

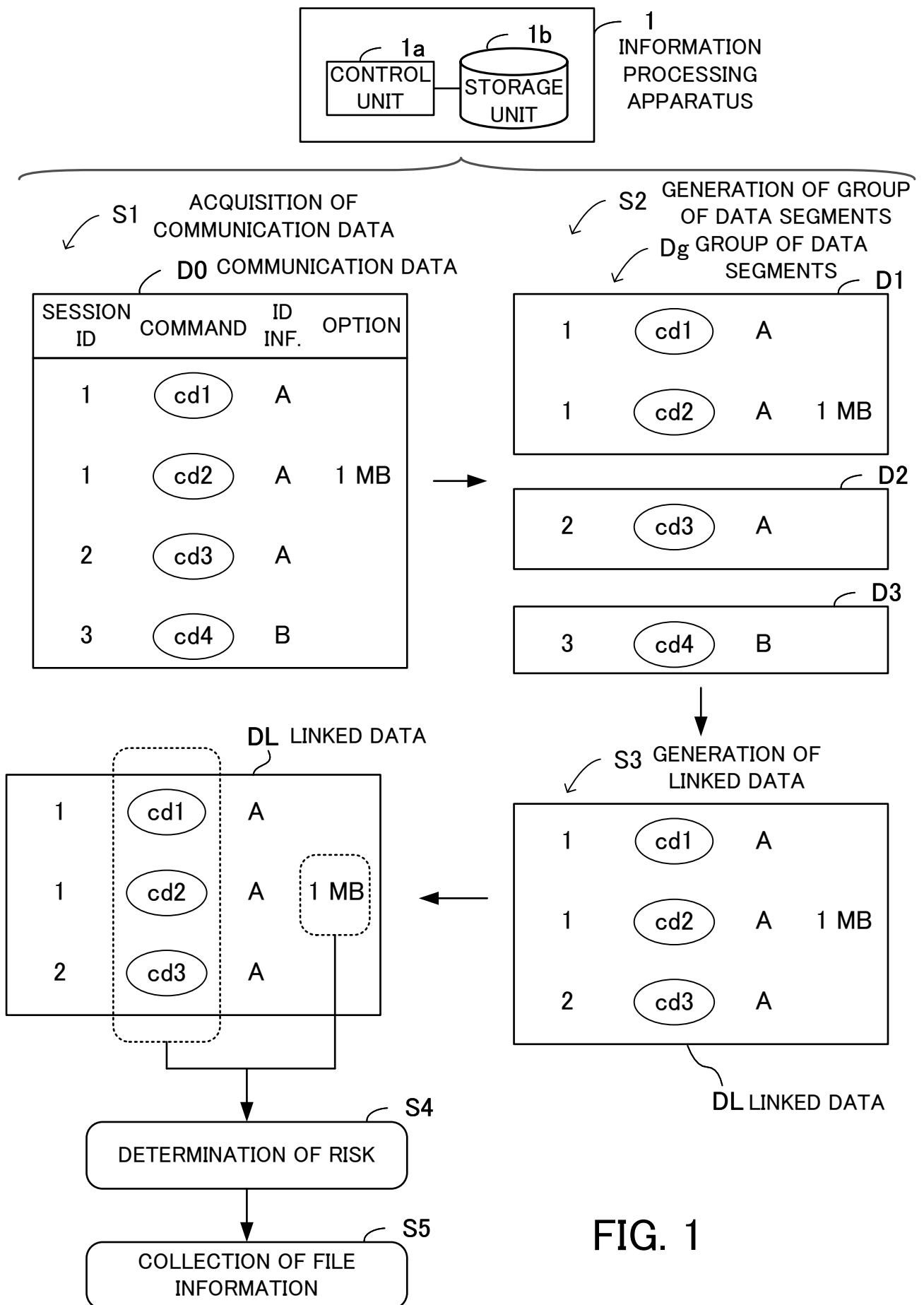


FIG. 1

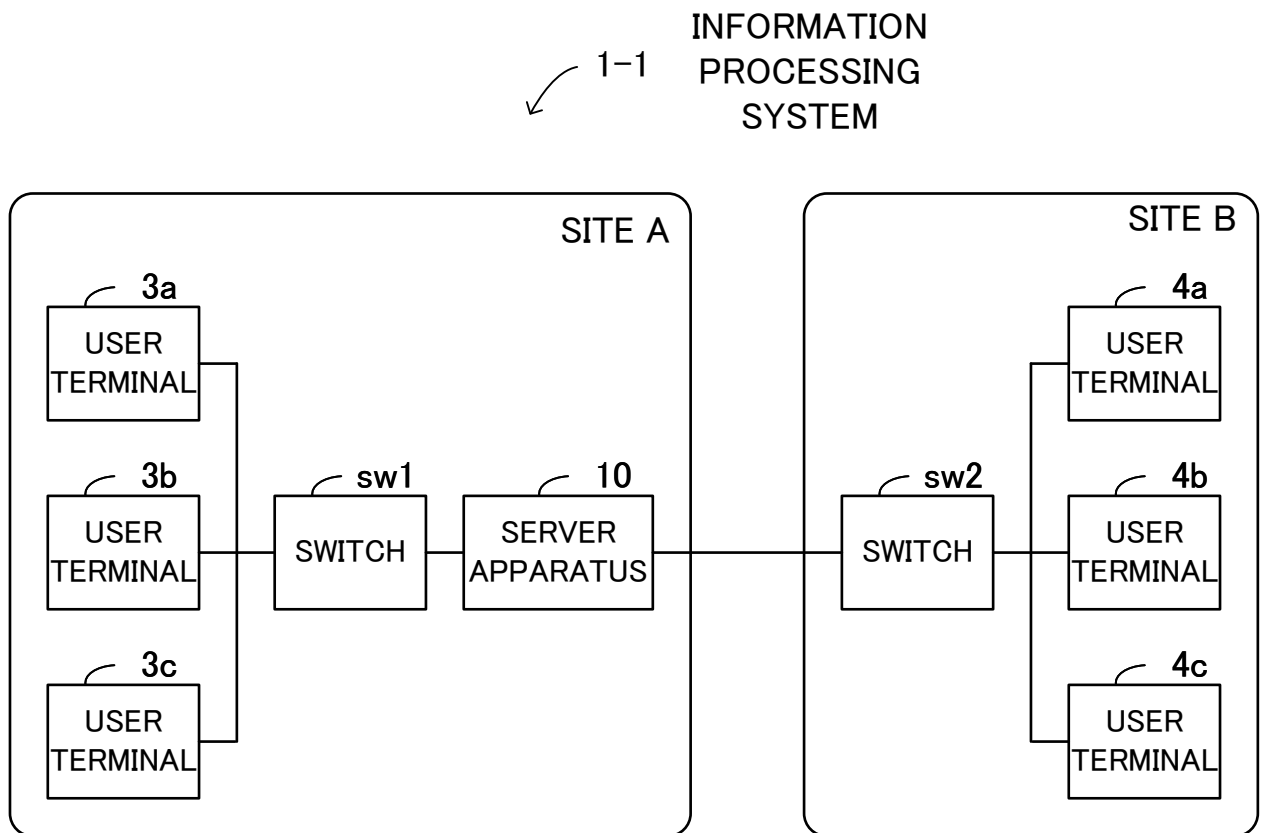


FIG. 2

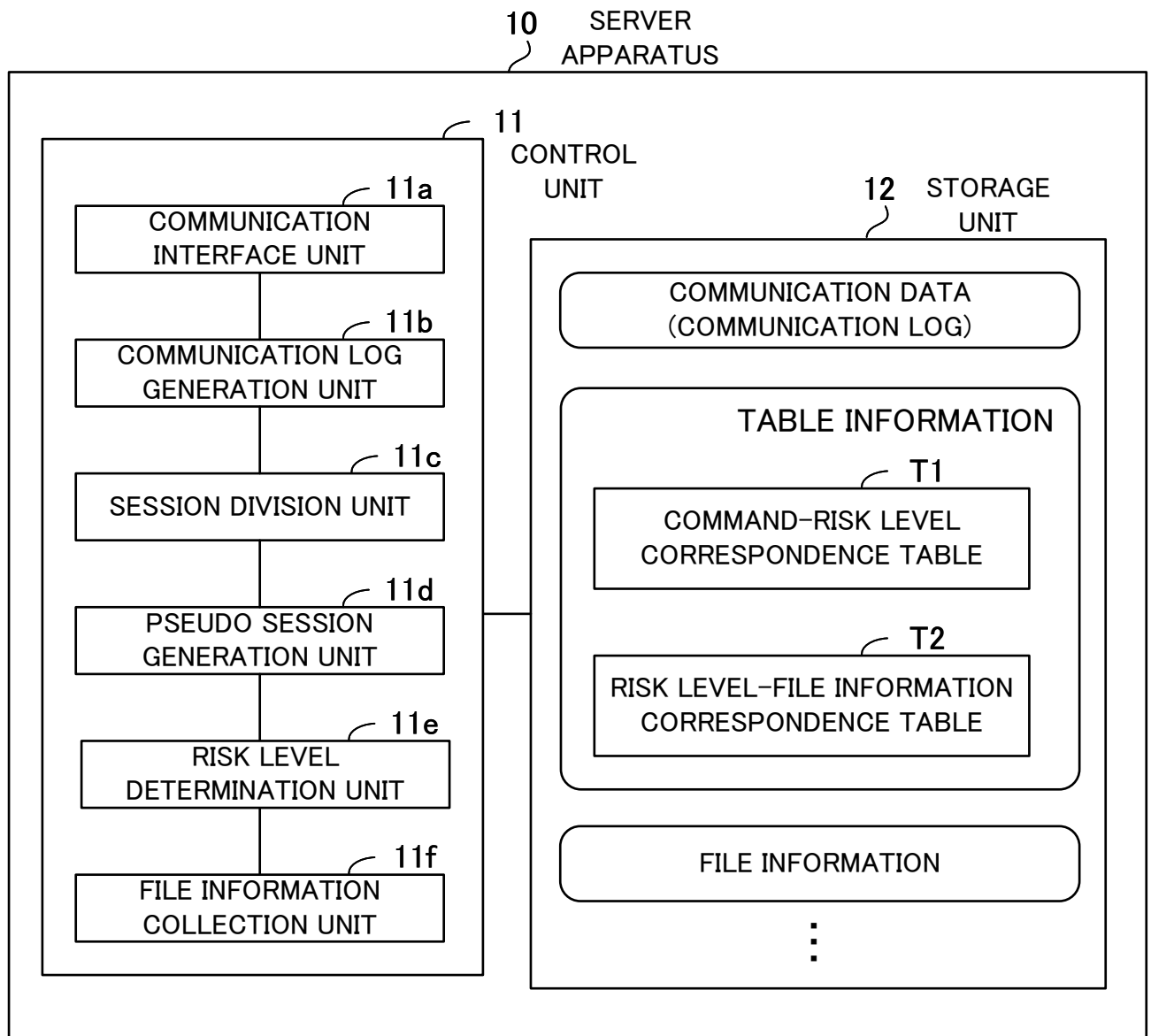


FIG. 3

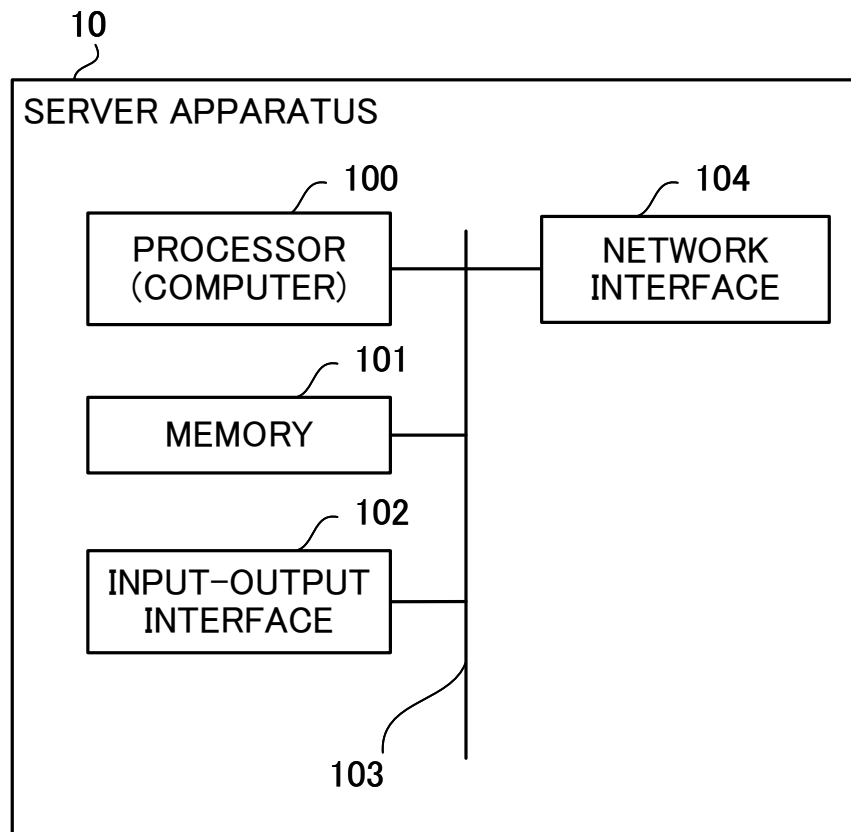


FIG. 4

T11

COMMAND	RISK LEVEL
net group	1
net use	2
schtasks	3

FIG. 5

T12

RISK LEVEL	FILE INFORMATION
1	META INFORMATION
2	META INFORMATION, FILE HASH VALUE
3	META INFORMATION, FILE HASH VALUE, FILE MAIN BODY

