SecureCheck: User-Centric and Geolocation-Aware Access Mediation Contracts for Sharing Private Data

Jacob Hopkins
jhopkins2@islander.tamucc.edu
Texas A&M University - Corpus Christi
Corpus Christi, Texas, USA

Carlos Rubio-Medrano
carlos.rubiomedrano@tamucc.edu
Texas A&M University - Corpus Christi
Corpus Christi, Texas, USA

ABSTRACT

Data oversharing is a critical issue in today's technologically driven society. Numerous entities, i.e., corporations, governments, criminal groups, are collecting individuals' data. One potential cause is that current systems, such as verification systems, do not prioritize the minimization of exchanged data. To address this issue, we propose SecureCheck, a novel *privacy-enhancing technology* (PET) framework that prioritizes data minimization. We aim to ensure that individuals control technology and its access to themselves, and not technology controlling individuals or their data. To that end, our proposed framework is comprised of two components: a novel access control model, called *access mediation contracts*, that enables users to negotiate with third parties over what data is used in a verification event, and a novel recommendation system that recommends the access mediation contracts in situationally-aware manner using geolocation data. As a part of ongoing work, we are developing a privacy calculus model detailing the decision process for data exchange. Also, we are conducting an exploratory study to better identify how to resolve conflicts between data owners and verifiers. Finally, we are actively working towards VaxCheck, a prototype implementation of SecureCheck focused on vaccine verification systems, so we can assess its effectiveness and suitability for future deployments in practice.

CCS CONCEPTS

• **Security and privacy** → **Privacy-preserving protocols**; **Access control**.

KEYWORDS

Privacy, Data Sharing, Verification, Privacy Enhancing Technology, Access Mediation, Geolocation-based Recommendation

ACM Reference Format:
Jacob Hopkins and Carlos Rubio-Medrano. 2024. SecureCheck: User-Centric and Geolocation-Aware Access Mediation Contracts for Sharing Private Data . In *Proceedings of the 29th ACM Symposium on Access Control Models and Technologies (SACMAT 2024), May 15–17, 2024, San Antonio, TX, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3649158.3657050

SACMAT 2024, May 15–17, 2024, San Antonio, TX, USA

ACM ISBN 979-8-4007-0491-8/24/05
https://doi.org/10.1145/3649158.3657050

1 INTRODUCTION

Privacy is a nebulous concept. Depending on the field, privacy can be defined differently. Warren and Brandeis originally defined privacy, in the American legal context, as "the right to be let alone" [29]. Other theories of privacy have been produced by various individuals: Westin [30] defined privacy as "the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Altman [2] defined privacy as "the selective control of access to the self." However, these definitions do not fully encompass what privacy is because the boundary between the self and others is fuzzy and thus difficult to completely differentiate those two spheres of our lives [1]. This difficulty has been and continues to be exploited by technology, which has made it easier for aspects of our lives to be known without permission. The leaking of private information is now the norm. This reality has become evident through numerous scandals, e.g., the 23andMe breach [19].

Credential verification is the process by which certified attributes of a *data owner* are verified according to some policy [3]. An example of this would be determining the vaccination status of a patron so that they can enter a venue such as a restaurant. In the verification process, some data about the data owner, e.g., the patron, must be exchanged with the *verifier*, e.g., the host/hostess, to establish the veracity of the data owner's claim, e.g., being vaccinated. Often, a third party, called the *issuer*, e.g., a legitimate medical service, is needed to establish the authenticity of the data owner's data. A critical issue of this process is that *data oversharing* often occurs because the minimization of the exchanged data is not prioritized. Going back to the vaccination status example, the patron would then share their vaccine passport which contains other information such as their name, date of birth, vaccine type, vaccination date, and other potentially sensitive data. In this context, the main cause of data oversharing may be that verification systems are designed for broad use in multiple situational contexts. Using a photo ID as an example, it is used in multiple situations such as age verification, identity verification, etc. Thus, the photo ID is designed to incorporate various attributes that are used for those different situations. However, the ID is unable to discern what the situational context that the verification is occurring in and thus data oversharing is able to occur. Most current verification systems are unresponsive to situational and cultural contexts for sharing data in a verification event. Since verification systems do not respond to the situations where verification events occur, data owners are rarely given say over what data must be shared in said event. Consequently, they are not able to maintain control over their sensitive data.

