stickers, that are easily destroyed if removed. Further, removing and remounting the device every time one goes through a toll can be a source of driver frustration which may lead to accidents [34]. Thus hiding the tag when not at toll stations is not practical and thus a solution like ours is required.

There is a benefit to smart cities that come from sharing some toll tag data points. Smart cities use data from toll tags to automatically adjust traffic lights and enable city planning. Thus traffic planners, who have a legitimate need for the rich data provided in toll tags could benefit from data if it were shared on an accessible blockchain. This would satisfy legal barriers presented in [1] by enabling the following:

- Enabling users to remain in control granting immediate access to data owners as required by CCPA & GDPR [11], [59]
- Enabling users to monetize their data as required in CCPA
- Revoking data access as required by CCPA & GDPR

[12], [61].We leverage [12]'s Pledge for its POCI consensus engine and search functions.

Algorithm 2: privatize() - The privatization function

Input : dataRaw
Input : gps.location

$sharedKey \leftarrow genKey(randNum(), gps.location)$
$rawData.encoded \leftarrow Encode(64bit, dataRaw)$
$rawData.encrypted \leftarrow fheEncrypt(sharedKey, rawData.encoded)$
$dataNew.randTID \leftarrow randomize(64bit, TagID)$
$dataNew.randSerialNumber \leftarrow randomize(28bit, SerialNumber)$
$dataNew.fakeSha1Hash \leftarrow computeSha1(DataNew.randTID)$
$dataNew.PrevTollTime \leftarrow NULL$
$blockchainLink \leftarrow tollsOnlyShare(rawData.encrypted)$
$dataNew.UserMemory \leftarrow (rawData.encrypted, blockchainLink)$
return($dataNew$)

1) TollsOnly Sharing Model: The encrypted 6c data is stored as an asset on a blockchain like BigchainDB [37] as a digital twin. We store our Homomorphic encrypted toll tag data on the blockchain to ensure decentralization and user control of their toll tag data. Prior to encrypting data, the transponder number is randomized, to prevent tracking, regardless of what is shared. When the anonymized data is returned to the RFID reader, see Algorithm 2, a URI of the access link on the blockchain is also saved in the available memory space. The ciphertexts produced by $fheEncrypt()$ are shared on the blockchain, presumably to be used by city planners or smart city automation systems (and any POCI buyers).

We theorize a TollsOnly decentralized application (dApp) smart contract, illustrated in Fig. 3, that would enable the end user to grant timed access to query the encrypted data without sharing the original shared secret key or decrypted data. To do so we propose the use of a second round of fheEncrypt() to create a FHE-type certificate which has the key and an expiry date for enforcing timed access. The dApp user with POCI would first buy the rights to use (rent) the homomorphic machine learning capabilities of the dApp.

The DPP would allow the POCI user to ask a question like, "was the target toll tag at GPS location X?" The response would be a percentage. This protects driver privacy because at no time did it ever reveal to the blockchain miner details that could be correlated with driver identity. It also does not enable the POCI buyer to ask for an infinite amount of locations. It would only respond with a high percentage if the GPS location was where their UHF reader was posted.

V. Performance Evaluation and Discussions

Table IV summarizes the state-of-art review from section III where each article's Risk Assessment Model (RASM) were rated 0-5. An articleś Driver Privacy Protection (DPP) ranges from 0-5. And an articleś level of enabling Driver Controlled Sharing capabilities (DCS) was also rated 0-5.

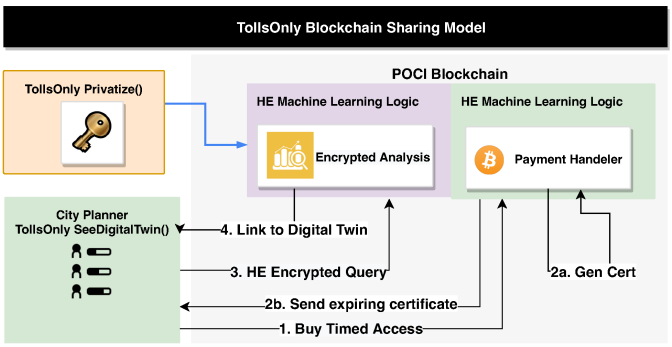

Fig. 3. The TollsOnly Blockchain Sharing Model enables city planners to use Proof of Common Interest to locate vehicle toll tag data. They then pay to rent the data and get access to use the digital twin data in a HE-based ML applications.

