MODULE *WebServer*

EXTENDS $\mathit{Naturals}$, $\mathit{FiniteSets}$, $\mathit{Sequences}$

CONSTANTS $\mathit{Clients}$, $\mathit{LoginInfo}$, FileId, $\mathit{FileData}$, M, NoFile, $\mathit{Inactive}$
CONSTANTS $\mathit{AuthClient}(\_, \_)$, $\mathit{Reply}(\_, \_)$

ASSUME $M \in \mathit{Nat} \land M > 0$
ASSUME $\forall\, c, l \; : \mathit{AuthClient}(c, l) \in \text{BOOLEAN}$
ASSUME $\forall\, c, m : \mathit{Reply}(c, m) \in \text{BOOLEAN}$

VARIABLES $\mathit{pendingReqs}$, $\mathit{connections}$, files, auths, $\mathit{attending}$

$\mathit{vars} \triangleq \langle \mathit{pendingReqs}, \mathit{connections}, \mathit{files}, \mathit{auths} \rangle$

$\mathit{File} \triangleq [\mathit{data} : \mathit{FileData}, \mathit{access} : \text{SUBSET } \mathit{Clients}]$

$$\begin{aligned}\mathit{Request} \triangleq\;& [\mathit{type} : \{\text{“GET”}\}, \mathit{fid} : \mathit{FileId}] \cup [\mathit{type} : \{\text{“AUTH”}\}, \mathit{data} : \mathit{LoginInfo}] \cup \\ & [\mathit{type} : \{\text{“POST”}\}, f : \mathit{File}, \mathit{fid} : \mathit{FileId}]\end{aligned}$$

$\mathit{Msg} \triangleq \{$“Succesful login”, “Invalid Login”, “File Not Found”, “Succesful file upload”, “File stored”$\}$

$\mathit{Respond} \triangleq \mathit{MSG} \cup \mathit{File}$

$\mathit{NoFile} \triangleq \text{CHOOSE } f : f \notin \mathit{File}$

$\mathit{Inactive} \triangleq \text{CHOOSE } x : x \notin \mathit{Request} \cup \mathit{Respond}$

$$\begin{aligned}\mathit{TypeInv} \triangleq\;& \land\, \mathit{connections} \subseteq \mathit{Clients} \\ & \land\, \mathit{auths} \subseteq \mathit{Clients} \\ & \land\, \mathit{IsFiniteSet}(\mathit{connections}) \\ & \land\, \mathit{pendingReqs} \in \mathit{Seq}([c : \mathit{Clients}, \mathit{req} : \mathit{Request}]) \\ & \land\, \mathit{files} \in [\mathit{fid} \in \mathit{FileId} \mapsto \mathit{File} \cup \mathit{NoFile}] \\ & \land\, \mathit{attending} \in [c : \mathit{Clients}, r : \mathit{Request}] \cup \mathit{Inactive}\end{aligned}$$

$$\begin{aligned}\mathit{Init} \triangleq\;& \land\, \mathit{pendingReqs} = \langle\rangle \\ & \land\, \mathit{connections} = \{\} \\ & \land\, \mathit{auths} = \{\} \\ & \land\, \mathit{files} = [\mathit{fid} \in \mathit{FileId} \mapsto \mathit{NoFile}] \\ & \land\, \mathit{attending} = \mathit{Inactive}\end{aligned}$$

$$\begin{aligned}\mathit{Connect}(c) \triangleq\;& \land\, \mathit{Cardinality}(\mathit{connections}) < M \\ & \land\, \mathit{connections}' = \mathit{connections} \cup c \\ & \land\, \text{UNCHANGED } \langle \mathit{pendingReqs}, \mathit{files}, \mathit{auths}, \mathit{attending} \rangle\end{aligned}$$

$$\begin{aligned}\mathit{Req}(c) \triangleq\;& \land\, c \in \mathit{connections} \\ & \land\, \exists\, r \in \mathit{Request} : \\ & \qquad \land\, \mathit{pendingReqs}' = \mathit{pendingReqs} \cup \langle c, r \rangle \\ & \qquad \land\, \mathit{connections}' = \mathit{connections} \setminus c\end{aligned}$$

$$\land \textsc{unchanged}\ \langle \mathit{files}, \mathit{auths}, \mathit{attending} \rangle$$

$$\mathit{SelectNextReq} \triangleq \begin{array}[t]{l} \land \mathit{attending} = \mathit{Inactive} \\ \land \mathit{pendingReqs} \neq \langle \rangle \\ \land \mathit{attending}' = \mathit{Head}(\mathit{pendingReqs}) \\ \land \mathit{pendingReqs}' = \mathit{Tail}(\mathit{pendingReqs}) \\ \land \textsc{unchanged}\ \langle \mathit{connections}, \mathit{files}, \mathit{auth} \rangle \end{array}$$

$$\mathit{GetFile} \triangleq \begin{array}[t]{l} \land \mathit{attending} \neq \mathit{Inactive} \\ \land \mathit{attending.req.type} = \textsf{"GET"} \\ \land \mathit{files}[\mathit{attending.req.fid}] \neq \mathit{NoFile} \\ \land \mathit{files}[\mathit{attending.req.fid}].\mathit{access} = \{\} \\ \land \mathit{Reply}(\mathit{attending.c}, \mathit{files}[\mathit{attending.req.fid}].\mathit{data}) \\ \land \mathit{attending}' = \mathit{Inactive} \\ \land \textsc{unchanged}\ \langle \mathit{connections}, \mathit{pendingReqs}, \mathit{auth}, \mathit{files} \rangle \end{array}$$