Our guiding philosophy is that people should control technology, and not technology controlling people. Previous work has shown

that individuals are indeed able to set cyber-protections correctly and efficiently with previous work demonstrating efficiency rates of 92% on common case scenarios [7]. Our research goal is to ensure the privacy of individuals' data being shared during a verification event. Our approach will target information privacy, which is related to the control that the data owners exert on their information, similar to how Westin defined privacy as the claim of individuals and organization to decide how their information is disbursed to others [30]. While information privacy is the targeted aspect that this research is aiming to be achieved in verification systems, information privacy does not sufficiently describe the proposed objective. To fully describe the proposed objective, the concept of information flows from Nissenbaum [20] needs to be incorporated. Information, including sensitive data such as medical information, is shared through a multitude of channels all the time. Many of these channels or flows do not raise the ire of the data owners despite the loss of control of that information because these information flows align with social conventions, i.e., sharing your health and family history with your doctor. The sharing of privileged information according to social norms allows for various social activities to be completed. It is when flows violate social norms that data owners become concerned and angry [20].

Our primary research objective (based on our philosophy) is to provide significant evidence that **users can effectively control the dissemination of sensitive information contained within verification systems by crafting their own data-sharing contracts, a.k.a., access mediation contracts (*AM-Contracts*), for a variety of situational contexts, while enabling the proper flow of the information between the users and other parties according to appropriate situational and social norms**.

With that in mind, we propose `SecureCheck`, a two-part framework to address the data oversharing issue. The proposed framework will combine a novel access control model that emphasizes consensus building between data owners and verifiers, and a geolocation-based recommender model that leverages spatial data to improve the usability of the framework. The first part is the novel access control model dubbed AM-Contracts, which will facilitate the mediation between data owners and verifiers to establish a data sharing policy during a verification event. The second part of the proposed solution is a geolocation-based recommendation system for sharing AM-Contracts. The recommendation system will provide situational context to data owner via AM-Contract recommendations, thus ensuring data minimization in every situational context that a verification event can occur, and guaranteeing that data owners retain control over the release of data. Thus, the main contributions of our work are the following:

- An access mediation scheme enabling data owners and verifiers to negotiate what data is to be shared for verification.
- A conflict resolution strategy that resolves potential issues between data owners and verifiers.
- A geolocation based recommendation system that provides situational recommendations to data owners to ensure that only the necessary information is exchanged.
- A proof-of-concept vaccination certification system to demonstrate `SecureCheck`'s capabilities.

2 BACKGROUND & RELATED WORKS

2.1 Privacy Enhancing Technologies

The use of digital technologies and media have disrupted long standing data sharing norms [20]. To address this problem, *Privacy-enhancing technologies* (PETs) [17] were introduced. PETs are sets of technologies that are designed using the *privacy-by-design* paradigm to ensure the privacy requirements in their targeted domains [18]. The aim of PETs is to protect an individual's privacy through the use of technical means by providing data minimization, anonymity, unlinkability, and/or unobservibility services [18]. The goals of these PETs have been to share fine-grained data while ensuring the privacy of the individual. However, efforts to produce an all-encompassing PET solution that ensures the utility of the data and privacy of the individual has stalled [23]. Instead, a recent article by Stadler and Troncoso has suggested that researchers should identify use cases where both the usability of fine grain data and the privacy of that data can be maintained and to develop PETs for those use cases [23].

2.2 Vaccination Certification Systems

To better elucidate `SecureCheck`, we will use an exemplar domain: *digital vaccination certification* (DVC) systems, also colloquially known as digital vaccine passport systems. DVCs are an ideal test case because vaccination information is private health data that is widely distributed across the US health system that in extraordinary circumstances needs to be shared with a broad range of people and locations. However, most people or locations need only access to some of the data, but depending on the person or location that can be a different subset of vaccination information.

The COVID-19 pandemic was a significant disruptive event for the global society. It caused approximately 7 million deaths [9] and a significant economic cost as well [8]. In response to the pandemic, nations and organizations promoted and implemented various interventions to mitigate the spread of the disease or prevent it. One such solution was DVC systems. Multiple DVCsystems were implemented by various countries and governmental organizations during the pandemic such as the Green Pass by Israel, the EU's Digital COVID Certificate, and many more [28]. With this in mind, the concepts behind `SecureCheck` will be used to develop a novel vaccine passport called `VaxCheck`: a PET to preserve the privacy of the vaccination data shared during a vaccine verification event.