TABLE IV
Related Approaches and TollsOnly Approach comparison using risk reduction model (RASM), data preserving privacy (DPP), and enabling user's to control how their data is shared (DCS) in the range of 0 (lowest) to 5 (highest).

Reference Paper	RASM	DPP	DCS
Approach in [57]	2	3	0
Approach in [29]	2	2	0
Approach in [51]	3	0	0
Approach in [48]	0	4	0
Approach in [6]	0	4	0
Approach in [38]	0	1	0
Approach in [14]	0	0	1
Approach in [17]	2	2	0
Approach in [26]	0	1	1
Approach in [33]	3	4	4
Approach in [27]	0	2	2
Approach in [31]	0	4	3
Approach in [49]	0	0	1
Approach in [62]	4	3	0
Approach in [36]	1	0	0
Approach in [12]	0	3	5
Approach in [10]	3	5	0
Approach in [22]	3	2	4
Approach in [7]	0	5	0
Approach in [32]	0	3	4
Approach in [58]	1	5	4
Approach in [56]	5	3	3
Proposed TollsOnly Approach	5	5	5

Table IV shows that the TollsOnly Risk Assessment model (RASM) presented in this paper is the most comprehensive. Our privacy protection was matched with CaseGHX [7] and [58] but TollsOnly went a step further in applying a fast cryptographic FHE protocol to a real-world use case with specific parameters. Our blockchain sharing model was only paralleled by [12]. TollsOnly, however, went further by presenting an engineered solution for a real-world application of their theorized Proof of Common Interest. [33] and [56] came closest to TollsOnly but as can be seen in Table. IV, TollsOnly offers better outcomes.

Table IV shows that this paper adds novel end-to-end pri-

vacy controls for toll tags: risk assessment, privacy preserving FHE, and a user-controlled sharing model.

Our residual risk model in (11) is validated with Fig. 4, 5 and 6. Since we chose to consider the fixed scenario where $\tau = 2$, $B = 2$ and $\Omega = 4$. With these values, our base Privacy risk, and effectively Risk, $R_r = 75$. Further since we consider the case of data in compute, we set $\lambda = 3$. We are left with user controls, υ, and encryption controls, $\varkappa$. In the first graph, fig. 4, we set $\kappa = 0$, i.e. no encryption. We see that as υ, is increased, residual risk reduces. In fig. 5 we set $\upsilon = 0$ and demonstrate that increasing $\varkappa$ has the same affect, reducing residual risk but only to a fixed level. When we increase both, fig. 6, the residual risk reduces to 15%, down 65%.

As Fig. 4 shows, residual risk is inversely proportional to the amount of user-controlled shareability applied. That is, as we increased levels of shareability residual risk decreased. We also note in Fig. 5 that when we increase the encryption levels, $\varkappa$, independent of shareability, we reduce residual risk. But as can be seen in Fig. 6, if we apply the maximum encryption controls, a lattice-based HE system to the Control Type, together with the maximum user shareability controls, time-bound decentralized sharing over blockchain, we reduce residual risk the most. Interesting to note is that we were never able to get risk down to 0. This can be attributed to the observation that if tracking capabilities exist, and they do, then the risk of privacy breach will always be non-zero.

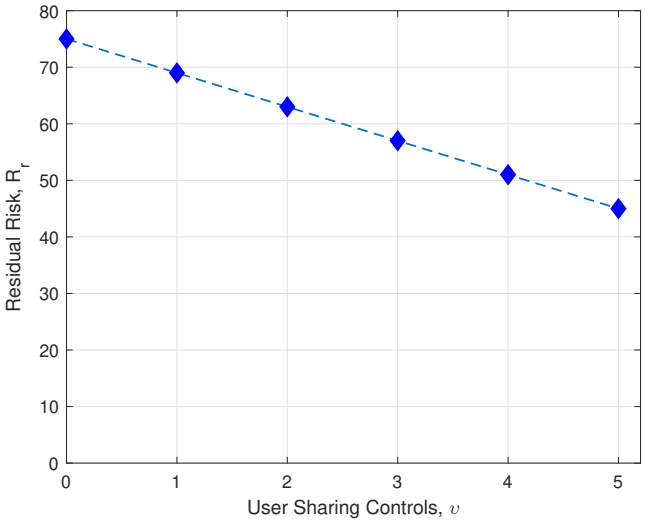

Fig. 4. υ, being inversely proportional to R_r, when we increase only user sharing controls, υ, we reduce residual risk, R_r, to 45

