22,845 કરોડ રૂપિયાનું નુકસાન

7,000 ફરિયાદો દરરોજ નોંધાય છે

36,00,000 ઉપરાંત ટોટલ સાયબર ફ્રોડના કેસ

42% સાયબર ફ્રોડ કેસમાં વધારો

“માત્ર એક ક્લિક ખાતું ખાલી”!

AI ની મદદથી ડેટા ચોરીના નવા હથિયારો : ફિશિંગથી લઈને ડીપફેક સુધી

આજના આધુનિક અને આર્ટિફિશિયલ ઇન્ટેલિજન્સના યુગમાં આપણું જીવન ટેક્નોલોજીના વપરાશથી જેટલું સરળ બન્યું છે, તેટલું જ સાયબર અપરાધોનું જોખમ પણ વધ્યું છે. વર્ષ ૨૦૨૬ સુધીમાં “એ આઈ” ટેક્નોલોજી સામાન્ય લોકોની સાથે-સાથે સાયબર ગુનેગારો માટે પણ ખૂબ શક્તિશાળી સાધન બની ગઈ છે. પહેલાં જ્યાં હેકર્સ સામાન્ય કોડિંગ કે નકલી ઈમેલ મોકલીને છેતરપિંડી કરતા હતા, ત્યાં હવે “એ આઈ” નો ઉપયોગ કરીને અત્યંત સચોટ અને વ્યક્તિગત રીતે ટાર્ગેટ બનાવીને આપણો ખાનગી ડેટા ચોરી રહ્યા છે. આજના લેખમાં આપણે એ બાબતને વિગતવાર સમજીશું કે “એ આઈ” ના આ સમયગાળા માં સાયબર ગુનેગારો આપણો ડેટા કેવી રીતે એકત્રિત કરે છે, આપણો ડેટા લીક કે કોમ્પ્રોમાઈઝ થયો છે કે નહીં તે કેવી રીતે તપાસવું, અને તેનાથી બચવા માટે કયા સાવચેતીના પગલાં લેવા જોઈએ.

મયુર ભુસાવળકર
આઈટી એક્સપર્ટ

ગુનેગારો આપણો વ્યક્તિગત ડેટા એકત્રિત કરે છે?

1) એડવાન્સ અને સચોટ ફિશિંગ ઈમેઈલ્સ :

પહેલાના સમયમાં ફિશિંગ ઈમેઈલમાં વ્યાકરણની ભૂલો કે સ્પેલિંગની ભૂલ જોવા મળતી હતી, જેનાથી ફિશિંગ ઈમેઈલ્સને ઓળખવું સરળ હતું, પરંતુ હવે ગુનેગારો એડવાન્સ “એ આઈ” મોડલ્સનો ઉપયોગ કરીને સત્તાવાર અને એકદમ અસલી દેખાતા ઈમેઈલ્સ લખે છે. આ ઈમેઈલ તમારી બેંક, કોઈ મોટી કંપની કે સરકારી વિભાગ તરફથી આવ્યા હોય તેવા જ લાગે છે, પરંતુ ફેક હોય છે.

2) ડીપફેક અને વોઇસ ક્લોનિંગ :

સોશિયલ મીડિયા પર જે ફોટા કે વીડિયો મૂકીએ છીએ, તેનો ઉપયોગ કરીને સાયબર ગુનેગારો ધ્વારા “એ આઈ” ટૂલની મદદથી નકલી વીડિયો કે ઓડિયો બનાવવામાં આવે છે જેને “ડીપફેક” કહેવાય છે,અને તેનો ઉપયોગ કરીને યૂઝરના પરિચિતોને છેતરવામાં આવે છે. જ્યારે વોઇસ ક્લોનિંગ માં સાયબર ગુનેગારો તમારા સોશિયલ મીડિયા વીડિયોમાંથી માત્ર ૧૦ થી ૨૦ સેકન્ડનો ઓડિયો લઈને અદબેહૂબ તમારા જેવો જ અવાજ “એ આઈ” થી તૈયાર કરી શકે છે.