FIG. 6

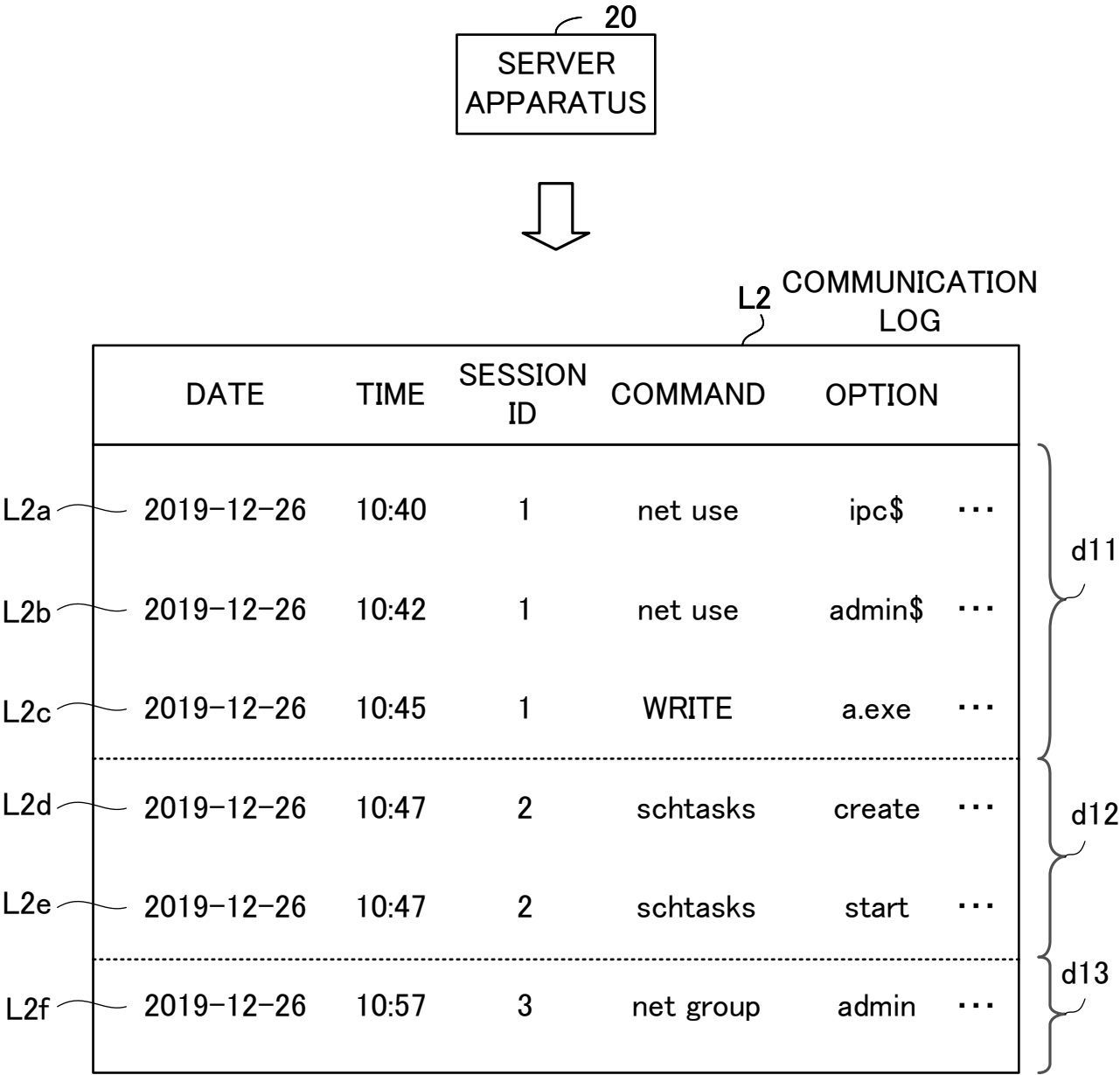
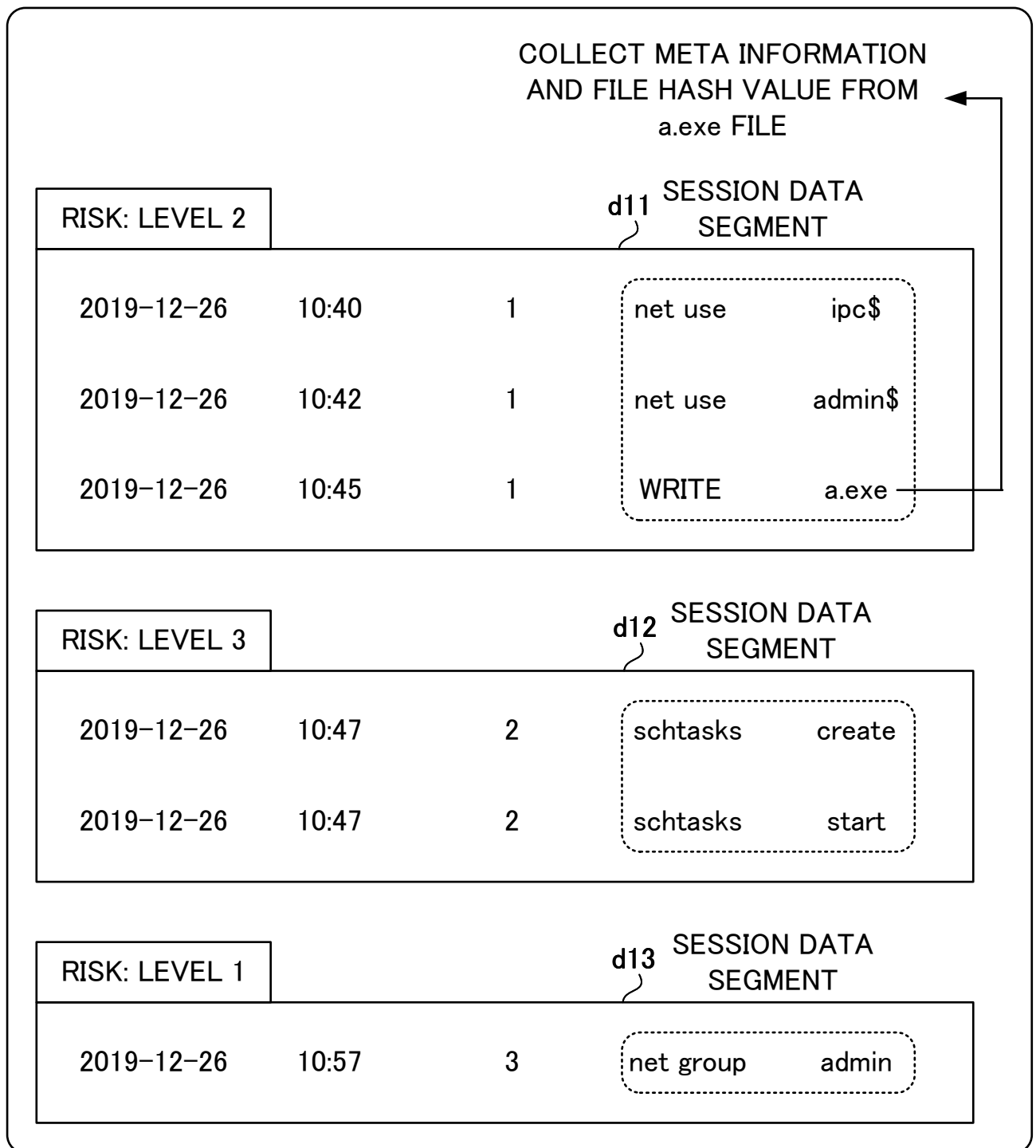


FIG. 7



ALTHOUGH COMMUNICATION LOG INCLUDES
DATA WHOSE RISK LEVEL IS 3, FILE MAIN
BODY IS NOT COLLECTED.

FIG. 8

9/19

10

SERVER APPARATUS
(CONTROL UNIT 11)

FIG. 9



L1 COMMUNICATION LOG

	DATE	TIME	SESSION ID	COMMAND	OPTION	
L1a	2019-12-26	10:40	1	net use	ipc\$	account:A ...
L1b	2019-12-26	10:42	1	net use	admin\$	account:A ...
L1c	2019-12-26	10:45	1	WRITE	a.exe	account:A 1 MB
L1d	2019-12-26	10:47	2	schtasks	create	account:A ...
L1e	2019-12-26	10:47	2	schtasks	start	account:A ...
L1f	2019-12-26	10:57	3	net group	admin	account:B ...