VI. Conclusions & Future Works

In conclusion, We have proposed a novel TollsOnly risk assessment model with formal mathematical analysis for private data sharing in IoV. Our FHE enabled protocol and selected parameters used with blockchain is a practical and promising

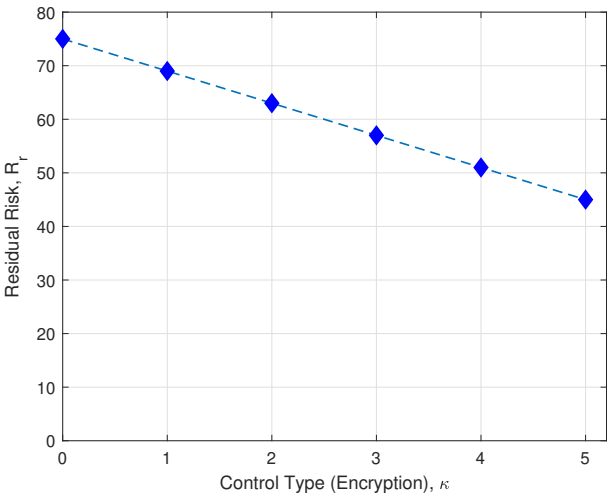

Fig. 5. When we increase only Control Type, κ, residual risk, R_r, decreases to 45

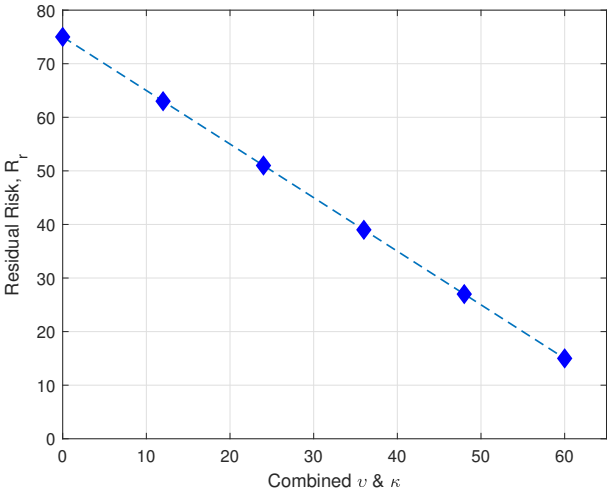

Fig. 6. This figure shows that residual risk, R_r, is highest by default at 75 when no controls are applied, 0 on the x axis. But as combined controls are applied, R_r is reduced to 15.

solution for reducing risk with Homomorphic encrypted toll tag data that drivers can share with granular GDPR required controls. If security engineers and city planners adhere to international privacy laws and new norms, they may reduce the privacy gaps presented by electronic toll tags and unauthorized toll readers by first understanding the privacy issues and risks. They can use the proposed TollsOnly risk assessment model to determine the appropriate level of encryption when deploying toll transponders probe for traffic congestion purpose. FHE paired with a user-controlled sharing model can easily preserve drivers' privacy while still providing traffic planning benefits to the city officials.

Our future work includes a) the exploration of a semantic-based digital twin law-enforcement blockchain (LEB) model to share private IoV data since all of the potential dynamic interactions and players on an LEB would need to address the long-term privacy controls promised by HE; and b) inves-

tigation of the HE based certificate concept since the X.509 standard does not currently use ciphers that leverage ideal-lattice type encryption.

Acknowledgment

This work was supported in part by the US NSF under grants CNS/SaTC 2039583, and HRD 1828811, by the U.S. Department of Homeland Security under grant DHS 2017-ST-062-000003, and by the DoD Center of Excellence in AI and Machine Learning (CoE-AIML) at Howard University under Contract Number W911NF-20-2-0277 with the US Army Research Laboratory. However, any opinion, finding, and conclusions or recommendations expressed in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the funding agencies.

