CONCLUSION & FUTURE SCOPE

Cryptographic techniques and tools are playing an important role in designing emerging network security technologies. It is evident from the fact that world's most developed countries like U.S are considering cryptographic technology as the standard technology keeping in view the security aspect of the fast growing commerce, banking, military activities of the world and it is need of the day that it should be standardised so that the whole world can benefit from it. Cryptographic Key Management (CKM) is a fundamental part of cryptographic technology and is considered one of the important aspects associated with its use. Scalability of the methods used to distribute keys and the usability of these methods are of particular concern. That is why NIST (National institute of Standards and Technology) of USA, has undertaken an effort to improve the overall key management strategies used by the public and private sectors in order to enhance the usability of cryptographic technology to provide scalability across cryptographic technologies, and support a global cryptographic key management infrastructure.

This preamble to the conclusion is just to emphasize the need to work more on these techniques. Present work is also an effort to peep into these techniques. From the work done it is very much clear that using cryptographic algorithms for key exchange like Diffie-Hellman to applying digital signatures to authenticate the user as well as the content of the information are important linking elements to enhance the security feature of the system, information as well as the network. Hashing techniques like SHA1, SHA256, SHA384, SHA512 and MD5 have been used for computing the message digests and further computing components of the digital signature. Blowfish algorithm also has been used for encryption being light weight and in public domain which can handle keys from 64 bits to 448 bits. The level of security provided by Message Digest Algorithms is considered to be sufficient for implementing very high security hybrid digital signature schemes
based on MD5 and a public-key cryptosystem.

The nature of the Diffie-Hellman key exchange does make it susceptible to man-in-the-middle attacks since it doesn't authenticate either party involved in the exchange. This is why Diffie-Hellman is used in combination with an additional authentication method digital signatures given name Integrated Digital Signature Diffie-Hellman (IDHDS) algorithm. When using RSA, a 1024-bit key is considered suitable both for generating digital signatures and for key exchange when used with encryption, while a 2048-bit key is recommended when a digital signature must be kept secure for an extended period of time such as a certificate authority’s key. Work has been done using Blowfish Algorithm and an intrusion detection system. A hypothetical model has been proposed which is supposed to have an inherent feature of matching encrypted signatures. Proposed security model will help in preventing evasion of the deployed IDS. Security of the network system can be enhanced with use of encryption algorithms like Blowfish before an IDS. Study shows that Blowfish has better encryption (i.e. stronger against data attacks) than the other algorithms. Blowfish has an additional advantage over other algorithms in terms of throughput and execution time. It is an excellent choice in combination with digital signature algorithm (DSA) for adding system security, data integrity and confidentiality capabilities to embedded and other systems being lightweight in public domain and considered secure even after extensive analysis. Further working with an open source IDS like Snort gives much of leverage to the strategic security design teams. Rule options give ample scope for modification and manipulation as per the need of the security requirements of a concern.

Further variable working modes of the Snort IDS (passive, inline) makes it more versatile because it can also work as an intrusion prevention system, which otherwise it is not in its default mode. Results of protocol wise packets received per minute in the present work show that throughput is more in inline mode with
faster packet processing and decreased memory requirements when used with improved rule options. In default snort automata does matches against all the rules whereas smart snort does it according to the new automata which makes it to do pattern matches against only specific part of the option portion of the rule. Automata is basically the guiding program which IDS has to follow for pattern matching. This has been achieved by working on the automata of the multipattern matching algorithm, which it uses for pattern matching and made snort more secure and versatile.

**Future Work**- The proposed model can be improved by using Twofish Algorithm for pattern matching in the intrusion detection system. Better Key length will provide better symmetric algorithm implementation and security. Signatures can be added across databases of multiple IDS systems based on the level of threat to the network.