

## INTISARI

Pengembangan *firmware* pada mikrokontroler sering kali menghadapi tantangan keterbatasan sumber daya, seperti memori, kecepatan pemrosesan, dan konsumsi daya. Salah satu pendekatan yang dapat mengatasi masalah ini adalah metode *build to order*, yang awalnya digunakan dalam industri manufaktur untuk menekan biaya produksi. Pada pendekatan ini, produk dibuat berdasarkan kebutuhan spesifik pengguna. Dalam konteks pengembangan *firmware*, *build to order* diterapkan melalui optimalisasi *firmware* sebelum dikompilasi ke perangkat keras. Optimalisasi ini melibatkan kustomisasi dan modularitas, sehingga setiap bagian *firmware* dapat diatur sesuai kebutuhan. Penggunaan konsep *Model-View-Controller* (MVC) dalam pengembangan *firmware* meningkatkan modularitas, memungkinkan pengaturan dan pemisahan fungsi dengan lebih baik. Pada sistem *home automation*, di mana perangkat dapat dikendalikan dari jarak jauh tanpa interaksi fisik langsung, keamanan menjadi sangat penting. Teknologi *Secure Over-The-Air* atau (OTA) dengan enkripsi AES-256-CBC memungkinkan pembaruan *firmware* secara aman melalui jaringan nirkabel, sehingga pengguna dapat memutakhirkan perangkat mereka dengan tingkat keamanan yang tinggi. Penggunaan metode enkripsi AES-256-CBC yang dikembangkan menjadi *Octa AES-256-CBC* untuk keamanan transmisi data dengan protokol HTTP memberikan tingkat keamanan yang melampaui AES-256-CBC sehingga data perangkat IoT tidak dapat dibaca oleh pihak yang tidak berwenang dan mengurangi risiko pencurian informasi sensitif. Penelitian ini bertujuan untuk menerapkan metode *build to order* pada perangkat *home automation* dengan meningkatkan efisiensi *firmware* sebelum proses kompilasi. Setiap komponen *firmware* dirancang dalam bentuk kelas atau objek yang dapat ditambahkan atau dihapus sesuai dengan permintaan pengguna. Dengan demikian, hanya *class* atau objek yang diperlukan yang akan dikompilasi dan diinstal ke dalam perangkat. Pendekatan ini menghasilkan *firmware* yang lebih ringan dan penggunaan sumber daya perangkat yang lebih efisien, karena hanya komponen yang benar-benar dibutuhkan yang akan dipasang.

Kata kunci: AES-256-CBC, *Octa AES-256-CBC*, *Over the air update*, *Build to order*, *Firmware* dan *Model-View-Controller*.

## **ABSTRACT**

*Firmware development on microcontrollers often faces challenges of resource limitations, such as memory, processing speed, and power consumption. One approach that can overcome this problem is the build to order method, which was originally used in the manufacturing industry to reduce production costs. In this approach, products are made based on the specific needs of users. In the context of firmware development, build to order is applied through firmware optimization before being compiled into hardware. This optimization involves customization and modularity, so that each part of the firmware can be arranged as needed. The use of the Model-View-Controller (MVC) concept in firmware development increases modularity, allowing for better organization and separation of functions. In home automation systems, where devices can be controlled remotely without direct physical interaction, security becomes very important. Secure Over-The-Air (OTA) technology with AES-256-CBC encryption allows secure firmware updates over a wireless network, so users can upgrade their devices with a high level of security. The use of the AES-256-CBC encryption method developed into Octa AES-256-CBC for data transmission security with the HTTP protocol provides a level of security that exceeds AES-256-CBC so that IoT device data cannot be read by unauthorized parties and reduces the risk of theft of sensitive information. This study aims to apply the build to order method to home automation devices by increasing firmware efficiency before the compilation process. Each firmware component is designed in the form of a class or object that can be added or removed according to user requests. Thus, only the required classes or objects will be compiled and installed into the device. This approach results in lighter firmware and more efficient use of device resources, because only the components that are really needed will be installed.*

*Keywords: AES-256-CBC, Octa AES-256-CBC, Over the air update, Build to order, Firmware and Model-View-Controller.*