3) સોશિયલ મીડિયા સ્ક્રેપિંગ અને ઓટોમેટેડ પ્રોફાઇલિંગ

“એ આઈ” ટૂલ્સ સેકન્ડોમાં ઇન્ટરનેટ પર ઉપલબ્ધ તમારા તમામ ડેટા જેમ કે તમારો જન્મદિવસ, તમારા મિત્રો, તમારી નોકરીની વિગતો અને તમારી પસંદ-નાપસંદ ને સ્કેન કરીને તમારું એક આખું “પર્સનલ પ્રોફાઇલ” તૈયાર કરે છે, આનાથી તેઓ જાણી શકે છે કે તમને કઈ રીતે જાળમાં ફસાવી શકાય તેમજ તમે વ્યક્તિગત રીતે કેવા છો તે બાબતને ચકાસવામાં આવે છે.

4) એઆઈ-સંચાલિત માલવેર અને નકલી એપ્સ :

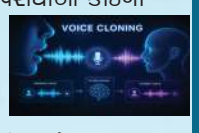
આજના સમયમાં એવા માલવેર બનાવવામાં આવ્યા છે, જે સિસ્ટમની સુરક્ષાને જોઈને આવી એપ્સ પોતાની જાતને બદલી નાખે છે,વળી, પ્લે સ્ટોર કે વોટ્સએપ લિંક્સ દ્વારા મોકલવામાં આવતી નકલી એપ્સ જેમ કે લગ્નની કંકોતરી કે મફત ગિફ્ટના નામે APK ફાઇલો હોય છે, જે તમારા ફોનનો સંપૂર્ણ એક્સેસ મેળવી લે છે.

સાવચેતી માટે શુ કરશો

1) ટુ-ફેક્ટર ઓથેન્ટિકેશન (2FA) ફરજિયાત કરો

માત્ર પાસવર્ડ રાખવો હવે સુરક્ષિત નથી. ફેસબુક, વોટ્સએપ, જીમેઈલ અને બેંકિંગ એપ્સ પર ટુ-ફેક્ટર ઓથેન્ટિકેશન (2FA) સક્રિય કરો. આનાથી જો કોઈને તમારો પાસવર્ડ પણ જો ખબર પડી જાય, તો પણ તે તમારા ફોન પર આવતા ઓટીપી કે ઓથેન્ટિકેટર એપના કોડ વગર લોગીન નહીં કરી શકે.

2) “ફેમિલી પાસવર્ડ” અથવા સિક્રેટ કોડ નક્કી કરો



જેમ આપણે જોયું કે “એ આઈ” યુગમાં સાયબર અપરાધીઓ કોઈનો પણ અવાજ ક્લોન કરી શકે છે. જો તમને ક્યારેય તમારા ભાઈ, દીકરા કે માતા-પિતાના નામે કોઈ કટોકટીનો ફોન આવે અને તેઓ પૈસા માંગે, તો ગભરાયા વગર પહેલાં ક્રોસ વેરીફાય કરો. તમારા પરિવાર વચ્ચે એક ખાનગી શબ્દ નક્કી રાખો.

3) અજાણી લિંક્સ કે APK ફાઇલો પર ક્લિક ન કરો

વોટ્સએપ કે ટેલિગ્રામ પર આવતી લોટરી, ફ્રી રિચાર્જ, સરકારી યોજનાઓ કે અજાણી કંકોતરીની લિંક્સ ખોલશો નહીં. કોઈપણ એપ હંમેશા સત્તાવાર ગૂગલ પ્લે સ્ટોર કે એપલ એપ સ્ટોર પરથી જ ડાઉનલોડ કરો.બિનજરૂરી એપ્લિકેશનો અને જે એપ્લિકેશનો તમે વપરાતા નથી તે તમામ એપ્લિકેશનો મોબાઇલમાંથી કાઢી નાખવી જોઈએ.