2.3 Related Works

The idea for privacy-preserving credentials was first proposed in 1982 by Chaum [6] with the first implementation created by Camenisch and Lysyanskaya in 2001 [5]. Since then, numerous privacy-preserving credential frameworks have been proposed which are designed to ensure some combination of these properties: anonymity, pseudonymity, selective disclosure, and unlinkability.

Functional credentials [10] is an anonymous credential scheme that allows users to prove that they posses an attribute set according to some policy using predicate encryption. Policies are expressed as polynomially computable predicates which then can be evaluated over any set of attributes. This scheme issues users decryption keys which correspond to a selected set of attributes in a policy predicate.

Thus users need only to decrypt the predicate ciphertext to show that they have the necessary attributes needed to satisfy the defined policy. Since all policies are encoded as a predicate ciphertext, this framework allows for designated third parties to verify users without learning about the policy or the users' attributes.

PriFoB [3] is a global accreditation and credential verification system. It is designed to utilize a pubic-permissioned blockchain integrated with a fog computing layer such that it can be used for any type of credentials at a global scale. PriFoB consists of three layers: the Distributed Trusted Third Party (DTTP) layer, the fog layer, and the end-user layer. The DTTP layer is the layer where blockchain is managed through verifying new blocks and maintaining the blockchain's consistency. The fog layer verifiable credentials are created and revoke. PriFoB implements a Proof-of-Authority and Signature-of-Work algorithms for handling the verifiable credentials and issuers on the blockchain.

The crucial difference between SecureCheck and the previously mentioned credential systems is the question of who decides what attributes or data is used in the verification policy. Most credential systems answer this question by having the verifiers solely handle verification policy creation. This presents verifiers with the opportunity to request more data than what is required and the data owners with little recourse. Our approach differs in that the verification policy is determined in an ad-hoc manner by both the verifiers and the data owners. This approach does not necessarily resolve the issue because not all data owners have privacy or cybersecurity training. Thus, SecureCheck also incorporates a recommender system to assist data owners.

3 PROBLEM STATEMENT

Referring back to Sec. 1, technology has had profound effects on our privacy rights by gathering, storing, and processing significant amounts of our personal data. Our data is being gathered, leaked, and/or sold by several entities such as malicious actors [15], corporations [24], government agencies [22], etc. There have been various solutions of different methodologies that have been developed to address this issue such as the legal means of the *European Union's* (EU's) *General Data Protection Regulation* (GDPR) [12]. However, there still remains a need for technological solutions to reduce data leakage or data oversharing including in credential verification.

As stated earlier in Sec. 1, two major contributing factors for data oversharing in verification systems are: (i) they are designed for broad use in multiple varied situations; and, (ii) they are not designed to enable data owners to have a voice in what data is shared for verification. To address both factors, the following six functionalities must be supported:

(1) Identify the current situational or cultural context.
(2) Specify the data to be exchanged in a verification event depending on the situational context, the data owners' expectations, and the verifier' expectations.
(3) Allow the data owners and verifiers to specify their custom verification policies.
(4) Ensure that there is no conflict between both parties' policies.
(5) Resolve potential conflicts so that an agreed policy can be reached.
(6) Enforce the conditions of that policy.

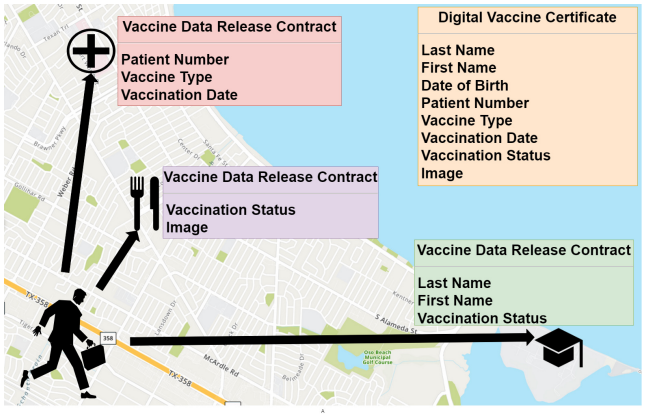

Figure 1: An essential function of SecureCheck: data owners leverage contracts to release specific data for various locations, e.g., hospitals, restaurants, and schools.