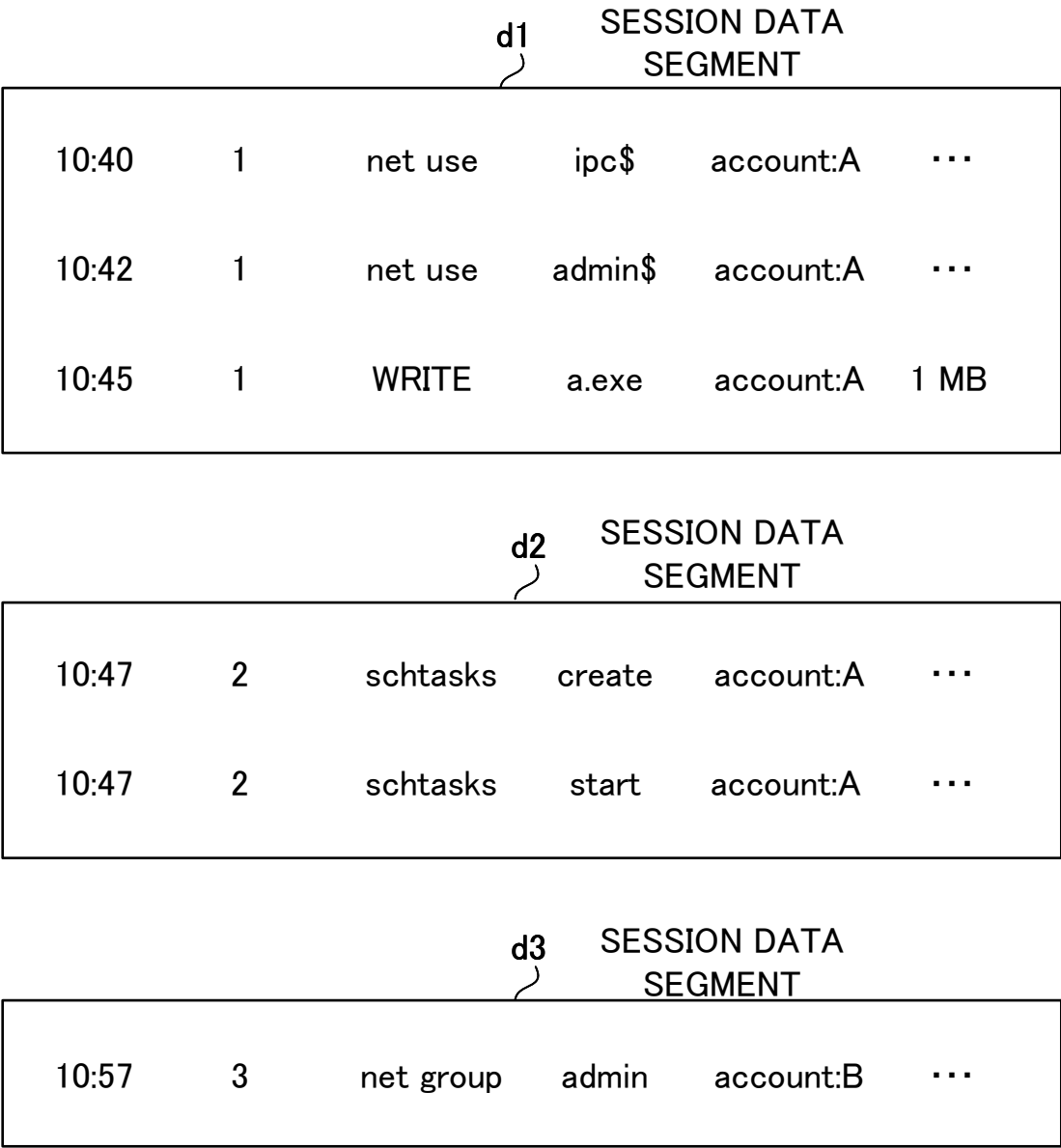


FIG. 10

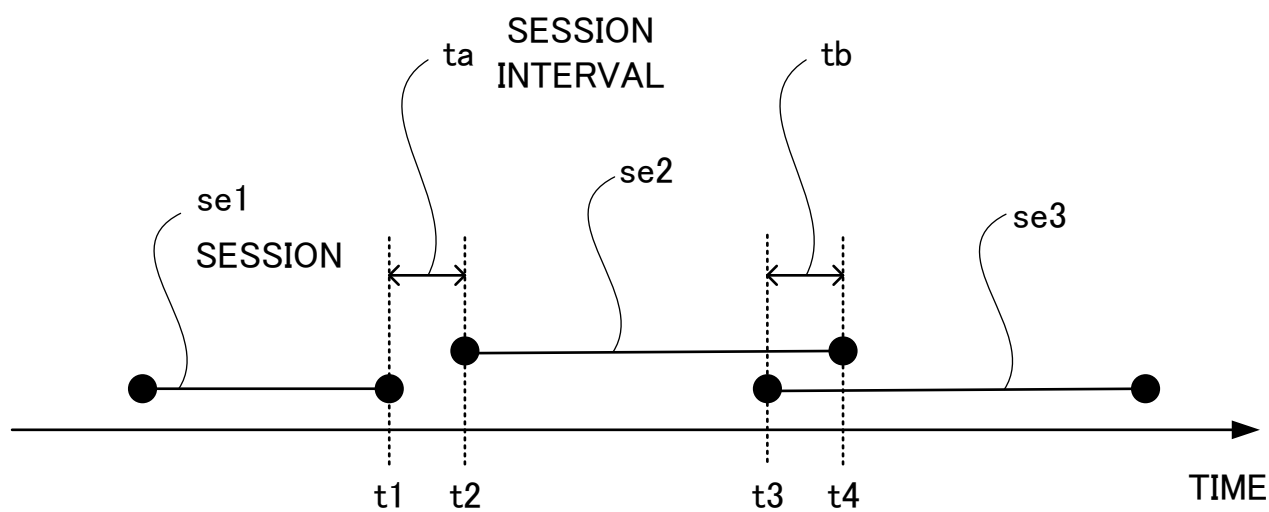


FIG. 11

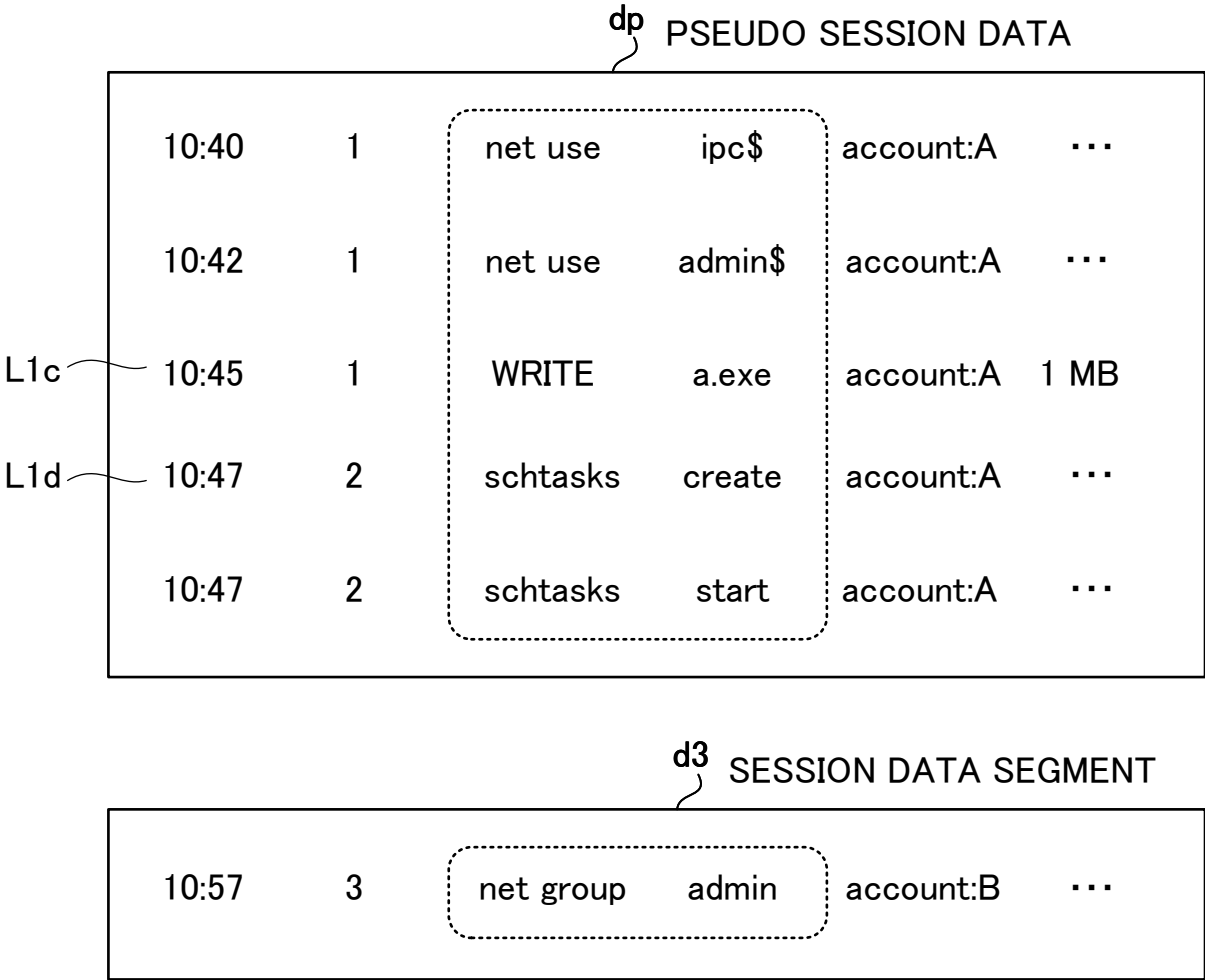


FIG. 12

T1 COMMAND-RISK LEVEL
CORRESPONDENCE TABLE

COMMAND	RISK LEVEL
net group	1
net use	2
schtasks (FILE SIZE ≥ THRESHOLD)	
schtasks (FILE SIZE < THRESHOLD)	3

FIG. 13

T2

RISK LEVEL-FILE INFORMATION
CORRESPONDENCE TABLE

RISK LEVEL	FILE INFORMATION
1	META INFORMATION
2	META INFORMATION, FILE HASH VALUE
3	META INFORMATION, FILE HASH VALUE, FILE MAIN BODY

