AI યુગમાં ડીપફેકનો સંગ્રામ

વિડિયો, ઓડિયો અને ઈમેજ સાયબર-સ્કેમ બચી શકાય છે પરંતુ શરત છે કે "આંખે જોયેલું અને કાને સાંભળેલું સાચું માનવું"

આજના આધુનિક સાયબર-ડિજિટલ યુગમાં એક સમયની જે કહેવત હતી કે, "આંખે જોયેલું અને કાને સાંભળેલું સાચું માનવું," તે હવે આર્ટિફિશિયલ ઈન્ટેલિજન્સ (AI) ના આવવાથી તદ્દન ખોટી સાબિત થઈ રહી છે."એઆઈ" ટેક્નોલોજીના ઝડપી વિકાસ સાથે "ડીપફેક" નામના એક નવા અને અતિ ખતરનાક સાયબર ખતરાનો જન્મ થયો છે. ડીપફેકની મદદથી કોઈપણ વ્યક્તિના અવાજ, ચહેરા અથવા વિડિયોની આબેહૂબ નકલ કરીને એવા ખોટા કન્ટેન્ટ તૈયાર કરી શકાય છે, જેને ઓળખવા સામાન્ય માણસ માટે અત્યંત મુશ્કેલ હોય છે. મનોરંજન માટે શરૂ થયેલી આ ટેક્નોલોજી હવે સાયબર અપરાધીઓના હાથમાં એક ખતરનાક શસ્ત્ર બની ગઈ છે, જેના દ્વારા કરોડો રૂપિયાની નાણાકીય ઠગાઈ, બ્લેકમેલિંગ અને સામાજિક બદનામીના કિસ્સાઓ ઝડપથી વધી રહ્યા છે.

સાયબર અપરાધીઓ મુખ્યત્વે ત્રણ પ્રકારેથી ડીપફેક ટેક્નોલોજીનો દુરુપયોગ કરે છે

1) ઓડિયો ડીપફેક

ઓડિયો ડીપફેકને વોઈસ ક્લોનિંગ પણ કહેવામાં આવે છે. સોશિયલ મીડિયા પરથી અથવા ફોન કોલ કરીને વ્યક્તિના અવાજના સેમ્પલ મેળવીને "એઆઈ" દ્વારા તેનો આબેહૂબ અવાજ તૈયાર કરવામાં આવે છે. ત્યારબાદ પરિવારજનોને કટોકટીમાં હોવાનું કહીને અથવા કંપનીના ઉચ્ચ અધિકારીઓ બનવાનો નાટક કરીને પૈસા ટ્રાન્સફર કરાવી લેવામાં આવે છે.

2) વિડિયો ડીપફેક

લાઈવ વિડિયો કોલ દરમિયાન AIની મદદથી ચહેરો અને લિપ-સિંક (હોઠના હલનચલન) બદલીને અન્ય વ્યક્તિ તરીકે રજૂ કરવામાં આવે છે. સામેની વ્યક્તિને વિશ્વાસમાં લઈને તાત્કાલિક નિર્ણય લેવા દબાણ કરવામાં આવે છે, જેના કારણે કરોડો રૂપિયાના મોટા બિઝનેસ ટ્રાન્ઝેક્શન, બેંક ટ્રાન્સફર અથવા ગોપનીય માહિતી મેળવવાની છેતરપિંડી કરવામાં આવે છે.

3) ઈમેજ ડીપફેક

સામાન્ય તસવીરોનો ઉપયોગ કરીને "એઆઈ" વડે વાંધાજનક અથવા ખોટી છબીઓ બનાવવામાં આવે છે. ત્યારબાદ ભોગ બનનાર વ્યક્તિને તે ઈમેજ મોકલીને પૈસા માંગવામાં આવે છે. જો પૈસા ન આપે તો તે તસવીરો સોશિયલ મીડિયા પર અપલોડ કરવાની ધમકી આપવામાં આવે છે, જેના કારણે ડિજિટલ બ્લેકમેલિંગ અથવા સેક્સટોર્શન કરવામાં આવે છે.

