

آرٹیفیشل انٹیلی جینس یا مصنوعی ذہانت اور پاکستان



سائنس اور ٹیکنالوجی کی دنیا میں، یہ کہا جا رہا ہے کہ ہم چوتھے صنعتی انقلاب کے آغاز میں ہیں۔ جس میں مصنوعی ذہانت کا استعمال ہماری سوچ سے بھی زیادہ تیزی کے ساتھ ہماری زندگیوں کا حصہ بن رہا ہے، اب مشینوں کو کام کے لیے انسانوں کی ضرورت نہیں رہی اور مستقبل قریب میں اسی طرح کی مشینیں ہمارے سامنے آئیں گی۔ اس کی وجہ سمارٹ سپیکرز اور مصنوعی ذہانت کے حامل صوتی معاونت سے چلنے والے آلات ہیں۔ جرمن نرائع ابلاغ کی رپورٹ کے مطابق کرسمس کے موقع پر پیش کیے جانے والے ایمازون ایکو ڈاٹ کے اشتہارات صوتی معاونت سے چلنے والے مصنوعی ذہانت کے حامل آلات کی ایک مثال ہے ”ایکسا“ نامی مصنوعی ذہانت رکھنے والا یہ آلہ انسان کے زبانی احکامات پر عمل کرتا ہے۔

ایسے آلات بہت جلد گھروں میں نظر آئیں گے۔ جرمنی اور برطانیہ کی حکومتیں مصنوعی ذہانت کے حوالے سے پالیسیاں تشکیل دے چکی ہیں۔ یونیورسٹی آف ویروک کے سائنس دان جگنو کے جین کا استعمال کر کے ایسے کرسمس ٹریز پیدا کرنے پر کام کر رہے ہیں جو خود ہی روشن ہو جایا کریں۔ جگنو اپنے جسم کو ایک کیمیائی تعامل کے ذریعے روشن کرتے ہیں، جسے بائیولیومی نینس کہتے ہیں۔ سائنس دان اس کے ذریعے ایک سینتھٹک ڈی این اے تیار کرنا چاہتے ہیں، جو ان کرسمس ٹریز میں منتقل کیا جائے گا، یہ درخت اندھیرا ہونے پر خود ہی روشن ہو جایا کریں گے۔

اسی طرح مصنوعی ذہانت کی حامل گاڑیاں جلد ہی سڑکوں پر دکھائی دیں گی، جو خود چلا کریں گی۔ تاہم ناقدین کا یہ بھی کہنا ہے کہ مشینوں پر اس انداز سے بڑھتا انحصار انسانی فکری استعداد اور استطاعت کو نقصان پہنچا سکتا ہے۔ لیکن لگتا یوں ہے کہ اس انحصار کو کم کرنا اب خود انسان کے اپنے بس میں بھی نہیں رہا۔ اور ان جدید نظاموں کا استعمال اس جدید دور کی ضرورت بن چکا ہے۔

اسی طرح کے اور بھی بہت سے جدید نظام ہیں جو آج کے دور میں استعمال ہونا ضروری خیال کیے جن میں! چہرے کی شناختی نظام (اس کی مثال چین ہے جو کہ اپنی ایک ارب چالیس کروڑ کی آبادی کو اس سسٹم سے کنٹرول کرتا ہے) ، دور دراز سینسنگ، سائبر حملوں : پتہ لگانے اور سامنا، مواد کا تجزیہ، انٹیلی جنس مجموعہ اور تجزیہ، کمانڈ، کنٹرول، مواصلات، کمپیوٹر، انٹیلی جنس، نگرانی اور بحالی فریم ورک، غیر ملکیوں اور سپفنگ کے معاملے میں انسداد کی پیمائش کی شناخت اور ٹریکنگ کی سرگرمیاں، سرحد کی نگرانی کی کارروائیوں میں ریموٹ سینسنگ ڈیٹا جمع کرنے اور تجزیہ۔

انٹرنیٹ ٹریفک تجزیہ اور خطرات کی پیش گوئی، مشتبہ افراد کے درمیان رابطے کے سوشل میڈیا پر ایک سے زیادہ

شناختیں، ہیکنگ کی کوششوں کا پتہ لگانے اور فوری رد عمل کو خود کار طریقے سے تلاش کرنا، پیچیدہ ڈیٹا سیٹوں کی ہینڈلنگ، ریئل ٹائم تجزیہ، اعداد و شمار کے بڑے پیمانے پر سے پیچیدہ پیٹرن نکالنے، سیمنٹ انڈیکسنگ، ڈیٹا ٹیکنگ، تیزی سے معلومات کی بازیابی، بڑے اعداد و شمار پیش گوئی تجزیہ حل، تصویری درجہ بندی، تقریر کی شناخت، اور قدرتی زبان کی پروسیسنگ۔

