

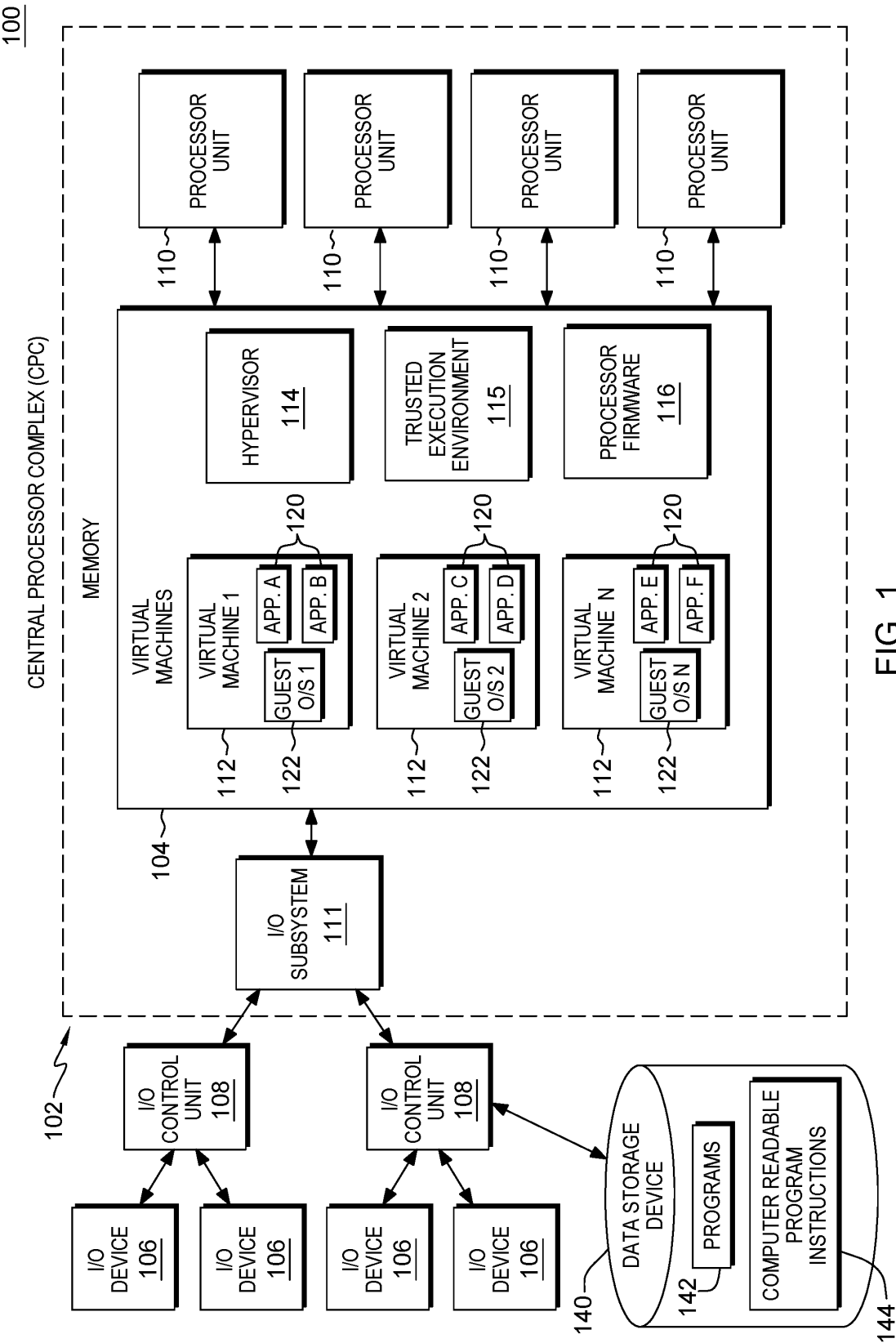


FIG. 1

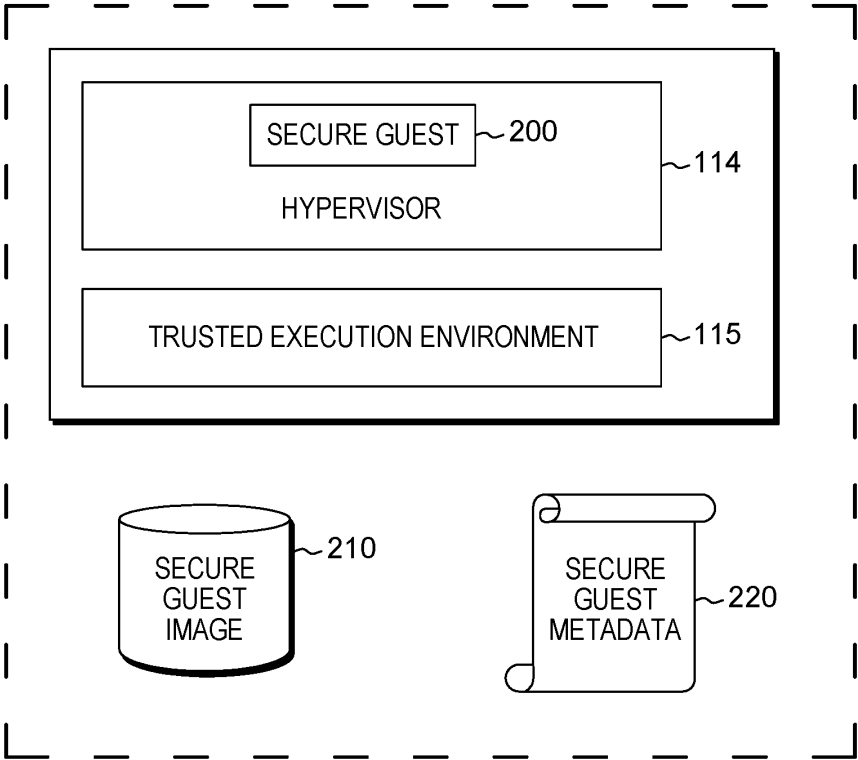


FIG. 2

300

310		312	314	316			
NAME		ABBREV	CONTENTS	PROTECTION			
REQUEST STRUCTURE TYPE		RHT	SG IMAGE UPDATE REQUEST	INTEGRITY			
302	REQUEST STRUCTURE INITIALIZATION VALUE	RHIV	INITIALIZATION VALUE USED FOR AES-GCM ENCRYPTION OF REQUEST STRUCTURE	INTEGRITY			
# OF KEY SLOTS		NKS		INTEGRITY			
318	CUSTOMER PUBLIC KEY	CPK	CUSTOMER PUBLIC KEY (ECDH P521)	INTEGRITY			
320	KEY SLOT 1	kslot1	RPK WRAPPED FOR HOST 1	INTEGRITY			
	...			INTEGRITY			
	KEYSLOT n	kslotn	RPK WRAPPED FOR HOST n	INTEGRITY			
322	REQUEST FLAGS	RF	E.G., OPTION INDICATIONS LIKE CHALLENGE REQUIRED	ENCRYPTED			
324	CHANGE INDICATION FLAGS	CIF	FLAGS DESCRIBING TYPES OF REQUIRED CHANGES	ENCRYPTED			
326	AUTHENTICATION DATA	AD	NONCE AES(oldCCK, NONCE)	OPTIONAL, ENCRYPTED			
	CHANGE DATA	CD	DATA SPECIFYING CHANGES	ENCRYPTED			
	REQUEST STRUCTURE TAG	RST	AES-GCM TAG	N/A			