4 METHODS

SecureCheck is comprised of two parts: AM-Contracts and a gelocation-based recommendation system. AM-Contracts are designed to implement the functionality of enabling the verifiers and data owners to generate a consensus about the verification policy as outline in the third, fourth, fifth, and sixth functionalities in Sec. 3. The geolocation-based recommendation system is designed to enable verification systems to be aware of where a verification event is occurring and to recommend what data should be exchanged for verification based on the most probable situation to occur within that space thereby implementing the first and second functionalities from Sec. 3. Our approach is illustrated by Fig. 1: an individual can travel to various locations such as a hospital, restaurant, or university and shared specific pieces of data to these locations for verification such as verifying their vaccination status. These spaces will obtain access to only the data that they need and the data owner can maintain control over their data.

4.1 Trust Model

The trust model being used is the untrusted client scenario [17] or also called the semi-trusted model [18]. In our model, the data owners do not fully trust the other actors involved in SecureCheck. We assume that the other involved actors are *honest-but-curious*, that is, actors using SecureCheck generate trustworthy input and outputs and/or produce honest calculations, but they may be curious and try to obtain extra data that they do not need.

There are three actors in this model. The first actor is the *data owner* which is the individual whose data is being collected or stored. The second entity involved in the trust model is the *verifier*. The verifier is the entity that uses the service to request the data owner's attributes. The last entity involved in the proposed model is the *issuer*. The issuer stores and certifies the data owner's attributes and issues credentials to them. The verifiers would determine the validity of the attributes within the credentials with issuers. In this scenario, the issuer would act as a *Trusted Third Party* (TTP) for both the data owners and the verifiers. The verifiers would be treated as semi-trusted entities by the data owners.

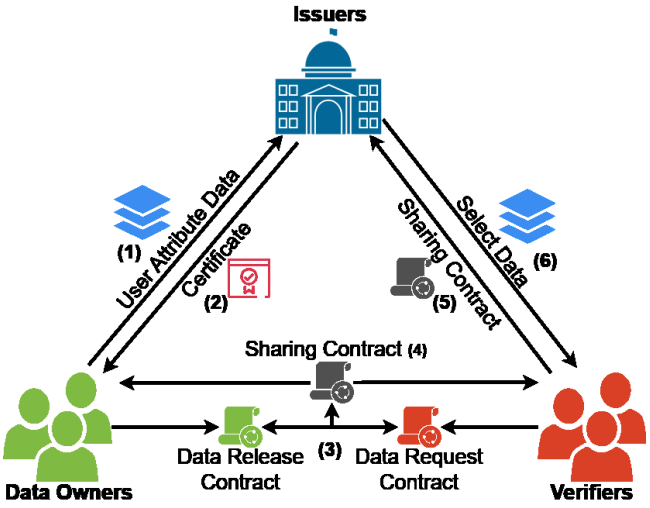

Figure 2: A foundational view of our proposed approach: the three entities: Data Owners, Verifiers, and Issuers, interact with each other according to a semi-trusted model.

4.2 Access Mediation Contracts

The core functionality of the proposed approach is the AM-Contracts. These contracts are designed to enable negotiations between the data owner and verifier in a verification event. The goal of enabling a negotiation between the two parties is to ensure data owners retain control of their data while verifiers still have access to necessary data. The AM-Contracts are used to communicate what data, contained with a certificate or credential, will be used in a verification event. AM-Contracts are composed of a set of permissions corresponding to the attributes within the credentials. Selecting a permission represents selecting an attribute to be used in the verification event. So the use of the AM-Contracts start with the issuance of a set of digital certificates or credentials. The data owner will still need to register a set of attributes, (1) in Fig. 2, to obtain the credential or certificate from the issuer, (2) in Fig. 2, but the proposed AM-Contracts will be designed to integrate with existing attribute-based credentialing systems.

The AM-Contracts will be used to mediate verification events. At the beginning of a verification event, the data owner and verifier will create their initial contracts, (3) in Fig. 2. Both parties use the same contract model, but the purpose of their contracts differ. The data owner will select their attributes from their credentials which are to be shared in the event. They will also define certain parameters that affect access to their attributes such as duration of access, etc. Once finished, the data owner will create an AM-Contract. As part of the contract creation phase, the AM-Contract will automatically review the selected attributes and conditions for the data owner. This review process calculates the privacy risk that the contract presents to the data owner. This risk is shown as a risk score to the data owner. The higher scores reflect a riskier contract, lower scores reflect a lower risk contract. The verifier will generate an AM-Contract to request specific attributes that they need for verification. In our approach, an AM-Contract generated by the data owner is called a *data release AM-Contract*, and the one created by the verifier is called a *data request AM-Contract*.

