WHITE PAPER

Creating a data privacy shield for borderless workplaces

Abstract

COVID-19 has forced businesses across the world to adopt almost overnight to the Work From Home (WFH) model for their staff. However, as most companies realized, Work From Home introduces new vulnerabilities into the IT ecosystem, creating unique challenges for information security to organizations. With borderless teams transcending the borders of towns, states and even nations, a lot of data, including potentially personal or sensitive information is flowing across the walls of the workplace and through a variety of apps, sometimes with questionable protection arrangements.

Preventing privacy breaches has therefore become increasingly challenging, given that the methods of deception are also becoming more advanced. In this paper, we explore four key remote work induced information security challenges to enterprises, and we propose a proactive and preventive method towards ensuring consumer data privacy.

Beware: Four key data privacy challenges posed by remote work

Workplace ineffectiveness is one of the biggest source of data breaches, with reports finding that *17% of data breaches in 2019 were triggered by employees*[1]. With the work from home model in place, companies are likely to see a rise in threats that might contribute to data breaches; the challenges being bigger in the IT services space where often, the critical nature of the work requires dealing with sensitive data and personal information. Some of the key challenges that work from home will likely introduce for IT services include:

- **Enforcing data security**

Ensuring data security in remote operations is the biggest challenge for enterprises. There could be:

- Accidental exposure of information (personal, sensitive or confidential) to non-employees, intentionally or unintentionally.
- Poor security on mobiles and devices
- Unsecure work locations (home, café, etc.), which are not within the control of official boundaries, that further complicate matters.

Access control, authorization and encryption are key methods to address some of these challenges. But protecting the enterprise against threats in the form of malicious insiders requires establishing an effective monitoring and controlling mechanism.

- **Building a trust model**

With remote work, there is a risk of not properly implementing access, authorization and authentication policies, which may result in employees accessing resources that they are not authorized to. Even after having secure technology and proper policies for access, authorization and authentication, establishing trust and intrinsic confidence in associates is a challenging task. Companies have implemented security tools ensuring zero trust principles but there is a dire need to build a trust model such that everyone is engaged and productive in a positive way. A mechanism that effectively allocates tasks to agents, considering their utilization and nature of work, to enhance productivity is the need of the hour.

- **Protecting data in transit and at rest**

Data in transit refers to data that is traveling from point A to B, while data at rest refers to stored data, such as that on a user's laptop hard drive or cloud servers. Encryption technology prevents attacks on data stored on cloud servers, and local hard drives. Network data is protected through encrypted HTTPS, VPN and other methods. Transit data in IT service operations has to be tracked and managed and remotely working employees should have proper justifcation for accessing personal data. Although a lot of research and technology is available for secure computation in cloud, vunerabilities of data in-use continue to be a daunting challenge for enterprises.

- **Ensuring GDPR compliance**

The General Data Protection Regulation (GDPR), which was implemented in May 2018, immediately became a big focus for companies and pressured them to change their activities rapidly. However, GDPR compliance remains a bigger challenge for remote employees as many subtle aspects of GDPR are still vague when it comes to device location in remote workplaces.

Moreover, remote employees often use public Wi-Fi or shared internet connections, and personal hotspots that are mostly insecure.

To be GDPR complaint, organizations with borderless workplaces must have clarity on how they collect, store, share and use data.

They must also articulate clearly how access to corporate data is managed and what sort of permissions do people have.

Addressing cybersecurity challenges for a borderless workplace: A TCS approach

Misuse of customer data and privacy breach can lead to heavy financial, legal and reputational damages for organizations. At TCS, we propose a privacy by design (PbD) mechanism to enable robust data security in a borderless workplace. PbD is based on seven foundational principles, such as adopting proactive measures than reactive, preventive measures than remedial, privacy embedded into the design, data minimization and so on.

In service delivery operations such as IT support help desk, agents need to access the internal systems of an organization and its data, to serve customers efficiently. This data often

includes sensitive and personally identifiable information of the customers. In most cases, data exposure to agents occurs inevitably, particularly, in those services where complete automation of customer issue resolution is difficult.

Agents are assigned tasks and they need to form database queries to resolve customer requests. Undesired exposure of data required to cater to a customer request could lead to a privacy breach. We propose the Privacy Enabled Task Allocation (PETA)[2,3] model *(See Figure 1)* for assigning customer requests to agents such that the amount of data exposure and overall cost of operations are minimized. Data exposure is a metric to compute the amount of data exposure for a task (customer query) if a specific agent performs it.

