International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.com | editor@ijrai.com | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 3, Issue 2, March – April 2020||

DOI:10.15662/IJRAI.2020.0302001

Privacy-Preserving Contact Tracing Protocols

Kiran Renuka Prasad

Dr. Babasaheb Ambedkar Marathwada University, Chh. Sambhajinagar, Maharashtra, India

ABSTRACT: Contact tracing is a critical tool in controlling infectious diseases by identifying and notifying individuals exposed to infected persons. The challenge lies in balancing public health benefits with individual privacy, particularly when using digital technologies. This paper reviews privacy-preserving contact tracing protocols—particularly those appearing in the early COVID-19 response—with an aim to outline key technologies, their advantages, limitations, and future research directions. Protocols such as **DP-3T**, **BlueTrace**, **TCN Protocol**, **Trace-Σ**, and **Epione** leverage cryptographic methods—like Temporary IDs, Bluetooth proximity tokens, Private Set Intersection (PSI), homomorphic encryption, zero-knowledge proofs, and k-anonymity techniques—to notify potential exposures without revealing identities or sensitive data. We analyze decentralized versus centralized designs, including Apple/Google Exposure Notification and PEPP-PT, exploring their trade-offs in privacy, scalability, and trust. Protocols are assessed based on their mechanisms, adoption feasibility, cryptographic resilience, and integration with public health infrastructure. Results highlight that decentralized approaches (e.g., DP-3T, TCN) offer stronger privacy guarantees by keeping contact logs on devices, while centralized models (like BlueTrace) allow human-in-the-loop validation but risk broader data exposure. Emerging proposals like Trace-Σ incorporate zero-knowledge proofs to allow anonymous graph construction. We discuss the methodological strengths and overheads of these schemes, including computational cost and reliance on user uptake. The paper concludes that while early protocols demonstrated feasibility and solid privacy foundations, challenges remain in adoption, interoperability, and governance. Future work should focus on enhanced cryptographic efficiency, formal privacy guarantees, decentralized governance, and empirical evaluation in diverse populations. The insights here lay groundwork for privacy-first contact tracing infrastructures adaptable beyond pandemic emergencies.

KEYWORDS: Contact tracing, Privacy-preserving protocols, Decentralized systems, Bluetooth proximity, Cryptographic protocols, Private set intersection (PSI), Homomorphic encryption, Zero-knowledge proofs, DP-3T, BlueTrace, TCN Protocol

I. INTRODUCTION

Contact tracing—identifying and notifying individuals who were in contact with a confirmed infected person—has proven critical in managing infectious disease outbreaks. Traditional manual tracing methods are labor-intensive and slow; digital contact tracing emerged as a scalable alternative. However, widespread deployment raises privacy and ethical concerns, given the sensitivity of location and interpersonal data. The emerging COVID-19 crisis (early 2020) accelerated the need for privacy-preserving digital tracing systems.

Early digital tracing protocols aimed to minimize collection of personally identifiable or location data. The **BlueTrace** protocol from Singapore's TraceTogether app uses Bluetooth Low Energy (BLE) to record ephemeral IDs locally; only upon infection confirmation would a user's contact log be shared with health authorities Wikipedia. Similarly, decentralized protocols such as **DP-3T** store contact data on the device, not on centralized servers, enhancing privacy by design WikipediaCommunications of the ACM.

Other cryptographic approaches include the **TCN Protocol**, one of the earliest open-source anonymous BLE-based exposure alerts, influencing later frameworks like Google/Apple's ENF Wikipedia. More advanced approaches like **Trace-Σ** apply zero-knowledge proofs and accumulators to anonymously build a social graph of interactions without revealing identities IACR Eprint Archive. **Epione** introduces a PSI-CA (private set intersection – cardinality) scheme to alert users if infected contacts exist in their logs without revealing who they are arXiv.

Given the nascent stage of these protocols pre-2020, the main aims were to prove feasibility and develop cryptographic backbones that could be implemented rapidly in emergency contexts. This paper maps the key privacy-preserving strategies, explains their cryptographic mechanisms and architectures, and sets the stage for deeper evaluation of effectiveness, trust, and scalability.

| ISSN: 2455-1864 | www.ijrai.com | editor@ijrai.com | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 3, Issue 2, March – April 2020||

DOI:10.15662/IJRAI.2020.0302001

II. LITERATURE REVIEW

Although few protocols existed exactly in 2019, foundational frameworks emerged in early 2020:

1. **BlueTrace / TraceTogether** (March–April 2020): Developed by Singapore's government, it uses BLE-generated temporary IDs exchanged between nearby devices. A central authority collects contact logs only when users test positive Wikipedia+1.
2. **DP-3T** (April 2020): A decentralized architecture that ensures contact logs remain on devices. Exposure is checked by matching anonymized identifiers broadcast by infected users. It inspired the Apple/Google Exposure Notification framework WikipediaCommunications of the ACMWIRED.
3. **TCN Protocol**: One of the earliest BLE-based anonymous tracing protocols, designed for decentralized alerting without exposing contact logs Wikipedia.
4. **Epione**: Introduces a PSI-CA cryptographic primitive to keep contact logs private while alerting users of exposure. It defends against linkage and false reporting arXiv.
5. **Trace-Σ**: Applies zero-knowledge proofs and cryptographic accumulators to let a central server infer the connectivity graph without revealing identities IACR Eprint Archive.
6. **Communications of the ACM overview**: Reviews the practical deployment and integrated challenges of decentralized protocols like DP-3T in real-world apps across Europe Communications of the ACM.

Although full multiparty computation or homomorphic encryption methods like **PROTECT** and **DIMY** emerged later (2021 and 2022 respectively), their mention indicates evolving cryptographic innovation beyond 2019 JMIRPubMed. Altogether, the literature reveals an initial push in 2020 toward decentralized BLE approaches, followed by advanced cryptographic enhancements. Foundations laid in early 2020 inform future research on scalable, privacy-respecting tracing.

