

DIGITAL SIKKERHED – FREMSTIDENS TRUSLER

Øvelser

Instruktioner: Udfyld de tomme felter i sætningerne nedenfor med det korrekte ord fra listen. Hvert ord bruges kun én gang.

Ordliste:

Kvantecomputere – Deepfakes – IoT – AI – Biometrisk - 5G – Blockchain - Cloud

Sætninger:

_____ vil kunne bryde nuværende krypteringsmetoder, hvilket skaber et presserende behov for kvantesikre krypteringsalgoritmer.

_____ teknologi kan misbruges til at skabe overbevisende falske videoer og lydoptagelser, hvilket udgør en trussel for troværdigheden af digitalt indhold.

Den eksplosive vækst i _____-enheder (Internet of Things) øger antallet af potentielle angrebepunkter i netværk drastisk.

Avancerede _____-drevne cyberangreb vil kunne tilpasse sig og lære af forsvarsmekanismer i realtid, hvilket gør dem sværere at opdage og stoppe.

Misbrug af _____ data, såsom fingeraftryk eller ansigtsgenkendelse, kan føre til identitetstyveri, der er meget vanskeligt at rette op på.

Den øgede hastighed og kapacitet i _____-netværk kan muliggøre mere sofistikerede og omfattende DDoS-angreb (Distributed Denial of Service).

Selvom _____ teknologi lover øget sikkerhed, kan den også misbruges til at skabe mere robuste og anonyme netværk for cyberkriminelle.

Efterhånden som flere virksomheder migrerer til _____-baserede løsninger, bliver datasikkerhed og privatlivs bekymringer mere komplekse og grænseoverskridende.

Løsninger i rækkefølge:

Kvantecomputere – Deepfakes – IoT – AI – Biometrisk - 5G – Blockchain - Cloud

2. Fremtidens Digitale værktøjer - forklaringer

Træk en streg fra Ord til forklaring i tabellen

Ord	Match	Forklaring
1. Kvantecomputere		A. Teknologi der muliggør hurtigere og mere pålidelig trådløs kommunikation med meget lav latenstid.
2. Deepfakes		B. En distribueret, kryptografisk sikret database-teknologi, der kan bruges til sikre, decentrale transaktioner.
3. IoT		C. Kraftige computere der udnytter kvantemekaniske principper til at udføre beregninger, potentielt truende nuværende kryptering.
4. AI		D. Teknologi der bruger unikke fysiske eller adfærdsmæssige karakteristika til identifikation og autentificering.
5. Biometrisk		E. Kunstigt genererede medier, typisk video eller lyd, der realistisk efterligner virkelige personer eller begivenheder.
6. 5G		F. Netværk af fysiske enheder indlejret med elektronik, software og sensorer, der muliggør dataudveksling.
7. Blockchain		G. Levering af computertjenester over internettet, herunder servere, storage, databaser, netværk, software og analyse.
8. Cloud		H. Simulering af menneskelig intelligens i maskiner, der er programmeret til at tænke og lære som mennesker.

Løsninger: 1. C, 2. E, 3. F, 4. H, 5. D, 6. A, 7. B, 8. G