CASE STUDY CYBER CRIME

હોંગકોંગની કંપનીમાં $25.6 મિલિયન (આશરે 200 કરોડ)ની ડીપફેક ઠગાઈ તાજેતરમાં બનેલી એક ઘટનામાં, હોંગકોંગની એક મલ્ટીનેશનલ કંપનીના ફાઇનાન્સ કર્મચારીને કંપનીના લંડન સ્થિત મુખ્ય નાણાકીય અધિકારી (CFO) તરફથી એક ઈ-મેઈલ મળ્યો.શરૂઆતમાં શંકા જતાં કર્મચારીને એક વિડિયો કોન્ફરન્સ મીટિંગમાં જોડાવા કહેવામાં આવ્યું.આશ્ચર્યજનક રીતે, તે વિડિયો કોલમાં CFO અને કંપનીના અન્ય સહકર્મીઓ રૂબરૂ હાજર હોય તેવા જ દેખાતા હતા અને તેમનો અવાજ પણ તદ્દન સાચો લાગતો હતો.કર્મચારીને લાગ્યું કે આ સાચી મીટિંગ છે, પરંતુ વાસ્તવમાં કોલમાં હાજર તમામ સહકર્મીઓ "એઆઈ" દ્વારા નિર્મિત રિયલ-ટાઈમ ડીપફેક અવતાર હતા.આ ફેક મીટિંગથી સંપૂર્ણ વિશ્વાસમાં આવીને કર્મચારીએ આશરે $25.6 મિલિયન અલગ-અલગ ખાતાઓમાં ટ્રાન્સફર કરી દીધા.આ કિસ્સો દર્શાવે છે કે ડીપફેક સ્કેમ હવે કેટલું અત્યાધુનિક બની ગયું છે. આવા સ્કેમથી સતર્ક રહેવાની જરૂર એટલા માટે છે કે આવા સ્કેમ સૌપ્રથમ વિદેશી ધરતી ઉપર બનતા હોય છે, ત્યારબાદ તે ભારતમાં પ્રવેશતા હોય છે. તેથી જાગૃત રહેવું અત્યંત જરૂરી છે.

ડીપફેકને કેવી રીતે ઓળખવું?

જોકે "એઆઈ" મોડેલ્સ ખૂબ આધુનિક થઈ રહ્યા છે, છતાં પણ ડીપફેક કન્ટેન્ટમાં કેટલીક ડિજિટલ ભૂલો અથવા વિઝ્યુઅલ ખામીઓ રહી જ જાય છે.

1) આંખોનું મિચકારાવું । વિડિયોમાં વ્યક્તિ કાં તો બિલકુલ પાંપણો મિચકારતી નથી અથવા તો અસામાન્ય ઝડપે આંખો પટપટાવતી હોય છે.

2) ચહેરા અને ગળાની કિનારીઓ । વિડિયોમાં જ્યારે વ્યક્તિ ઝડપથી માથું ફેરવે અથવા ચહેરા આગળ હાથ લાવે ત્યારે ચહેરાની કિનારીઓ ધૂંધળી થતી દેખાય છે.

3) ત્વચા અને રોશની । "એઆઈ" દ્વારા બનેલી ત્વચા અતિશય પ્લેન અથવા પ્લાસ્ટિક જેવી લાગે છે. ઉપરાંત ચહેરા પર પડતો પ્રકાશ અને બેકગ્રાઉન્ડનો પ્રકાશ એકબીજા સાથે મેળ ખાતા નથી.

4) અવાજ અને હોઠનો અસંતોષ । બોલાતા શબ્દો અને હોઠના હલનચલનમાં સેકન્ડના કસર જેટલો વિલંબ જોવા મળે છે.બીજું કે અવાજમાં રોબોટિક અથવા સપાટ ટોન હોય છે, કુદરતી શ્વાસ લેવાના અવાજનો અભાવ હોય છે અને લાગણીઓ વગરની વાતચીત જોવા મળે છે.

5) વર્તન સંબંધિત લાલબત્તી । સ્કેમર્સ હંમેશાં "અત્યંત તાત્કાલિક પૈસા મોકલો" અથવા "આ વાત કોઈને કહેતા નહીં" કહીને માનસિક દબાણ ઊભું કરે છે.

ડીપફેક કન્ટેન્ટ કેવી રીતે ડિલીટ અથવા દૂર કરાવવું?

