

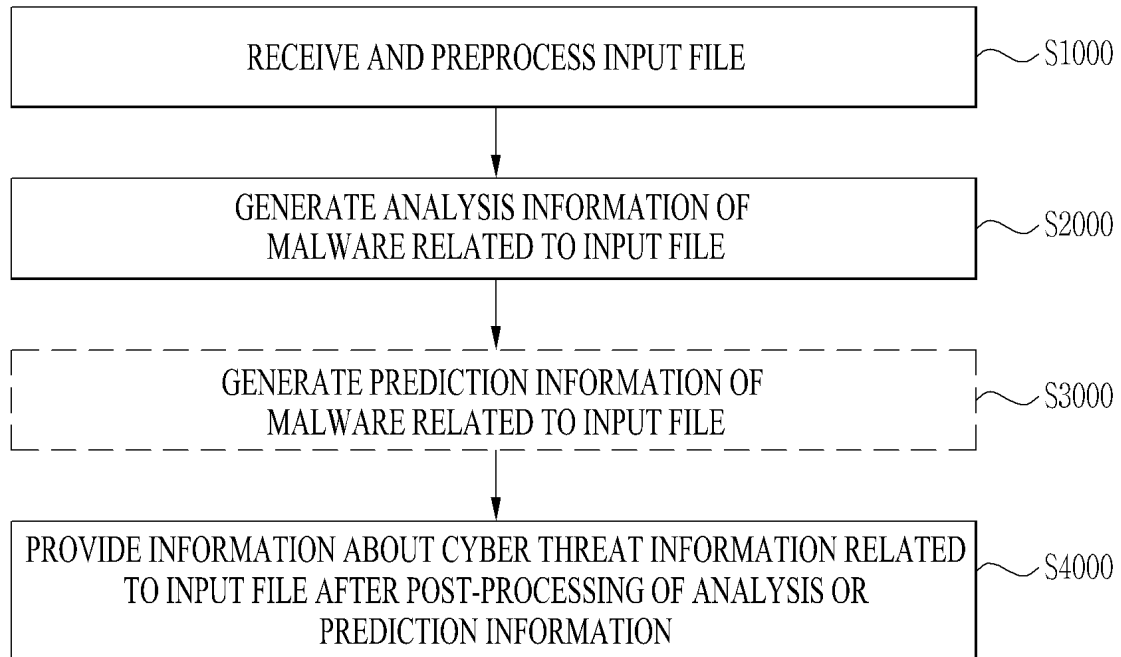
[fig. 1]

