Naveen Shodh Sansar (An International Refereed / Peer Review Multidisciplinary Research Journal)
RNI No.- MPHIN/2013/60638, ISSN 2320-8767, E- ISSN 2394-3793, Scientific Journal Impact Factor (SJIF)- 8.054,
October to December 2025, E-Journal, Vol. I, Issue LII (52), ISO 9001:2015 - E2024049304 (QMS)

वर्तमान परिदृश्य में साइबर सुरक्षा की स्थिति : चुनौतियाँ और संभावनाएँ

डॉ. शिवाकान्त तिवारी *

* प्रभारी प्राचार्य, आर्यावर्त शासकीय महाविद्यालय, मोहन बड़ोदिया (म.प्र.) भारत

शोध सारांश – आज का विश्व सूचना और तकनीक के नये युग में प्रवेश कर चुका है। इंटरनेट, कृत्रिम बुद्धिमत्ता(AI) क्लाउड कंप्यूटिंग, जैसी तकनीकों ने समाज को काफी गतिशील और सुविधाजनक बना दिया है परन्तु इसके साथ ही साइबर अपराध भी तेजी से बढ़े हैं। साइबर सुरक्षा आज के समय की सबसे महत्वपूर्ण आवश्यकता बन गयी है। यह शोध वर्तमान परिदृश्य में साइबर सुरक्षा की अवधारणा, उसकी आवश्यकता, उपयोग की जा रही तकनीकें, भारत की स्थिति ओर संभावित समाधान पर प्रकाश डालने का प्रयास है। इसका प्रमुख उद्देश्य बढ़ते तकनीकी प्रयोग के प्रभाव के बीच साइबर सुरक्षा को सशकत बनाने के उपायों पर ध्यान आकर्षित करना है।

शब्द कुंजी – साइबर सुरक्षा, साइबर अपराध, कृत्रिम बुद्धिमत्ता(AI), डिजिटल सदी।

प्रस्तावना – 21वीं सदी को डिजिटल सदी कहा जाता है। जीवन का कोई क्षेत्र आज डिजिटल क्रांति से अछूता नहीं है। शिक्षा, चिकित्सा, परिवहन, व्यापार, बैंकिंग, युद्ध जैसा प्रत्येक क्षेत्र आज डिजिटल तकनीक पर निर्भर है। अगर विकास की प्रतिस्पर्धा में बने रहना है तो डिजिटल तकनीक में निरन्तर नवाचार करना पड़ेगा। क्योंकि जैसे-जैसे डिजिटल तकनीक का विस्तार हो रहा है वैसे-वैसे ही इसके दुरूपयोग की घटनाएँ भी बढ़ रही है। आज साइबर अपराध बड़ी तेजी से अपने पैर पसार रहा है। डेटा चोरी हो जाने, बैंक से छलपूर्वक पैसे निकाल लेने जैसी घटनाएँ तेजी से बढ़ रही हैं। आजकल डिजिटली हाउस अरेस्ट कर जीवनभर की कमाई छीन लेने जैसी घटनाएँ बहुत अधिक हो रही हैं। ऐसी घटनाओं से बचने के लिए कौन-कौन से उपाय किये जायें जिससे हमारे कम्प्यूटर नेटवर्क, डेटा, संचार या व्यक्तिगत जानकारियाँ सुरक्षित रहें इस विषय में निरन्तर कार्य करने की आवश्यकता है।

साइबर सुरक्षा का महत्व – साइबर सुरक्षा का महत्व सर्वोपरि है क्योंकि अगर साइबर सुरक्षा खतरे में पड़ी तो इसके परिणाम बहुत दूरगामी हो सकते हैं विशेषकर निम्नलिखित क्षेत्र सर्वाधिक प्रभावित हो सकते हैं।