FIG. 3

4/12

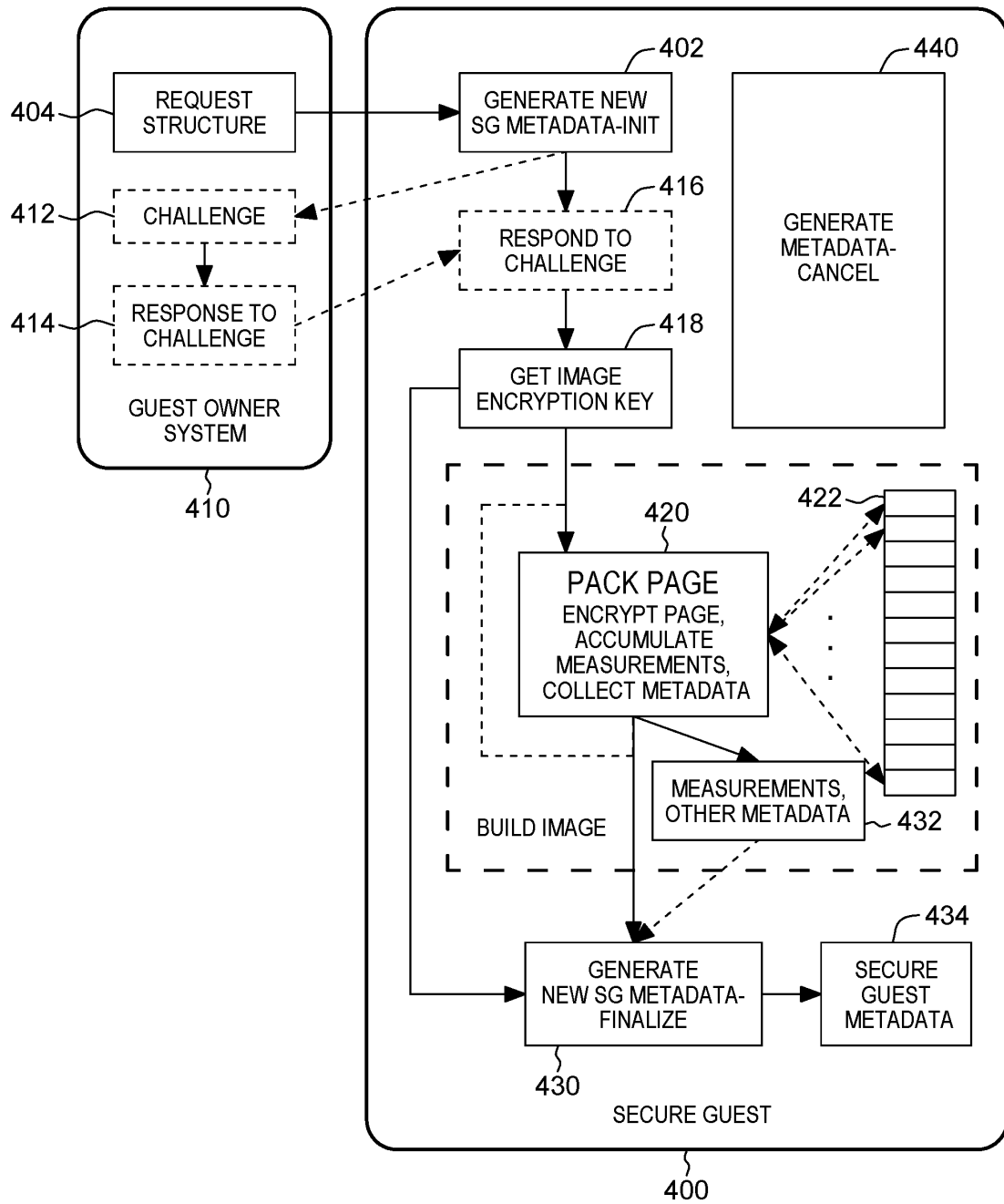


FIG. 4

5/12

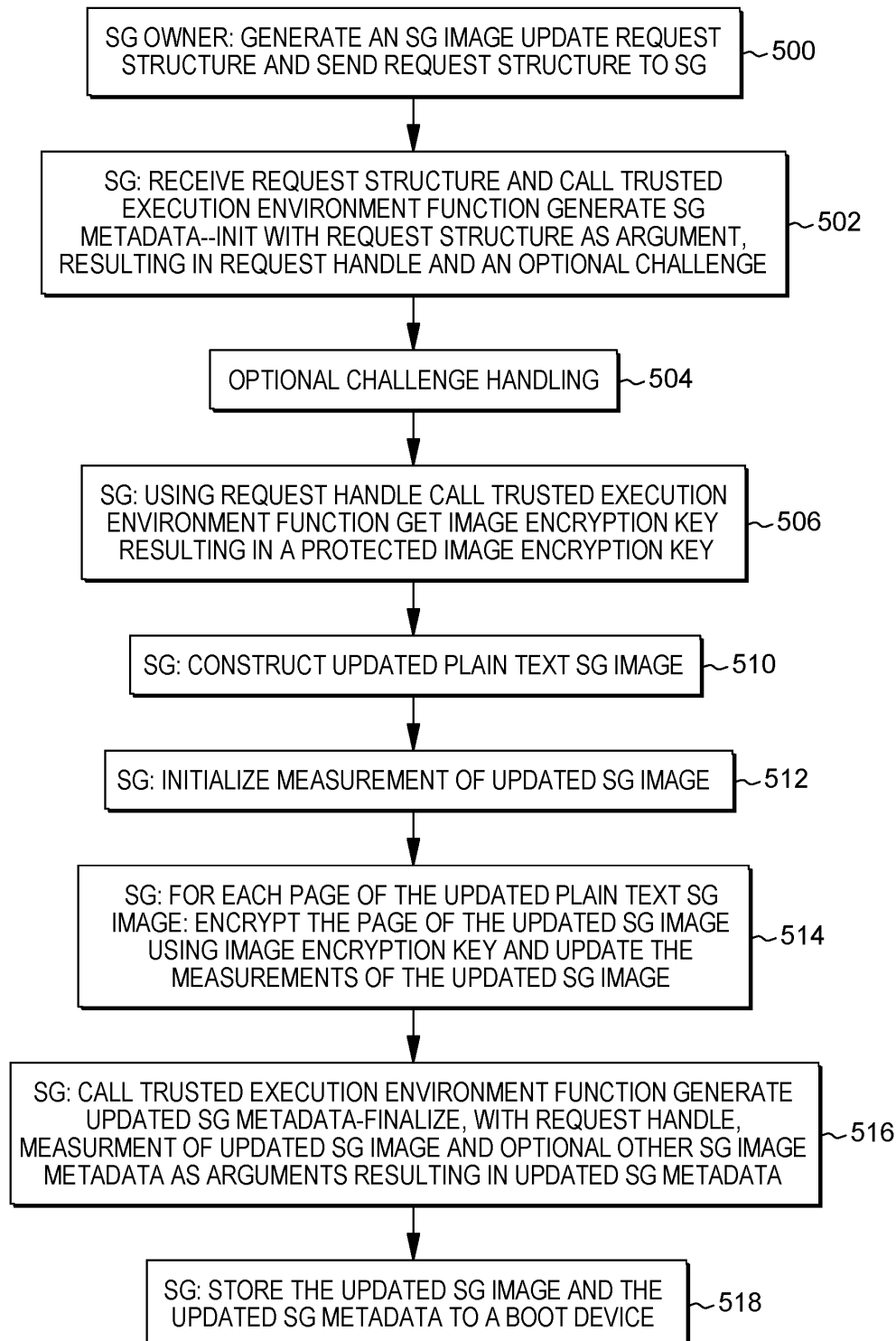