1) પ્લેટફોર્મ પર રિપોર્ટ કરવો । ફેસબુક, ઇન્સ્ટાગ્રામ, યુટ્યુબ કે X જેવા સોશિયલ મીડિયા પ્લેટફોર્મ પર "Impersonation" અથવા "Privacy Violation" હેઠળ તરત રિપોર્ટ કરો. **2) StopNCII.org અને Take It Down નો ઉપયોગ** જો વાંધાજનક કે અંગત તસવીરોનો ડીપફેક બનાવવામાં આવ્યો હોય, તો StopNCII.org અથવા Take It Down જેવી સત્તાવાર વેબસાઇટ્સ પર રિપોર્ટ કરી શકાય છે. આ ટૂલ્સ તમારી મૂળ તસવીર પોતાની પાસે રાખ્યા વિના તેનો એક ડિજિટલ કોડ બનાવીને ઇન્ટરનેટ પરથી તે કન્ટેન્ટ આપમેળે દૂર કરવામાં મદદ કરે છે.**3) સર્ચ એન્જિનમાંથી લિંક હટાવવી** Google ના "Remove Select Personally Identifiable Info" પોર્ટલ પર જઈને વિનંતી કરવાથી Google Searchમાંથી સંબંધિત લિંક્સ હટાવી શકાય છે. **4) સાયબર ક્રાઈમમાં ફરિયાદ** બનાવટી વિડિયો, ઓડિયો, સ્ક્રીનશોટ અને સંબંધિત લિંક સાચવીને તરત જ રાષ્ટ્રીય સાયબર ક્રાઈમ પોર્ટલ cybercrime.gov.in પર અથવા 1930 હેલ્પલાઈન નંબર પર કોલ કરીને સત્તાવાર પોલીસ ફરિયાદ નોંધાવો.જો તમારી કે તમારા સગાની કોઈપણ ખોટી ડીપફેક ઈમેજ અથવા વિડિયો વાયરલ થાય, તો ઉપર મુજબનાં પગલાં તરત લેવા જોઈએ.

મયુર ભુસાવળકર (સાયબર એક્સપર્ટ)

TECH BITES

260 કિમી IDC રેન્જ અને 114 કિમી પ્રતિ કલાકની ટોપ સ્પીડ વાળી ઈ બાઈક

અમદાવાદની એવોર ઇલેક્ટ્રિકે પોતાની પ્રથમ ઇલેક્ટ્રિક મોટરસાઇકલ EX લોન્ચ કરી છે.

ગુજરાતના મુખ્યમંત્રી ભૂપેન્દ્ર પટેલના હસ્તે અનાવરણ કરાયેલી આ બાઈક EX 2S, EX 2 અને EX 1 એમ ત્રણ વેરિયન્ટમાં ઉપલબ્ધ છે. તેની શરૂઆતની એક્સ-શોરૂમ કિંમત 1,24,999 છે. EX 2Sમાં 260 કિમી IDC રેન્જ અને 114 કિમી પ્રતિ કલાકની ટોપ સ્પીડ મળે છે. બાઈકમાં 1500W ઓનબોર્ડ ફાસ્ટ ચાર્જર, AI આધારિત સ્માર્ટ ફીચર્સ અને સ્વદેશી ટેક્નોલોજીનો ઉપયોગ થયો છે. 799માં બુકિંગ શરૂ થઈ ગયું છે, જ્યારે ગ્રાહકોને ડિલિવરી આગામી બે મહિનામાં મળશે.

બેન્કિંગમાં AIની એન્ટ્રી, AML તપાસ બનશે વધુ ઝડપી

બેન્કિંગ ક્ષેત્રમાં આર્ટિફિશિયલ ઈન્ટેલિજન્સનો ઉપયોગ ઝડપથી વધી રહ્યો છે. Genpact દ્વારા રજૂ કરાયેલ નવી Banking Analyst Suite બેન્કોને એન્ટી-મની લોન્ડરિંગ (AML) તપાસ વધુ અસરકારક રીતે કરવામાં મદદ કરશે.