III. RESEARCH METHODOLOGY

The research methodology of this paper is structured as follows:

Protocol Identification
Collected initial digital contact tracing protocols developed in late 2019 to early 2020 (e.g., BlueTrace, DP-3T, TCN, Epione, Trace-Σ) via literature and preprint archives.

Protocol Classification
Categorized protocols by architecture: centralized (e.g., BlueTrace), decentralized (e.g., DP-3T, TCN), cryptographic-enhanced (e.g., Epione with PSI-CA, Trace-Σ with zero-knowledge proof accumulators).

Mechanism Analysis
Examined how each protocol manages identity, data storage, and exposure notification. Focused on cryptographic primitives used—temporary IDs, PSI, zero-knowledge proofs, accumulators.

Comparative Evaluation
Assessed protocols on:

Privacy protection – risk of deanonymization or data leakage.
Scalability & adoption – dependence on user uptake, device capabilities.
Computational overhead – cryptographic cost on mobile devices and servers.
Integration feasibility – ability to tie into public health workflows.

Threat Modeling
Considered adversarial scenarios: linkage attacks, re-identification, false reporting, metadata inference, central authority misuse.

Synthesis and Reporting
Compiled findings into structured sections: advantages, disadvantages, results/discussion, conclusion, future work. Developed cohesive narrative linking cryptographic design choices to practical trade-offs.

International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.com | editor@ijrai.com | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 3, Issue 2, March – April 2020||

DOI:10.15662/IJRAI.2020.0302001

Advantages

- **Strong privacy by design**: Decentralized approaches such as DP-3T and TCN avoid central storage of contact logs, reducing surveillance risk Wikipedia+1.
- **Anonymity with accountability**: BlueTrace balances privacy and traceability by using temporary IDs and consented log upload Wikipedia+1.
- **Advanced cryptographic protections**: Epione's PSI-CA allows exposure detection without revealing identities; Trace-Σ's zero-knowledge proofs enable anonymous graph analysis arXivIACR Eprint Archive.
- **Rapid deployment**: BLE-based protocols can be deployed using existing smartphone capabilities, essential during emergency rollout Communications of the ACM.
- **Public trust enhancement**: Transparent, privacy-centered designs (decentralized) encourage adoption Communications of the ACM.

Disadvantages

- **Adoption dependence**: Effectiveness relies on widespread app usage; many countries failed to reach required adoption levels (~60%) TIME.
- **Limited oversight**: Fully decentralized designs may struggle with verification or human-in-the-loop checks, risking false positives or errors.
- **Computational overhead**: Cryptographic techniques like PSI and zero-knowledge proofs can tax mobile devices and servers, affecting performance Reddit.
- **Metadata vulnerabilities**: Even with anonymization, metadata or pseudonymous logs can be re-identified or used to construct social graphs Reddit.
- **Interoperability and governance challenges**: Varying national protocols (centralized vs decentralized) impede cross-border functionality Oxford AcademicWikipedia.

IV. RESULTS AND DISCUSSION

Analysis shows that **decentralized BLE protocols**, especially DP-3T and TCN, deliver strong privacy guarantees by avoiding central data retention. However, their effectiveness is constrained by adoption rates and potential for false alerts without authority oversight.

The **BlueTrace model**, while preserving some privacy, introduces a trusted central authority that may raise concerns over data misuse or re-identification via social graphs.

Cryptographic enhancements (e.g., Epione, Trace-Σ) show promising privacy extensions beyond basic protocols, but their computational demands and real-world feasibility require further empirical validation.

Threat modeling reveals that even anonymized datasets are vulnerable to linkage and deanonymization attacks—particularly when combined with external metadata. Adoption and trust remain critical bottlenecks: without user buy-in, even best-designed systems fall short of public health goals.

V. CONCLUSION

Privacy-preserving contact tracing protocols developed in early 2020 established foundational architectures—especially decentralized BLE-based systems—that balance exposure notification with data minimization. These laid the groundwork for later enhancements that embed stronger cryptographic guarantees. Yet challenges in adoption, computational efficiency, metadata risk, and governance persist. Overall, decentralized systems represent a meaningful stride toward responsible digital contact tracing, but real-world impact hinges on trust, usability, and cross-system cooperation.

VI. FUTURE WORK

- **Optimized cryptographic efficiency**: Research efficient PSI, ZK, and accumulator schemes tailored for resource-limited mobile devices.
- **Formal privacy guarantees**: Rigorous modeling (e.g., differential privacy, formal proofs) to quantify anonymity and unlinkability.

| ISSN: 2455-1864 | www.ijrai.com | editor@ijrai.com | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 3, Issue 2, March – April 2020||

DOI:10.15662/IJRAI.2020.0302001

- **Interoperability frameworks**: Develop standards enabling cross-jurisdiction protocol compatibility without compromising privacy.
- **Human factors research**: Study user perceptions, consent models, and strategies to boost adoption and trust.
- **Hybrid governance models**: Investigate architectures that blend decentralization with scalable oversight, e.g., verifiable authority involvement without data exposure.

REFERENCES

1. Epione: PSI-CA based protocol for strong privacy contact tracing arXiv
2. Trace-Σ: Zero-knowledge proof protocol for anonymous graph collection IACR Eprint Archive
3. DP-3T and deployment overview Communications of the ACMWikipedia
4. BlueTrace / TraceTogether centralized model Wikipedia+1
5. TCN Protocol early decentralized design Wikipedia
6. Adoption challenges in European apps (~60% needed) TIME
7. Metadata/linkage vulnerability risks Reddit