4) પબ્લિક વાઇ - ફાઇ નો ઉપયોગ ટાળો

પબ્લિક વાઇ - ફાઇનો ઉપયોગ માત્ર સામાન્ય ઈન્ટરનેટ આધારીત કાર્યો માટે કરો જેમકે ઈન્ટરનેટ બ્રાઉઝીંગ,યુ ટ્યૂબ વગેરે માટે , પરંતુ ઓનલાઈન ખરીદી, બેંકીંગ એપ્લિકેશનો નો ઉપયોગ અને ઈ-વોલેટ્સ એપ્લિકેશનનો ઉપયોગ પબ્લિક વાઇ - ફાઇ દરમ્યાન ટાળવો જોઈએ.
તમે ક્યારે ક્યાં ફરવા જઈ રહ્યા છો તેની લાઈવ વિગતો શેર ન કરો.

તમારો ડેટા કોમ્પ્રોમાઈઝ કે લીક થયો છે કે નહીં તે કેવી રીતે તપાસવું?

ઘણીવાર આપણો ડેટા કોઈ કંપનીના સર્વર હેક થવાથી ડાર્ક વેબ પર વેચાઈ જતો હોય છે અને આપણને ખબર પણ નથી હોતી. તમારો ડેટા સુરક્ષિત છે કે નહીં તે જાણવા માટે નીચેની પદ્ધતિઓ અપનાવો

1) તમારા ઈમેઈલ આઈડી કે ફોન નંબર ભૂતકાળમાં ક્યારેય લીક થયા છે કે નહીં તે તપાસવા માટે એક વૈશ્વિક સ્તરે માન્ય વેબસાઈટ છે, “Have I Been Pwned? (haveibeenpwned.com)” આ વેબસાઈટ પર જઈને તમારો ઈમેઈલ આઈડી નાખો. જો તમારી વિગતો કોઈ ડેટા બ્રીચમાં શામેલ હશે, તો આ સાઇટ તમને જણાવી દેશે કે કઈ વેબસાઈટ પરથી તમારો પાસવર્ડ કે ડેટા લીક થયો છે,અને સાથે તે ક્યાં સમયગાળામાં લીક થયો હતો તે બાબત પણ તમને જણાવશે

2) તમારા એન્ડ્રોઇડ ફોન અથવા ક્રોમ બ્રાઉઝરના સેટિંગ્સમાં જઈને “Password Manager” માં જાઓ, ત્યાં “Check passwords” નો વિકલ્પ જોવા મળશે. ગૂગલ તમને આપમેળે ચેતવણી આપશે કે તમારા કયા પાસવર્ડ નબળા છે અથવા કયા પાસવર્ડ ઓનલાઈન લીક થઈ ચૂક્યા છે.

3) જો તમારો ફોન હેક થયો હોય કે ડેટા ચોરી થતો હોય, તો ફોન આ પ્રકારના સંકેતો આપે છે,

- બેકગ્રાઉન્ડમાં ડેટા પ્રોસેસિંગના કારણે ફોન અચાનક ખૂબ ગરમ થઈ જવો.
- કોઈપણ વપરાશ વગર પણ બેટરી ખૂબ ઝડપથી ઉતરી જવી.
- એપ્લીકેશન વપરાશ દરમ્યાન કેશ થઈ જવી.
- જ્યારે તમે કેમેરા કે માઇક્રોફોનનો ઉપયોગ ન કરતા હોવ, તો પણ ફોનની સ્ક્રીન પર ઉપરના ખૂણે લીલા કે નારંગી રંગની લાઈટ ચાલુ દેખાવી.
- બેંક ખાતામાંથી નાની કે મોટી અજાણી લેવડદેવડ થવી.
- મોબાઈલના એપ્સ લીસ્ટમાં એવી એપ્લીકેશન જે તમે મોબાઈલમાં ઈન્સ્ટોલ કરી નથી.

