Protocols and Security in Blynk:

Blynk cloud has multiple layers of security:

- Every message sent through Blynk is encrypted and secure (unless you're using hardware that doesn't support TLS)
- Granular permissions allow you to manage who and how can see your devices and their data
- Every user should have a valid email address. Blynk offers a built-in verification process
- Server system design doesn't allow any other user than allowed by you to view the devices within your organization hierarchy
- Each device has own unique OAuth token and Product Id. Combination of both these fields grants access of the device only for your organization
- Constant monitoring allows us to react quickly on any possible incidents

Blynk mostly relies on industry standards - transport layer security protocol, known as TLS. Blynk server by default tries to use the latest available protocol TLSv1.3 (or TLSv1.2 in case TLSv1.3 version is not supported).
Lower versions of TLS protocols TLSv1 and TLSv1.1 are not supported as they are considered being not secure.
The server will automatically close connections with not supported TLS versions.
Blynk uses 443 port for TLS connections and 80 port for plain connections (in case your hardware doesn't support it). We highly recommend using hardware that supports TLS.
When we are talking about the security of Blynk cloud, we take into account these Blynk Products and components:

- Blynk.Edgent that runs on the device
- Blynk.Console and Blynk.App for iOS and Android
- Blynk.Cloud (or private servers for white-label solutions)

Blynk.Edgent (hardware library)

By default, Blynk.Edgent library tries to use TLS (v1.2) connection between the hardware and server. This is true for popular hardware like ESP32, ESP8266, NodeMCU, MKR 1000, etc (full list). However, some boards don't support TLS, in that case, a plain (non-encrypted) connection is used. You can check that in the serial console output of your board. A typical TLS connection port would be 443. For the plain connections, port 80 is used.
Default authentication for the hardware is OAuth secured token, it looks like this `xw7ITVneg1DifRRQuPGcA7fJvV8-FAVl` and represents 24 bytes in base 64 encoding. The token could be changed with the re-provision flow.

Blynk.Apps for iOS and Android

Blynk uses secured web sockets (TLSv1.3 in case you browser supports it, TLSv1.2 otherwise) communication and basic authentication (email/password). for Blynk.Console and mobile apps

Passwords are encrypted on the client side before transferring to the cloud server and never stored or transferred in the plain format. Only encrypted password hash is stored and used on the server.
After 5 failed login attempts from the same IP - IP is not allowed to login for the next 10 minutes.

Blynk.Cloud

- All data transferred between cloud and database is always encrypted
- Database is fully isolated within the private network
- Database doesn't have access from the internet and can be accessed from the private network only
- Database itself is not encrypted. Encryption is available for white-label solution as a paid add-on

Certificates

Blynk uses Let's Encrypt certificates for TLS connections. Certificates are renewed every 2 months.

Ports

Blynk doesn't require any non-standard ports.

- 443 port is used for TLS connections
- 80 port is used for plain connections