Description

Modern-day innovations are increasingly relying on data. The quantum of innovation with data generated by proliferating digital applications, products, and services gives rise to many new ideas of making use of data. Without providing access to the data and sharing, it would be challenging to realize the true potential of digitization. Digital footprint of users captured in the form of data is also useful for criminal investigation, apart from serving the purposes of digitization. On the other hand, concerns about privacy associated with digitization are rising across the globe. Governments are responding by enacting rules, imposing increasing obligations and liabilities to protect citizen/resident’s privacy. Balancing benefits of digitization and privacy protection demand intervention of technology solutions. The problem of privacy during the investigation of crime also demands careful attention. Privacy preservation during the analytics and forensics not only gives comfort to citizens/residents but also help realize the goals of digitization and enforcing law.

Background

Low cost storage, variety of connectivity coupled with various sensors and applications, a significant amount of data is being generated, be it IoT, cloud-based system, or mobile apps. The variety of domains such as cloud-based healthcare systems, digital forensics investigations, BFSI, Critical infrastructure would gain significantly by mining the data if it is done in a privacy-preserving manner. Maximizing data utility while minimizing risk would be the key to the wave of digitization. The construct of digitization, without engineering attention to privacy, would fail to achieve its objectives. The ability of law enforcement officials to gain from the growing footprint of data would be constrained, if privacy is not ensured. It would need safeguarding privacy for structured and unstructured data in untrusted environments. The solution should meet the requirements of speed and heterogeneity of computing. It should be agnostic to the underlying hardware and operating environment. It should support multiple identities and key management protocols and offer built-in support for on-prem and cloud deployments.
Possible Targets

- Integrated Platform for processing big data in privacy preserving manner for effective decision making
- Real time, offline Privacy preserving authentication mechanisms
- Endpoint data collection in privacy preserving manner
- Mobile platform complying to privacy preserving requirements
- Cloud based solution offering privacy preserving technologies

Industry Use Cases

- Transaction processing industry (BFSI, Telecom)
- Industries such as Healthcare, E-commerce, e-Governance, etc.
- Government institutions and public sector for delivering public services and benefits transfer
- Law enforcement for preserving privacy during the investigation process
- Curbing frauds in educational and skill building industry
- Authentication of people in offline privacy preserving manner

Expected Outcome

- Solution or product that relies on software, hardware, cloud capability - any of it or combination
- Solution or product that provides high throughput, delivers a higher level of performance, and scalable
- Solution or product that promises higher accuracy, and lower false positives and negatives
- Solution or product that is interoperable and integrable