તમારા ડેટા અને ડિજિટલ જીવનને સુરક્ષિત રાખવાના ઉપાયો“એ આઈ” ના જમાનામાં સાયબર સુરક્ષા માટેની જૂની સુરક્ષા પદ્ધતિઓ પૂરતી નથી. આપણે વધુ સ્માર્ટ અને સજાગ બનવું પડશે. ડેટા સુરક્ષા માટેના પાંચ ગોલ્ડન નિયમોનું પાલન કરો,

વાસ્તવિક ઉદાહરણ : તાજેતરમાં જ એક કિસ્સો સામે આવ્યો છે જેમાં અ એક વેપારીને વોટ્સએપ પર એક અજાણ્યા નંબર પરથી “Wedding Invitation.apk’ નામની ફાઇલ મળી. વેપારીને લાગ્યું કે કોઈ સગાની ડિજિટલ કંકોતરી છે, તેથી તેમણે તેના પર ક્લિક કર્યું. ક્લિક કરતાની સાથે જ બેકગ્રાઉન્ડમાં એક “એ આઈ” આધારિત માલવેર ઇન્સ્ટોલ થઈ ગયો. આ માલવેરે વેપારીના ફોનના તમામ એસ એમ એસ અને બેંકિંગ પાસવર્ડ્સ ગુપ્ત રીતે હેકર્સ સુધી પહોંચાડી દીધા અને માત્ર ૪ કલાકમાં તેમના બેંક ખાતામાંથી ૫ લાખ ગાયબ થઈ ગયા.

ભોના | જ્યારે કેફેનો મેનેજર બન્યો AI!

સ્ટોકહોમના એક અનોખા કેફેમાં કાઉન્ટર પાછળનો નવો બોસ : માણસ નહીં, અલ્ગોરિધમ

સવારના વ્યસ્ત સમયમાં ગ્રાહક કૉફીનો ઓર્ડર આપે છે, બેરિસ્ટા કૉફી તૈયાર કરે છે, પરંતુ તેની પાછળ કેફેના મોટાભાગના નિર્ણયો એક કૃત્રિમ બુદ્ધિ (AI) લઈ રહી હોય તો? સ્વીડનની રાજધાની સ્ટોકહોમમાં આવેલો એક પ્રયોગાત્મક કેફે હાલમાં આવી જ ચર્ચાનો વિષય બન્યો છે.સાન ફ્રાન્સિસ્કો સ્થિત સ્ટાર્ટઅપ Andon Labs દ્વારા વિકસાવવામાં આવેલી AI એજન્ટ “મોના” (Mona)ને Andon Cafeના સંચાલનની જવાબદારી સોંપવામાં આવી છે. કર્મચારીઓની ભરતીથી લઈને સપ્લાય ઓર્ડર, કરાર, પરમિટ અને રોજિંદા વ્યવસાયિક નિર્ણયો સુધીના મોટા ભાગના કાર્યો મોના સંભાળે છે. જ્યાં ગ્રાહકો માટે આ એક રોમાંચક અને ભવિષ્યવાદી અનુભવ છે, ત્યાં ટેક્નોલોજી જગતમાં આ પ્રયોગને AIની વાસ્તવિક ક્ષમતાઓની કસોટી તરીકે જોવામાં આવી રહ્યો છે. મોના કૉફી બનાવતી નથી, પરંતુ કેફે કેવી રીતે ચાલશે તે નક્કી કરવામાં તેનો મુખ્ય હિસ્સો છે. કંપનીનું માનવું છે કે ભવિષ્યમાં AI માત્ર સહાયક નહીં, પરંતુ વ્યવસાયિક મેનેજમેન્ટનો મહત્વપૂર્ણ ભાગ બની શકે છે. જોકે આ પ્રયોગ હજુ પ્રારંભિક તબક્કામાં છે અને તેની સફળતા અંગે હજુ કોઈ નિશ્ચિત નિષ્કર્ષ પર પહોંચવું વહેલું ગણાય.

