TECH BITES

વાહન સુરક્ષામાં વર્ચ્યુઅલ ક્રેશ ટેસ્ટિંગ

ઓટોમોટિવ સેફ્ટી કંપની Autolivએ 'Human Body Model Safety Suite' નામનું વર્ચ્યુઅલ ક્રેશ-ટેસ્ટિંગ પ્લેટફોર્મ રજૂ કર્યું છે. આ ટેક્નોલોજીમાં માનવ શરીરના ડિજિટલ મોડલનો ઉપયોગ કરીને વાહન અકસ્માત દરમિયાન થતી ઇજાના જોખમનું મૂલ્યાંકન કરવામાં આવે છે. પરંપરાગત ક્રેશ ટેસ્ટની સરખામણીએ આ પ્રકારનું ડિજિટલ સિમ્યુલેશન વાહન વિકાસના પ્રારંભિક તબક્કામાં જ વિવિધ અકસ્માતની પરિસ્થિતિઓનું પરીક્ષણ કરવાની તક આપે છે. એન્જિનિયરો જટિલ અકસ્માતોનું વર્ચ્યુઅલ સિમ્યુલેશન કરીને મુસાફરોના શરીર પર થતી અસરનો અભ્યાસ કરી શકે છે. Toyota આ ટેક્નોલોજીનું મૂલ્યાંકન કરનાર પ્રથમ ઓટોમેકર બની છે. Autoliv આ પ્લેટફોર્મને આ વર્ષ દરમિયાન વધુ વ્યાપક રીતે ઉપલબ્ધ કરાવવાની યોજના ધરાવે છે.

એઆઈથી ઔદ્યોગિક ઉત્પાદન વધારવાનો પ્રયાસ

ઇન્ડિયાAI મિશનના સહયોગથી સ્ટાર્ટઅપ શોધ AIએ 'LUAN' નામનું નવું આર્ટિફિશિયલ ઇન્ટેલિજન્સ મોડલ વિકસાવ્યું છે. આ મોડલનો હેતુ પ્રયોગશાળામાં થતી વૈજ્ઞાનિક શોધોને ઔદ્યોગિક સ્તરે ઉપયોગી ઉત્પાદનોમાં પરિવર્તિત કરવામાં મદદ કરવાનો છે. LUAN વિવિધ ઉત્પાદન પરિસ્થિતિઓમાં અણુઓ, સામગ્રી, રસાયણો અને જૈવિક પ્રક્રિયાઓ કેવી રીતે વર્તે છે તે સમજવામાં સક્ષમ છે. કંપનીના જણાવ્યા મુજબ, આ ટેક્નોલોજીએ સ્પેશિયાલિટી કેમિકલ્સના એક પ્રયોગમાં પ્રક્રિયામાં જરૂરી ફેરફારો ઓળખવામાં મદદ કરી હતી. પરિણામે સમાન જથ્થાના કાચા માલમાંથી ઉત્પાદન ક્ષમતામાં 17 ટકા વધારો નોંધાયો હતો. આથી ઉત્પાદનક્ષમતા વધારવા અને સંસાધનોનો વધુ કાર્યક્ષમ ઉપયોગ કરવામાં એઆઈની ભૂમિકા વધી રહી છે.

QR કોડ સ્કેન કરી કે WhatsApp આધારિત પ્રક્રિયા દ્વારા અભિયાન

લેયઝે 'ખેલો, રણબીર સે મિલો' નામે નવું ગ્રાહક અભિયાન શરૂ કર્યું છે. છ અઠવાડિયા ચાલનારા આ અભિયાનમાં રૂ.20ના લાયકાત ધરાવતા લેયઝ પેક ખરીદીને ગ્રાહકો ભાગ લઈ શકશે. પેક પરનો QR કોડ સ્કેન કરી અથવા WhatsApp આધારિત પ્રક્રિયા દ્વારા પેકની વિગતો ચકાસવાની રહેશે.