چہرے کی شناخت میں اعلیٰ جہتی اعداد و شمار کو ہینڈل کرنے، سیکھنے اور نیورل نیٹ ورک، نامعلوموں کی درست پیش گوئی وغیرہ وغیرہ۔ ان تمام چیزوں کا استعمال دنیا کے تمام ترقی یافتہ ممالک کر رہے ہیں اور اپنی سیکورٹی کو دن بدن بہتری کی طرف لا رہے ہیں اسی طرح پاکستان بھی ایک اچھے انداز میں اس جدید ٹیکنالوجی کو استعمال میں لا کر ترقی کی راہ میں گمزن ہے کیونکہ پاکستان کافی سال مشکلات میں رہا ہے ابھی پاکستان کو کافی سیکورٹی چیلنجز کا سامنا ہے جن میں سرحدی سیکورٹی کے مسائل، سرحد کی نگرانی، کنٹرول ٹریفک، ریاستی سپانسر دہشت گردی، سوشل میڈیا کے ذریعے پروپاگینڈا، متاثرہ ہائبرڈ جنگ اور بھارت کے ساتھ ہائی ٹیک پاور اسرائیل کے گٹھ جوڑ جیسے چیلنجز شامل ہیں۔

اسی طرح جہاں اس طرح کے جدید نظام موجود ہیں وہیں ان میں بہت سی خامیاں بھی نظر آرہی ہیں۔ جیسا کہ فنگر پرنٹس جیسے نظام کو دھوکا دینا ایک واضح مثال ہے جو کہ میں یہاں پر بیان کر رہا ہوں۔ نیویارک یونیورسٹی میں وقع ٹینڈن اسکول آف انجینیئرنگ کے فلپ بونٹریگر اور ان کے ساتھیوں نے نہ صرف اس نظام کو دھوکہ دینے میں کامیابی حاصل کی ہے بلکہ مشین لرننگ الگورتھم سے جعلی فنگر پرنٹس بھی تشکیل دیے ہیں جنہیں 'ماسٹر پرنٹس' کا نام دیا گیا ہے۔

دنیا بھر میں لاکھوں کروڑوں جگہوں اور آلات میں یہ فنگر پرنٹ پر مبنی سیکورٹی نظام روزانہ استعمال ہو رہے ہیں۔ جس طرح تمام تالوں کو کھولنے والی کوئی 'ماسٹر کی' ہوتی ہے عین اسی طرح فنگر پرنٹس ڈیٹا بیس کو پڑھ کر ڈیپ لرننگ اور مصنوعی ذہانت کا نظام 'ڈیپ ماسٹر پرنٹس' بناتا ہے اور نظری طور پر اس سے بہت سے بند تالے کھولے جاسکتے ہیں۔ اس کی وجہ یہ ہے کہ فنگر پرنٹ پڑھنے والی مشینیں انگلیوں کے نشانات کی پوری تفصیل کی بجائے جزوی پرنٹ پر ہی اکتفا کرتی ہیں اور اسی کے ذریعے نظام کھلتے اور بند ہوتے ہیں۔

کسی فنگر پرنٹ نظام میں انگلی یا انگوٹھے کا جزوی اور تھوڑا حصہ ہی دیکھتے ہوئے وہ نظام کام کرنے لگتا ہے اور ان لاک ہو جاتا ہے۔ ماہرین نے پہلے مصنوعی فنگر پرنٹ کی مکمل تصاویر بنائیں جس کے دو مقصد تھے۔ اول ماسٹر پرنٹس بنا کر انہیں حقیقی فنگر پرنٹ سیکورٹی نظام یا آلات پر استعمال کیا جانا تھا جسے بعد میں آزما یا جائے گا۔ دوم یہ فنگر پرنٹس معیاری نشانات پر مبنی ہیں انہیں سیکورٹی نظام کے ڈیٹا بیس سے ہیک بھی کیا جاسکتا ہے جو عین ممکن بھی ہے۔ ماہرین کا اعتراف ہے کہ فنگر پرنٹ ایک ایسا مؤثر طریقہ ہے جو بہت کامیابی سے استعمال ہو رہے ہیں۔ مگر اکثر نظام یہ جانتے ہی نہیں کہ یہ اصلی فنگر پرنٹس ہیں یا کسی نے جعلی انداز میں تیار کیے ہیں۔ اسی بنا پر ماسٹر پرنٹس سے کئی آلات کو کھولا جاسکتا ہے۔

پس جیسا کہ پاکستان جس طرح اپنی سیکورٹی کو اس نظام کو استعمال کر کے بہتر کرنے کی کوشش کر رہا ہے اس طرح پاکستان کو اس جدید نظام میں موجود خامیوں کو بھی مد نظر رکھنا ہو گا۔ اور اپنے سیکورٹی کے نظام کو اس کے مطابق اچھے طریقے سے ڈھالنا ہو گا۔ اللہ پاکستان کا حامی و ناصر ہو۔

تحریر: محمد عامر فاروق ملک چین سے