References

[1] Smith v. maryland, 1979. Accessed on Dec 10, 2020, https://www.oyez.org/cases/1978/78-5374.

[2] MAP-21 - moving ahead for progress in the 21st century act, July 2012. https://www.fhwa.dot.gov/map21/.

[3] 6C Toll Operators Coalition. AVI standard - requirements and guidance document. Technical Report 3.1, Revision 1, 6C Toll Operators Coalition, May 2017.

[4] Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. *ACM Trans. Inf. Syst. Secur.*, 9(1):1–30, February 2006.

[5] Jean-Philippe Aumasson, Samuel Neves, Zooko Wilcox-O'Hearn, and Christian Winnerlein. BLAKE2: Simpler, smaller, fast as MD5. In *Applied Cryptography and Network Security*, pages 119–135. Springer Berlin Heidelberg, 2013.

[6] Josep Balasch, Alfredo Rial, Carmela Troncoso, Bart Preneel, Ingrid Verbauwhede, and Christophe Geuens. PrETP: Privacy-Preserving electronic toll pricing — USENIX. In *Proceedings of the 19th USENIX Security Symposium*, 2010.

[7] Benjamin Mark Case. *Homomorphic Encryption and Cryptanalysis of Lattice Cryptography*. PhD thesis, Clemson University, May 2020.

[8] Central Florida Expressway Authority. E-ZPass accepted on our roads — central florida expressway authority. https://www.cfxway.com/e-zpass/. Accessed: 2020-2-28.

[9] K Chalkias, J Brown, M Hearn, T Lillehagen, I Nitto, and T Schroeter. Blockchained Post-Quantum signatures. In *2018 IEEE iThings and GreenCom and CPSCom and SmartData*, pages 1196–1203, July 2018.

[10] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. TFHE: Fast fully homomorphic encryption over the torus. *J. Cryptology*, 33(1):34–91, April 2019.

[11] Council of the European Union. Regulation (EU) 2016/679 of the european parliament (general data protection regulation), April 2016.

[12] Ronald Doku and Danda B. Rawat. Pledge: A private ledger based decentralized data sharing framework. In *2019 Spring Simulation Conference (SpringSim)*, pages 1–11, April 2019.

[13] T. Elgamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *CRYPTO 1984*, 1984.

[14] A Michael Froomkin. Regulating mass surveillance as privacy pollution: Learning from environemntal impact statements. *Univ. Ill. Law Rev.*, page 1713, 2015.

[15] Craig Gentry. *A Fully Homomorphic Encryption Scheme*. PhD thesis, Stanford University, 2009.

[16] L Greenwald, K Rohloff, and D Stott. Secure Proxy-Reencryption-Based Inter-Network key exchange. In *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, pages 780–785, October 2018.

[17] GS1 AISBL. EPC Radio-Frequency identity protocols generation-2 UHF RFID. Technical Report Release 2.1, GS1 AISBL, Brussels, Belgium, July 2018.

[18] Shai Halevi, Yuriy Polyakov, and Victor Shoup. An improved RNS variant of the BFV homomorphic encryption scheme. In *Topics in Cryptology – CT-RSA 2019*, pages 83–105. Springer International Publishing, 2019.

[19] Walter Hinz, Klaus Finkenzeller, and Martin Seysen. Secure UHF tags with strong cryptography - development of ISO/IEC 18000-63 compatible secure RFID tags and presentation of first results. In *Proceedings of the 2nd International Conference on Sensor Networks*, pages 5–13. SciTePress - Science and and Technology Publications, 2013.

[20] Mariko Hirose. Newly obtained records reveal extensive monitoring of E-ZPass tags throughout new york. https://www.aclu.org/blog/privacy-technology/location-tracking/newly-obtained-records-reveal-extensive-monitoring-e-zpass, April 2015. Accessed: 2019-10-9.

[21] Jeffrey Hoffstein, Jill Pipher, and Joseph H Silverman. NTRU: A ring-based public key cryptosystem. In Joe P Buhler, editor, *Algorithmic Number Theory*, volume 1423 of *Lecture Notes in Computer Science*, pages 267–288. Springer Berlin Heidelberg, 1998.