ત્રણ પેક પર ગેમિંગ કન્સોલ, પાંચ પેક પર સ્માર્ટફોન અને 10 પેક પર આંતરરાષ્ટ્રીય પ્રવાસ જીતવાની તક હોવાનું કંપનીએ જણાવ્યું છે. 20 પેક વેરિફાય કરાવનારા ભાગ લેનારાઓમાંથી વિજેતાઓને રણબીર કપૂરને મળવાની તક મળશે. કંપની અનુસાર અભિયાનમાં કુલ રૂ.2 કરોડના ઇનામો રાખવામાં આવ્યા છે.

10 નવા આધુનિક ટેક્નોલોજીથી સજ્જ મશીનો મેદાનમાં ઉતાર્યા

ગ્રેટર નોઇડામાં યોજાયેલા bauma CONEXPO India 2026માં JCB ઇન્ડિયાએ 10 નવા મશીનો રજૂ કર્યા. કંપનીએ કુલ 21 પ્રોડક્ટ્સ પ્રદર્શિત કરી, જેમાં નવી 3DX, 3DX Plus અને 3DX Super બેકહો લોડર્સ મુખ્ય આકર્ષણ રહ્યા. નવા મશીનોમાં ઉત્પાદકતા, ઇંધણ કાર્યક્ષમતા અને ઓપરેટર સુવિધા વધારવા પર ભાર મૂકાયો છે. કંપનીના જણાવ્યા અનુસાર ભારતમાં ડિઝાઇન, એન્જિનિયરિંગ અને ઉત્પાદિત મશીનોની નિકાસ 135થી વધુ દેશોમાં થાય છે. પ્રદર્શનમાં એક્સકેવેટર્સ, એગ્રીમેક્સ, જેનસેટ્સ, એક્સેસ પ્લેટફોર્મ અને વ્હીલ લોડર્સ સહિતના સાધનો પણ રજૂ કરાયા. JCB LiveLink જેવી ડિજિટલ ટેકનોલોજીથી મશીન મોનિટરિંગ અને પ્રિડિક્ટિવ મેઇન્ટેનન્સની સુવિધા મળે છે.

