**STUDYING AND ANALYZING THE VARIOUS METHODS FOR CROSS PLATFORM DATA ENCRYPTION AND DECRYPTION METHODS FOR SECURE IoT DEVICES**

**Abstract:**

Internet of Things is an internetwork where people interact with the environment via sensors and machines to perform physical activities remotely. IoT allows objects to be sensed and controlled remotely via internet such as changing the room temperature by controlling an air conditioner, switching on the lights in your apartment, using smart watches to gather information about your body health (blood pressure and heart beat rate) and sends it to your private doctor to monitor it and so on. Performing a research on issues faced with IoT, it was realized that most challenges were of privacy/confidentiality and data integrity. This project further conducts research on finding ways of securing information that is shared between two or more interactive IoT devices. The main objective of the project was to develop a strategy of securing the IoT technology world. The method that was proposed to provide data security and integrity was through cryptographic methods/security algorithms that require decent memory and equitable CPU processing power. There were three security methods that were focused on in this project i.e. RSA, AES and TDES algorithms. Each of the encryption/decryption methods were presented with their detailed design and functionality. The most suitable and better performing security algorithm for IoT technology was chosen according to the measures of time, memory and processing power. With the tests performed on the proposed security algorithms, AES encryption standard seemed to perform better than other security algorithms in terms computational time, memory consumption and the required processing power. The test results also showed that it has a large encryption/decryption key size which also means better protection for data. However, through testing of the encryption methods there were shortcomings that were encountered such as inability of the security algorithms to provide authentication and encrypt different data formats such as video, picture and audio. The short comings will be further dealt with on the future work. The success of this research has potential impact on increasing the security of IoT internetwork which intern will increase the number of users in the IoT world.

