# Now most widely used security protocol on

Nowa day’s IT industries moving towards web based technology from softwareapplications.  Secure communication is anintegral part of today’s world of on-line transactions. Users on the internetexchanging financial, business or personal information, want to know whetherthe information is secured or not and they wish to ensure that the informationis during transaction is not modified and disclosed. 11 We can say websecurity is one of the crucial topic in both technology and everyday life. Tomaintain secure communication on web, communication between client and servermust be secured by SSL (securesocket layer).

SSL protocolprovide security in network layer which consist of encryption algorithms. The SSL protocol can apply on any application that runsover TCP can also run over SSL. SSLis the most widely used security protocol on the Internet today. It offersencryption, source authentication and integrity protection for data and isflexible enough to accommodate different cryptographic algorithms for keyagreement, encryption and hashing. However, the specification describesparticular combinations of these algorithms, called cipher suites, which havewell understood security properties. Today, SSL is trusted to securetransactions for sensitive applications ranging from web banking, to stocktrading, to e-commerce. 11 Unfortunately, the use of SSL imposes asignificant performance penalty on web servers. secure web servers running 3.

4to 9 times slower compared to regular web servers on the same hardwareplatform. SSL utilizes RSA encryption to transmit a randomly chosen secret thatis used to derive keys for data encryption and authentication. The RSAdecryption operation is the most compute intensive

part of an SSL transactionfor a secure web server. Fig 1. 1 SystemSecurityButthe level of security RSA gives with larger key size can be achieved by ECCwith much smaller key size that reduced the server load and accessing the databecome much faster.

8