તમારા જ હાથે કમ્પ્યુટરમાં વાયરસ ઇન્સ્ટોલ કરાવતી સાયબર ઠગોની નવી જાળ

ક્લિકફિક્સ સ્કેમ

ડિજિટલ વિશ્વમાં સાયબર ગુનેગારો નિર્દોષ લોકોને શિકાર બનાવવા માટે સતત નવી પદ્ધતિઓ અપનાવી રહ્યા છે. હવે એક નવા પ્રકારનો સાયબર સ્કેમ સામે આવ્યો છે, જેને 'ક્લિકફિક્સ' (ClickFix) તરીકે ઓળખવામાં આવે છે. આ સ્કેમની સૌથી ખતરનાક બાબત એ છે કે સાયબર ઠગો સીધા કમ્પ્યુટરમાં વાયરસ કે માલવેર ડાઉનલોડ કરાવતા નથી, પરંતુ સોશિયલ એન્જિનિયરિંગની મદદથી યુઝરને જ એવી પ્રક્રિયા કરાવે છે, જેના પરિણામે માલવેર તેના કમ્પ્યુટરમાં ઇન્સ્ટોલ થઈ જાય છે. આ પ્રકારના હુમલામાં યુઝરની ઉતાવળ, ટેકનિકલ જાણકારીનો અભાવ અને સ્ક્રીન પર દેખાતા વિશ્વાસપાત્ર સંદેશાનો ગેરલાભ લેવામાં આવે છે. સામાન્ય રીતે કોઈ વેબસાઇટ ખોલતી વખતે, ઈમેલમાં આવેલી લિંક પર ક્લિક કરતી વખતે અથવા ઓનલાઈન કન્ટેન્ટ જોતી વખતે સ્ક્રીન પર ખોટું CAPTCHA, બ્રાઉઝર એરર કે સિસ્ટમ એરર દર્શાવવામાં આવે છે. ત્યારબાદ સમસ્યા દૂર કરવા માટે યુઝરને ચોક્કસ બટન દબાવવા અથવા કીબોર્ડ શોર્ટકટનો ઉપયોગ કરવાની સૂચના આપવામાં આવે છે.યુઝર 'Fix Error', 'Verify' અથવા તેના જેવા બટન પર ક્લિક કરે ત્યારે તેની જાણ બહાર એક ખતરનાક કમાન્ડ કમ્પ્યુટરના ક્લિપબોર્ડમાં કોપી થઈ શકે છે. ત્યારબાદ સ્ક્રીન પર યુઝરને Windows + R જેવી કી દબાવવા, Run Window ખોલવા અને Ctrl + V દ્વારા કમાન્ડ પેસ્ટ કરીને Enter દબાવવાની સૂચના આપવામાં આવે છે. યુઝર સૂચનાનું પાલન કરે ત્યારે સિસ્ટમનું આંતરિક ટૂલ સક્રિય થઈ શકે છે અને દૂરના સર્વર પરથી માલવેર ડાઉનલોડ થઈ કમ્પ્યુટરમાં ઇન્સ્ટોલ થઈ શકે છે.આ સમગ્ર પ્રક્રિયા ખૂબ જ ચાલાકીપૂર્વક તૈયાર કરવામાં આવે છે. પ્રથમ તબક્કામાં યુઝરને વિશ્વાસ આવે તેવો ખોટો એરર અથવા CAPTCHA દર્શાવવામાં આવે છે. તેમાં 'વેબસાઇટ ખોલવા માટે CAPTCHA વેરીફાઈ કરો', 'બ્રાઉઝર અપડેટ કરવું જરૂરી છે' અથવા 'સિસ્ટમ એરર દૂર કરો' જેવા સંદેશા હોઈ શકે છે.

મયુર ભુસાવળકર
આઇટી એક્સપર્ટ

ખતરનાક કોડ ક્લિપબોર્ડમાં કોપી થાય છે

ખતરનાક કોડ ક્લિપબોર્ડમાં કોપી થઈ શકે છે અને યુઝરને તે કોડ જાતે ચલાવવાની સૂચના આપવામાં આવે છે.આ હુમલાની ખાસિયત એ છે કે શરૂઆતમાં કોઈ શંકાસ્પદ ફાઇલ ડાઉનલોડ થતી ન હોવાથી સામાન્ય સુરક્ષા વ્યવસ્થાઓ માટે હુમલાને ઓળખવાનું મુશ્કેલ બની શકે છે. વધુમાં, કમાન્ડ યુઝર પોતે ચલાવતો હોવાથી તે સામાન્ય સિસ્ટમ પ્રક્રિયા જેવી દેખાઈ શકે છે. ખોટું CAPTCHA અથવા Windows Error વાસ્તવિક જેવું દેખાડવામાં આવતું હોવાથી ટેકનિકલ જાણકારી ઓછી ધરાવતા યુઝર સરળતાથી છેતરાઈ શકે છે.ક્લિકફિક્સ સ્કેમ સફળ થાય તો તેના ગંભીર પરિણામો આવી શકે છે. કમ્પ્યુટરમાં રહેલા બ્રાઉઝર પાસવર્ડ, ક્રેડિટ અથવા ડેબિટ કાર્ડની વિગતો, UPI સંબંધિત માહિતી તથા અન્ય સંવેદનશીલ ડેટા ચોરી થવાનો ખતરો રહે છે. અંગત ફોટા, દસ્તાવેજો અને અન્ય ફાઇલો પણ હુમલાખોરોના હાથમાં જઈ શકે છે. કેટલાક કિસ્સામાં હુમલાખોર કમ્પ્યુટર પર દૂરથી નિયંત્રણ મેળવવાનો પ્રયાસ કરી શકે છે.