1. **व्यक्तिगत सुरक्षा**- आज एक आम व्यक्ति साइबर तकनीक का प्रयोग मोबाइल, ईमेल, सोशल मीडिया, बैंकिंग, मनोरंजन जैसे अनेक क्षेत्रों में कर रहा है लेकिन साइबर अपराधियों का सबसे आसान शिकार भी आम व्यक्ति ही बन रहा है। अगर आम आदमी की व्यक्तिगत सुरक्षा खतरे में पड़ी तो वह डिजिटल तकनीक से दूर हो जायेगा।
2. **आर्थिक स्थिरता**- आनलाइन लेन-देन और ई कामर्स जेसे क्षेत्रों की सुरक्षा आर्थिक स्थिरता की दृष्टि से आवश्यक है। बड़े-बड़े हैकर्स किसी बड़ी कम्पनी का डेटा हैक कर उसे कुछ ही समय में अरबों की आर्थिक क्षति पहँचा देते हैं। हैकिंग का समय बढ़ने से क्षति भी बढ़ जाती है।
3. **राष्ट्रीय सुरक्षा**- राष्ट्रीय सुरक्षा सदैव सर्वोपरि रही है। आज के युग में किसी भी देश की सुरक्षा इस बात पर निर्भर करती है कि वह डिजिटल रूप से कितना सक्षम है। हाल ही में भारत द्वारा चलाये गये आपरेशन सिंदूर में भी इसकी झलक देखने को मिली। हमारे देश की सेनाओं ने डिजिटल तकनीक का बेहतरीन उपयोग करके दुश्मन देश पाकिस्तान की हवाई सुरक्षा व्यवस्था को तहस-नहस कर दिया और कुछ ही घण्टों में उसे घुटनों पर ला दिया। रूस-यूक्रेन युद्ध में भी इसका भरपूर उपयोग देखने को मिल रहा है।
4. **विश्वसनीयता**- किसी की बात की सफलता इस बात पर निर्भर करती है कि सामान्य व्यकित उस पर कितना भरोसा करता है। कोरोना महामारी के दौर से हमारे देश में सामान्य व्यक्तियों के बीच में डिजटल तकनीक का उपयोग तेजी से बढ़ा है। लेकिन डिजिटल तकनीक का भविष्य इस बात पर निर्भर है कि आम व्यक्ति कितना सुरक्षित रह सकता है। वह सुरक्षित महसूस करेगा तभी डिजिटल तकनीक का उपयोग करेगा।

विश्व में साइबर सुरक्षा की स्थिति – वर्तमान में साइबर सुरक्षा परम्परागत तरीकों से काफी आगे निकल चुकी है। अब एंटी वायरस और फायर बॉल जैसे साधनों से आगे बढ़कर नई-नई तकनीकों का उपयोग सायबर सुरक्षा में हो रहा है जिनमें से प्रमुख निम्नलिखित हैं।

1. **कृत्रिम बृद्धिमत्ता(AI)** - कृत्रिम बुद्धिमत्ता का उपयोग वर्तमान में साइबर सुरक्षा के लिए प्रमुखता से किया जा रहा हे। यह खतरे का संकेत मिलते ही तुरन्त पहचान कर सुरक्षा के लिए स्वचलित प्रतिक्रियाओं को सक्रिय कर देती है। यह बड़ी तेजी से डेटा का विश्लेषण कर खतरों से आगाह करती है ओर स्वत: ही खतरों से बचने के लिए आवश्यक प्रणाली को सक्रिय कर धोखाधड़ी और दुर्भावनापूर्ण गतिविधियों को रोक देती है। इसके साथ ही कृत्रिम बुद्धिमत्ता अनुभव से सीखकर आगामी खतरों से बचने में भी मदद्गार साबित होती है। गूगल और माइक्रोसाफ्ट अख आधारित खतरा विश्लेषण मॉडल का उपयोग अपने सर्वर में कर रहे हैं।
2. **क्लाउड सुरक्षा**- क्लाउड आधारित सुरक्षा अपने डेटा, एप्लीकेशन,