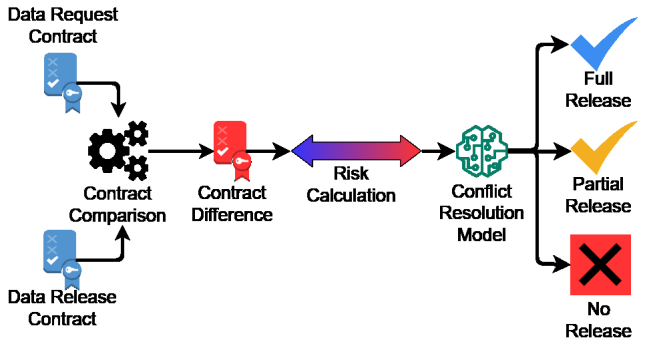

Figure 3: Conflict Resolution Strategy: if the symmetrical difference of the contracts from the data owners and verifiers is nonzero, further action is determined based on a risk score.

Once the data owner and verifier have defined their contracts, the contracts are to be shared and compared with one another, (Fig. 2, (4)). If there are no conflicts between them, they will resolve into a *data sharing agreement contract*. Both parties will receive the resulting contract, but the verifier will forward it to the issuer to obtain the agreed upon attributes of the data owner (Fig. 2, (5)). With the attributes sent to the verifier (Fig. 2, (6)), the verification event is completed. This negotiation process for verification must be completed by both parties for each event that occurs.

If the comparison between the contracts result in a conflict then there are three possible outcomes (U refers to the data release AM-Contract and S refers to the data request AM-Contract):

(1) $U \supset S$ - The data owner is releasing more attributes than the verifier is requesting.
(2) $U \subset S$ - The data owner is releasing less fields than the verifier is requesting.
(3) $U \not\subseteq S \wedge S \not\subseteq U$ - The data owner has created a data release AM-Contract where at least one or more attribute differs from the requested set of attributes.

The first case as described is straightforward. Despite being a conflict between U and S in case one, the data owner has already agreed to allow the verifier access to the requested attributes. The attributes that make up the contract difference, L, are attributes that have not been requested by the verifier. Thus the solution is to only release the requested attributes and not release L to the verifier. For example, suppose a patron enters into a restaurant and that restaurant has a policy that diners need only show their COVID-19 vaccination status to enter. Within the proposed framework, if the patron decides to release their vaccination status and additional information, such as their name, then only their status will be released to the restaurant. The second and third cases represent major conflicts between the data release AM-Contract and the data request AM-Contract. The second case represents when a verifier requests more data than the data owner is willing to release. The difference between U and S is calculated as $L = S - U$. Using the restaurant example, the restaurant is requesting the patron's vaccination status, vaccination date, and vaccination type and the patron is only releasing their vaccination status. `SecureCheck` would resolve this conflict depending upon circumstances that verification event is

occurring in, e.g., by recognizing that this is a restaurant and thus resolve the conflict by siding with the patron. The third case represents when the data owner is releasing different attributes than what is being requested. The difference between U and S would be calculated as the symmetric difference: $L = U \ominus S$. For example, the restaurant is requesting the patron's vaccination status and name, but the patron is releasing their vaccination date, vaccination type, and name. SecureCheck would determine which of the conflicting attributes should be shared given the circumstances and is of less risk to the data owner. In this case, SecureCheck would side with the restaurant and request the patron to only release their status in addition to their name.

For the three cases, L is calculated and the conflict resolution subsystem will analyzes the attributes in L through a privacy risk assessment. This is done to determine the risk of releasing additional data. The risk calculation will be shown as a simple numeric risk metric to the data owner, enabling them to understand the cost of releasing more or different data.

4.3 Geolocation-based Recommendations

One method for discerning the type of situation that the verification event is occurring in is determining the location of where it is happening. There is a dependency of the situational context on the physical space in which the verification event occurs. Thus, there is a dependency between what data needs to be shared for verification and the location where the event takes place. It is possible to improve the situational awareness of verification systems by leveraging geolocation data through geofences.