FIG. 5A

6/12

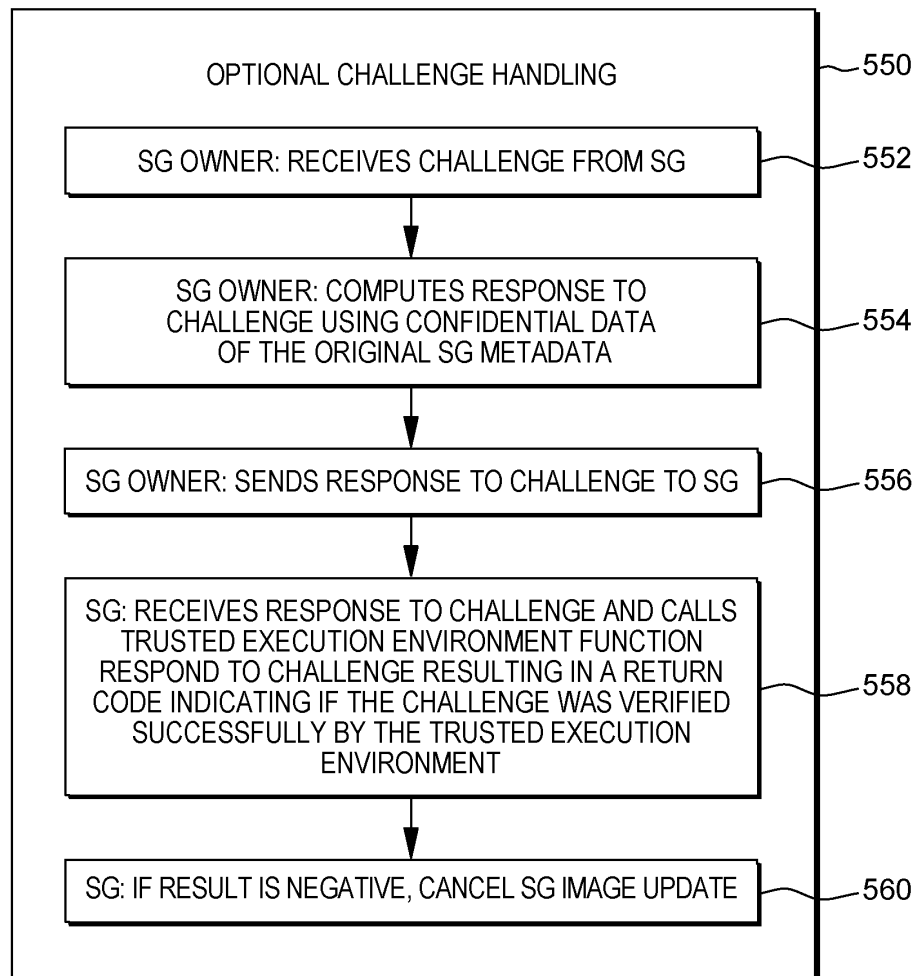


FIG. 5B

7/12