કમાન્ડ ચલાવવાની સૂચના આપતું CAPTCHA શંકાસ્પદ ગણવું

કેટલીક પરિસ્થિતિમાં ફાઇલોને લોક કરીને રેન્સમવેર હુમલો પણ થઈ શકે છે અને તેને અનલોક કરવા માટે પૈસાની માગ કરી શકે. કોઈપણ વેબસાઇટ, CAPTCHA અથવા પોપ-અપ તમને Windows + R, Ctrl + V, PowerShell અથવા Command Prompt ખોલીને કોઈ કમાન્ડ ચલાવવાનું કહે તો આવી સૂચનાનું પાલન કરવું નહીં. સામાન્ય CAPTCHA સામાન્ય રીતે ચેકબોક્સ પર ટિક કરવા-તસવીરો ઓળખવાની પ્રક્રિયા કરાવે છે. કમ્પ્યુટરમાં કમાન્ડ ચલાવવાની સૂચના આપતું CAPTCHA શંકાસ્પદ ગણવું.

'બ્રાઉઝર અપડેટ કરવું જરૂરી છે'

ક્લિકફિક્સ સ્કેમથી બચવા માટે અજાણી વ્યક્તિ, વેબસાઇટ કે પોપ-અપ દ્વારા મળેલી "કમ્પ્યુટર ઠીક કરો", "વાયરસ દૂર કરો" અથવા "સિક્યુરિટી એલર્ટ" જેવી સૂચનાઓ પર તરત ક્લિક ન કરવું. કોઈપણ અજાણી લિંક પરથી સોફ્ટવેર, એપ્લિકેશન કે રિમોટ-એક્સેસ ટૂલ ડાઉનલોડ ન કરવું. ટેકનિકલ સપોર્ટના નામે કોઈ વ્યક્તિ ફોન કરીને પાસવર્ડ, OTP, બેંક વિગતો કે સ્ક્રીન શેરિંગની માગણી કરે તો માહિતી આપવી નહીં. કમ્પ્યુટર અથવા મોબાઇલમાં સિક્યુરિટી અપડેટ અને એન્ટિવાયરસ સોફ્ટવેર હંમેશાં અપડેટ રાખવું. બ્રાઉઝરમાં અચાનક દેખાતા "તમારા ડિવાઇસમાં વાયરસ છે" જેવા સંદેશાઓથી ગભરાઈને નંબર પર ફોન ન કરવો. સમસ્યા હોય તો સંબંધિત કંપનીની સત્તાવાર વેબસાઇટ પરથી જ સપોર્ટ નંબર મેળવવો. કોઈ રિમોટ-એક્સેસ એપ ઇન્સ્ટોલ થઈ ગઈ હોય તો તરત ઇન્ટરનેટ બંધ કરી એપ દૂર કરવી, પાસવર્ડ બદલવા અને જરૂરી હોય તો સાયબર ક્રાઇમ વિભાગમાં ફરિયાદ કરવી.

સુવર્ણ નિયમો

અજાણી લિંક પર ક્લિક નહીં પોપ-અપથી સોફ્ટવેર અપડેટ નહીં અજાણી કમાન્ડ Run નહીં Windows/macOS અપડેટ રાખો એન્ટિવાયરસ અપડેટ રાખો

ક્લિકફિક્સ સ્કેમ શું છે?

ક્લિકફિક્સ એક સોશિયલ એન્જિનિયરિંગ આધારિત સાયબર હુમલાની પદ્ધતિ છે, જેમાં યુઝરને ખોટા CAPTCHA, સિસ્ટમ એરર અથવા બ્રાઉઝર એલર્ટ બતાવીને પોતે જ ખતરનાક કમાન્ડ ચલાવવા માટે પ્રેરિત કરવામાં આવે છે. અજાણ્યા ઈમેલ, મેસેજ અથવા સોશિયલ મીડિયા પરથી મળેલી લિંક્સ પર ક્લિક કરવાનું પણ ટાળવું જોઈએ. બ્રાઉઝર કે કોઈ સોફ્ટવેર અપડેટ કરવા માટે પોપ-અપ દેખાય તો તેને અનુસરવાને બદલે સંબંધિત સોફ્ટવેરની સત્તાવાર વેબસાઇટ અથવા અધિકૃત અપડેટ સિસ્ટમનો ઉપયોગ કરવો જોઈએ. Windows અથવા macOS તથા એન્ટિવાયરસ અને અન્ય સુરક્ષા સોફ્ટવેરને પણ નિયમિત રીતે અપડેટ રાખવા જરૂરી છે.