The geolocation-based recommender system is comprised of two components: a geofence and a recommender system. A geofence is a service that triggers an action when a device crosses a defined virtual boundary [4]. Recommender systems have been used as a solution for filtering substantial amounts of information and finding relevant information [13]. The geolocation-based recommender system's purpose is identifying the location where the verification event occurs. Using the location data, the system will generate an AM-Contract recommendation for the data owner to use in the verification event. By leveraging the location data of the data owner during verification, the recommender system can produce a contract recommendation that tailors the verifiers' access to the data owners' data according to the current situational context.

The operation of geolocation-based recommender system is shown in Fig. 4. It starts with the data owner, **(1)** in Fig. 4, going to a physical space with the geofence enabled. Upon crossing the geofence, the system will retrieve the space's data request AM-Contract (if it has been created), **(2a)** in Fig. 4. The geofence will also identify the space the owner has entered and inform the recommender component. Around the same time as **(2a)**, the recommender component will generate a recommendation, shown as **(2b)** in Fig. 4, using the data related to that space including the type of space it is (i.e. academic area, government building, business), history of data shared with that space, and the risk associated with sharing that data. The recommender system will produce an AM-Contract recommendation that indicates what data can be safely shared , which is **(3)** in Fig. 4. The recommender system will forward its recommendation to the data owner. The data owner can use the recommended contract or create their own for the negotiation.

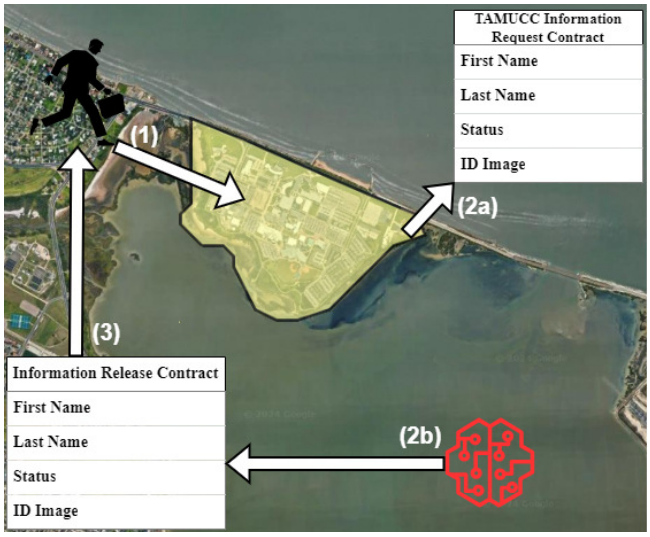

Figure 4: Geolocation-based Recommendations: the geofence system and recommender system work in tandem to identify the space the owner has entered and its attributes; then produces a contract recommendation the owner can use.

5 ONGOING WORK

There are a number of items we are currently working on to complete the proposed framework. These items are related to completing the access control model and development of the geolocation-based recommender system. For our access control model, we are working on four items. First, we are examining various technologies to use as the foundation for developing AM-Contracts. These technologies are attribute based credentials [18] and *attribute-based access control* (ABAC) systems [27]. The current design of the negotiation protocol has both parties create AM-Contracts for each verification event. This places an increase burden on both parties. Thus, we are working on a solution where both parties can establish one AM-Contract for all verification events between them until one wishes to alter it. Also, we are developing a privacy risk metric. There has been research into developing a metric for measuring data leaks [26] and privacy risk [16]. Thus, we are developing a risk metric that targets the release of data for the individual user. In addition, we are working on how to resolve potential contract conflicts between verifiers and data owners. We are conducting a two-part exploratory mixed method study targeting both the verifier and data owner populations. The first portion is a qualitative study where participants from both populations will be interviewed. The objectives of the qualitative portion is to (1) identify the factors that are used in an individual's decision process for releasing sensitive information, (2) uncover further design requirements for verification systems, and (3) understand the privacy attitudes towards sharing sensitive data in verification systems. The data collected from the qualitative portion will be used to develop a model that documents the decision making process using *privacy calculus theory* [11]. The second portion of the study will include a quantitative survey to experimentally verify the results, i.e., the privacy calculus model, and to gather AM-Contract recommendations for various location

types, which will be used to create the geolocation recommender model and the conflict resolution subsystem.