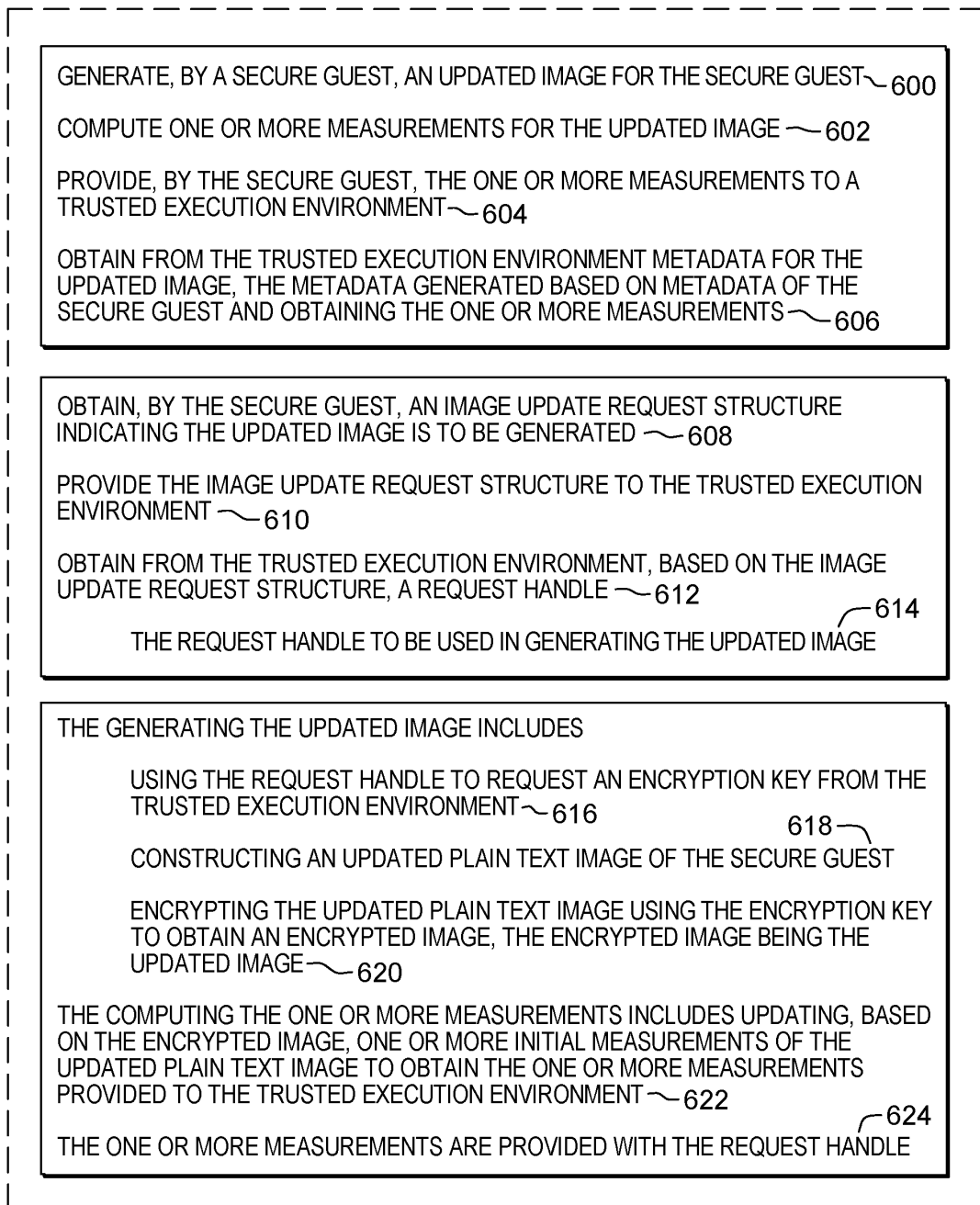


FIG. 6A

8/12

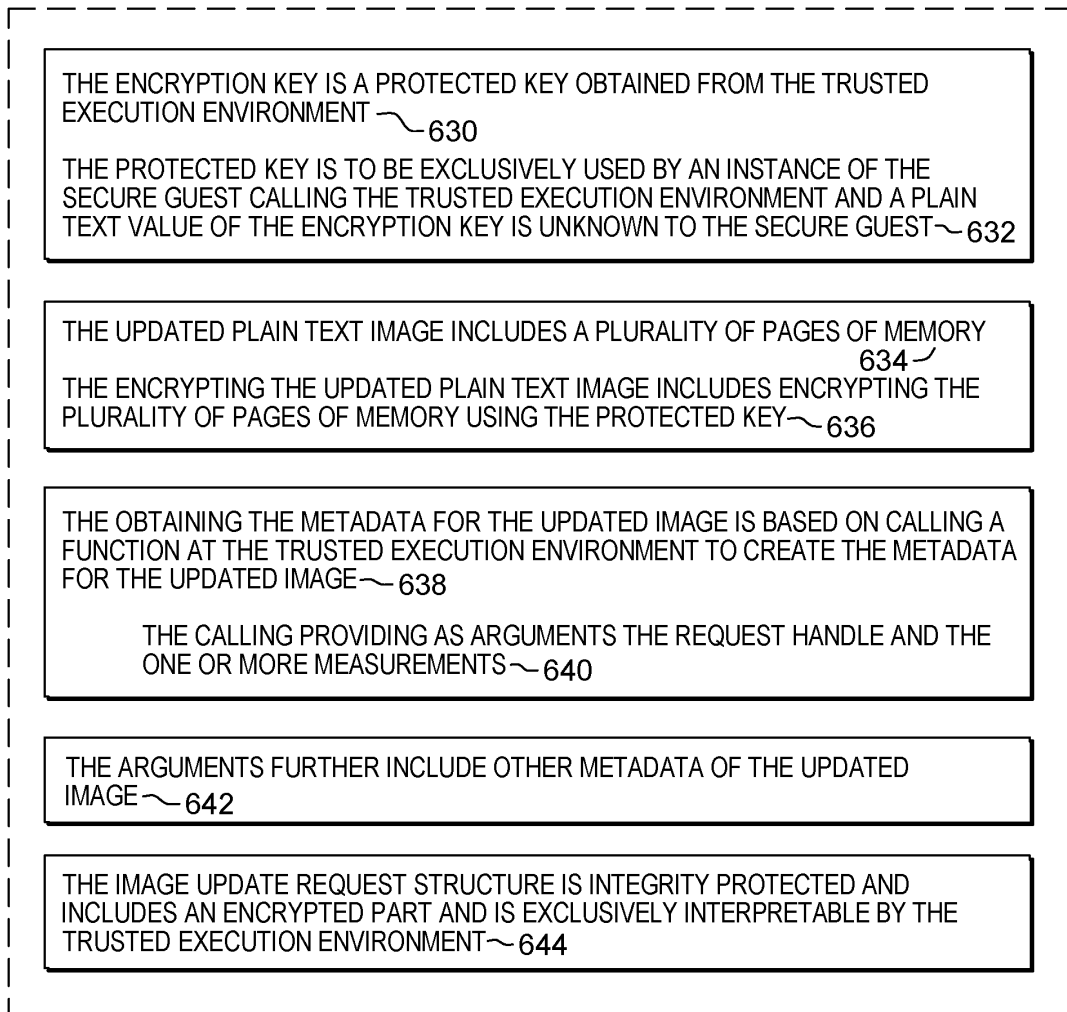


