Sensing node principally is only responsible forsending data to the server that later on will forward the datato the user. Through this mechanism, the user will receive thedata from the sensing node based on the value sent withoutany data verification at the server-side. The data in this case could be invalid. Thus, error handling as the main problem of the research is needed. By ensuring that this problem is worth objectivity raising, then through the Risk Management Process Model, it is certain that this problem will cause an adverse threat. After identification, 6 arising risk were found, with the level of control at threat". Furthermore, 7 Mitigation Actions (MA) were designed and grouped into 3 Mitigation Phases (MP). Mitigation plan was realized into a platform with several system blocks including 2 middleware blocks giving data error handling service directly. Moreover, to ensure that the proposed platform has covered all existing risks, service guarantee agreement was made in the form of a Service Level Agreement (SLA).The test results showed that both SLA 1 and SLA 2 succeed in guaranteeing no more risk arising. The test results showed the security level value is 6/6 =1, which means all of the risks are "handled" status and succeed in scope of "eliminate". Eventually, when the proposed platform is adopted directly to the organizations that need it, it is expected that it can be the answer to the problem of error in data sensing.