EXPLORATION OF CRYPTOGRAPHIC ALGORITHMS ON EMBEDDED RISC ARCHITECTURE

The protection of sensitive information against unauthorized access or fraudulent changes has been of prime concern throughout the centuries. Modern communication techniques, using computers connected through networks (wired / wireless), make all date even more vulnerable for these threats. Cryptography is an essential process to assure confidentiality over wired/wireless communication channels, these channels are an open medium to intruders in which they can intercept and alter the contents of any transmitted information. Cryptography is the foundation of all information security which deals secrecy and authentication of data. Implementation of secrecy and authentication features for data and sensor data applications on wired/wireless embedded networks becomes crucial, because of stringent resource constraints (SOC processor, Memory, complexity of computational algorithm, protocols, data integrity. QOS, area, power, speed and etc..) to implement on various embedded reconfigurable architectures. To enhance the system performance including these features (secrecy and authentication), the present researchers have lot of scope to further investigation of various security algorithms to implements on modern tinny resource constraints secured embedded systems.

The cryptographic algorithms are categorized in to a block cipher is an encryption / decryption scheme in which a block of data is used to produce the cipher text and a stream cipher is one that encrypts a digital data as a stream of data. The well known block cipher algorithms are TDES, AES and the stream ciphers are RC$, SEAL. The basic functions of any security algorithm consist of transposition, substitution, rotation and confusion. To design or implement above set functions the researchers proposed and proposing various computation procedures. TDES algorithm mainly includes two basic functions transposition and rotation. The AES algorithm uses with the three different key lengths are “AES-128”, “AES-192”, and “AES-256”. The basic transformation functions used in AES algorithm are **sub-bytes, shift-rows, mix-column** and **add-round key** transformations. Block ciphers uses fixed length key and data. RC4 is a famous stream cipher includes basic functions like key initialization, key setup and key streaming. Stream cipher uses variable key and data lengths.

Reset data communication protocols implementation consists of transferring of data (sensor, text and image) on various embedded networks (wired/wireless) become crucial, because of several constraints like network design, buffering, integrity, QOS and etc. upto now most of the researchers investigated the performance of various protocols implementation on embedded wire and wireless communication networks. They did lot of research on data integrity (error correction and detection) and QOS etc. adding the security (secrecy and authentication) features for existing research work would definitely encourages the present researchers and system implementation engineers upto great extent.

Now a day's implementation of various security algorithms (block and stream ciphers) on embedded reconfigurable RISC architecture, for sensor and image data applications become a challenge job for current researchers, because of resource constraints like area, power, speed etc.. The research work focuses on effective implementation of various security algorithms (Block Ciphers : AES and TDES and Stream Cipher : RC4 and SEAL) for embedded wire and wireless sensor data networks, our research work may extract the desired security algorithms from existing algorithms or proposes the design of new algorithms for resource constraints tinny embedded system applications, the work includes study and investigate the feasibility of various security algorithms, those suits for image data security applications.

To carry out the proposed research work by adapting various industries driven embedded EDA tools, embedded design, simulation & implementation methodologies. Source of the following familiar basic tools, IDE's & ISE's.

Embedded software Tools	**:** Cross compilers, Emulators, Simulators & etc..
Hardware Tools	**:** ORCAD (schematic & PCB) design, simulation & validation.
Languages	**:** Embedded – C, MATLAB : Language & tools box.
Processors	**:** 8 – bit Amtel, 32 – bit embedded ARM RISC Architecture.