FIG. 6B

9/12

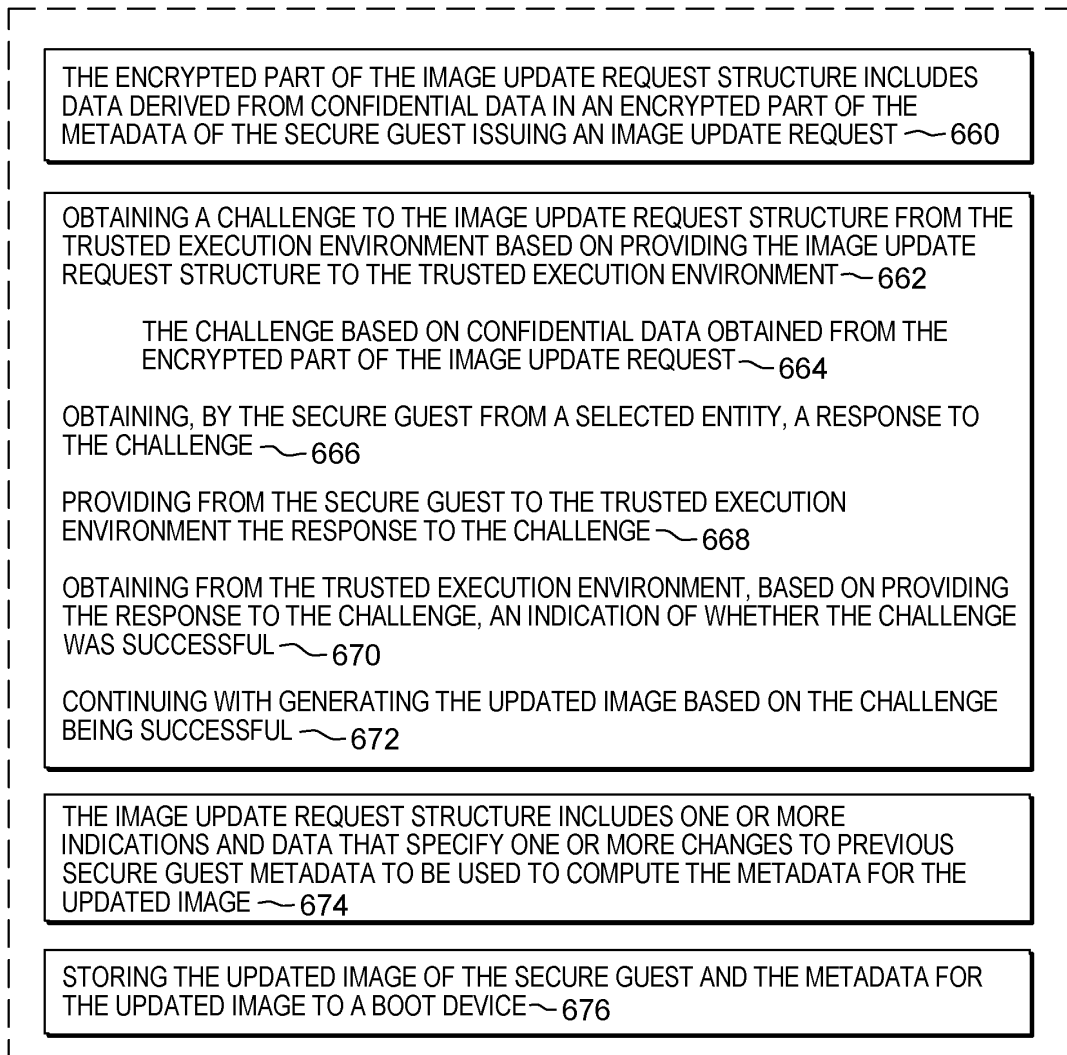


FIG. 6C