ખતરનાક પ્રક્રિયા કરાવવાની યુક્તિ

ઓફિસ અને સંસ્થાઓમાં ખાસ સાવચેતી જરૂરી છે. સામાન્ય કર્મચારીઓ માટે PowerShell અને Command Prompt જેવા ટૂલ્સનો ઉપયોગ જરૂરી ન હોય ત્યાં સુધી મર્યાદિત રાખવો, તેમજ સંસ્થાકીય કમ્પ્યુટરોમાં સુરક્ષા નીતિઓ અને એક્સેસ કંટ્રોલ લાગુ કરવા જોઈએ. સાયબર સુરક્ષામાં માત્ર એન્ટિવાયરસ પર નિર્ભર રહેવાને બદલે યુઝરની જાગરૂકતા પણ એટલી જ મહત્વપૂર્ણ છે. કારણ કે ક્લિકફિક્સ જેવા હુમલામાં સૌથી મોટું હથિયાર ટેક્નિકલ ખામી નહીં, પરંતુ યુઝરને વિશ્વાસમાં લઈને તેની પાસેથી જ ખતરનાક પ્રક્રિયા કરાવવાની યુક્તિ છે.

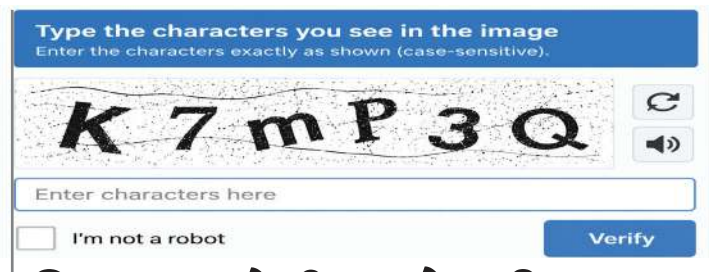
હુમલાની 4 મુખ્ય સ્ટેપ

1. ફેક એરર: ખોટું CAPTCHA અથવા સિસ્ટમ એરર દેખાડવામાં આવે છે. **2. કોડ કોપી:** 'Fix' અથવા 'Verify' પર ક્લિક કરતાં કમાન્ડ ક્લિપબોર્ડમાં કોપી થઈ શકે છે.**3. કમાન્ડ ચલાવવી:** યુઝરને Windows + R, Ctrl + V અને Enter દબાવવાનું કહેવામાં આવે છે.**4. માલવેર ઇન્સ્ટોલ:** કમાન્ડ ચાલ્યા બાદ માલવેર ડાઉનલોડ થઈ શકે છે.

'તમે રોબોટ નથી'

તો,CAPTCHAને કોણ ચકમો આપે છે?

રોબોટઅનેમાણસવચ્ચેનીડિજિટલ'ચોર-પોલીસ'ની રમત હવે AIના યુગમાં વધુ રસપ્રદ બની રહી છે ઇન્ટરનેટ પર કોઈ વેબસાઇટ ખોલો, લૉગિન કરો કે કોઈ ફોર્મ ભરો અને અચાનક સવાલ આવે– 'I'm not a robot'. ક્યારેક ટ્રાફિક લાઇટવાળા ફોટામાંથી ચોક્કસ તસવીરો પસંદ કરવાની હોય, તો ક્યારેક વિકૃત અક્ષરો વાંચીને ટાઇપ કરવાના હોય. સામાન્ય વપરાશકર્તા માટે આ માત્ર થોડા સેકન્ડનું કામ છે, પરંતુ ઇન્ટરનેટની સુરક્ષા વ્યવસ્થા માટે તે માણસ અને મશીન વચ્ચેનો મહત્વનો 'પરીક્ષણ બિંદુ' છે. CAPTCHA એટલે Completely Automated Public Turing test to tell Computers and Humans Apart. શરૂઆતના 2000ના દાયકામાં તેનો ઉપયોગ શરૂ થયો ત્યારે હેતુ સરળ હતો–માણસ માટે સહેલું, પરંતુ કમ્પ્યુટર પ્રોગ્રામ માટે મુશ્કેલ એવું કામ આપીને નક્કી કરવું કે સામેનો વપરાશકર્તા ખરેખર માણસ છે કે બૉટ. પરંતુ હવે પરિસ્થિતિ બદલાઈ ગઈ છે. કૃત્રિમ બુદ્ધિમત્તા (AI) એટલી શક્તિશાળી બની રહી છે કે ક્યારેક CAPTCHA ઉકેલવામાં માણસ કરતાં મશીન વધુ સક્ષમ સાબિત થઈ શકે છે.