Finally, there are two items that we are working on in regards to the geolocation-based recommender system. First, we are researching what fundamental model and parameters to use to construct the recommender system. For the fundamental model, there are two ideas that are being examined: association rule mining [21] or graph neural network using a bipartite graph [31]. Currently, the only parameter the recommender system uses is the location data of a data owner. We recognize that there are other potential parameters such as the privacy risk score that could be used in the recommendation process. Thus, we are exploring other potential parameters to use. The second item we are working on is the geofence model leveraging OpenStreetMap [14]: a community built database that documents various geographical features such as buildings, roads, and other structures. We will use OpenStreetMap to develop our geofence model by leveraging alpha shapes and Voronoi diagrams inspired by a method for dynamically generating a geofence for UAVs proposed by Vagal et al. [25].

6 CONCLUSION

Data oversharing is a crucial privacy issue that needs to be addressed. In our current technologically driven climate, there is no balance between preserving the individuals' right to determine how their data is shared with others and third parties having access to various types of data. We proposed a novel PET framework, called `SecureCheck`, that promotes data minimization in verification systems to address some of the data oversharing. We are developing an exploratory mixed method study to determine how individuals approach verification events and what data do they prefer to exchange. Using this data, we will finish the development of both components for `SecureCheck`. Also, we are using `SecureCheck` to develop a vaccine verification system called `VaxCheck` to demonstrate the capabilities of the framework. We will also determine the efficacy of `VaxCheck` through a series of experiments.

ACKNOWLEDGMENTS

This work was partially supported by the National Science Foundation (NSF) under Grants No. 2232911 and No. 2131263, and by a SAGE Scholarship from Texas A&M University - Corpus Christi.

REFERENCES

[1] Alessandro Acquisti, Curtis Taylor, and Liad Wagman. 2016. The economics of privacy. *Journal of economic Literature*, 54, 2, 442–492.

[2] Irwin Altman. 1975. *The environment and social behavior: privacy, personal space, territory, crowding*. Brooks/Cole Pub. Co, Monterey, Calif. ISBN: 9780818501685.

[3] Hamza Baniata and Attila Kertesz. 2022. Prifob: a privacy-aware fog-enhanced blockchain-based system for global accreditation and credential verification. *Journal of Network and Computer Applications*, 205, 103440.

[4] Christoph Bösch. 2018. An efficient privacy-preserving outsourced geofencing service using bloom filter. In *2018 IEEE Vehicular Networking Conference (VNC)*. IEEE, Taipei, Taiwan, 1–8. DOI: 10.1109/VNC.2018.8628406.

[5] Jan Camenisch and Anna Lysyanskaya. 2001. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *Advances in Cryptology — EUROCRYPT 2001*. Birgit Pfitzmann, (Ed.) Springer Berlin Heidelberg, Berlin, Heidelberg, 93–118. ISBN: 978-3-540-44987-4.

[6] David Chaum. 1982. Blind signatures for untraceable payments. In *Advances in Cryptology Proceedings of Crypto 82*. Plenum Press, New York, USA, Santa Barbara, California, 199–203.

[7] Luis Claramunt, Carlos Rubio-Medrano, Jaejong Baek, and Gail-Joon Ahn. 2023. Spacemediator: leveraging authorization policies to prevent spatial and privacy attacks in mobile augmented reality. In *Proc. of the 28th ACM Symposium on Access Control Models and Technologies* (SACMAT '23). Association for Computing Machinery, Trento, Italy, 79–90. DOI: 10.1145/3589608.3593839.

[8] David M. Cutler and Lawrence H. Summers. 2020. The covid-19 pandemic and the $16 trillion virus. English. *JAMA : the journal of the American Medical Association*, 324, 15, 1495.

[9] World Health Organization 2023 data.who.int. 2023. Who coronavirus (covid-19) dashboard > cases [dashboard]. (2023). https://data.who.int/dashboards/covid19/cases.

[10] Dominic Deuber, Matteo Maffei, Giulio Malavolta, Max Rabkin, Dominique Schröder, Mark Simkin, et al. 2018. Functional credentials. In *Proc. on Privacy Enhancing Technologies Symposium* number 2. Vol. 2018. Barcelona, Spain, 64–84. DOI: https://doi.org/10.1515/popets-2018-0013.

[11] Tamara Dinev and Paul Hart. 2006. An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17, 1, 61–80.

[12] European Parliament and Council of the European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council. (May 4, 2016). Retrieved Jan. 19, 2024 from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

[13] Leonardo Ferreira, Daniel C. Silva, and Mikel U. Itzazelaia. 2023. Recommender systems in cybersecurity. English. *Knowledge and information systems*, 65, 12, 5523–5559. DOI: https://doi.org/10.1007/s10115-023-01906-6.