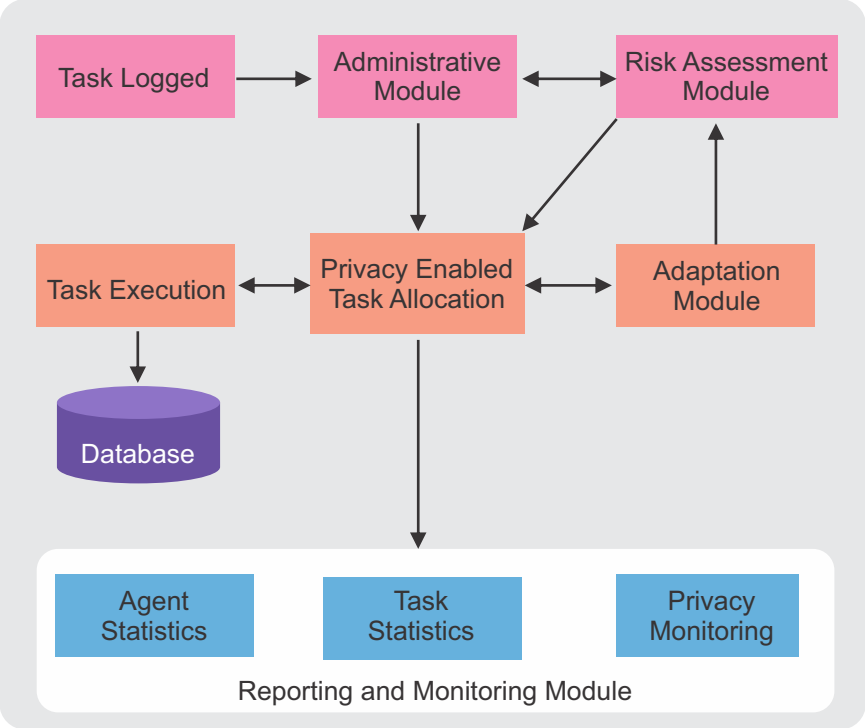

Figure 1 : PETA system for Secure borderless workplace

The exposure could vary if an agent with different expertise performs the same task. For example, if the agent is a trainee then the amount of data exposure would be high compared to an expert agent. Our model restricts this unintentional or intentional data exposure by limiting it per agent. This restriction in the amount of data exposure per agent is termed as privacy budget.

However, restricting this data exposure alone is not enough to avoid privacy breach. Some agents could intentionally gather more information than required from subsequent customer

requests. This could also lead to a privacy breach. For example, consider a scenario wherein a customer request reveals <age, gender> data. It is possible that in another request assigned to the same agent, <zipcode> data attribute could be exposed. In such a case, it is easier for the agent to uncover the identity of the person using these three data attributes. These are a set of tasks (customer requests), from which inferences could be derived by an agent (task-conflict set). In such scenarios where inferences could be derived from the allocated tasks, our PETA model regulates these allocations by assigning the tasks to different agents.

The PETA model restricts the data exposure per agent as well as regulates the task in the conflict set. It helps adopt the principles of privacy by design into service operations by minimizing data exposure and taking proactive measures. A detailed description of the approach along with quantification of data exposure and illustration can be found in Figure 2 .