CAPTCHAનો અર્થ શું?

CAPTCHAનું પૂરું નામ છે:Completely Automated Public Turing test to tell Computers and Humans Apart સરળ ભાષામાં કહીએ તો–'સામેનો વપરાશકર્તા માણસ છે કે ઓટોમેટેડ બોટ?' તે તપાસવાની પદ્ધતિ. તેનો મુખ્ય હેતુ સ્પામ, ફેક એકાઉન્ટ, ઓટોમેટેડ ફોર્મ સબમિશન અને અન્ય બોટ આધારિત દુરુપયોગને રોકવાનો છે. હવે બોટ માત્ર CAPTCHA જ નથી ઉકેલતા, માણસની જેમ વર્તે પણ છેઆજના આધુનિક બોટની સૌથી મોટી ખાસિયત એ છે કે તેઓ માત્ર એક CAPTCHA ઉકેલવા પૂરતા મર્યાદિત નથી. કેટલાક બોટ હવે માણસની જેમ માઉસ ચલાવવાનો પ્રયાસ કરે છે, પેજ પર કેવી રીતે આગળ વધે છે તેની નકલ કરે છે અને બ્રાઉઝિંગ વર્તન પણ માનવીય બનાવે છે.એટલે સુરક્ષા કંપનીઓ પણ માત્ર 'તમે શું ક્લિક કર્યું?' એ જોવાને બદલે વધુ સંકેતો તપાસવા લાગી છે.

ઉદાહરણ તરીકે–

માઉસની હિલચાલ, ટાઇપિંગની રીત, બ્રાઉઝરનું વર્તન, ડિવાઇસ સંબંધિત તકનિકી સંકેતો અને અગાઉની પ્રવૃત્તિ જેવા અનેક ડેટા પરથી અંદાજ લગાવવામાં આવે છે કે વપરાશકર્તા માણસ છે કે બોટ.
અર્થાત્, ભવિષ્યનું CAPTCHA કદાચ તમને કોઈ ચિત્ર પસંદ કરવાનું પણ નહીં કહે. સિસ્ટમ કદાચ તમારી આખી ઓનલાઇન વર્તણૂકનું વિશ્લેષણ કરીને નક્કી કરશે કે તમે માણસ છો કે મશીન.