$$\mathit{GetFileRestricted} \triangleq \begin{array}[t]{l} \land \mathit{attending} \neq \mathit{Inactive} \\ \land \mathit{attending.req.type} = \textsf{"GET"} \\ \land \mathit{files}[\mathit{attending.req.fid}] \neq \mathit{NoFile} \\ \land \mathit{files}[\mathit{attending.req.fid}].\mathit{access} \neq \{\} \\ \land \mathit{attending.c} \in \mathit{auths} \cap \mathit{files}[\mathit{attending.req.fid}].\mathit{access} \\ \land \mathit{Reply}(\mathit{attending.c}, \mathit{files}[\mathit{attending.req.fid}].\mathit{data}) \\ \land \mathit{attending}' = \mathit{Inactive} \\ \land \textsc{unchanged}\ \langle \mathit{connections}, \mathit{pendingReqs}, \mathit{auth}, \mathit{files} \rangle \end{array}$$

$$\mathit{GetFileNotAuth} \triangleq \begin{array}[t]{l} \land \mathit{attending} \neq \mathit{Inactive} \\ \land \mathit{attending.req.type} = \textsf{"GET"} \\ \land \mathit{files}[\mathit{attending.req.fid}] \neq \mathit{NoFile} \\ \land \mathit{files}[\mathit{attending.req.fid}].\mathit{access} \neq \{\} \\ \land \mathit{attending.c} \notin \mathit{auths} \cap \mathit{files}[\mathit{attending.req.fid}].\mathit{access} \\ \land \mathit{Reply}(\mathit{attending.c}, \textsf{"Unauthorized Access"}) \\ \land \mathit{attending}' = \mathit{Inactive} \\ \land \textsc{unchanged}\ \langle \mathit{connections}, \mathit{pendingReqs}, \mathit{auth}, \mathit{files} \rangle \end{array}$$

$$\mathit{GetFileError} \triangleq \begin{array}[t]{l} \land \mathit{attending} \neq \mathit{Inactive} \\ \land \mathit{attending.req.type} = \textsf{"GET"} \\ \land \mathit{files}[\mathit{attending.req.fid}] = \mathit{NoFile} \\ \land \mathit{Reply}(\mathit{attending.c}, \textsf{"File not founded"}) \\ \land \mathit{attending}' = \mathit{Inactive} \\ \land \textsc{unchanged}\ \langle \mathit{connections}, \mathit{pendingReqs}, \mathit{auth}, \mathit{files} \rangle \end{array}$$

$$\mathit{Get} \triangleq \begin{array}[t]{l} \lor \mathit{GetFileFree} \\ \lor \mathit{GetFileRestricted} \\ \lor \mathit{GetFileNotAuth} \\ \lor \mathit{GetFileError} \end{array}$$

$$\mathit{AuthOk} \triangleq \land \mathit{attending} \neq \mathit{Inactive}$$

```
          $\land\ attending.req.type = \text{“AUTH”}$
          $\land\ AuthClient(attending.c,\ attending.req.data)$
          $\land\ auths' = auths \cup attending.c$
          $\land\ Reply(attending.c,\ \text{“Succesful login”})$
          $\land\ attending' = Inactive$
          $\land\ \textsc{unchanged}\ \langle files,\ connections,\ pendingReqs \rangle$

$AuthError \triangleq$ $\land\ attending \neq Inactive$
            $\land\ attending.req.type = \text{“AUTH”}$
            $\land\ \neg AuthClient(attending.c,\ attending.req.data)$
            $\land\ Reply(attending.c,\ \text{“Invalid Login”})$
            $\land\ attending' = Inactive$
            $\land\ \textsc{unchanged}\ \langle auth,\ files,\ connections,\ pendingReqs \rangle$

$Auth \triangleq$ $\lor\ AuthOk$
       $\lor\ AuthError$

$PostOk \triangleq$ $\land\ attending \neq Inactive$
         $\land\ attending.req.type = \text{“POST”}$
         $\land\ files[attending.req.fid] = NoFile$
         $\land\ files' = [files\ \textsc{except}\ ![attending.req.fid] = attending.req.f]$
         $\land\ Reply(attending.c,\ \text{“Successful upload”})$
         $\land\ attending' = Inactive$
         $\land\ \textsc{unchanged}\ \langle connections,\ auths,\ pendingReqs \rangle$

$PostError \triangleq$ $\land\ attending \neq Inactive$
            $\land\ attending.req.type = \text{“POST”}$
            $\land\ files[attending.req.fid] \neq NoFile$
            $\land\ Reply(attending.c,\ \text{“File already stored”})$
            $\land\ attending' = Inactive$
            $\land\ \textsc{unchanged}\ \langle files,\ connections,\ auths,\ pendingReqs \rangle$

$Post \triangleq$ $\lor\ PostOk$
       $\lor\ PostError$

$Next \triangleq$ $\lor\ \exists\, c \in Clients : Connect(c)$
       $\lor\ \exists\, c \in Clients : Req(c)$
       $\lor\ SelectNextReq$
       $\lor\ Get$
       $\lor\ Auth$
       $\lor\ Post$

$Spec \triangleq Init \land \Box[Next]_{vars} \land \mathrm{WF}_{vars}(SelectNextReq \lor Get \lor Auth \lor Post)$
```

THEOREM $Spec \Rightarrow TypeInv$