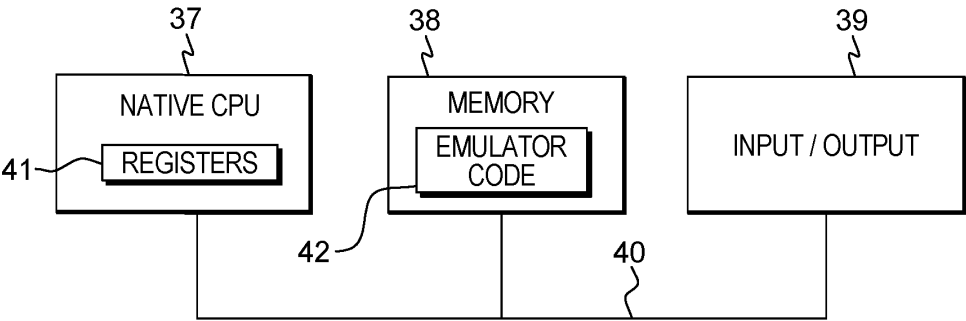


FIG. 7A

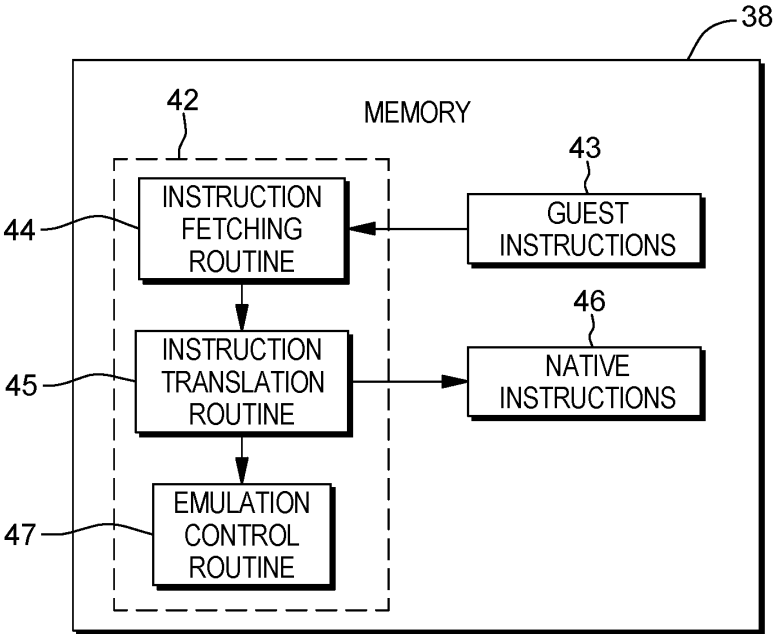


FIG. 7B