FIG. 2

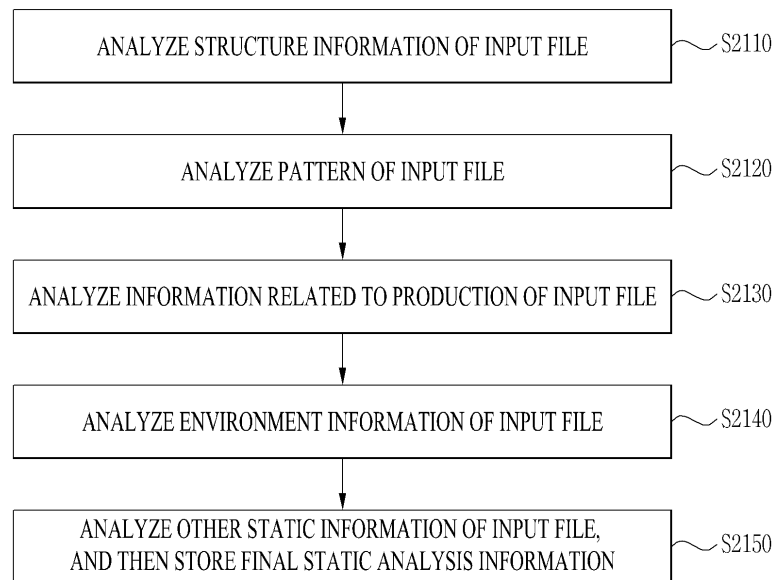


FIG. 3

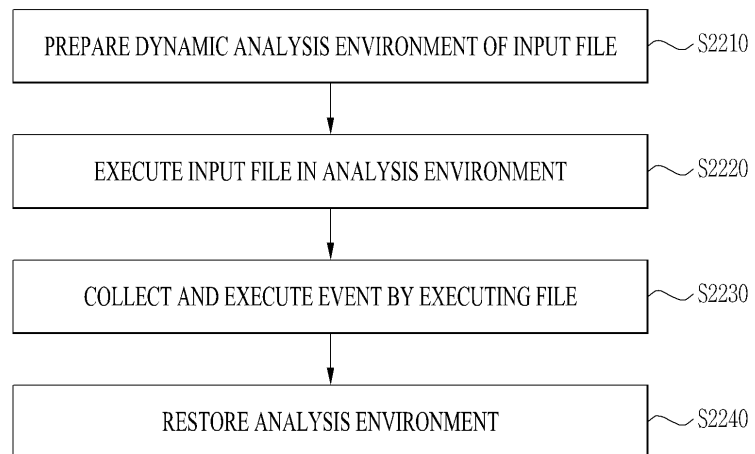


FIG. 4

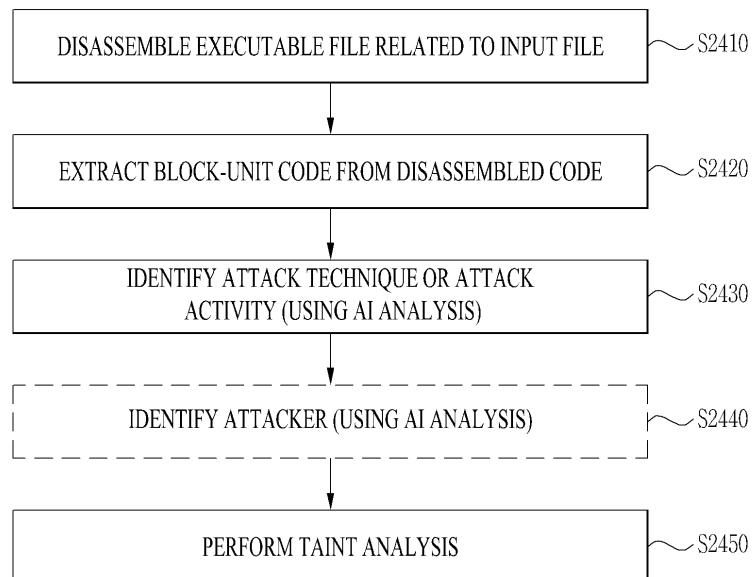


FIG. 5

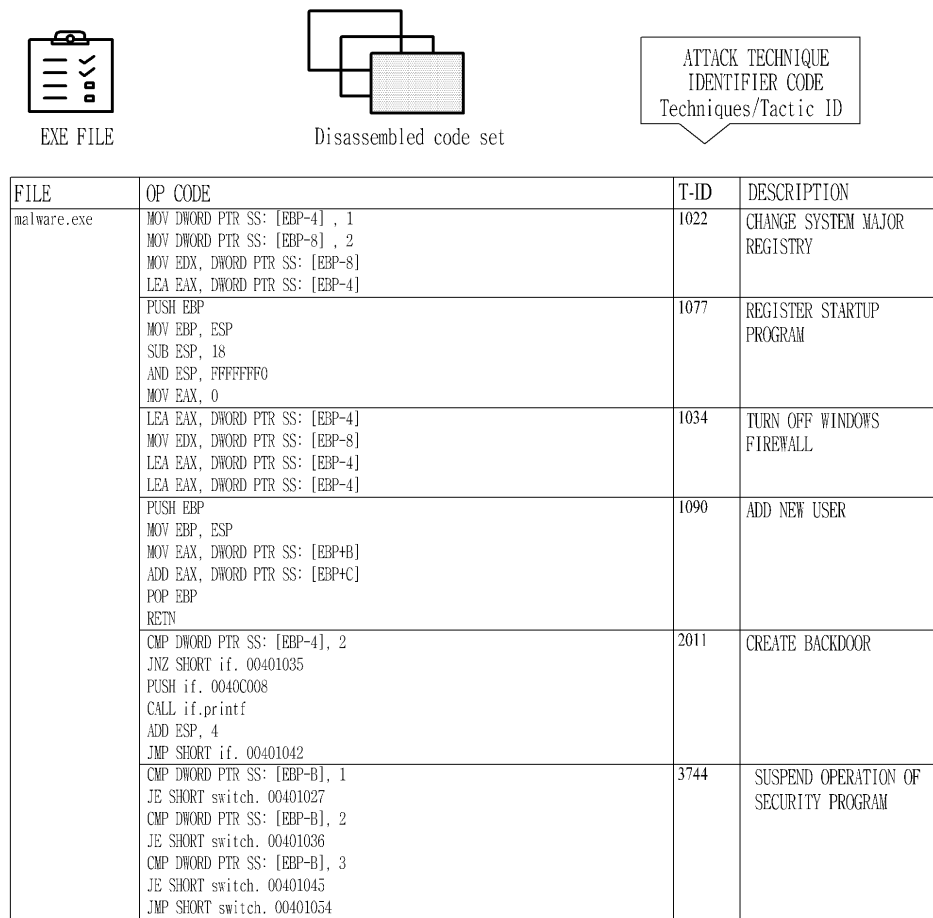


FIG. 6

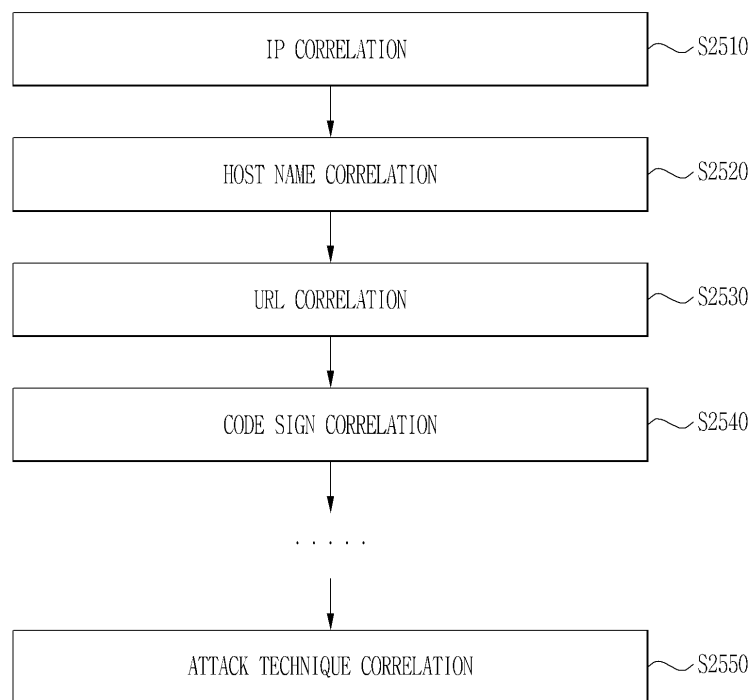


FIG. 7

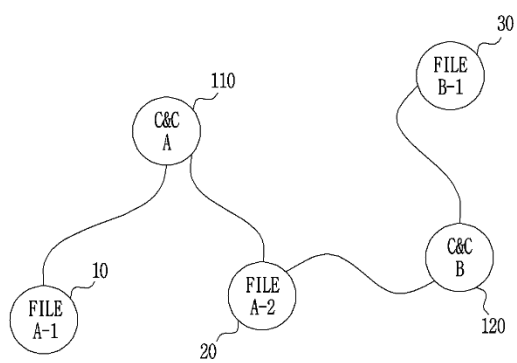


FIG. 8

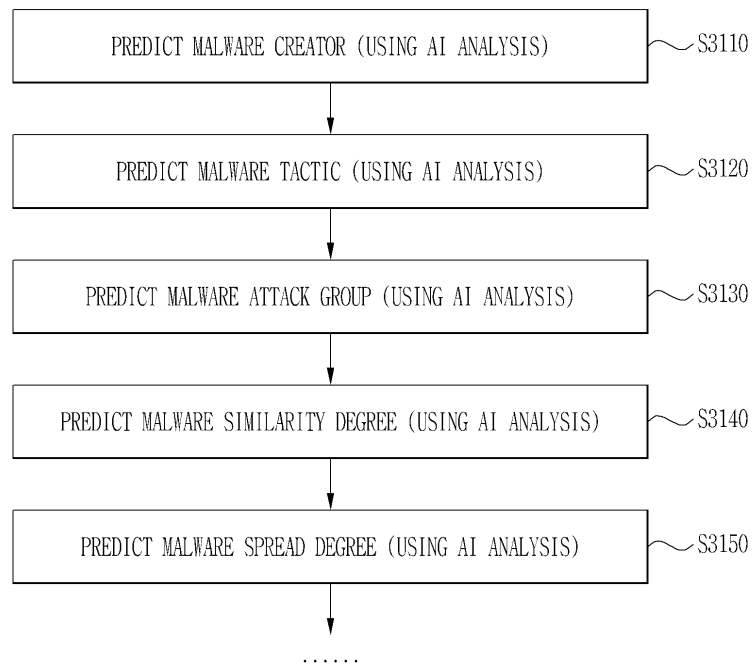


FIG. 9

QUERY (A)

"FILE IN WHICH WORD "ransomware*" IS INCLUDED IN ANTI-VIRUS DETECTION NAME DETECTED IN MALWARE DETECTING 40 OR MORE ANTI-VIRUSES FROM 4 PM MARCH 1, 2020 TO 9 AM MARCH 2, 2020, FILE TYPE IS EXE, DISTRIBUTION SITE (ITW) IS "go.kr*", CODE SIGN SIGNATURE INFORMATION IS PRESENT, AND FILE SIZE IS 10 MB OR LESS"

QUERY (B)

"FILE IN WHICH FILE TYPE IS HWP, DOC, PPT, PDF, OR XLS, DISTRIBUTION SITE IS PRESENT, "powershell.exe" OR "vbscript.exe" IS EXECUTED AS RESULT OF ACTIVITY ANALYSIS, AND FILE SIZE IS 10 MB OR LESS IN FILE DETECTING 10 OR FEWER ANTI-VIRUSES ON MARCH 1, 2020"

Query (C)

"FILE IN WHICH FILE TYPE IS EXE_32 OR EXE_64, DISTRIBUTION SITE IS PRESENT, DISTRIBUTION SITE ADDRESS IS NOT "nexon.com", "nexon" IS INCLUDED IN FILE NAME, ACTIVITY "CORRECT FIREWALL SETTING" OR "REGISTER IN START PROGRAM" IS EXECUTED TO ATTEMPT ACCESS TO 184.55.38.2 AS RESULT OF ACTIVITY ANALYSIS, AND FILE SIZE IS 100 KB OR MORE IN FILE DETECTING FIVE OR MORE ANTI-VIRUSES IN JANUARY TO DECEMBER 2019"

Query (D)

"DAILY STATISTICAL INFORMATION OF FILE IN WHICH FILE TYPE IS DOCUMENT (HWP, DOC, PPT, XLS, PDF), "not-virus" IS NOT INCLUDED IN DETECTION NAME OF Kaspersky, DISTRIBUTION SITE ADDRESS INCLUDES "*.kr*" IN FILE DETECTING 20 OR MORE ANTI-VIRUSES IN JANUARY TO DECEMBER 2019"