[22] Junqin Huang, Linghe Kong, Guihai Chen, Min-You Wu, Xue Liu, and Peng Zeng. Towards secure industrial IoT: Blockchain system with Credit-Based consensus mechanism. *IEEE Trans. Ind. Inf.*, 15(6):3680–3689, June 2019.

[23] Indiana Finance Authority. Rfp ... toll collection system ... for the louisville-southern indiana ohio river bridges project. Technical report, Indiana Finance Authority, May 2014.

[24] ISO/IEC JTC 1/SC 31 Automatic identification and data capture techniques. ISO/IEC 18000-63:2015. Technical Report 18000-63:2015, ISO, October 2015.

[25] Don Johnson, Alfred Menezes, and Scott Vanstone. The elliptic curve digital signature algorithm (ECDSA). *Int. J. Inf. Secur.*, 1(1):36–63, August 2001.

[26] Christian Kaiser, Marco Steger, Ali Dorri, Andreas Festl, Alexander Stocker, Michael Fellmann, and Salil Kanhere. Towards a Privacy-Preserving way of vehicle data Sharing–A case for blockchain technology? In *International Forum on Advanced Microsystems for Automotive Applications*, pages 111–122. Springer, 2018.

[27] J Kang, R Yu, X Huang, M Wu, S Maharjan, S Xie, and Y Zhang. Blockchain for secure and efficient data sharing in vehicular edge computing and networks. *IEEE Internet of Things Journal*, 6(3):4660–4670, June 2019.

[28] Stanley Kaplan and B John Garrick. On the quantitative definition of risk. *Risk Anal.*, 1(1):11–27, March 1981.

[29] A Karygiannis, T Phillips, and A Tsibertzopoulos. RFID security: A taxonomy of risk. In *2006 First International Conference on Communications and Networking in China*, pages 1–8. ieeexplore.ieee.org, October 2006.

[30] Yutaka Kawai, Takahiro Matsuda, Takato Hirano, Yoshihiro Koseki, and Goichiro Hanaoka. Proxy Re-Encryption that supports homomorphic operations for Re-Encrypted ciphertexts. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E102.A(1):81–98, 2019.

[31] Sam Kumar, Yuncong Hu, Michael P Andersen, Raluca Ada Popa, and David E Culler. JEDI: Many-to-Many End-to-End encryption and key delegation for IoT. In *Proceedings of the 28th USENIX Security Symposium*, pages 1519–1536. The USENIX Association, 2019.

[32] Benjamin Leiding. *The M2X Economy - Concepts for Business Interactions, Transactions and Collaborations Among Autonomous Smart Devices*. PhD thesis, Georg-August University School of Science, December 2019.

[33] K Leo Brousmiche, A Durand, T Heno, C Poulain, A Dalmieres, and E Ben Hamida. Hybrid cryptographic protocol for secure vehicle data sharing over a consortium blockchain. In *2018 IEEE iThings and GreenCom and CPSCom and SmartData*, pages 1281–1286. ieeexplore.ieee.org, July 2018.

[34] Andreas Löcken, Klas Ihme, and Anirudh Unni. Towards designing Affect-Aware systems for mitigating the effects of In-Vehicle frustration. In *Proceedings of the 9th International Conference on Automotive User Interfaces and Interactive Vehicular Applications Adjunct*, AutomotiveUI '17, pages 88–93, New York, NY, USA, September 2017. Association for Computing Machinery.

[35] Jaime Lutz. Big brother has it 'E-Z': City now tracking cars through local streets thanks to E-ZPass - brooklyn paper. https://www.brooklynpaper.com/big-brother-has-it-e-z-city-now-

tracking-cars-through-local-streets-thanks-to-e-zpass/, May 2013. Accessed: 2019-11-27.

[36] Vinita Malik and Sukhdip Singh. Security risk management in iot environment. *Journal of Discrete Mathematical Sciences and Cryptography*, 22(4):697–709, 2019.

[37] Trent McConaghy, Rodolphe Marques, Andreas Müller, Dimitri De Jonghe, Troy McConaghy, Greg McMullen, Ryan Henderson, Sylvain Bellemare, and Alberto Granzotto. Bigchaindb: a scalable blockchain database, 2016.