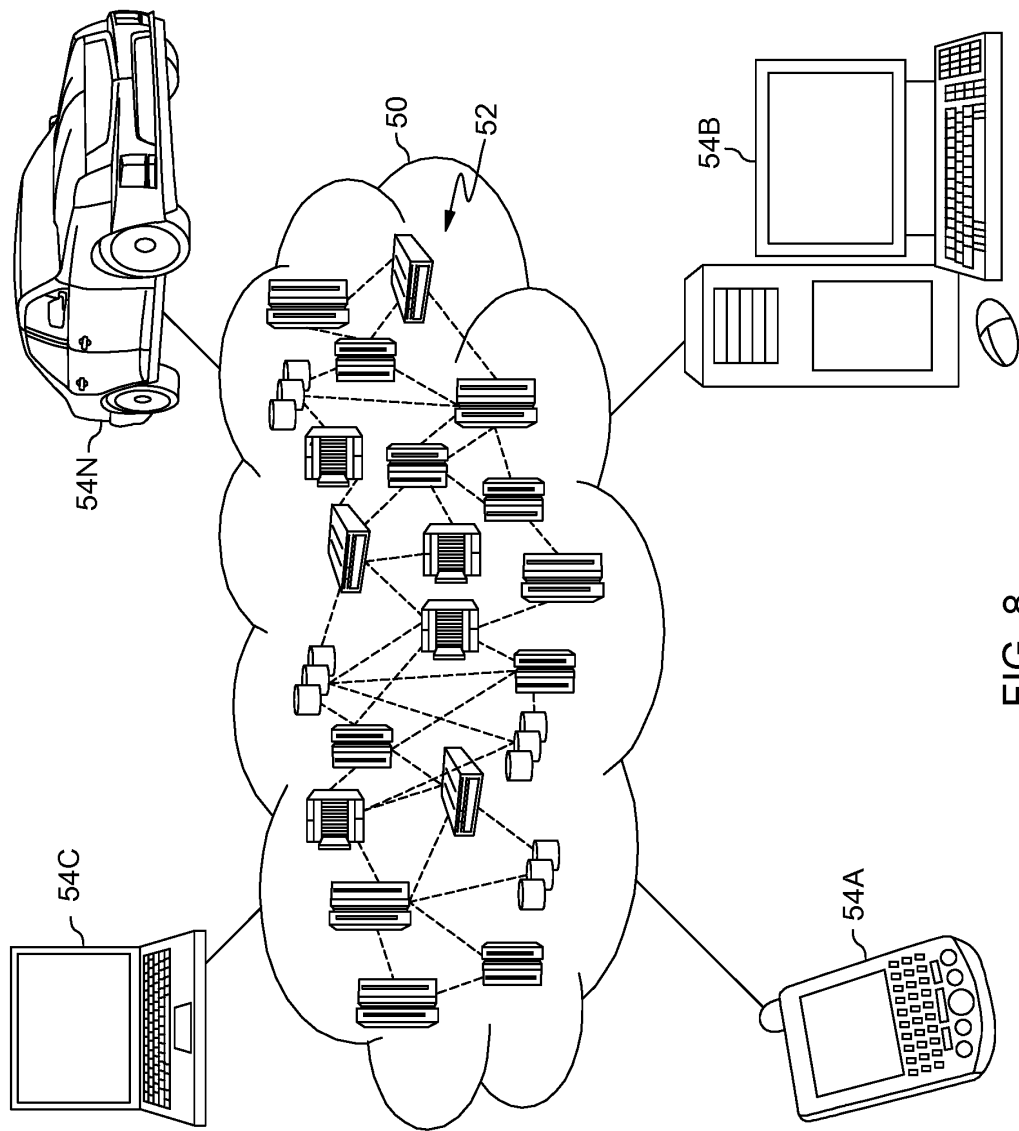


FIG. 8

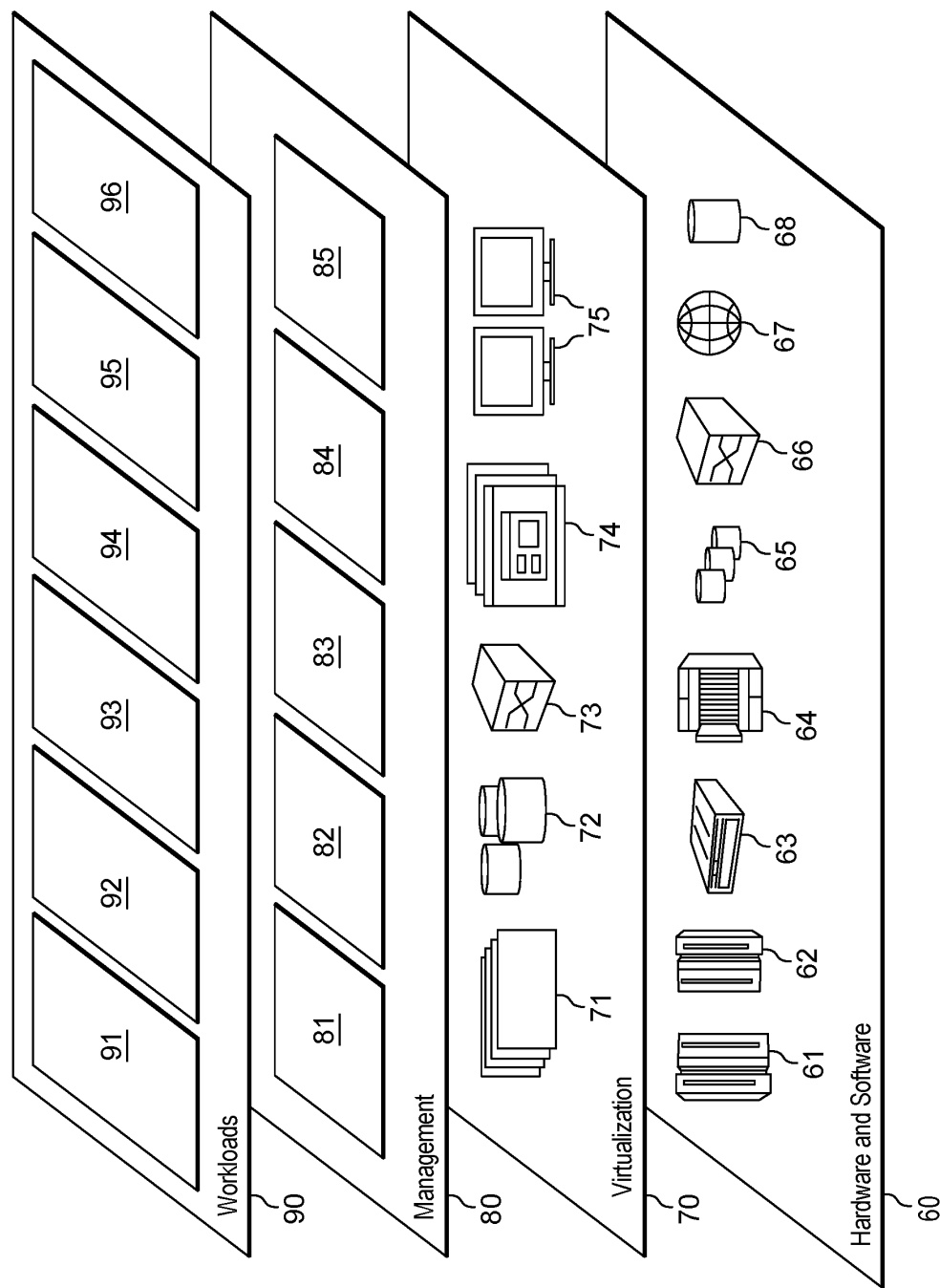


FIG. 9