ABSTRACT

Smart phones and hand held devices have become integral part of the digital era. Humans are increasingly dependent on these devices for daily survival, both personally and professionally. With the advent of Cloud Computing, digital users access, process and store information anywhere, anytime with the help of handheld devices. Furthermore, with the emergence of 4G/ 5G technologies and IoT based smart devices, Cloud Computing has branched to another area called Mobile Cloud Computing, popularly known as *Mobile Cloud*. Mobile Cloud enables the users of mobile devices to perform complex functionalities and data storage via thin clients such as smart phones and tablets. Mobile devices have the constraint of limited battery power and memory. Mobile Cloud provides requested services through a legal agreement between Cloud service providers and mobile users which is called as Service-Level Agreement (SLA). In Mobile Cloud, resources can be dynamically reconfigured for better performance. In Mobile Cloud, confidentiality is achieved by authorization and authentication of users. Only authenticated users are allowed to modify the data to ensure integrity. Availability is another important QoS parameter for Mobile Cloud. This Thesis addresses the above mentioned issues i.e. confidentiality, integrity and availability, by proposing new framework with the corresponding procedures.

First, a SiteKey authentication mechanism is proposed in this Thesis, in which an image specified by the user is used for encryption. The encrypted image is divided into three equal image shares and is distributed among three entities, namely, the Mobile Cloud user, Internet Service Provider (ISP) and Cloud Service Provider (CSP) to deter unauthorized access. In order to increase the security, a secret phrase is embedded in three

image shares of the original image using steganography to prevent cheating by any compromised entity. The proposed authentication mechanism enhances the security further when compared to the existing fingerprint authentication for Mobile. There are two phases in the proposed authentication mechanism, namely, enrolment phase and login phase. In the enrolment phase, the users while registering with CSP, choose their username and password credentials along with other necessary information. After registering with the CSP, the user is redirected to choose secured authentication mechanism. Then, the users are requested to choose a secret image of their own choice and a secret phrase or sentence. The performance evaluation is done using the proposed SiteKey authentication for 30 participants by allowing each user to perform enrolment and login phases. The QoS parameters considered are enrolment time and login time for authentication. The average enrolment time and login time are 2.1 seconds and 1.7 seconds respectively. The average processing time for enrolment and login phase using the proposed framework is lower, when compared with fingerprint authentication for Mobile Cloud. Furthermore, the use of steganography with visual cryptography prevents unauthorized hackers from reproducing the image share and adds another level of security which deters phishing attacks.

Next, an agent based Secured Data Storage Classification Architecture (SDSCA) for Mobile Cloud is proposed in this Thesis. The agent classifies the users data into three different groups, namely, low, medium and high. Then, the data are encrypted using Advanced Encryption Standards (AES). Encrypted data is transferred to the broker for selecting suitable service agent. But, the broker has many-to-one relationship with service agents. The data is encrypted and sent to the CSP for storage which enables the Cloud provider and Cloud user to process the data without the

need for decryption. The proposed work relies on homomorphic encryption. The proposed agent based naive classifier provides better results in terms of processing time and security in Mobile Cloud. Performance evaluation of the proposed framework includes encryption time. Results are taken for files of varying sizes such as 32, 64, 128, 256 and 512 MB. The speedup value is better with an average of 7.6%, when compared with the results using RSA along with SHA scheme.

The SLA is managed by third party entities, and in some cases, it is managed by intelligent autonomic agents. In order to cater to the growing needs and demands of customers, dynamic SLA is offered by service providers. A dynamic SLA is updated and redefined whenever new services are demanded by the customer after SLA negotiation. Consequently, these dynamic SLA need tamper protection from unauthorized users to prevent unnecessary changes which may lead to SLA violations. As a result, all stakeholders, namely, autonomous intelligent agents, customers and CSP can modify the SLA without decrypting the encrypted SLA and SiteKey authentication, and thereby achieving tamper protection. This Thesis has proposed a protection scheme for the dynamic SLA using visual cryptography homomorphic encryption. The proposed work also ensures multiparty involvement in achieving dynamic SLA management. The simulation environment consists of mobile user, agent and CSP. The simulated environment handled 10 to 30 service requests. The measured results are compared with established threshold values and checked for SLA violations. The availability of service is high i.e. 93% during business hours, average i.e. 83%, during end user hour and low i.e. 80% during keep-up hours. Furthermore, the proposed framework prevents the identity thefts by malicious insiders and phishing attacks by malicious outsiders by combining visual cryptography and homomorphic encryption techniques.