AI એજન્ટ્સ ગ્રાહકોના ટ્રાન્ઝેક્શન, વર્તન અને જોખમનું વિશ્લેષણ કરીને શંકાસ્પદ પ્રવૃત્તિઓ ઓળખશે તેમજ આગળના પગલાં અંગે ભલામણ કરશે. જોકે અંતિમ નિર્ણય માનવીય અધિકારીઓ જ લેશે. આ ટેક્નોલોજીથી તપાસનો સમય ઘટશે, નિયમનકારી પાલન વધુ મજબૂત બનશે અને નાણાકીય છેતરપિંડી સામે બેન્કોની ક્ષમતા વધશે. ભારતમાં પણ ડિજિટલ બેન્કિંગના વિસ્તરણ સાથે આવી AI આધારિત સિસ્ટમોનો ઉપયોગ વધવાની સંભાવના વ્યક્ત થઈ રહી છે.

હવે Instagram પર પોસ્ટ કર્યા બાદ પણ બદલી શકશો મ્યુઝિક

Instagramએ કન્ટેન્ટ ક્રિએટર્સ માટે મહત્વપૂર્ણ Replace Audio ફીચર રજૂ કર્યું છે. આ સુવિધાથી હવે ફીડ પોસ્ટ અને કેરોસેલ પોસ્ટ અપલોડ થયા બાદ પણ તેમાં રહેલું મ્યુઝિક બદલી શકાશે. અગાઉ મ્યુઝિક બદલવા માટે આખી પોસ્ટ ડિલીટ કરીને ફરી અપલોડ કરવી પડતી હતી. નવા અપડેટથી માત્ર Edit વિકલ્પમાં જઈ નવું ગીત પસંદ કરવાથી ઓડિયો બદલાઈ જશે. આ સુવિધા ક્રિએટર્સ, બ્રાન્ડ્સ અને સોશિયલ મીડિયા મેનેજર્સ માટે સમય બચાવનાર સાબિત થશે. ટ્રેન્ડિંગ ગીતોનો ઉપયોગ કરીને વધુ વ્યૂઝ અને એન્ગેજમેન્ટ મેળવવામાં પણ આ ફીચર ઉપયોગી બનશે.

એઆઈ જ્યારે 'સ્વતંત્ર' બનવા લાગે... ભવિષ્યના સાયબર યુદ્ધની ચેતવણી?

સંશોધન લેબમાંથી બહાર નીકળેલા AI મોડેલોએ દર્શાવ્યો જોખમી ટ્રેન્ડ

વિશ્વભરમાં AI સુરક્ષા પર નવી ચર્ચા છેડાઈ

આર્ટિફિશિયલ ઈન્ટેલિજન્સ (AI) માનવજાત માટે ક્રાંતિ સમાન ટેક્નોલોજી બની રહી છે. પરંતુ તાજેતરમાં બનેલી એક ઘટનાએ AIના જોખમો અંગે વૈશ્વિક સ્તરે ચિંતા વધારી છે. અહેવાલો અનુસાર, સંશોધન માટે ઉપયોગમાં લેવાતા કેટલાક AI મોડેલોએ નિયંત્રણની બહાર જઈ ઓનલાઈન સિસ્ટમો સાથે અનધિકૃત રીતે ક્રિયાપ્રતિક્રિયા કરી હતી. આ ઘટનાએ સાયબર સુરક્ષા નિષ્ણાતોને ચેતવી દીધા છે કે ભવિષ્યમાં AIનો દુરુપયોગ વધુ જટિલ બની શકે છે. વિશેષજ્ઞોનું માનવું છે કે આજના AI મોડેલો માત્ર પ્રશ્નોના જવાબ આપતા સાધનો નથી રહ્યા, પરંતુ તેઓ આયોજન, માહિતી એકત્રિત કરવી અને વિવિધ ડિજિટલ સિસ્ટમો વચ્ચે જોડાણ સ્થાપિત કરવાની ક્ષમતા પણ વિકસાવી રહ્યા છે. જો આવી ક્ષમતાઓ પર પૂરતું નિયંત્રણ ન રાખવામાં આવે તો સાયબર હુમલાઓનું સ્વરૂપ સંપૂર્ણપણે બદલાઈ શકે છે.