ओर इंफ्रास्ट्रक्चर को खतरों से बचाने के लिए एन्क्रिप्शन, एक्सेस कन्ट्रोल ओर वास्तविक समय में खतरों का पता लगाने जैसे उपायों का उपयोग करती है। मल्टी फैक्टर अथेंटिकेशन(MFA) और डेटा लैप्स प्रिवेंशन(DLP) जैसे तरीकों का उपयोग भी इसके द्वारा किया जाता है।

3. ब्लॉकचेन– ब्लॉकचेन तकनीक डेटा को अपरिवर्तनीय (Immutable) बनाती है और लेन–देन की पारदर्शिता को बढ़ाती है। बैंकिंग क्षेत्र और आपूर्ति श्रृंखला में इसका उपयोग किया जाता हे। ब्लॉकचेन में नियंत्रण केन्द्रीकृत ना होकर नेटवर्क के सभी प्रतिभागियों के बीच वितरित होता है जिस कारण यह सुरक्षित और पारदर्शी बनता है।

4. बायोमेट्रिक सुरक्षा– बायोमेट्रिक सुरक्षा प्रणाली अत्याधुनिक तकनीक है जो किसी व्यक्ति की शारीरिक विशिष्टताओं का उपयोग कर उसकी पहचान की पुष्टि करती है। इस कारण इसमें सेंध लगाना लगभग असम्भव है। इसमें व्यक्ति की उंगलियों के निशान, आँखों की स्कैनिंग, चेहरे की पहचान यहाँ तक कि डी.एन.ए. का उपयोग भी उसकी पहचान को सत्यापित करने के लिए किया जाता है।

5. क्वांटम एन्क्रिप्शन– सायबर सुरक्षा की यह सबसे नवीनतम तकनीक है जो डेटा को सुरक्षित करने के लिए क्वांटम यांत्रिकी का उपयोग करती है। इसमें गुप्त एन्क्रिप्शन कुंजियों के वितरण का इस्तेमाल किया जाता है। कुंजियों को प्रकाश के क्वांटम कणों (फोटान) पर एनकोड किया जाता है। यह सुरक्षा तकनीक उच्च स्तर की सुरक्षा प्रदान करती है जो भविष्य में सायबर सुरक्षा का प्रमुख आधार बन सकती है।

भारत में साइबर सुरक्षा की स्थिति – भारत की वर्तमान जनसंख्या 146 करोड़ से अधिक है। इसमें से लगभग 90 करोड़ से अधिक व्यक्ति इंटरनेट का उपयोग करते हैं। ऐसे में इतनी बड़ी संख्या के उपयोगकर्ताओं की साइबर सुरक्षा एक बड़ी चुनौती है। विश्व में साइबर सुरक्षा के लिए किये जा रहे प्रयास तो भारत में किये ही जा रहे हैं, साथ ही यहाँ की परिस्थिति अनुसार कुछ अतिरिक्त प्रयास भी भारत सरकार द्वारा किये गये हैं जो निम्न प्रकार हैं–

(1) राष्ट्रीय साइबर सुरक्षा नीति (2013)– सायबर सुरक्षा की चुनौती से निपटने के लिए राष्ट्रीय साइबर सुरक्षा नीति (2013) बनायी गयी है जिसका उद्देश्य उपयोगकर्ताओं के लिए एक सुरक्षित साइबर परिस्थिति के तंत्र का विकास करना है।

(2) इंडियन कम्प्यूटर इमरजेंसी रिस्पॉन्स टीम (CERT- In) – यह संगठन साइबर हमलों की समय पर सूचना उपलब्ध कराने, उनकी रोकथाम करने ओर त्वरित, उचित प्रतिक्रिया करने के लिए बनाया गया है।

(3) डिजिटल पर्सनल डेटा प्रोटेक्शन एक्ट 2023 –देश के नागरिकों के व्यक्तिगत डेटा को सुरक्षा प्रदान करने के लिए इस अधिनियम के द्वारा कानूनी प्रावधान किये गये हैं।

