SPOT A FAKE

Denzil Correa
Data Scientist,
Max Planck Institute for
Software Systems, Germany

Educational qualifications and work experience records of potential employees serve as important information for any professional organisation's recruitment team. However, about 40% of job applicants lie about their employment and educational histories while 20% present false credentials and licences, reports the Society for Human Resource Management. An organisation which chooses not to verify a job seeker's credentials risks higher staffing costs, performance issues, criminal liability and disrepute to organisational goodwill. Not only this, even the recent alleged Delhi rape case involving a cab driver, who reportedly had a run-in with the law earlier as well, underscores how crucial document and crime record verification are.

Currently, most credential checks are carried out manually, which requires job applicants to furnish original certificates. The employer may or may not verify the furnished degree based on manual inspection, which is tedious, expensive and can lead to unauthorised verification compromising the individual's privacy. To counter this issue, some universities require employers to submit original copies of certificates in person. However, given the issues in the process, if employers do not verify all recruits' documents, they could jeopardise organisational well-being.

There are various systems in the market that provide fast credential authentication but at the cost of user privacy. However, technology needs to be employed to achieve the twin goals of maintaining confidentiality and vetting documents. An online system that can quickly scrutinise documents while respecting applicants' privacy can be a win-win. The e-system combines three computer science fundamentals — cryptography, distributed computing and databases. The interplay of these fundamentals, in conjunction with ubiquitous computing, helps achieve the objectives.

An individual's credentials are distributed across different local organisations via a local credential server to which s/he is affiliated, such as a workplace, university or school. The main credential server receives an online request for credential authentication and directs it to each appropriate credential database server — work, university or school. Each of these requests is encrypted using state-of-the-art cryptographic techniques to ensure a high level of security. This, along with the distributed server design, is meant to ensure that the system is secure against targeted attacks. The e-request is then forwarded to the individual for whom the information is sought (credential owner); s/he approves the request via any internet-enabled device — using a mobile application, email, etc. The credential owner may decide to provide partial or full information as sought and could even restrict the timeframe for which the information is accessible by the credential seeker. S/he could even reject the request. Therefore, the system can ensure timely, automatic verification, with a privacy mechanism to deal with unauthorised requests.

[Correa completed his PhD at Indraprastha Institute of Information Technology (IIIT) Delhi in December 2014. Ashish Sureka, adjunct professor, IIIT Delhi, and he developed a system and method for verifying credentials]