A Secure Cloud Based Digital Signature Application for IoT

Sahar A. El-Rahman, Benha University, Cairo, Egypt & Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia
Daniyah Aldawsari, Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia
Mona Aldosari, Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia
Omaimah Alrashed, Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia
Ghadeer Alsubaie, Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia

ABSTRACT

IoT (Internet of Things) is regarded as a diversified science and utilization with uncommon risks and opportunities of business. So, in this article, a digital signature mobile application (SignOn) is presented where, it provides a cloud based digital signature with a high security to sustain with the growth of IoT and the speed of the life. Different algorithms were utilized to accomplish the integrity of the documents, authenticate users with their unique signatures, and encrypt their documents in order to provide the best adopted solution for cloud-based signature in the field of IoT. Where, ECDSA (Elliptic Curve Digital Signature Algorithm) is utilized to ensure the message source, Hash function (SHA-512) is used to detect all information variations, and AES (Advanced Encryption Standard) is utilized for more security. SignOn is considered as a legal obligated way of signing contracts and documents, keeping the data in electronic form in a secure cloud environment and shortens the duration of the signing process. Whereas, it allows the user to sign electronic documents and then, the verifier can validate the produced signature.

KEYWORDS


1. INTRODUCTION

The vast evolution of the communication and networks in the last two decades changed the way our world works drastically (Srivastava, 2013). Using signature in paper transactions has been spread over the last years as a way of gaining assurance of the identity and authority of the parties involved in a contract (Sumroy and Sherrard, 2012). Electronic communication methods such as Email and the Internet make it potential to execute contracts. The most important formal requirements are the signature; therefore, a contract requiring a signature need to be able to do so electronically (Laborde, 2010). Digital Signature that is defined as an electronic data that is logically associated with or
attached to other data in electronic form and that is considered as an authentication method (United Nations Publication, 2009). Also, a digital signature is an arithmetical model used to validate the authenticity and integrity of a digital document, message, or software (Martoni and Palmirani, 2013). Including assurance as to its authenticity even if later the verifying party or signer tries to deny (Chiranth and Shashikala, 2012). Because of the Internet’s security protection holes, several of the digital community members explored how to allocate risk if a security breach were to occur. From this investigation, three main issues were identified as security risks: integrity, non-repudiation, and authentication (Stern, 2001).

Digital signature should provide three main services: Authentication which is linking the creator of the information, Integrity, which means easily detecting any variations to the information provided and Non-repudiation for making sure of the satisfaction (from a legal perspective) about where the electronic signature is coming from (Wang, 2014). Digital signature laws had three generations, which started appearing since 1995 (Blythe, 2007; Embrogno, 2012). Moreover, mobile signatures are predicted to get a great future. To grant signatory mobility apart from a fixed, secure desktop workstation that has a trusted, personal signing tool (Rossnagel and Royer, 2005), and because of how smart devices are taking over PC’s a need for signature applications emerge and many applications started to hit the different markets (Google Play, App Store and windows store).

2. CLOUD COMPUTING

Now that almost all companies that used to rely on paperwork are moving to cloud services due to the powerful benefits those services provide this issue is becoming even more critical (Srinivasan, 2014). Whereas, cloud computing becomes a novel paradigm to offer computing as a utility. It is considered as a scheme to enable convenient, ubiquitous, on demand access to the network to share a configurable compute resources (Kinastowski, 2013; Mella and Grance, 2011). So, when two people are making a deal and they form an agreement to sign a document to accomplish the deal and to prove that neither party can oppose the deal later. Now what if one party used a fake signature and is planning to fool the other party? Digital signature should provide the non-repudiation needed (Azizi, 2011). A cloud based digital signature is considered as a paradigm for proper, reliable, secure infrastructure, with flexible access to the network that implements digital signature cryptographic processes. The main variation between a cloud based digital signature model and a standard one is the first comprises a network data interchange between signing-enabled cloud environment and the signer, but the second works in the closed environment of a plugged-in a dedicated device (card reader and microchip card) and PC (Kinastowski, 2013; Shakil et al., 2017). The most notable feature of cloud computing technology that related to the IoT is the storage over internet, so the document availability becomes 24/7 over the cloud and the users can digitally sign documents and request the digital signature of other individuals (AlZain et al., 2015; Stergiou et al., 2018).

3. INTERNET OF THINGS (IOT)

Recently, IoT has been given a significant research awareness. IoT is considered the networking future. Where, IoT is a novel paradigm that involves everyday physical world entities by enabling exchange among them (Koppula and Muthukuru, 2016). IoT utilization in various applications is predicted to rise quickly in the forthcoming years. IoT permits billions of services, peoples, and devices to connect each other and interchange the information. So, the increasing of IoT objects utilization, the networks of IoT are subject to different security attacks. The privacy protocols, and efficient security deployment in IoT networks is highly required to ensure authentication, integrity, access control, and confidentiality, among others (AbdurRazzaq et al., 2017; Elmisery et al., 2017; Singh and Singh, 2015). The combination of IoT with cloud computing will provide the convenience of the proposed application (Stergiou et al., 2018).
Hybrid Data Security Model for Cloud
www.igi-global.com/article/hybrid-data-security-model-for-cloud/95043?camid=4v1a

Resource Management Mechanisms to Support SLAs in IaaS Clouds
www.igi-global.com/chapter/resource-management-mechanisms-support-slas/66238?camid=4v1a