FIG. 10

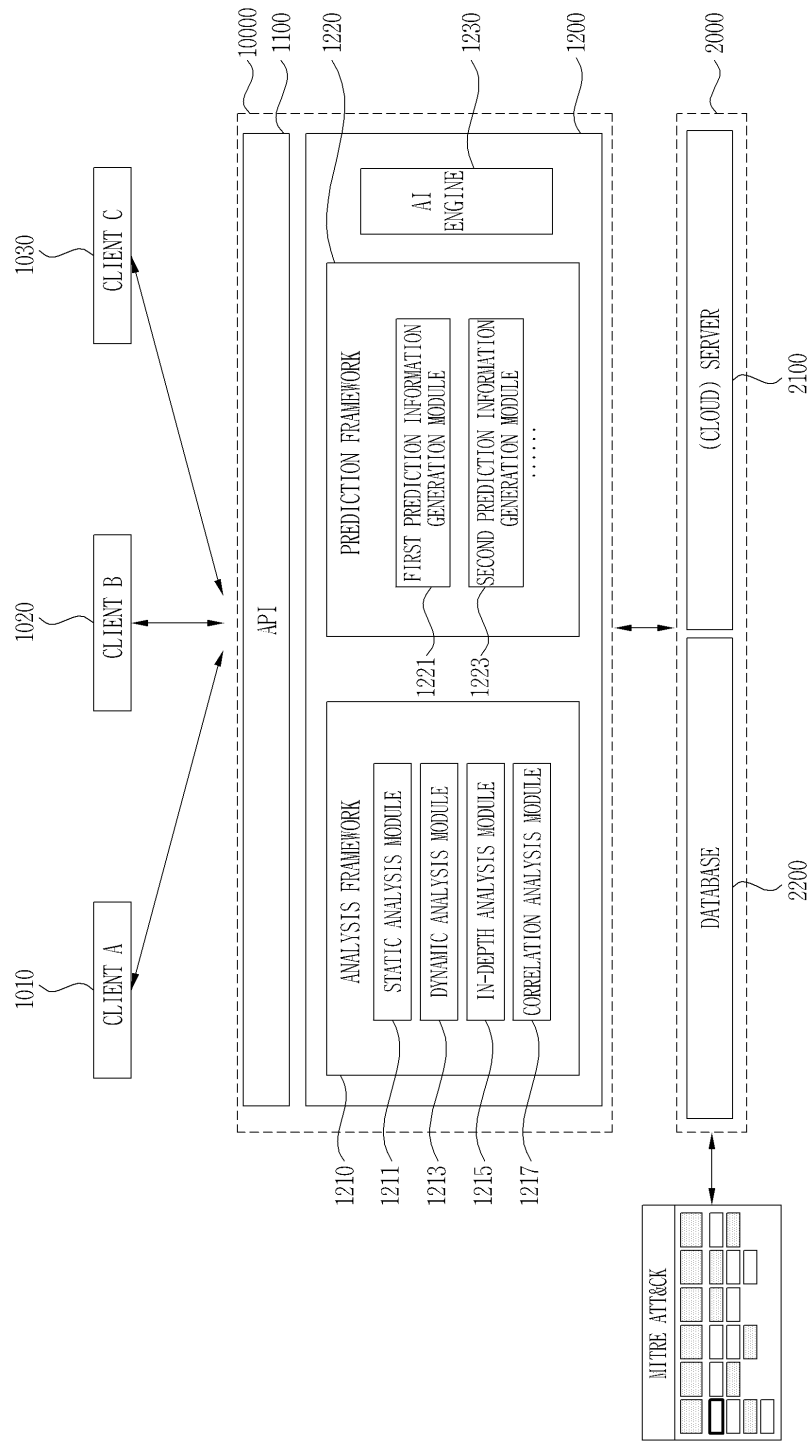


FIG. 11

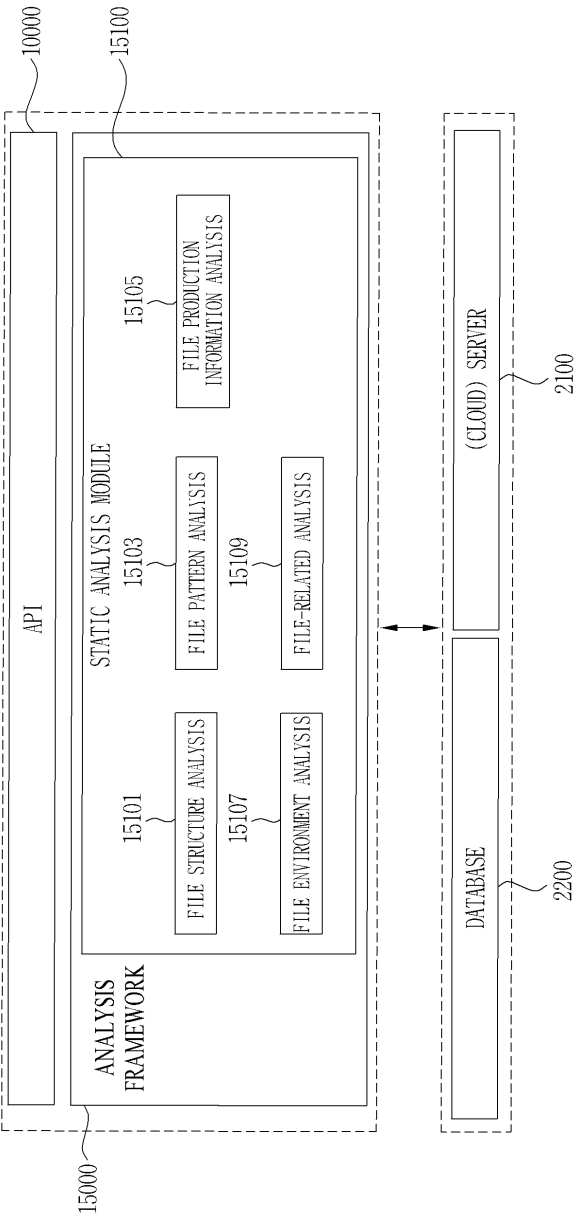


FIG. 12

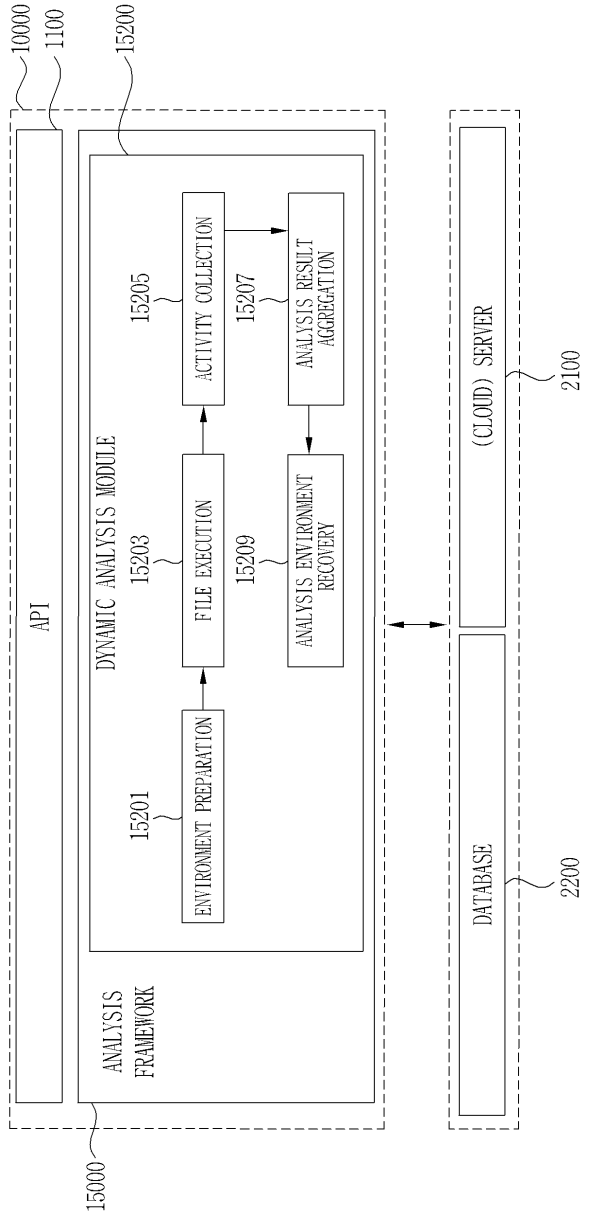


FIG. 13

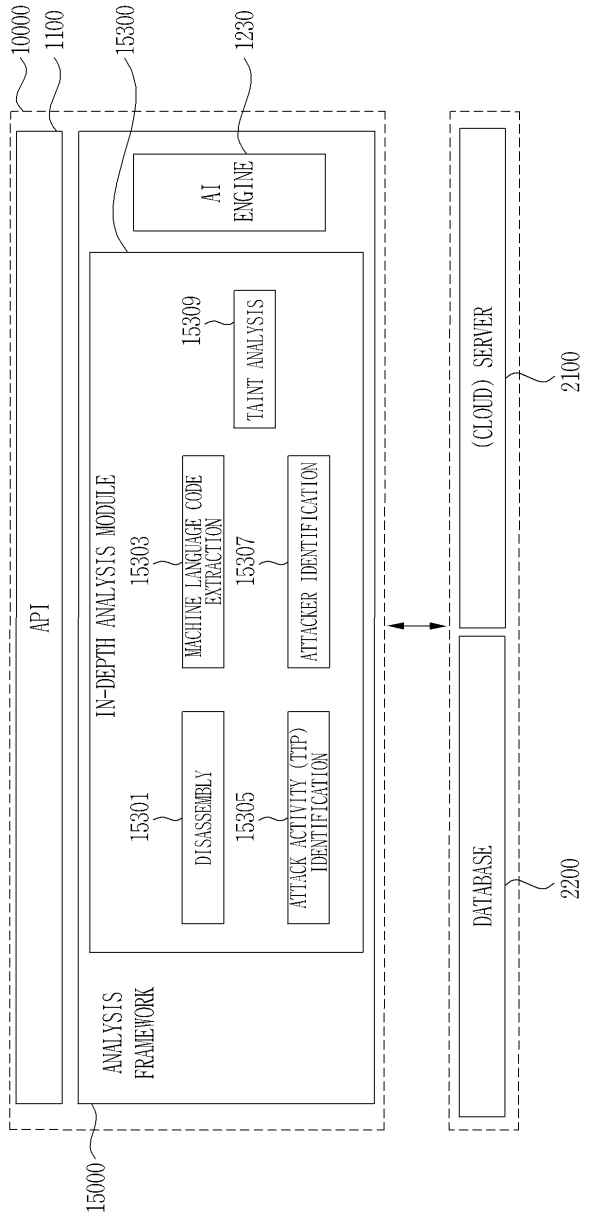


FIG. 14

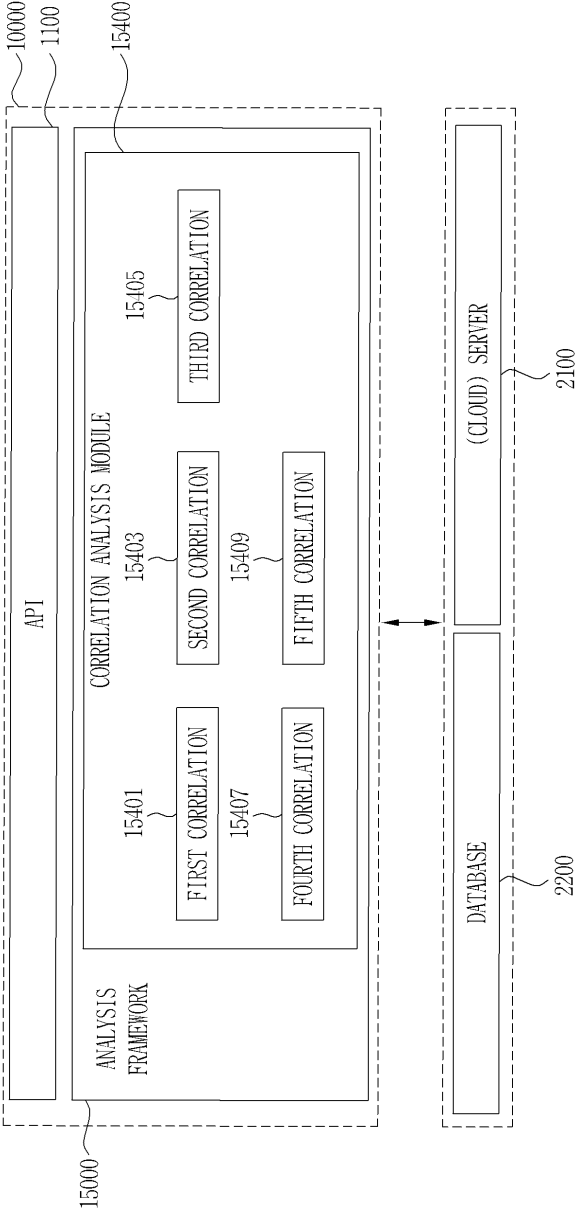


FIG. 15

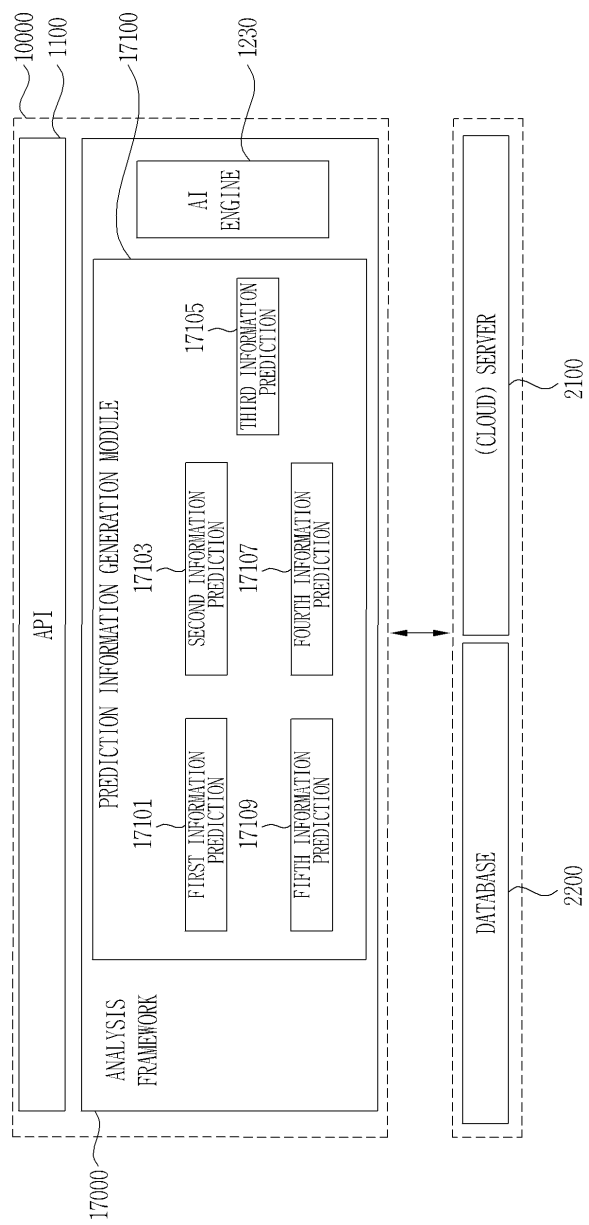


FIG. 16

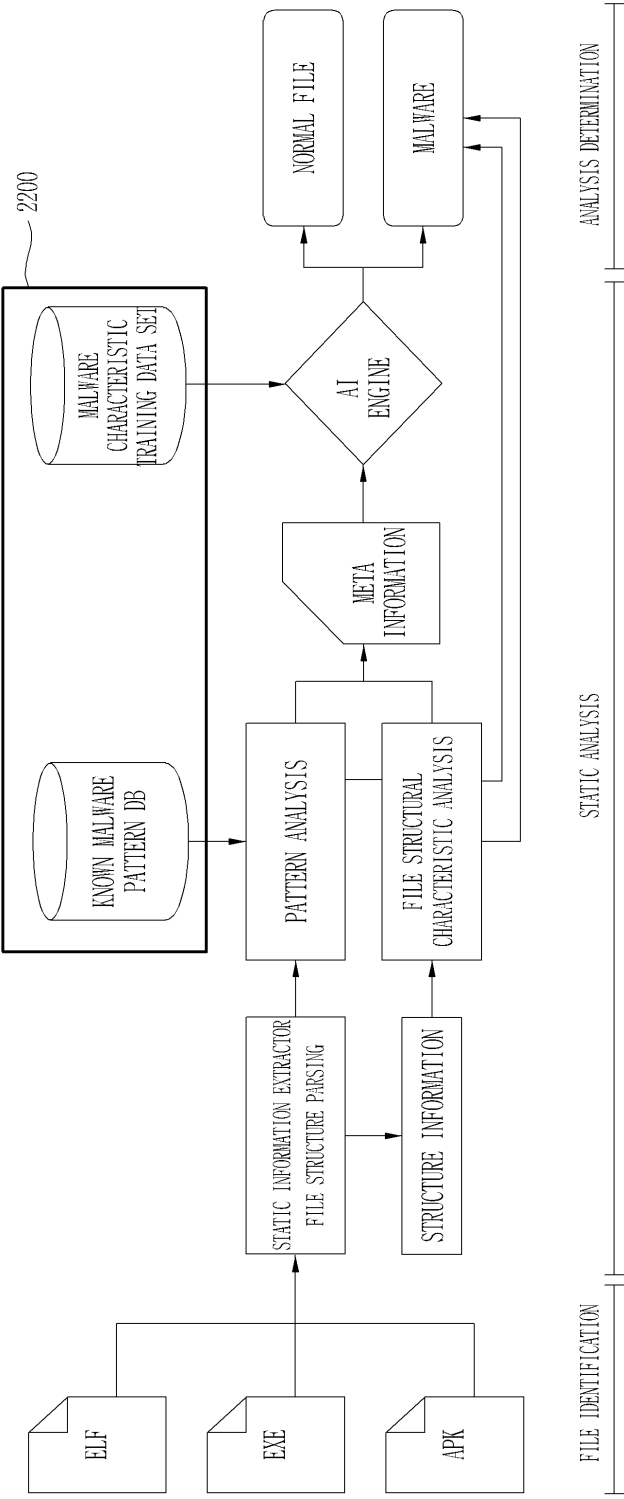


FIG. 17

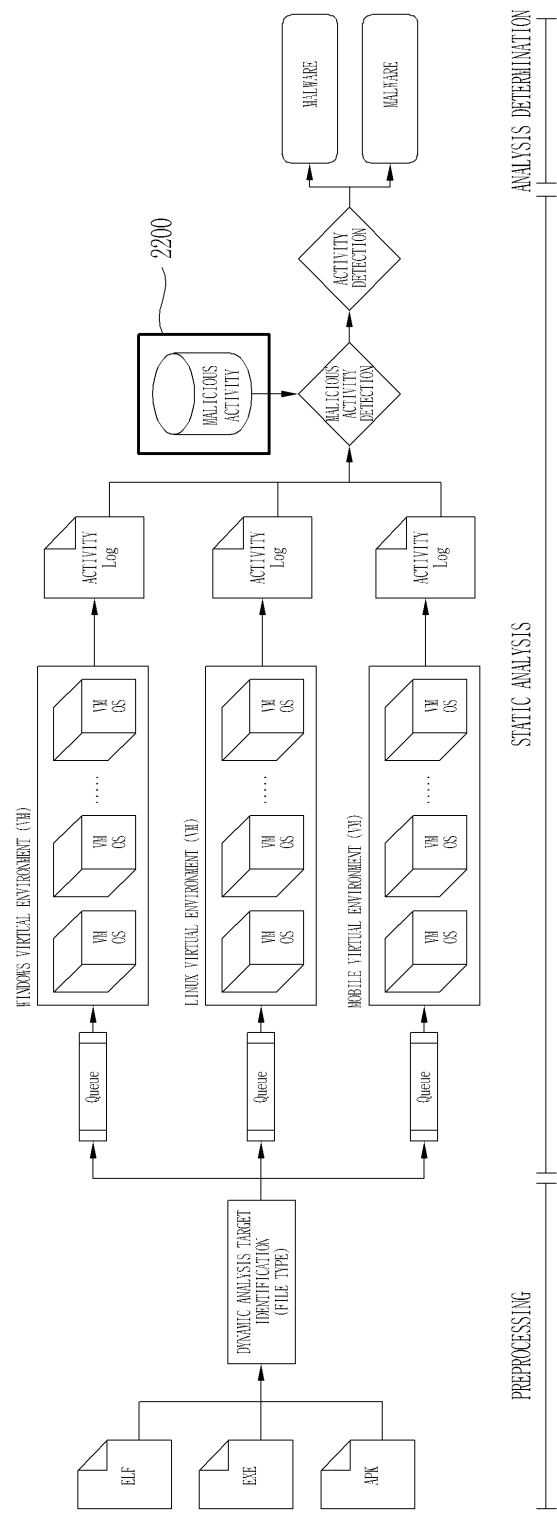


FIG. 18