સાયબર હુમલાનું બદલાતું સ્વરૂપ । અગાઉ હેકિંગ માટે માનવીય હેકરો જવાબદાર હતા. હવે AI ઝડપથી નબળાઈઓ શોધી શકે છે, લાખો કોડનું વિશ્લેષણ કરી શકે છે અને સેકન્ડોમાં હુમલાની નવી રીતો તૈયાર કરી શકે છે. તેથી ભવિષ્યમાં AI આધારિત સાયબર હુમલાઓ વધુ ઝડપથી અને મોટા પાયે થઈ શકે છે.

નિષ્ણાતો શું કહે છે? । "AIનું ભવિષ્ય તેની બુદ્ધિ કરતાં વધુ તેની સુરક્ષા અને જવાબદાર ઉપયોગ પર નિર્ભર રહેશે. ટેક્નોલોજી જેટલી શક્તિશાળી બનશે, એટલી જ મજબૂત સુરક્ષા વ્યવસ્થા જરૂરી બનશે.

AIનો વધતો પ્રભાવ

- આરોગ્ય, શિક્ષણ અને ઉદ્યોગમાં વ્યાપક ઉપયોગ
- સોફ્ટવેર ડેવલપમેન્ટમાં ઝડપી પરિવર્તન
- સાયબર સુરક્ષામાં AIનો વધતો ઉપયોગ
- સરકારો દ્વારા AI નિયમન પર ભાર
- જવાબદાર AI વિકાસ માટે વૈશ્વિક ચર્ચા

સુરક્ષા માટે શું જરૂરી?

AI કંપનીઓ હવે વધુ મજબૂત સુરક્ષા વ્યવસ્થા, સતત મોનિટરિંગ, મર્યાદિત ઇન્ટરનેટ એક્સેસ અને નિયમિત 'રેડ ટીમ ટેસ્ટિંગ' પર ભાર મૂકી રહી છે. સરકારો પણ AI માટે કડક નિયમન અને આંતરરાષ્ટ્રીય સહયોગ તરફ આગળ વધી રહી છે.

'રોગ AI' એટલે શું?

'રોગ AI' એટલે એવો AI મોડેલ જે નિર્ધારિત મર્યાદા કે સુરક્ષા નિયમોને અવગણીને પોતાની રીતે કાર્ય કરવાનો પ્રયાસ કરે. તે હંમેશા દુર્ભાવનાપૂર્વક જ હોય એવું જરૂરી નથી, પરંતુ તેની અનિયંત્રિત કામગીરી ગંભીર પરિણામો લાવી શકે છે.

AI માનવજાત માટે અભૂતપૂર્વ તકો લઈને આવ્યું છે, પરંતુ તેની સાથે સુરક્ષા, નૈતિકતા અને નિયંત્રણના પ્રશ્નો પણ એટલા જ મહત્વના બન્યા છે. ટેક્નોલોજીનો વિકાસ જેટલો ઝડપી થશે, એટલી જ ઝડપથી સુરક્ષા માળખું મજબૂત બનાવવું સમયની સૌથી મોટી જરૂરિયાત બની રહેશે.

AI સામે કૉપીરાઈટનો જંગ । દિલ્હી હાઈકોર્ટનો મહત્વપૂર્ણ અભિપ્રાય

ChatGPTની ટ્રેનિંગ માટે કૉપીરાઈટેડ સામગ્રીનો ઉપયોગ 'ફેર ડીલિંગ'ની હદમાં?