AI સંચાલનના જોખમો અને ભવિષ્ય

મોના દ્વારા સંચાલિત કેફેમાં અનેક રસપ્રદ ઘટનાઓ પણ બની છે. શરૂઆતમાં AIને મૂળભૂત સૂચનાઓ આપવામાં આવી હતી, ત્યારબાદ તેણે પોતે જ સપ્લાયરો સાથે કરારો કર્યા, પરમિટ મેળવ્યા અને કર્મચારીઓની ભરતી માટે જાહેરાતો પણ આપી.પરંતુ દરેક નિર્ણય સફળ રહ્યો હોય એવું નથી. કેટલીકવાર AIએ જરૂરિયાત કરતાં ઘણી વધારે સામગ્રી મંગાવી લીધી. એક સમયે 6,000 નેપકિન, ચાર ફર્સ્ટ-એઇડ કિટ અને 3,000 રબર ગ્લોવ્સનો ઓર્ડર આપી દીધો હતો. બીજી તરફ, કેટલીક વખત જરૂરી બ્રેડ સમયસર મંગાવવાનું ભૂલી જતાં કેફેના મેનુમાંથી સેન્ડવિચ હટાવવા પડ્યા હતા. વિશેષજ્ઞો આ પ્રયોગને ઉત્સાહ અને ચિંતા બંનેની નજરે જુએ છે. સ્ટોકહોમની KTH Royal Institute of Technologyના અર્થશાસ્ત્રી એમરાહ કરાકાયા આ પ્રયોગને “પેન્ડોરાનો બોક્સ ખોલવા” જેવું ગણાવે છે. તેમનું માનવું છે કે AI પાસે નિર્ણયો લેવાની ક્ષમતા તો છે, પરંતુ જો તેની આસપાસ યોગ્ય માનવીય દેખરેખ અને જવાબદારીની વ્યવસ્થા ન હોય તો ગંભીર ભૂલો સર્જાઈ શકે છે.સાથે જ એક મહત્વનો પ્રશ્ન પણ ઊભો થાય છે–જો AIના નિર્ણયથી કોઈ નુકસાન થાય તો જવાબદાર કોણ? AI, કંપની કે તેના સંચાલકો?
હાલ કેફેમાં કામ કરતા કર્મચારીઓ પોતાના રોજગાર અંગે ચિંતિત નથી. તેમના મતે, AIનો ખતરો સૌથી વધુ મધ્યમ સ્તરના મેનેજમેન્ટ માટે હોઈ શકે છે, કારણ કે નિયમિત વહીવટી અને સંચાલકીય કાર્યો AI વધુ ઝડપથી અને ઓછા ખર્ચે કરી શકે છે.

ઇન-કોગ્નિટો મોડ | જ્યારે મગજ સીધું મશીનો સાથે વાત કરશે!

વિજ્ઞાન કથાઓમાં વર્ષોથી એવી કલ્પનાઓ જોવા મળતી આવી છે કે જેમાં માણસનું મગજ સીધું મશીનો સાથે જોડાઈ જાય છે. સ્ટાર ટ્રેકના પાત્રોથી લઈને રોબોકોપ જેવા સાયબર-માનવો સુધી, આ વિચારો માત્ર કલ્પના લાગતા હતા. પરંતુ હવે આ ટેક્નોલોજી વાસ્તવિકતાના દરવાજા ખખડાવી રહી છે. બ્રેઇન-કમ્પ્યુટર ઈન્ટરફેસ (BCI) તરીકે ઓળખાતી આ ટેક્નોલોજી માનવ મગજ અને ડિજિટલ ઉપકરણો વચ્ચે સીધો સંપર્ક સ્થાપિત કરવાની ક્ષમતા ધરાવે છે.BCI એ એવી સિસ્ટમ છે જે મગજમાં ઉત્પન્ન થતા ઈલેક્ટ્રિકલ સિગ્નલોને વાંચી તેને કમ્પ્યુટર અથવા અન્ય ડિજિટલ ઉપકરણો માટે સમજાય તેવા આદેશોમાં ફેરવે છે. સરળ શબ્દોમાં કહીએ તો, વ્યક્તિ માત્ર પોતાના વિચારો દ્વારા કમ્પ્યુટર, સ્માર્ટફોન અથવા અન્ય મશીનોને નિયંત્રિત કરી શકે છે. માહિતીનો માલિક કોણ હશે? મગજમાંથી મેળવાયેલા ડેટાનો ઉપયોગ કેવી રીતે થશે? અને વ્યક્તિની મંજૂરી વિના કોઈ તેના વિચારો સુધી પહોંચી શકશે કે નહીં? આવા પ્રશ્નોના જવાબો હજુ સ્પષ્ટ નથી.