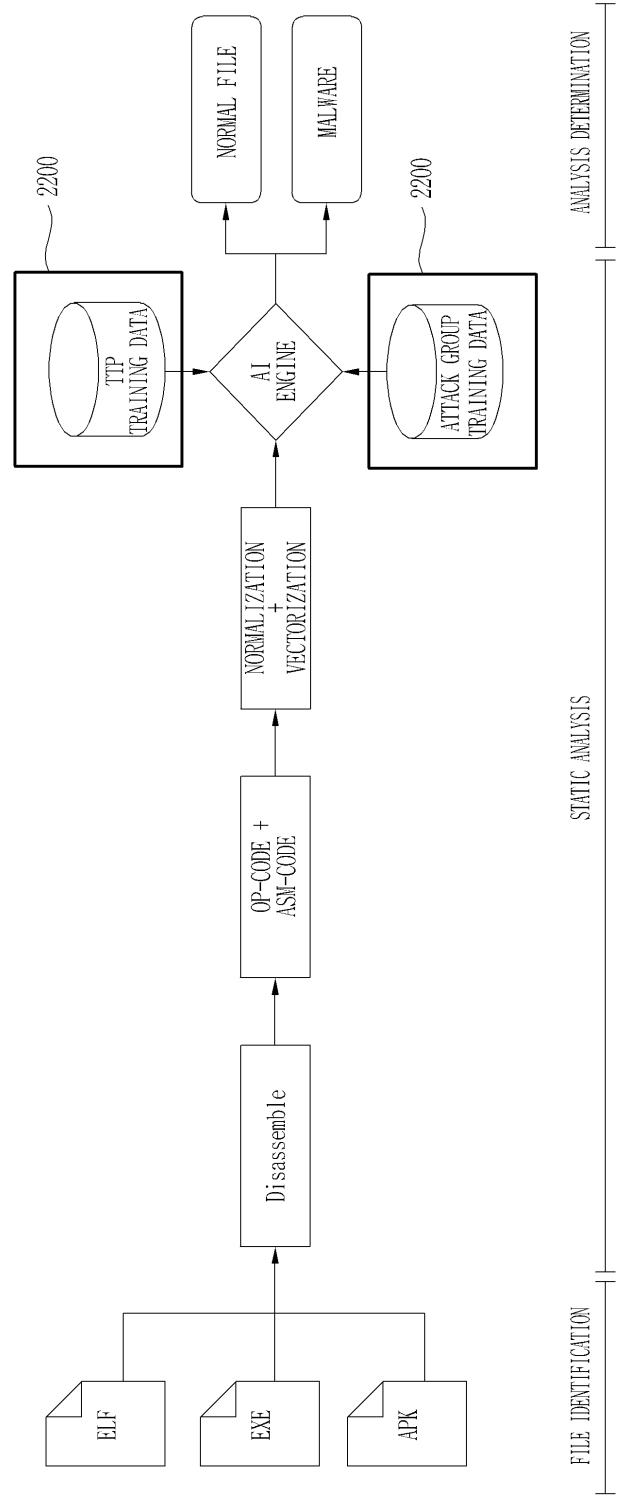


FIG. 19

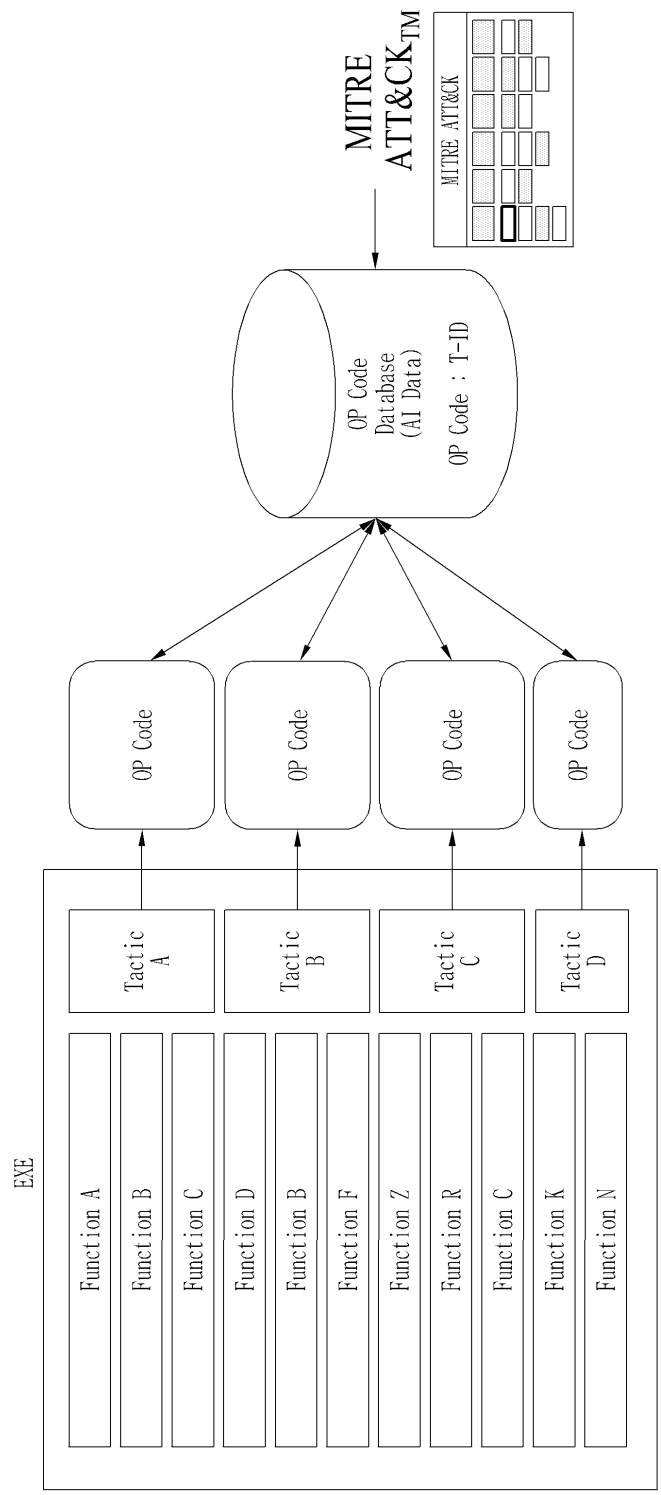


FIG. 20

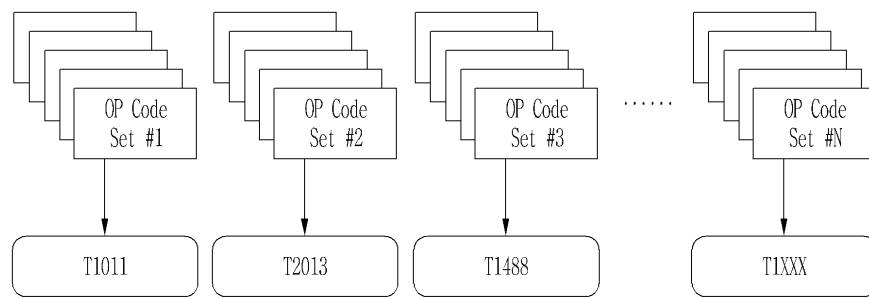


FIG. 21

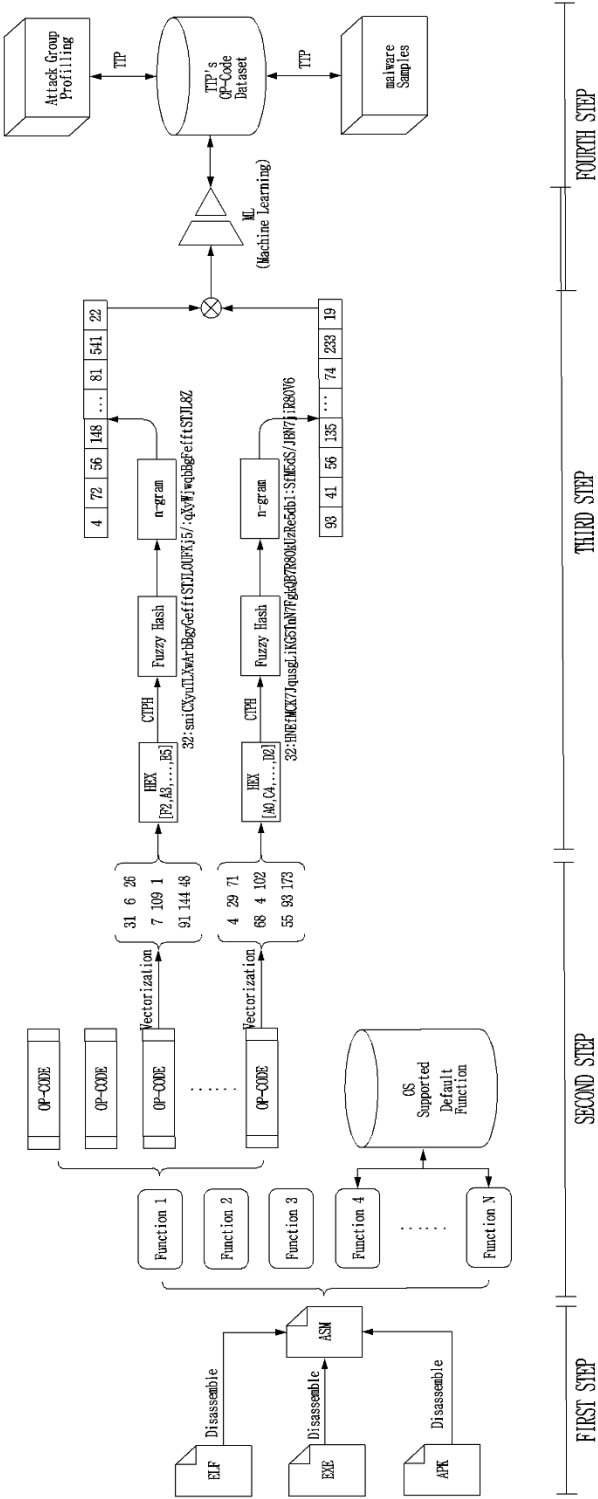


FIG. 22

OP-CODE`	OP-CODE → CRC-16	ASM-CODE	ASM-CODE → CRC-32
push	0x45E9	55	0xC9034AF6
mov	0x10E3	8B EC	0x3012FD2C
lea	0xAACE	8D 45 0C	0x9214A6AA
push	0x45E9	50	0xB969BE79
push	0x45E9	6A 00	0xDECB91D2
push	0x45E9	FF 75 08	0x1D4AE87E
push	0x45E9	6A 01	0xA9CCA144
call	0x09F8	FF 15 B0 20 40 00	0x284055E2
pop	0x7117	59	0xC0B506DD
push	0x45E9	50	0xB969BE79
call	0x09F8	E8 AB FF FF FF	0x4452C315
add	0x8B0B	83 C4 10	0xAE137EE5
pop	0x7117	5D	0xC7D8C2C4
retn	0x12B3	C3	0xD06F7C87

FIG. 23

OP-CODE Vector	ASM-CODE Vector
17897	201 3 74 246
4323	48 18 253 44
43726	146 20 166 170
17897	185 105 121 44
17897	222 203 145 210
17897	29 74 232 126
17897	169 204 161 68
2552	40 64 85 226
28951	192 181 6 221
17897	185 105 190 121
2552	68 82 195 21
35595	174 19 126 229
28951	199 216 194 196
4787	208 111 124 135

FIG. 24

Fixed block Original	content		a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	0	1
	ascii val		97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	48	49
	ascii sum		394			410			426			442			458			474			340									
	Kaq6KaU		K		a		q		6		K		a		U															