[38] Sarah Meiklejohn, Keaton Mowery, Stephen Checkoway, and Hovav Shacham. The phantom tollbooth: Privacy-Preserving electronic toll collection in the presence of driver collusion — USENIX. In *Proceedings of the 20th USENIX Security Symposium*. USENIX, 2011.

[39] Aikaterini Mitrokotsa, Michael Beye, and Pedro Peris-Lopez. Classification of RFID threats based on security principles. *Delft University of Technology*, 2011.

[40] National Bureau of Standards. Federal information processing standards publication: data encryption standard (DES) fips pub 46. Technical report, National Institute of Standards and Technology, Gaithersburg, MD, 1977.

[41] NJTA. Request for proposal (RFP) for NJ E-ZPass customer service center (NJ E-ZPASS CSC) contractor. Technical Report RM-112649, New Jersey Turnpike Authority, January 2015.

[42] North Carolina Turnpike Authority (NCTA). AVI readers and transponders RFP. Technical report, North Carolina Turnpike Authority (NCTA), August 2016.

[43] David Nuñez, Isaac Agudo, and Javier Lopez. Proxy Re-Encryption: Analysis of constructions and its application to secure access delegation. *Journal of Network and Computer Applications*, 87:193–209, June 2017.

[44] N Ohmura, S Ogino, and Y Okano. Optimized shielding pattern of RF faraday cage. In *2014 International Symposium on Electromagnetic Compatibility, Tokyo*, pages 765–768. ieeexplore.ieee.org, May 2014.

[45] Pascal Paillier. Public-Key cryptosystems based on composite degree residuosity classes. In *Advances in Cryptology — EUROCRYPT '99*, pages 223–238. Springer Berlin Heidelberg, 1999.

[46] Lucio Pastena et al. Bluetooth communication interface for EEG signal recording in hyperbaric chambers. *IEEE Trans. Neural Syst. Rehabil. Eng.*, 23(4):538–547, July 2015.

[47] Yuriy Polyakov, Kurt Rohloff, and Gerard W Ryan. PALISADE lattice cryptography library. *Cybersecur. Res. Center, New Jersey Inst. Technol. , Newark, NJ, USA, Tech. Rep*, 2018.

[48] Raluca Ada Popa, Hari Balakrishnan, and Andrew J Blumberg. VPriv: Protecting privacy in Location-Based vehicular services. *USENIX Security Symposium*, 2009.

[49] R Ramaguru, M Sindhu, and M Sethumadhavan. Blockchain for the internet of vehicles. In *Advances in Computing and Data Sciences*, pages 412–423. Springer Singapore, 2019.

[50] Shruthi Ramesh. *An efficient framework for privacy-preserving computations on encrypted IoT data*. PhD thesis, Iowa State University, 2019.

[51] S Rao, N Thanthry, and R Pendse. RFID security threats to consumers: Hype vs. reality. In *2007 41st Annual IEEE International Carnahan Conference on Security Technology*, pages 59–63. ieeexplore.ieee.org, October 2007.

[52] Danda B Rawat and Chandra Bajracharya. *Vehicular cyber physical systems*. Springer, 2017.

[53] M R Rieback, Bruno Crispo, and Andrew S Tanenbaum. The evolution of RFID security. *IEEE Pervasive Computing*, 5(1):62–69, February 2006.

[54] R L Rivest, A Shamir, and L Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, February 1978.

[55] K Rohloff. Computer arithmetic research to accelerate Privacy-Protecting encrypted computing such as homomorphic encryption. In *2019 IEEE 26th Symposium on Computer Arithmetic (ARITH)*, pages 197–197, June 2019.

[56] Omaji Samuel and Nadeem Javaid. A secure blockchain–based demurrage mechanism for energy trading in smart communities. *Int. J. Energy Res.*, 45(1):297–315, January 2021.

[57] Sanjay E Sarma, Stephen A Weis, and Daniel W Engel. Radio-Frequency identification: Security risks and challenges. *RSA Laboratories Crypt*, 6(1):3–9, 2003.