FIG. 14

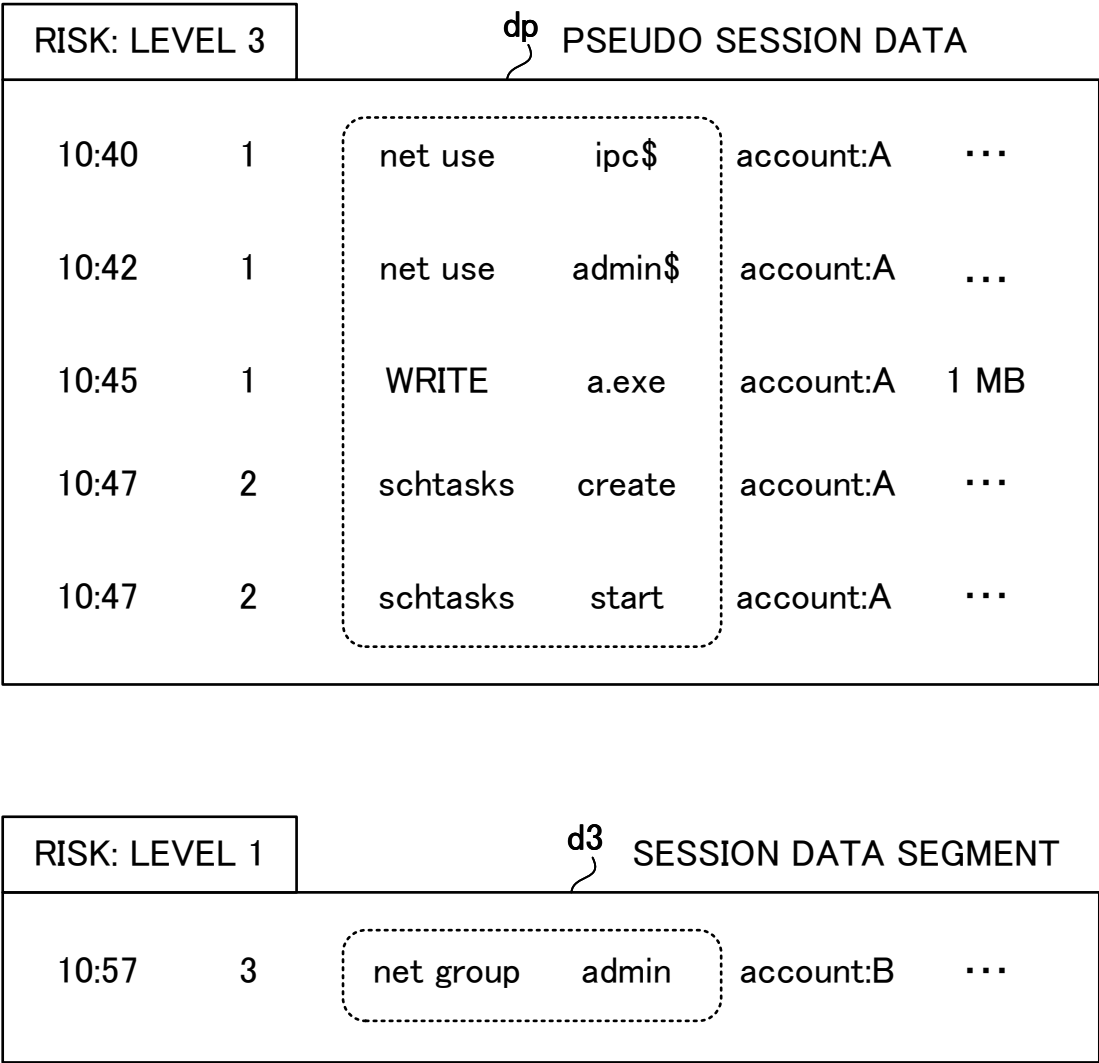
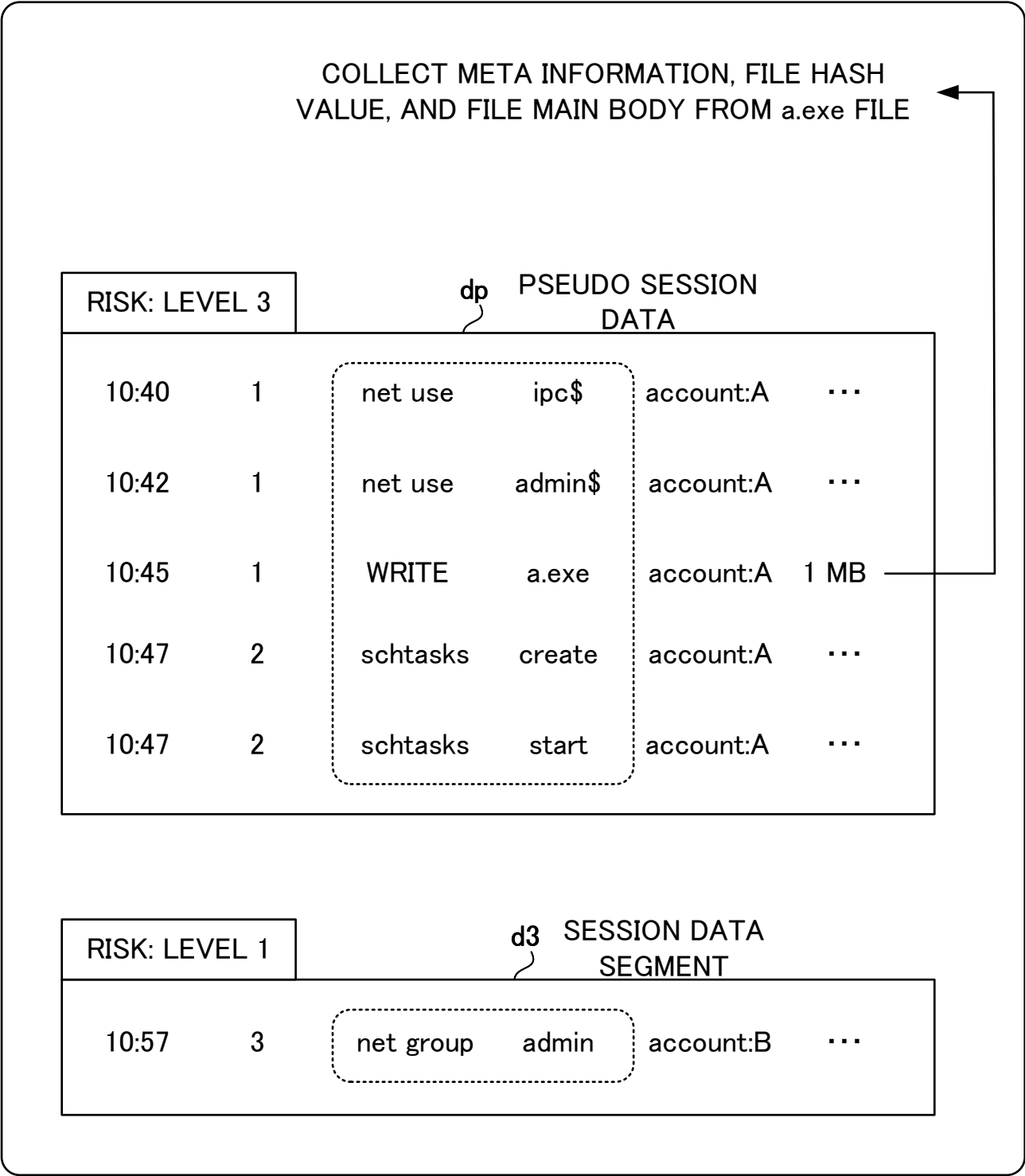