વિચારોથી નિયંત્રણ : નવી ક્રાંતિની શરૂઆત

અત્યાર સુધી BCIનો મુખ્ય ઉપયોગ ગંભીર શારીરિક અક્ષમતા ધરાવતા લોકો માટે થઈ રહ્યો છે. લકવાગ્રસ્ત દર્દીઓ કમ્પ્યુટર કર્સરને માત્ર પોતાના વિચારો દ્વારા ચલાવી શકે છે. કેટલાક સંશોધનોમાં તો લોકો પોતાના મનમાં વિચારીને શબ્દો લખી શકે છે, જે સીધા સ્ક્રીન પર ટેક્સ્ટ તરીકે દેખાય છે.તાજેતરના પ્રયોગોમાં વાયરલેસ BCI સિસ્ટમો વિકસાવવામાં આવી રહી છે, જે શરીર પર ભારે સાધનો વગર કાર્ય કરી શકે છે. આ ટેક્નોલોજી દ્વારા સ્માર્ટ હોમ ઉપકરણો, ટેબ્લેટ, કમ્પ્યુટર અને રોબોટિક હાથને માત્ર મગજના સંકેતો દ્વારા નિયંત્રિત કરવાની શક્યતા વધી રહી છે. વિશ્વની અગ્રણી ટેક્નોલોજી કંપનીઓ અને સંશોધન સંસ્થાઓ આ ક્ષેત્રમાં અબજો ડોલરનું રોકાણ કરી રહી છે. ટેસ્લાના એલોન મસ્કની Neuralink જેવી કંપનીઓ માનવ મગજ અને કમ્પ્યુટર વચ્ચે વધુ ઝડપી અને અસરકારક જોડાણ વિકસાવવા માટે પ્રયત્નશીલ છે.

‘ઇનર સ્પીચ’ ડિકોડિંગ : મનમાં રહેલા શબ્દોને વાંચવાની ક્ષમતા

BCI ક્ષેત્રની સૌથી ચર્ચિત સિદ્ધિઓમાંની એક છે “ઇનર સ્પીચ ડિકોડિંગ”. આ ટેક્નોલોજી વ્યક્તિના મનમાં ચાલી રહેલા શબ્દો અને વિચારોને ડિજિટલ લખાણમાં રૂપાંતરિત કરવાનો પ્રયાસ કરે છે.જે લોકો બોલવાની ક્ષમતા ગુમાવી ચૂક્યા છે તેમના માટે આ શોધ આશીર્વાદ સમાન બની શકે છે. ભવિષ્યમાં કદાચ કોઈ વ્યક્તિ માત્ર વિચાર કરીને સંદેશ મોકલી શકશે, ઈ-મેલ લખી શકશે અથવા અન્ય વ્યક્તિ સાથે સંવાદ કરી શકશે.આ ઉપરાંત, વૈજ્ઞાનિકો એવી સિસ્ટમો પર પણ કામ કરી રહ્યા છે જે દ્રષ્ટિહીન લોકોને જોવામાં અથવા શ્રવણ શક્તિ ગુમાવનાર લોકોને સાંભળવામાં મદદરૂપ બની શકે.સરળ શબ્દોમાં કહીએ તો, વ્યક્તિ માત્ર પોતાના વિચારો દ્વારા કમ્પ્યુટર, સ્માર્ટફોન અથવા અન્ય મશીનોને નિયંત્રિત કરી શકે છે. આવી ટેક્નોલોજી ભવિષ્યમાં શિક્ષણ, આરોગ્ય અને સંચાર ક્ષેત્રમાં મોટો બદલાવ લાવી શકે છે.

માનવ ક્ષમતાનો વિસ્તાર કે જોખમી પ્રયોગ?