(4) राष्ट्रीय साइबर समन्वय केन्द्र NCCC – साइबर सुरक्षा को और सुदृढ़ करने के लिए उक्त केन्द्र का निर्माण किया गया जिसका मुख्य कार्य नेटवर्क ट्रैफिक की निगरानी और विश्लेषण करने में सहायता प्रदान करना है।

साइबर अपराधों के मुख्य कारण – लगातार अनेक प्रयासों के बावजूद भारत में साइबर अपराधों में लगातार वृद्धि हो रही है। NCRB की 2024 की रिपोर्ट अनुसार पिछले पाँच वर्षों में साइबर अपराधों में लगभग तीन गुना की वृद्धि हुई है। इसके प्रमुख कारण निम्नानुसार हैं –

1. जागरूकता की कमी– हमारे देश के अधिकांश उपयोगकर्ता तकनीकी रूप से जागरूक नहीं है। उन्हें यह पता नहीं होता कि साइबर सुरक्षा के लिए क्या–क्या आवश्यक कदम उठाने चाहिए। इस कारण वे आसानी से साइबर अपराधियों के शिकार बन जाते हैं।

2. तकनीकी असमानता– हमारे देश की बहुत बड़ी जनसंख्या आज भी गाँवों में निवास करती है जो साइबर सुरक्षा की जानकारी में काफी पीछे है जबकि शहरी क्षेत्रों में अपेक्षाकृत जागरूकता बढ़ी है।

3. विदेशी हमले– हमारे देश में कई बार साइबर हमले विदेशी धरती से संचालित होते हैं जिन्हें ट्रैक करना और रोकना अधिक कठिन हो जाता है।

4. कानूनी जटिलताएँ –यद्यपि भारत में साइबर सुरक्षा को मजबूत बनाने के लिए कई कानूनी प्रावधान किये गये हैं लेकिन अभी भी साइबर अपराधों की जाँच करना और तकनीकी प्रमाण जुटाना काफी दुष्कर है जिसका लाभ अपराधी उठा लेते हैं।

5. तेजी से बदलती तकनीक – इंटरनेट के क्षेत्र में बड़ी तेजी से नई–नई तकनीकों का विकास हो रहा है। जब तक उपयोगकर्ता साइबर अपराधों से बचाव को समझ पाता है, तब तक अपराधी अपराध की नई तकनीक खोज लेते हैं।

साइबर सुरक्षा को सशक्त बनाने के उपाय – साइबर अपराधों के बढ़ते खतरे से निपटने के लिए वर्तमान समय में Zero Trust Architecture को अपनाने पर जोर दिया जा रहा है। जिसमें किसी भी उपयोगकर्ता या उपकरण पर बिना सत्यापन के भरोसा नहीं किया जाता है। इसलिए सभी का सत्यापन आवश्यक है। साथ ही व्यावहारिक विश्लेषण Behavioral Analytics एवं खतरा खुफिया प्लेटफार्म Threat Intelligence Platforms का उपयोग करके सुरक्षा प्रणालियों को और अत्याधुनिक और मजबूत बनाया जा रहा है।

भारतीय रिजर्व बैंक ने डिजिटल भुगतान की सुरक्षा के लिए ओबड्समैन स्कीम लागू की है। गृह मंत्रालय ने साइबर स्वच्छ केन्द्र की स्थापना की है जो हानिकारक साफ्टवेयर की पहचान अधिक सटीक तरीकों से करता है।

साइबर सुरक्षा के लिए उठाये उपरोक्त कदमों के साथ–साथ निम्नांकित दिशा में भी तेजी से कार्य करने की आवश्यकता है।

1. शिक्षा और प्रशिक्षण – साइबर सुरक्षा की शिक्षा और प्रशिक्षण पर और अधिक बल देना होगा। शिक्षण संस्थाओं में साइबर सुरक्षा को पाठ्यक्रम में शामिल करना चाहिए।