FIG. 15



FILE MAIN BODY IS ALSO COLLECTED FROM COMMUNICATION LOG INCLUDING DATA WHOSE RISK LEVEL IS 3.

FIG. 16

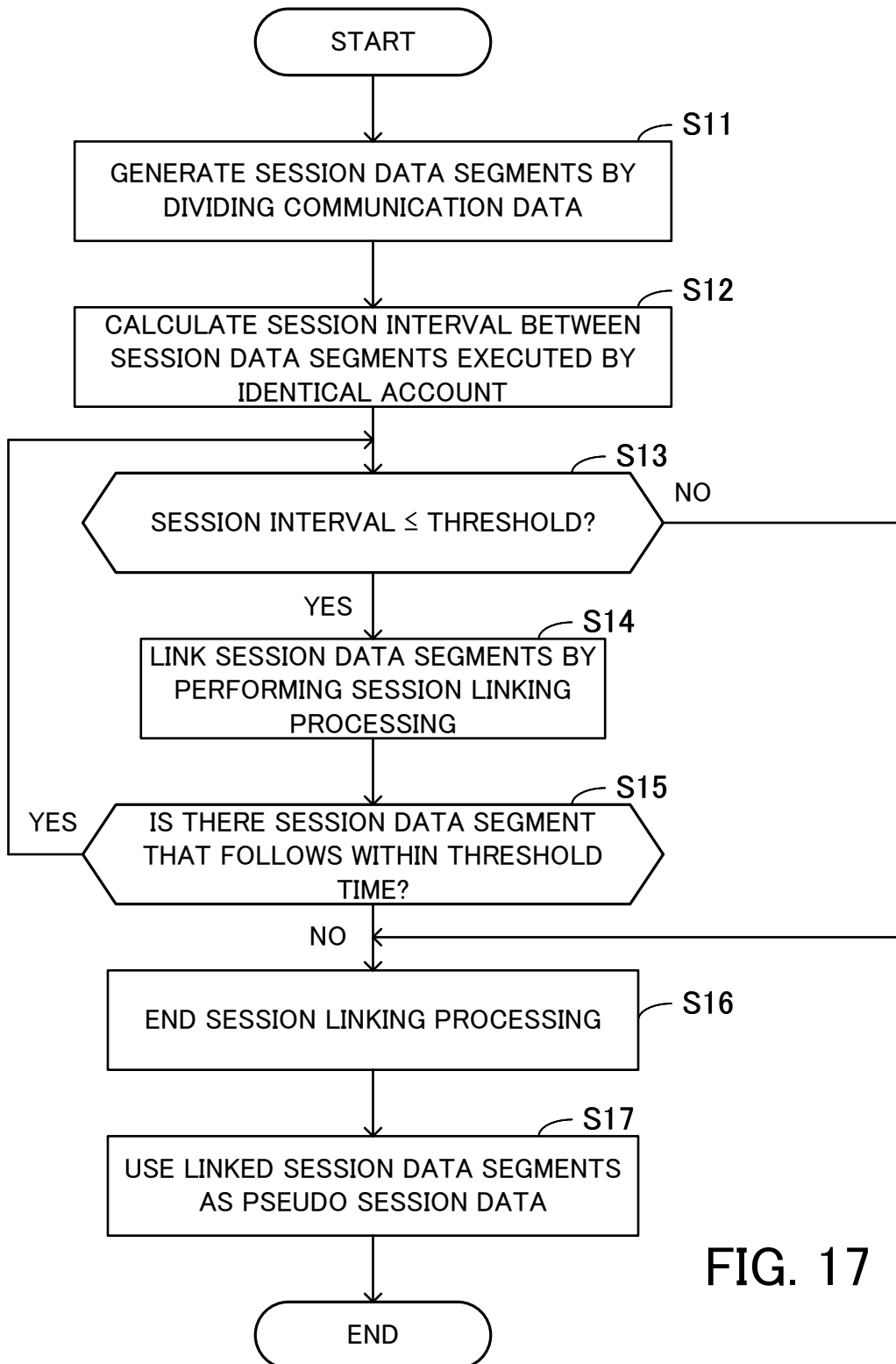


FIG. 17

FIG. 18