વિકૃત અક્ષરોથી લઈને ટ્રાફિક લાઇટ સુધી... CAPTCHAની સફર

શરૂઆતના CAPTCHAમાં વાંકાચૂકા અને વિકૃત અક્ષરો દર્શાવવામાં આવતા. માણસ તેને ઓળખી શકતો, જ્યારે પરંપરાગત કમ્પ્યુટર પ્રોગ્રામ માટે તે મુશ્કેલ હતું. પરંતુ ટેક્નોલોજી આગળ વધતાં માત્ર લખાણ ઓળખવાની જ નહીં, ચિત્ર અને દૃશ્ય સમજવાની AIની ક્ષમતા પણ ઝડપથી વધી.
એટલે CAPTCHA પણ બદલાયા. હવે વપરાશકર્તાને પૂછવામાં આવે છે–
1.ક્યા ફોટામાં ટ્રાફિક લાઇટ છે?
2.કઈ તસવીરમાં સાઇકલ છે?
3.ક્યા ચિત્રમાં બસ કે મોટરસાઇકલ છે?
4.આપેલા ચિત્રોમાંથી ચોક્કસ વસ્તુ ધરાવતી તસવીરો પસંદ કરો.
અહીં રસપ્રદ વાત એ છે કે જે પ્રકારની દૃશ્ય ઓળખવાની ક્ષમતા પહેલાં માણસને મશીનથી અલગ પાડતી હતી, એ જ ક્ષમતા હવે AIમાં વિકસતી જાય છે. કેટલાક સંશોધકોએ તો CAPTCHA આધારિત સુરક્ષા વ્યવસ્થાઓને સફળતાપૂર્વક પાર કરવાની રીતો પણ દર્શાવી છે. એટલે CAPTCHA હવે અચૂક 'માણસ ઓળખનાર' કસોટી રહી નથી.

'હેડલેસ બ્રાઉઝર' શું છે?

સામાન્ય બ્રાઉઝરમાં આપણે સ્ક્રીન પર વેબપેજ જોઈએ છીએ અને માઉસ-કીબોર્ડથી તેનો ઉપયોગ કરીએ છીએ. પરંતુ હેડલેસ બ્રાઉઝર મુખ્યત્વે કોડ દ્વારા નિયંત્રિત થાય છે અને તેને સામાન્ય વપરાશકર્તા ઇન્ટરફેસની જરૂર પડતી નથી. સુરક્ષા નિષ્ણાતો માટે આવા ઓટોમેટેડ બ્રાઉઝર પડકારરૂપ બની શકે છે, કારણ કે આધુનિક બોટ માનવીય બ્રાઉઝિંગનું અનુકરણ કરી શકે છે.

'બૉટ ટ્રાફિક' વધી રહ્યો છે, એટલે પડકાર પણ મોટો

ઇન્ટરનેટ પર થતી દરેક ઓટોમેટેડ પ્રવૃત્તિ ખરાબ હોય એવું નથી. સર્ચ એન્જિનના ક્રોલર્સ, મોનિટરિંગ સિસ્ટમો અને અન્ય ઉપયોગી બોટ પણ વેબસાઇટની મુલાકાત લે છે. પરંતુ બીજી તરફ સ્પામર્સ અને સાયબર હુમલાખોરો પણ બોટનો ઉપયોગ કરે છે.આથી વેબસાઇટ સંચાલકો માટે મોટો સવાલ છે–'ઉપયોગી બોટને પ્રવેશ આપવો અને જોખમી બોટને અટકાવવો કેવી રીતે?'ક્લાઉડ સર્વિસ અને વેબ સુરક્ષા ક્ષેત્રની કંપનીઓ હવે બોટને ઓળખવા માટે અનેક પ્રકારના બિહેવિયરલ અને ટેક્નિકલ સિગ્નલ્સનું વિશ્લેષણ કરે છે. હેતુ એ છે કે સાચા માણસ માટે પ્રક્રિયા સરળ રહે, પરંતુ હુમલાખોર માટે ઓટોમેશનનો ખર્ચ અને મુશ્કેલી વધે.