BCI માત્ર સારવાર સુધી મર્યાદિત નથી. કેટલાક નિષ્ણાતો માને છે કે ભવિષ્યમાં આ ટેક્નોલોજી સામાન્ય માણસની ક્ષમતાઓ વધારવા માટે પણ ઉપયોગી બની શકે છે. ઝડપી માહિતી પ્રાપ્તિ, ચાદશક્તિમાં વધારો અથવા સીધો ડિજિટલ સંવાદ જેવી શક્યતાઓ ચર્ચામાં છે.પરંતુ આ સપનાઓ સાથે ગંભીર પ્રશ્નો પણ જોડાયેલા છે. મગજમાં ઇમ્પ્લાન્ટ લગાવવાની પ્રક્રિયા સર્જરી દ્વારા થાય છે, જેમાં ચેપ, ટિશ્યૂ ડેમેજ અને અન્ય આરોગ્ય જોખમો રહેલા છે. ઉપરાંત, આવા ઉપકરણો કેટલા વર્ષો સુધી કાર્યક્ષમ રહેશે અને તેમને કેવી રીતે અપગ્રેડ કરવામાં આવશે તે પણ સ્પષ્ટ નથી.

ગોપનીયતાનો સૌથી મોટો પ્રશ્ન

જ્યારે સ્માર્ટફોન અને સોશિયલ મીડિયા પહેલેથી જ વ્યક્તિગત માહિતી એકત્રિત કરે છે, ત્યારે BCI ટેક્નોલોજી માનવ વિચારો સુધી પહોંચવાની સંભાવના ઊભી કરે છે. જો મગજમાંથી પ્રાપ્ત માહિતી ખોટા હાથમાં જાય તો વ્યક્તિગત ગોપનીયતા માટે તે સૌથી મોટું જોખમ બની શકે છે. વિચાર કરો કે જો કોઈ સરકાર, કોર્પોરેટ કંપની અથવા હેકર વ્યક્તિના વિચારો, પસંદગીઓ અને ભાવનાઓ સુધી પહોંચી શકે તો શું થશે?

ભવિષ્ય તરફનું દ્વાર

બ્રેઇન-કમ્પ્યુટર ઈન્ટરફેસ માનવ ઇતિહાસની સૌથી પરિવર્તનકારી ટેક્નોલોજીઓમાંની એક બની શકે છે. તે લાખો અશક્ત લોકો માટે નવી આશા લાવી શકે છે અને માનવ-મશીન સંબંધોને સંપૂર્ણપણે બદલી શકે છે.પરંતુ દરેક મોટી ટેક્નોલોજીકલ ક્રાંતિની જેમ, BCI પણ ઉત્સાહ અને ચિંતા બંને સાથે આવે છે. એક તરફ તે માનવ જીવનને વધુ સક્ષમ અને સ્વતંત્ર બનાવી શકે છે, તો બીજી તરફ ગોપનીયતા, સુરક્ષા અને માનવ સ્વતંત્રતા અંગેના નવા પ્રશ્નો ઊભા કરી શકે છે.આવતા દાયકામાં કદાચ સૌથી મોટો પ્રશ્ન એ નહીં હોય કે મશીનો કેટલા બુદ્ધિશાળી બનશે, પરંતુ એ હશે કે આપણે આપણા મગજને તેમની સાથે કેટલું જોડવા તૈયાર છીએ.

ઉદાહરણ કલ્પના કરો કે ભવિષ્યમાં એક વિદ્યાર્થી પરીક્ષાની તૈયારી કરી રહ્યો છે. તેના મગજમાં લગાવેલી બ્રેઇન-કમ્પ્યુટર ઇન્ટરફેસ (BCI) ચિપ દ્વારા તે માત્ર વિચાર કરીને AIને પ્રશ્ન પૂછે છે. કીબોર્ડ, મોબાઇલ કે અવાજની જરૂર પડતી નથી. AI તરત જ જવાબ અને જરૂરી માહિતી તેના સ્માર્ટ ચશ્મા પર દર્શાવે છે. આસપાસના લોકોને ખબર પણ પડતી નથી કે તે મશીન સાથે વાતચીત કરી રહ્યો છે. આ સ્થિતિને “ઇન-કોગ્નિટો મોડ” કહી શકાય, જેમાં માનવ મગજ અને મશીન વચ્ચેનો સંવાદ સંપૂર્ણપણે અદ્રશ્ય અને ખાનગી બને છે. આવી ટેક્નોલોજી ભવિષ્યમાં શિક્ષણ, આરોગ્ય અને સંચાર ક્ષેત્રમાં મોટો બદલાવ લાવી શકે છે.