FIG. 25

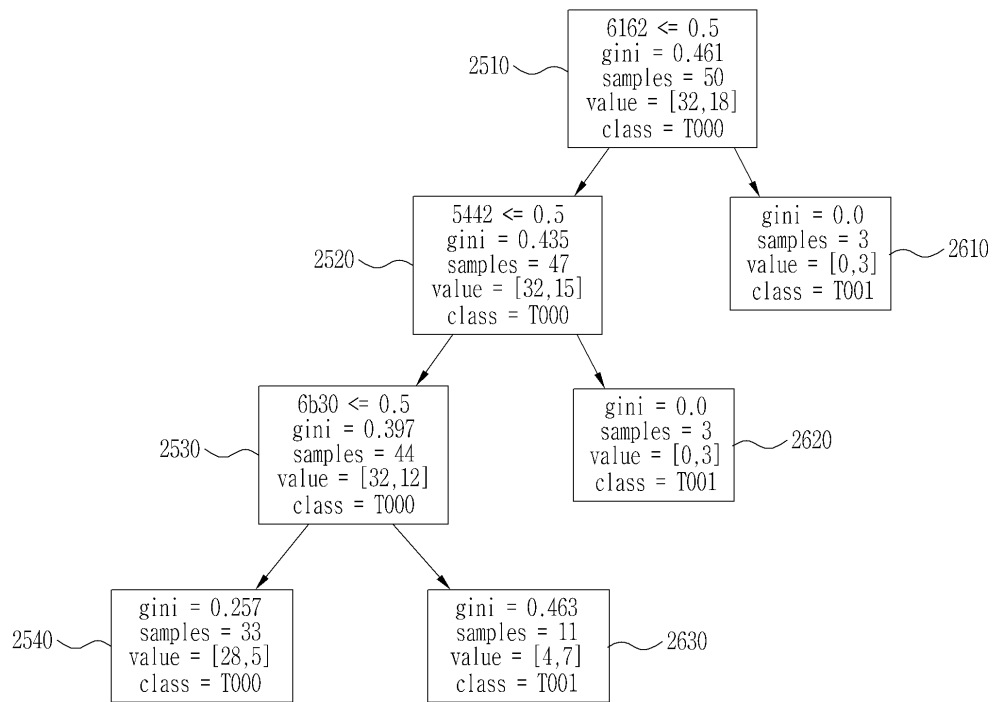


FIG. 26

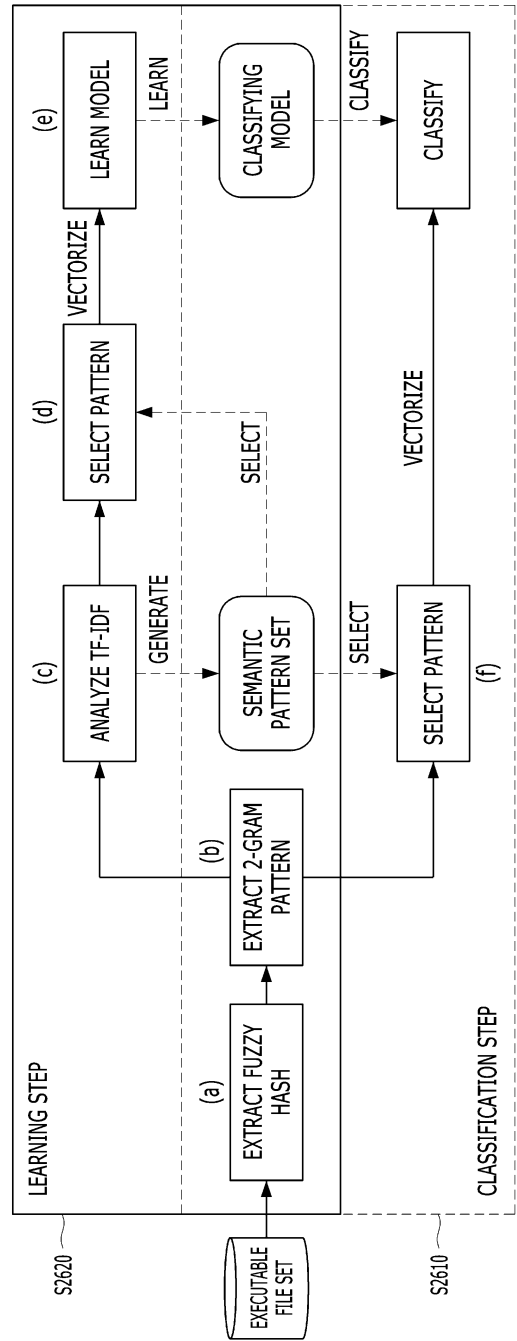


FIG. 27

Label		SHA-256 (size)	N-gram
T-ID	Attacker (or Group)	(OP-CODE + ASM-CODE)'s Fuzzy Hash	
T10XX	TA504	389E03B1A1FD1C5....	{ "3736":1, "3645":1, "4563":1, "6344":1, "4472":1, "7255":1
		32:76EcDrURBPQk58t...	
	TA504	E3EC2AA04AFECC6...	{ "3736":1, "3645":1, "4563":1, "6344":1, "4472":1, "7255":1, "5552":1, "5242":1, "4250":1.....
		32:76EcDrURBPQk58tGcoHE...	

FIG. 28

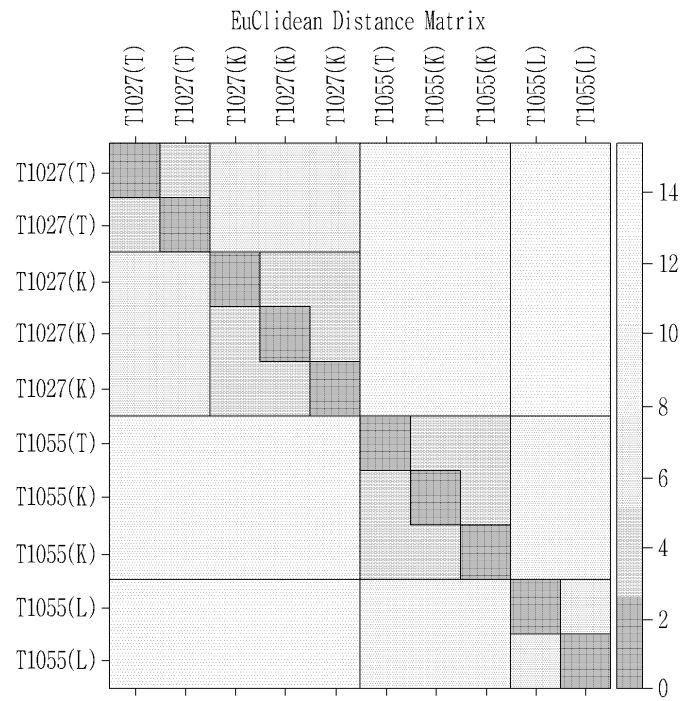


FIG. 29

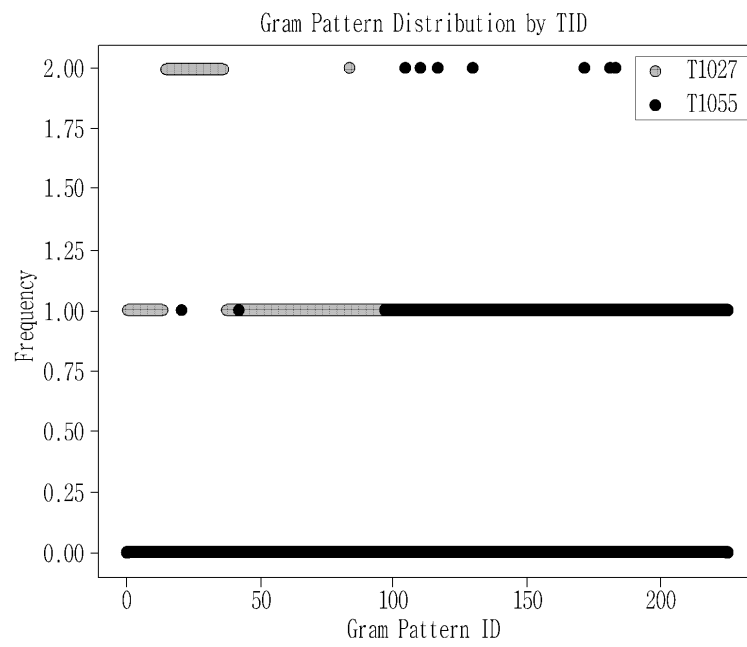


FIG. 30

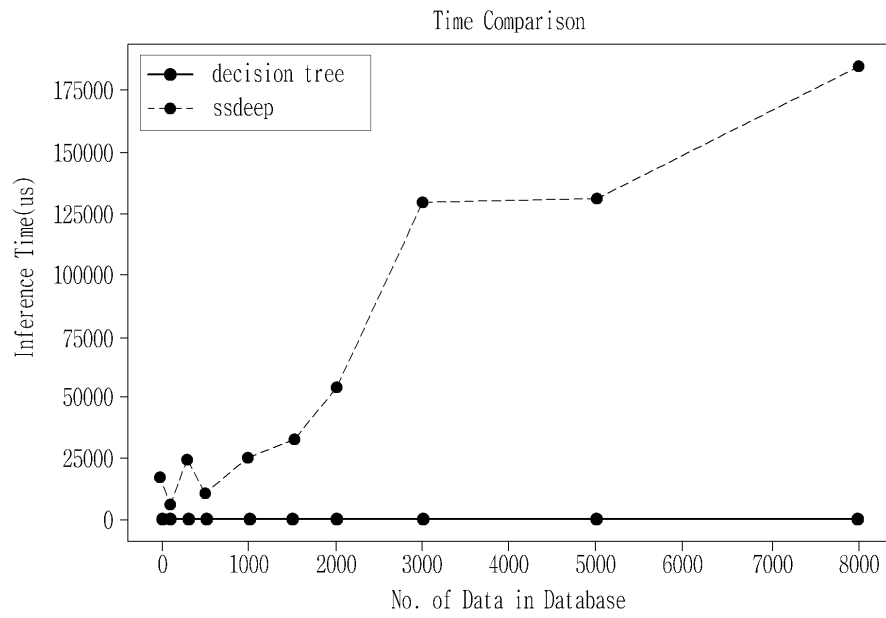


FIG. 31

Cylance	① Unsafe
eGambit	① Unsafe.AI_Score_100%
SentinelOne (Static ML)	① Static AI-Malicious PE
Symantec	① ML.Attribute.HighConfidence
SecureAge APEX	① Malicious
AVG	① FileRepMalware
Bkav Pro	① W32.AIDetect.malware1
Cynet	① Malicious (score:99)
Sophos	① ML/PE-A