કેમેરાની આંખ હવે માત્ર જોતી નથી, સમજતી પણ થઈ

ક્યારેક CCTV કેમેરા માત્ર ઘટના બાદ પુરાવા મેળવવાનું સાધન ગણાતા હતા. હવે કૃત્રિમ બુદ્ધિમત્તા (AI)ની મદદથી કેમેરા અસામાન્ય હલનચલન ઓળખી જરૂરી સમયે એલર્ટ આપી શકે છે. રેસ્ટોરાંમાં ઉંદર કે અન્ય વસ્તુ શોધવી, બંદૂક જેવી વસ્તુ ઓળખવી અથવા ચોક્કસ વ્યક્તિની હિલચાલ શોધવી જેવી કામગીરી AI આધારિત વિઝન સિસ્ટમ કરી શકે છે. લાંબા સમયના ફૂટેજમાંથી વ્યક્તિ, વાહન કે ચોક્કસ ઘટના ઝડપથી શોધી શકાય છે. ભારતની ટેક્નોલોજી કંપનીઓ આ સિસ્ટમનો ઉપયોગ સુરક્ષા ઉપરાંત રિટેલ, બેન્ક, એરપોર્ટ, રેસ્ટોરાં, ઉદ્યોગો અને જાહેર સ્થળોએ પણ કરી રહી છે.

રિયલ-વર્લ્ડ સમસ્યાઓ માટે AI

CMS Info Systems જેવી કંપનીઓ રેસ્ટોરાં અને અન્ય વ્યવસાયોમાં CCTV ફીડનું AI દ્વારા વિશ્લેષણ કરવાના ઉપયોગો પર કામ કરી રહી છે. કેટલાક કિસ્સાઓમાં સિસ્ટમને એવી રીતે તાલીમ આપવામાં આવે છે કે તે ચોક્કસ વસ્તુ અથવા અસામાન્ય પરિસ્થિતિ ઓળખીને એલર્ટ આપી શકે. AI આધારિત કમ્પ્યુટર વિઝનનું એક મહત્વનું પાસું એ છે કે સિસ્ટમ માત્ર "શું દેખાય છે?" એટલું જ નથી પૂછતી, પરંતુ "અહીં શું થઈ રહ્યું છે?" તે સમજવાનો પ્રયાસ કરે છે.ઉદાહરણ તરીકે, એરપોર્ટ પર મુસાફરોની અવરજવર, વાહનોની હિલચાલ, ભીડનું પ્રમાણ અથવા કોઈ ચોક્કસ ઘટના જેવી માહિતીનું વિશ્લેષણ કરી શકાય છે. આથી સુરક્ષા અને ઓપરેશનલ કાર્યક્ષમતા બંનેમાં મદદ મળી શકે છે.

લાખો કલાકના ફૂટેજમાંથી જરૂરી ક્ષણ શોધવાની ક્ષમતા

AI આધારિત વિડિયો એનાલિટિક્સની સૌથી મોટી શક્તિ તેની સ્કેલ છે. માણસ માટે હજારો કેમેરાના સતત ફૂટેજ પર નજર રાખવી અશક્ય જેવી બાબત છે. AI સિસ્ટમ એકસાથે અનેક કેમેરામાંથી આવતા ડેટામાં પેટર્ન શોધી શકે છે.Staqu જેવી ભારતીય કંપનીઓ વિડિયો એનાલિટિક્સને વિવિધ ક્ષેત્રોમાં ઉપયોગી બનાવવા માટે કામ કરી રહી છે. બીજી તરફ Awiros જેવી ટેક્નોલોજી કંપનીઓ પણ CCTV ફૂટેજને વધુ ઉપયોગી અને શોધી શકાય તેવા ડેટામાં પરિવર્તિત કરવાની દિશામાં કામ કરે છે.આ ટેક્નોલોજીનો અર્થ માત્ર વધુ કેમેરા લગાવવાનો નથી. તેનો સાચો અર્થ છે–હાલમાં લાગેલા લાખો કેમેરામાંથી વધુ બુદ્ધિશાળી માહિતી મેળવવી.

ભારત માટે મોટી તક | ભારતમાં પહેલેથી જ વિશાળ CCTV નેટવર્ક છે. જો આ કેમેરામાંથી મળતા વીડિયોને AI દ્વારા સમજવામાં આવે, તો સુરક્ષા ઉપરાંત સ્માર્ટ રિટેલ, ટ્રાફિક મેનેજમેન્ટ, એરપોર્ટ ઓપરેશન, ઔદ્યોગિક સલામતી અને જાહેર વ્યવસ્થા જેવા ક્ષેત્રોમાં નવી શક્યતાઓ ઊભી થઈ શકે છે.