2. सार्वजनिक जागरूकता – नागरिकों को इस दिशा में और अधिक जागरूक करने की आवश्यकता है। उन्हें पासवर्ड के सही उपयोग, दो स्तरीय सत्यापन ओर फिशिंग से बचने के उपायों की जानकारी निरन्तर देना आवश्यक है।

3. नवाचार को प्रोत्साहन – साइबर अपराधी नित नये तरीकों का उपयोग साइबर ठगी के लिए करते हैं। उनसे सुरक्षा के लिए भारतीय एजेंसियों और स्टार्टअप्स को नयी–नयी सुरक्षा तकनीकें विकसित करने हेतु प्रोत्साहित करना चाहिए।

4. अंतर्राष्ट्रीय सहयोग– साइबर अपराध आज विश्वव्यापी हो गये हैं। वे किसी भी देश की सीमा के बाहर से ही बड़े आराम से अपराध करते हैं। अत: इनसे निपटने के लिए वैश्विक स्तर पर सहयोग कर डेटा साझाकरण किया जाना चाहिए। साथ ही सुरक्षा एजेंसियों को भी वैश्विक स्तर पर एक दूसरे का सहयोग करना चाहिए।

भविष्य की दिशा – भविष्य में इंटरनेट का उपयोग बहुत तेजी से बढ़ने वाला है। धीरे–धीरे लगभग सभी कार्य ऑफलाइन मोड से ऑनलाइन मोड पर शिफ्ट हो जायेंगे। इंटरनेट ऑफ थिंग्स (IOT) 5G नेटवर्क और कम्प्यूटर तथा स्मार्ट डिवाइस की संख्या में तेजी से वृद्धि होगी। इसके साथ ही साइबर अपराधों का खतरा भी बढ़ेगा। जिससे बचने के लिए साइबर सुरक्षा को एक निरन्तर प्रक्रिया के रूप में सक्रिय करना पड़ेगा तथा तकनीकी सुधार के साथ–साथ उपयोगकर्ताओं को भी निरन्तर जागरूक और सतर्क रहना होगा।

निष्कर्ष – वर्तमान काल में इंटरनेट का व्यापक प्रयोग सभी क्षेत्रों में किया जा रहा है। भारत जैसे देश में एक विशाल जनसंख्या इसका उपयोग कर रही है। आधुनिक तकनीक ने कई कार्यों को बहुत आसान और आम जनता के लिए सुलभ बना दिया है। किन्तु इंटरनेट के उपयोग ने सुविधा के साथ–साथ कई समस्याओं को भी जन्म दिया है। साइबर अपराधियों ने इंटरनेट का दुरूपयोग करके कई बड़ी–बड़ी घटनाओं को अंजाम दिया है। व्यक्तियों को हानि पहुँचाने के साथ कई बड़ी–बड़ी कम्पनियों तथा कई बार तो देशों को भी अपराधियों ने अपनी ठगी का शिकार बनाया है। ऐसे में आवश्यकता इस बात की है कि साइबर अपराधों को रोकने के लिए मजबूत अधोसंरचना का निर्माण किया जाये। सभी नागरिकों को निरन्तर जागरूक किया जाए। सभी की सामूहिक जिम्मेदारी और नीति निर्माण का संतुलन ही साइबर सुरक्षा को पर्याप्त सुदृढ़ करेगा।

संदर्भ ग्रंथ सूची :–

1. राष्ट्रीय साइबर सुरक्षा नीति, भारत सरकार (2013)
2. CERT- In वार्षिक रिपोर्ट, 2024
3. डिजिटल पर्सनल डेटा प्रोटेक्शन एक्ट 2023
4. नासकॉम और डेलॉइट, भारत में साइबर सुरक्षा की स्थिति रिपोर्ट 2024
5. आर.के. शर्मा, साइबर अपराध और विधिक प्रावधान, नई दिल्ली : प्रकाश पब्लिशिंग,2022

****