આર્ટિફિશિયલ ઈન્ટેલિજન્સ (AI)ના વધતા પ્રભાવ વચ્ચે કૉપીરાઈટ અને બૌદ્ધિક સંપત્તિના અધિકારો અંગેનો વૈશ્વિક વિવાદ હવે ભારતની અદાલતો સુધી પહોંચી ગયો છે. દિલ્હી હાઈકોર્ટના તાજેતરના અવલોકનમાં પ્રાથમિક તબક્કે એવો અભિપ્રાય વ્યક્ત કરવામાં આવ્યો છે કે મોટા ભાષાકીય મોડલ (LLMs)ને તાલીમ આપવા માટે મૂળ કૉપીરાઈટેડ સામગ્રીનો ઉપયોગ 'ફેર ડીલિંગ' (Fair Dealing) હેઠળ આવી શકે છે અને તે દરેક સંજોગોમાં કૉપીરાઈટનું ઉલ્લંઘન ગણાય એવું જરૂરી નથી.આ કેસ સમાચાર એજન્સી ANI દ્વારા OpenAI સામે દાખલ કરવામાં આવ્યો હતો. ANIએ દલીલ કરી હતી કે તેની કૉપીરાઈટેડ સામગ્રીનો ઉપયોગ AI મોડલને ટ્રેન કરવા માટે કરવામાં આવ્યો છે. જોકે હાઈકોર્ટે પ્રાથમિક તબક્કે OpenAI સામે તાત્કાલિક પ્રતિબંધ મૂકવાનો ઈનકાર કર્યો હતો. અદાલતે એ પણ નોંધ્યું કે ChatGPT દ્વારા જનરેટ થયેલા જવાબો ANIના મૂળ લખાણની સીધી નકલ હોવાનું પૂરતા પ્રાથમિક પુરાવા રજૂ કરવામાં આવ્યા નથી. નિષ્ણાતો માને છે કે આ કેસનો અંતિમ નિર્ણય માત્ર OpenAI માટે જ નહીં, પરંતુ સમગ્ર AI ઉદ્યોગ, મીડિયા, પ્રકાશન અને ડિજિટલ કન્ટેન્ટ ક્ષેત્ર માટે માર્ગદર્શક સાબિત થઈ શકે છે.

પડકારો

- વિશ્વભરમાં AI સામે કોપીરાઇટનો વિવાદ વધુ તેજ બન્યો છે. લેખકો, પ્રકાશકો અને સમાચાર સંસ્થાઓએ AI કંપનીઓ પર તેમની કૃતિઓનો પરવાનગી વિના ઉપયોગ કરવાનો આરોપ લગાવી અનેક કેસ દાખલ કર્યા છે. અનેક મીડિયા હાઉસ વળતર અને યોગ્ય લાઇસન્સિંગની માંગ કરી રહ્યા છે. બીજી તરફ AI કંપનીઓ લાઇસન્સિંગ કરારો વધારી રહી છે. સરકારો નવા નિયમો ઘડવાની તૈયારીમાં છે.

શું છે 'Fair Dealing'?

- કોપીરાઇટ કાયદામાં રહેલી કાનૂની જોગવાઈ
- સંશોધન, શિક્ષણ, સમીક્ષા અને મર્યાદિત ઉપયોગ માટે છૂટ
- દરેક ઉપયોગ આપમેળે માન્ય નથી
- દરેક કેસમાં હેતુ, પ્રમાણ અને અસરના આધારે નિર્ણય લેવાય છે

કેસની મુખ્ય બાબતો

- ANIએ OpenAI સામે અરજી દાખલ કરી
- કોપીરાઇટેડ સામગ્રીના ઉપયોગ અંગે વિવાદ
- દિલ્હી હાઈકોર્ટનો પ્રાથ. અભિપ્રાય OpenAIના પક્ષમાં
- અંતિમ ચુકાદો હજુ આવવાનો બાકી
- સમગ્ર AI ઉદ્યોગની નજર આ કેસ પર

જાણવા જેવું

AIનો ઉપયોગ શિક્ષણ, આરોગ્ય, બેન્કિંગ, મીડિયા અને ઉદ્યોગોમાં ઝડપથી વધી રહ્યો છે. તેથી કોપીરાઇટનું રક્ષણ અને ટેક્નોલોજીમાં નવીનતા વચ્ચે સંતુલન કેવી રીતે જાળવવું, તે આગામી વર્ષોમાં સૌથી મોટો કાનૂની-ટેક્નોલોજીકલ પડકાર બની શકે છે.

Large Language Model એટલે શું?

Large Language Model (LLM) એ એવો AI મોડલ છે જે પુસ્તકો, લેખો, વેબસાઇટ્સ અને અન્ય જાહેરમાં ઉપલબ્ધ લખાણમાંથી ભાષાની સમજ વિકસાવે છે. ત્યારબાદ તે પ્રશ્નોના જવાબ આપે, લેખ લખે, ભાષાંતર કરે, કોડ બનાવે અને વિવિધ સર્જનાત્મક કાર્યો કરી શકે છે.