حماية أمن البيانات العملاقة خلال التخزين والإرسال

يمثل الأمان والخصوصية للبيانات الكبيرة تحديًا كبيرًا لمالكي البيانات وموفري الخدمات على حد سواء. أصبحت البيانات الضخمة ضرورة لرجال الأعمال والباحثين والرعاية الصحية والوكالات الحكومية. ومع ذلك، لا يتم تصميم الأدوات والتقنيات التي يتم تطويرها لإدارة هذا الحجم من البيانات لمعالجة متطلبات الأمان والخصوصية .أصبح أمان البيانات الكبيرة وخصوصيتها أمرًا صعبًا مع نمو البيانات وزيادة إمكانية الوصول إليها من قبل المزيد والمزيد من العملاء. أصبح تخزين البيانات على نطاق واسع ضرورة للرعاية الصحية، قطاعات الأعمال، الإدارات الحكومية، المساعي العلمية والأفراد. سيركز بحثنا على الخصوصية والأمان وكيف يمكننا التأكد من تأمين البيانات الضخمة. تمثل إدارة سياسة الأمان تحديًا سيتناوله إطار عملنا للبيانات الكبيرة. يجب أن تكون سياسة الخصوصية متكاملة ومرنًة ومراعية للسياسات وقابلة للتخصيص . ركز بحثنا على تجزئة البيانات الحساسة ثم تشفيرها بناءً على سياسة مالك البيانات. لقد أنشأنا إطارًا لتلقي البيانات من العملاء، وتحليل البيانات المستلمة، وتحديد البيانات الحساسة وغير الحساسة، وتطبيق التجزئة، وتشفير البيانات الحساسة، وأخيرًا تخزين البيانات. سيحمي الإطار البيانات ويضمن خصوصية العملاء. تم إنشاء تقنيات مختلفة لاستخدامها في إطار عملنا .قدم إطارًا جديدًا يحمي البيانات من البداية إلى النهاية. تطبيق المصادقة إلى مركز البيانات ومن ثم فرض السياسة على البيانات المراد تخزينها واستردادها. نحن نفرض أيضًا السياسة على إجراءات المستخدم ويتم تشفير البيانات الحساسة وتطبيق التجزئة أيضًا. كما تم تطبيق نموذج التدقيق لجميع إجراءات وطلب البيانات.

وأخيرًا، قمنا بتقييم الإطار والتحقق من صحته عن طريق تطوير النموذج الأولي وحالات الاختبار المطبقة على النموذج الذي أظهر إنجازًا ناجحًا ومحققا للأهداف المنشودة.

SECURING BIG DATA ON STORAGE AND DURING TRANSMITTING

Big Data security and privacy is a big challenge for both data owner and service providers. Big Data has become a necessity for business, researchers, healthcare, and government agencies. However, the tools and technologies that are being developed to manage this volume of data are not designed to address security and privacy requirements.

Security and privacy of big data becomes challenging as data grows and more accessible by more and more clients. Large-scale data storage is becoming a necessity for healthcare, business segments, government departments, scientific endeavors and individuals. Our research will focus on the privacy, security and how we can make sure that big data is secured. Managing security policy is a challenge that our framework will handle for big data. Privacy policy needs to be integrated, flexible, context-aware and customizable.

Our research focused on fragmentation of sensitive data and then encrypt sensitive data based on the policy of the data owner. We built a framework to receive data from customers, analyze received data, identify sensitive and non-sensitive data, apply fragmentation, encrypt sensitive data, and finally, store data. The framework will protect data and secure privacy of the customers. Different techniques were created to be used in our framework.

We introduced a new framework that protects the data from end to end. Enforcing the authentication to the data center and then enforcing the policy to the data to be stored and retrieved. We also enforce the policy to the user actions. Encryption of sensitive data and applying fragmentation is done too. Auditing model also implemented to audit all actions and requests to data.

Finally, we evaluated and validated the framework by prototype implementation and applied test cases to the prototype which showed a successful and target achievement.