1. Introduction

1.0 Subject Introduction

Now a days, security of any form is a basic requirement for all most every intelligent systems in the embedded world. It include systems for general purpose or domestic purpose to highly sensible systems like missile and rocket launching and military purposes. Some examples are smart cards, sensors that are connected to network or individual systems. [109] With the advancement of technology which has caused tremendous technological improvement in the world of electronics has also aided in the increased the latest advancement and technical usage in developing sophistication of security attacks. Number of sensitive applications such as mobile banking on a cell phone, using wrist watch that can monitor a patient’s health and connecting oneself to the office while physically away from the office demands data protection and authentication. Along with the basic needs of reliable connectivity, high data transfer rate and optimized storage and processing, the data and information security is equally very vital. [48]

Though embedded systems are used for highly domain specific one another factors to be considered is that the other side domains themselves are expanding for such systems. Latest embedded devices demands information transfer between other devices within networks and hence the need for network security is increasing for all these domain specific systems. Usually as the embedded systems are classified to be resource constrained one, the small key size of ECC makes it effective to implement on such systems. Among all the cryptographically methods the ECC is now treated as the most trusted and best solution for providing security on embedded systems. It was Neal koblitz and Victor Miller who put forward the concept and design of elliptic curve cryptosystems during mid 80s. This elliptic curve is taken as the advancement of the
previous discrete logarithm cryptographical systems (DLC). The computational intractability and
the tough mathematical calculations are the basis of the high level protection and security of
elliptic curve cryptosystem that makes it highly secured and the best one.[100] When two parties
exchange message, the Message authentication protects them from the third party who tries to
steal the information. But even the message authentication cannot be considered as full
protection ie when both the party that sends and that receives don’t have mutual trusts then the
Digital signatures are requires in addition to message authentication. A code that is attached to
the message will form or act as signature this mechanism that has been used to increase the
authentication to protect the creator of the message is termed as digital signature. Basically the
signature is formed by applying the hash function over the message taking the hash of the
message and encrypting the message with the existing secret key of the sender or author of the
message. So a signature always makes sure that source and integrity that one needs for the plain
sensitive information is retained that is protecting the information from being tampered. The
signatories identity can be confirmed and unauthorized modification of data by unknown parties
can be eliminated by the usage of digital signature. The signed data at the receiver end will be
using a digital signature in establishing another new party to make sure that the signature has
been in fact originated and made by the original owner who infact put the signature. The
standard for Digital Signature proposed and formulated by Federal Information Processing
Standard has specified it clearly.

The attribute of the logarithmic problem that its very hard to trace and do the reverse function
that the DSA has been developed on it and with that the security has been achieved to a great
extend. Signature generation and cross checking the signature are the steps in a Algorithm
concerned with the digital signature that is the DSA. First the generation process is applied by
the sender or communicator to form and initialize the digital signature over the data. The cross check from the receiver side uses a cross checking process to check the authentication or correctness as far as the signature is concerned. Every signatory will be having a public key and a secret key with them. In the generation of signature process the private key is used. The signatory is also called as the key pair owner is the only one authorized to use the private key to generate digital signatures. The private key should be kept highly secured and beyond the reach of second party other than the key pair owner to prevent unwanted claims and also to generated fraudulent and false signatures. So the person of the owner who is having both these keys is the only person entitled to keep the private key. In public key systems three basic choices are available for the following.

1. **RSA**

   RSA cryptosystems was put forwarded by Ron Rivest, Adi Shamir, and Len Adleman. Secrecy, security and keeping the authority of ownership of digital data are the main factors provided by RSA.[36]

2. **DH/DSA**

   A new algorithm in the public key cryptography called Digital signature algorithm was designed and developed by Diffie and hellman. It is based on prime field and is basically a discrete log problem. The Digital signature standard was proposed in 90s based on this algorithm by the United state government.

   **Elliptic Curve Diffie Helman Algorithm**.
A new algorithm called RSA was suggested in the 80s by cryptographers Rivest, Shamir, and Adleman with the basis that it is difficult to factoring large integers. In 1976 a system based on public key called Diffie-Hellman key exchange was conceptualized and kept forward by Whitfield Diffie and Martin Hellman.[37] During 1985 Elliptic curve groups was put forward that can be used in place for the multiplicative groups modulo p in protocols like the Digital signature algorithm etc. In 2004 a group of researchers led by Paul Kocher and his other four team members including the Anand Raghunadan and Indian did a study on the aspects like risk factors and security of embedded systems. In this paper the major points of concern were the to bring the design of a safe and protected embedded system has been introduced to the designers of embedded systems and design tool developers as such. A very general aspects of security of embedded systems from basically scrutinizing the requirements pertaining to the working security aspects in systems concerned with embedded world taken into consideration an end user angle of view, Next the underlying challenges are identified for different architectures of the embedded world also the in the design aspects of hardware and software sections are taken into considerations ie design that can resist tamper, then assimilating the requirements pertaining to security, impact of security of physical factors such as battery life of such battery powered systems has been attempted to provide a solution through this paper. Another group of researchers in 2009 have implemented Elliptic Curve Cryptography (ECC) over an multicore Embedded system, and tried to do an intense study on the scheduling methods pertaining to task at various levels. A method scheduling instructions that makes use of all the cores so as to implement a single modular operation in parallel has been proposed. Then operations pertaining to multiple and various modules with multiple cores in parallel are then operated and implemented. A method that
schedules and combines the above two kinds of parallelism was put forward and proposed after imposing a comparison study on the above. Then Rahat Afreen and S.C. Mehrotra (2011) proposed a study on public key cryptography (PKC) systems. In PKC system, to encode and decode the data we use separate keys. Among the two keys one is publicly distributed, the strength and security aspects of this system relies upon big size of the key in the case of a PKC system. In public key cryptographical systems the mathematical problems of prime factorization and discrete logarithm are used. After that R.L. Rivest, A. Shamir, and L. Adleman proposed and formulated a particular way in getting the Public key systems and the digital signature in the world of cryptography. After Introduction and literature reviews in chapter 1 and 2 respectively we will have a short and precise essence of the embedded system in chapter 3, in chapter 4 the security aspects in embedded systems are discussed, then in the next chapter the cryptography basics are discussed, in chapter 6 the Elliptic curve cryptography digital is discussed. In chapter 7 the protocols used in cryptosystems are discussed. In the last chapter we will discuss in detail the elliptic curve version of Signature Algorithm and at the last a modified digital signature algorithm model for embedded systems is proposed.