3210

3220

FIG. 32

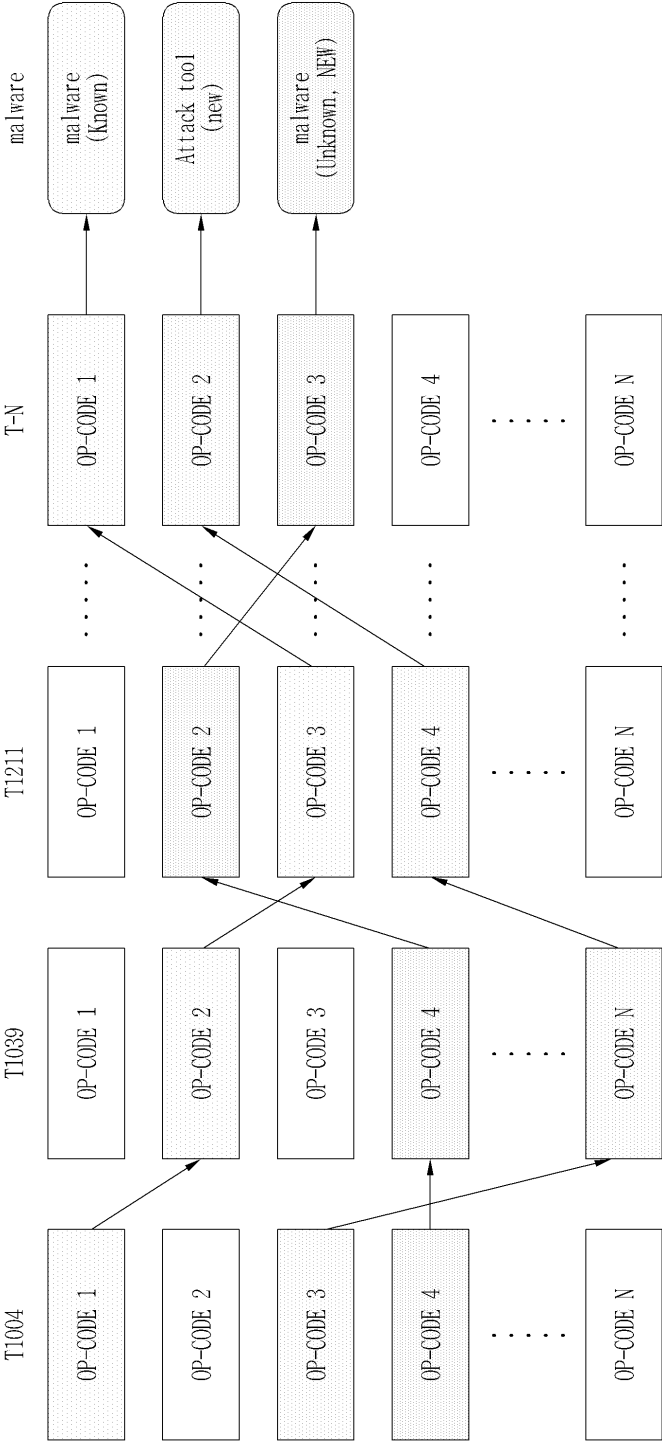


FIG. 33

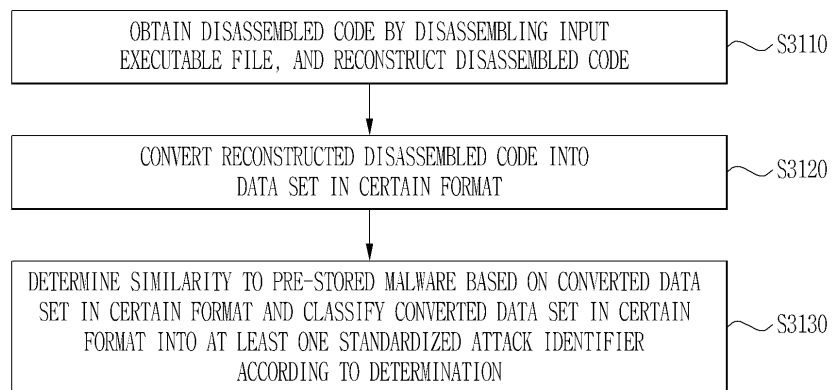


FIG. 34

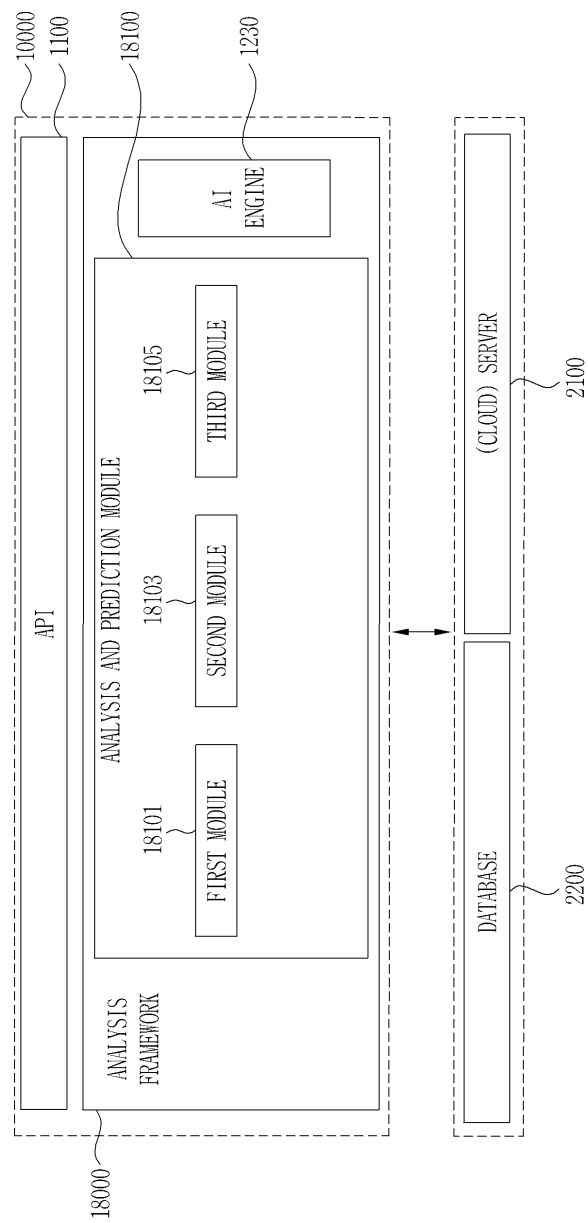


FIG. 35

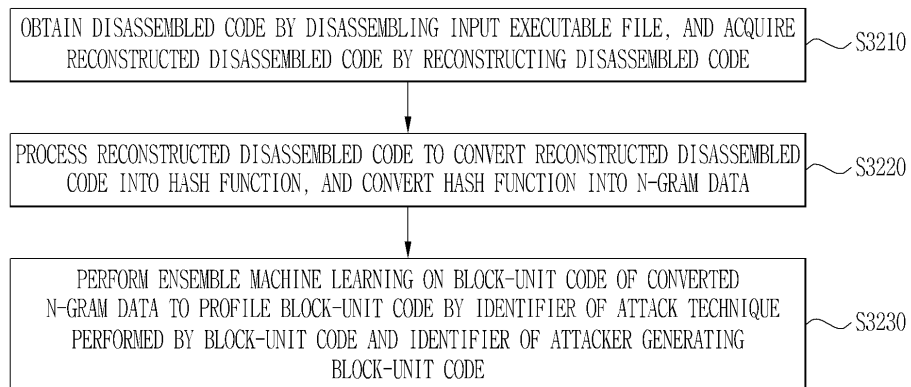


FIG. 36