[14] OpenStreetMap Foundation. 2004. (Aug. 2004). https://www.openstreetmap.org/copyright.

[15] Lorenzo Franceschi-Bicchierai. 2023. Hacker leaks millions more 23andme user records on cybercrime forum. (Oct. 2023). https://techcrunch.com/2023/10/18/hacker-leaks-millions-more-23andme-user-records-on-cybercrime-forum/.

[16] Matteo Giomi, Franziska Boenisch, Christoph Wehmeyer, and Borbála Tasnádi. 2023. A unified framework for quantifying privacy risk in synthetic data. English. *Proceedings on Privacy Enhancing Technologies*, 2023, 2, 312–328. DOI: https://doi.org/10.56553/popets-2023-0055.

[17] Johannes Heurix, Peter Zimmermann, Thomas Neubauer, and Stefan Fenz. 2015. A taxonomy for privacy enhancing technologies. *Computers & Security*, 53, 1–17. DOI: https://doi.org/10.1016/j.cose.2015.05.002.

[18] Nesrine Kaaniche, Maryline Laurent, and Sana Belguith. 2020. Privacy enhancing technologies for solving the privacy-personalization paradox: taxonomy and survey. *Journal of Network and Computer Applications*, 171, 102807. DOI: https://doi.org/10.1016/j.jnca.2020.102807.

[19] Lily Hay Newman. 2023. The 23andme data breach keeps spiraling. (Dec. 2023). https://www.wired.com/story/23andme-breach-sec-update/.

[20] Helen F. Nissenbaum. 2010. *Privacy in context: technology, policy, and the integrity of social life*. English. (1st ed.). Stanford Law Books. ISBN: 9780804772891.

[21] Deepjyoti Roy and Mala Dutta. 2022. A systematic review and research perspective on recommender systems. *Journal of Big Data*, 9, 1, 59. DOI: https://doi.org/10.1186/s40537-022-00592-5.

[22] T.C. Sottek and Janus Kopfstein. 2013. Everything you need to know about prism. (July 2013). https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet.

[23] Theresa Stadler and Carmela Troncoso. 2022. Why the search for a privacy-preserving data sharing mechanism is failing. *Nature Computational Science*, 2, 4, 208–210. https://doi.org/10.1038/s43588-022-00236-x.

[24] Rob Stumpf. 2023. Carmakers are allowed to collect so much data on you-even about your sex life. (Sept. 2023). https://www.thedrive.com/news/carmakers-are-allowed-to-collect-so-much-data-on-you-even-about-your-sex-life.

[25] Vihangi Vagal, Konstantinos Markantonakis, and Carlton Shepherd. 2021. A new approach to complex dynamic geofencing for unmanned aerial vehicles. In *2021 IEEE/AIAA 40th Digital Avionics Systems Conf. (DASC)*. IEEE, 1–7. DOI: 10.1109/DASC52595.2021.9594499.

[26] Sokratis Vavilis, Milan Petković, and Nicola Zannone. 2016. A severity-based quantification of data leakages in database systems. *Journal of Computer Security*, 24, 3, 321–345.

[27] K. Vijayalakshmi and V. Jayalakshmi. 2022. A study on current research and challenges in attribute-based access control model. In *Intelligent Data Communication Technologies and Internet of Things*. D. Jude Hemanth, Danilo Pelusi, and Chandrasekar Vuppalapati, (Eds.) Springer Nature Singapore, Singapore, 17–31. ISBN: 978-981-16-7610-9.

[28] Binhua Wang and Yuan Ping. 2022. A comparative analysis of covid-19 vaccination certificates in 12 countries/regions around the world: rationalising health policies for international travel and domestic social activities during the pandemic. *Health Policy*, 126, 8, 755–762.

[29] Samuel D. Warren and Louis D. Brandeis. 1890. The right to privacy. *Harvard Law Review*, 4, 5, 193–220. Retrieved Jan. 11, 2024 from http://www.jstor.org/stable/1321160.

[30] Alan F Westin. 1968. Privacy and freedom. *Washington and Lee Law Review*, 25, 1, 166. https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20.

[31] Shiwen Wu, Fei Sun, Wentao Zhang, Xu Xie, and Bin Cui. 2022. Graph neural networks in recommender systems: a survey. *ACM Comput. Surv.*, 55, 5, Article 97, (Dec. 2022), 37 pages. DOI: 10.1145/3535101.