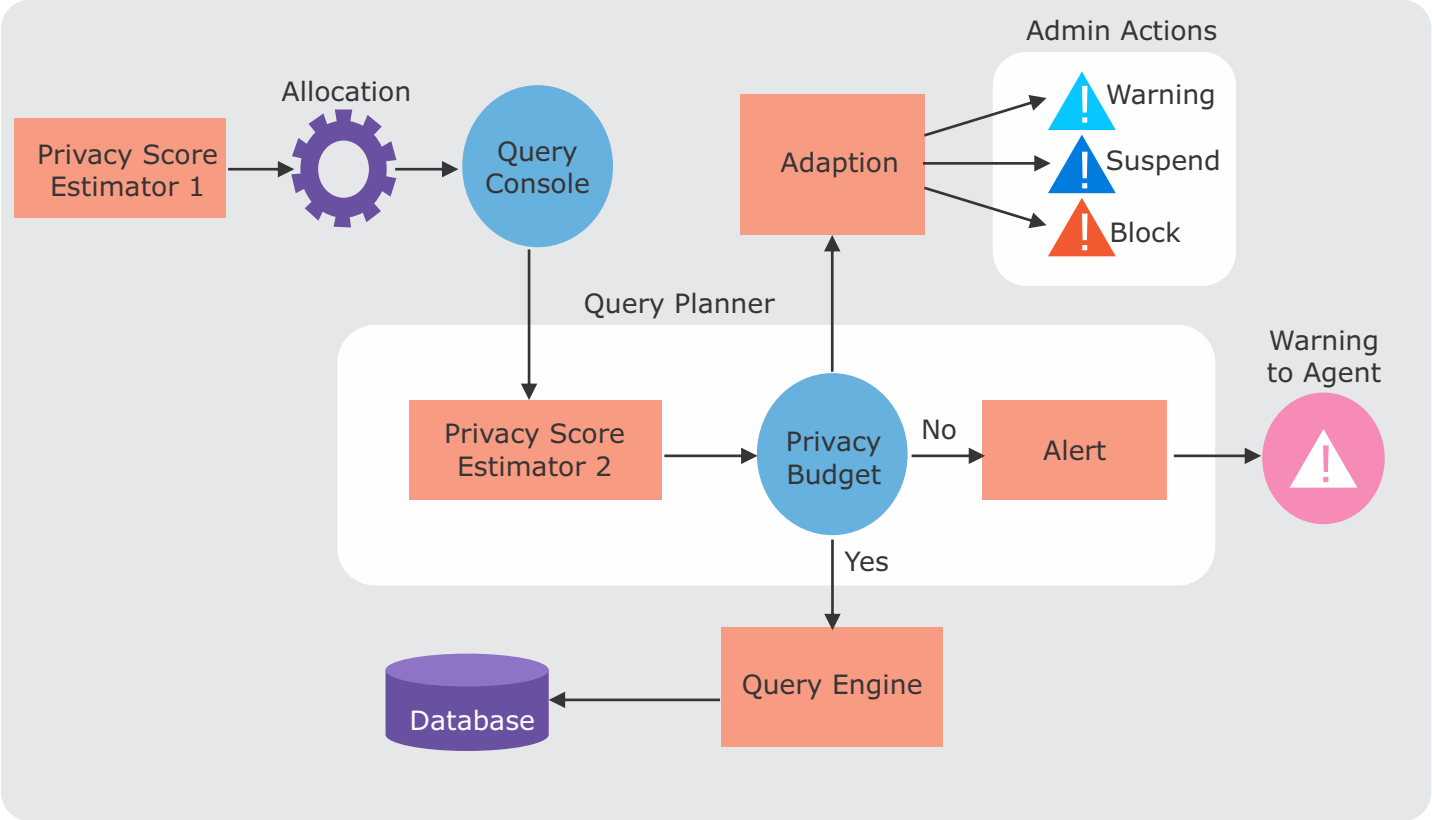

Figure 2: Limitation and quantification of data exposure with the PETA model

Securing privacy in the future of work

The PETA approach presents an efficient mechanism to control, monitor and restrict data exposure in IT services operations, making it well suited to the current borderless workplace scenario where security matters most. The best part - PETA is an external plug-and-play system that can be easily integrated with any existing process or system, without requiring any changes in the application architecture or code. It is a proactive centralized monitoring and alerting system for sensitive information access that helps organizations to take efficient and timely action against insider threats in work from home scenarios. The PETA model also helps increase agent productivity as its allocation mechanism efficiently handles work load balancing in task allocation to agents. Industry sectors such as finance and insurance, healthcare, public administration and Business Process Outsourcing (BPO) stand to benefit immensly from the PETA approach in securing privacy of the customers.

References

[1] *PETA: Privacy Enabled Task Allocation. Article accepted in IEEE Services and Computing conference 2020.*

[2] *Patent filed in India, US and Euro, 'Method and System for Privacy Enabled Task Allocation', 2019.*

[3] *https://haystax.com/wp-content/uploads/2019/07/Haystax-Insider-Threat-Report-2019.pdf*

TATA CONSULTANCY SERVICES

About The Authors

Nitin Phuke

Nitin Phuke is a researcher with the Cybersecurity and Privacy Research Lab, TCS, Pune. Prior to joining the CTO research team, he contributed to project development and production deployment for a large banking customer. As a researcher, Nitin has contributed in many research projects, building POC's and creating intellectual property. He has published several papers in refereed journals and has also presented these at international conferences. Nitin holds a Master's degree in Computer Engineering from the College of Engineering, Pune, India.

Dr. Mangesh Gharote

Dr. Mangesh Gharote is a Research Scientist with TCS Research Lab, Pune, and currently leads the Infonomy research group, addressing optimization problems in the Cybersecurity and Privacy areas. He has over 15 years of rich experience in research and has contributed to many customer projects, and has created intellectual property. Dr. Gharote has to his name several published papers in refereed journals. He has also presented these papers at several international conferences. He has a Ph.D. in Operations Management, and a Master's degree in Industrial Engineering & Operations Research -- both from IIT Bombay, India.

Contact

Visit the Research and Innovation page on www.tcs.com

Email: innovation.info@tcs.com

Blog: #Research and Innovation

Subscribe to TCS White Papers

TCS.com RSS: http://www.tcs.com/rss_feeds/Pages/feed.aspx?f=w
Feedburner: http://feeds2.feedburner.com/tcswhitepapers

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

Experience certainty. IT Services
Business Solutions
Consulting

TCS Design Services I M I 09 I 20