[58] Preeti Sharma and V K Srivastava. Trusted sharing of IOT data using an efficient re-encryption scheme and blockchain. In *Computational Methods and Data Engineering*, pages 295–306. Springer, 2020.

[59] State of California. California consumer privacy act of 2018. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375, June 2018. Accessed: 2019-11-2.

[60] Ellen Stuart, Melody Moh, and Teng-Sheng Moh. Security and privacy of RFID for biomedical applications: A survey. *RFID*, 2008.

[61] D Wang and X Zhang. Secure data sharing and customized services for intelligent transportation based on a consortium blockchain. *IEEE Access*, 8:56045–56059, 2020.

[62] Z Wei, J Li, X Wang, and C Gao. A lightweight Privacy-Preserving protocol for VANETs based on secure outsourcing computing. *IEEE Access*, 7:62785–62793, 2019.

Hassan Karim received his master's degree in computer science at Howard University in 2019. He is currently pursuing his PhD in Computer Science under the supevision of Prof. Danda B. Rawat in the Department of Electrical Engineering / Computer Science at Howard University in Washington, DC, USA. He is also a current member of the Data Science and Cybersecurity Center (DSC2) at Howard University. His research interests lie in security, privacy, and international public policy related to mobile cyber physical systems, industrial control system security, Internet of Vehicles (IoV), brain computer interfaces, artificial intelligence, blockchain and cybersecurity.

Danda B. Rawat (*IEEE Senior Member, 2013*) is a Full Professor in the Department of Electrical Engineering & Computer Science (EECS), Director of the Howard University Data Science and Cybersecurity Center, Director of DoD Center of Excellence in AI/ML (CoE-AIML), âDirector of Cyber-security and Wireless Networking Innovations (CWiNs) Research Lab, Graduate Program Director of Graduate CS Programs and Director of Graduate Cybersecurity Certificate Program at Howard University, Washington, DC, USA. Dr. Rawat is engaged in research and teaching in the areas of cybersecurity, machine learning, big data analytics and wireless networking for emerging networked systems including cyber-physical systems, Internet-of-Things, multi domain battle, smart cities, software defined systems and vehicular networks. His professional career comprises more than 18 years in academia, government, and industry. He has secured over $16 million in research funding from the US National Science Foundation (NSF), US Department of Homeland Security (DHS), US National Security Agency (NSA), US Department of Energy, National Nuclear Security Administration (NNSA), DoD and DoD Research Labs, Industry (Microsoft, Intel, etc.) and private Foundations. Dr. Rawat is the recipient of NSF CAREER Award in 2016, Department of Homeland Security (DHS) Scientific Leadership Award in 2017, âResearcher Exemplar Award 2019 and Graduate Faculty Exemplar Award 2019 from Howard University, the US Air Force Research Laboratory (AFRL) Summer Faculty Visiting Fellowship in 2017, Outstanding Research Faculty Award (Award for Excellence in Scholarly Activity) at GSU in 2015, the Best Paper Awards (IEEE CCNC, IEEE ICII, BWCA) and Outstanding PhD Researcher Award in 2009. He has delivered over 20 Keynotes and invited speeches at international conferences and workshops. Dr. Rawat has published over 200 scientific/technical articles and 10 books. He has been serving as an Editor/Guest Editor for over 50 international journals including the Associate Editor of IEEE Transactions of Service Computing, Editor of IEEE Internet of Things Journal, Associate Editor of IEEE Transactions of Network Science and Engineering and Technical Editors of IEEE Network. He has been in Organizing Committees for several IEEE flagship conferences such as IEEE INFOCOM, IEEE CNS, IEEE ICC, IEEE GLOBECOM and so on. He served as a technical program committee (TPC) member for several international conferences including IEEE INFOCOM, IEEE GLOBECOM, IEEE CCNC, IEEE GreenCom, IEEE ICC, IEEE WCNC and IEEE VTC conferences. He served as a Vice Chair of the Executive Committee of the IEEE Savannah Section from 2013 to 2017. Dr. Rawat received the Ph.D. degree from Old Dominion University, Norfolk, Virginia. Dr. Rawat is a Senior Member of IEEE and ACM, a member of ASEE and AAAS, and a Fellow of the Institution of Engineering and Technology (IET). He is an ACM Distinguished Speaker.