 ISSN: 2349-6002

Cyber Law, Digital Governance, Data Privacy

Jayeshgiri Pravingiri Meghanathi[1], Dr. Nitaben L Khunti[2]
[1]Department Of Economics, K.M.G.B Gov. Arts College, Vallbhipur
[2]Guide, Dr. V.R. Godhaniya P.G. Center, Porbandar
doi.org/10.64643/IJIRTV12I8-191411-459

સારાંશ—આજના ડિજિટલયુગમાં સાયબર સુરક્ષા અને ડિજિટલ સાક્ષરતા બંને ખૂબ જ મહત્વની બાબતો છે. ભારત ડિજિટલ ઈન્ડિયા તરફ આગળ વધી રહ્યું છે. ભારતના લોકો UPI, સોસિયલ મીડિયાં,ઓનલાઇન શિક્ષણ, ઓનલાઇન વ્યાપાર જેવી ડિજિટલ સુવિધાનો ઉપયોગ કરતાં થયા છે. સાયબરસુરક્ષા એટલે શું?... સાયબર સુરક્ષા એટલે ડિજિટલ માધ્યમો પર થતાં ગુનાઓની સામે રક્ષણ. પરંતુ ભારતના નાગરિકોમાં ડિજિટલ સાક્ષરતાનું પ્રમાણ ઓછું હોવા ને લીધે લોકો સાયબર ગુનાનો ભોગ બને છે, જેમાં મોટે ભાગે ફિશિંગ અને વૉટ્સએપ સ્કેમ, ઈમેલ હેક, ડેટા ચોરી, ઓળખ ચોરી જેવા સાયબર ગુનાનું પ્રમાણ વધ્યું છે. આવા ગુનાથી લોકોને બચાવવા માટે તેમનામાં સાયબર સુરક્ષા અને ડિજિટલ સાક્ષરતાની જાગૃતિ લાવવા માટે સરકારે લીધેલા પગલાં અને નીતિઓ ને પ્રોત્સાહન આપવું ખૂબ જરૂરી છે. સરકાર દ્વારા ભારત દેશમાં માહિતી અધિનિયમ, 2000(IT ACT 2000) કાયદો બાર પાડવામાં આવ્યો છે. આ બંને વચ્ચે ગાઢ સબંધ છે, કારણ કે ડિજિટલ સાક્ષરતા વિના સાયબર ધમકીઓ નો સામનો કરવો મુશ્કેલ બને છે. આમ ડિજિટલ સાક્ષરતા વગર સાયબર સુરક્ષા શક્ય નથી અને સાયબર સુરક્ષા અત્યારે રાષ્ટ્રની સુરક્ષાનો મહત્વ નો હિસ્સો બની છે. આમ લોકો સાયબર ગુનાનો ભોગ ન બને તે માટે લોકોમાં ડિજિટલ સાક્ષરતા લાવવા માટે સરકાર દ્વારા ઘણી યોજનાઓ બાર પાડવામાં આવી છે.

પ્રસ્તુત સાંસોધન પેપરમાં સાયબર સુરક્ષા અને ડિજિટલ સાક્ષરતા ના સબંધ વિશે વિગતવાર વિશ્લેષણ કરેલ છે, જેમાં આંકડાઓ, ઉદાહરણો, અને સરકાર ના પગલાંઓ નો સમાવેશ કરવા માં આવેલો છે.

ચાવીરૂપ શબ્દો—ડિજિટલ સાક્ષરતા,સાયબર સુરક્ષા, ડિજિટલ ઇન્ડિયા, સાયબર ગુનાઓ, સરકારી યોજનાઓ, ફિશિંગ

I. વિષય પ્રવેશ

૨૧મી સદીમાં ભારત ડિજિટલ ઇન્ડિયા થવા તરફ આગળ વધી રહ્યું છે. તેની સાથે ભારતમાં ડિજિટલાઇઝેશનના કારણે અર્થતંત્ર અને સમાજમાં ઘણા ફેરફાર જોવા મળી રહ્યા છે, પરંતુ સાથે સાથે સાયબર હુમલા નું જોખમ પણ વધી રહ્યું છે. ભારતના લોકો રોજિંદા જીવનમાં બહોળા પ્રમાણમાં ડિજિટલ સેવાઓ, લેપટોપ, મોબાઈલ અને ઇન્ટરનેટનો ઉપયોગ કરી રહ્યા છે. હાલના સમયમાં બેન્કિંગ, શિક્ષણ, આરોગ્ય, વેપાર બધા ક્ષેત્રોમાં ડિજિટલ માધ્યમનો ઉપયોગ કરવામાં આવી રહ્યો છે. આમ આ બધા માધ્યમોને સાયબર ગુનાથી બચાવવા માટે લોકોમાં સાયબર સુરક્ષા વિશે જાગૃતિ લાવવી જરૂરી છે. મોટા ભાગ ના લોકો સાયબર હુમલાનો શિકાર ડિજિટલ સાક્ષરતાના અભાવે બને છે. હાલના અહેવાલ મુજબ ભારત વિશ્વના સૌથી વધુ સાયબર હુમલાઓ નો સામનો કરનાર દેશોમાંથી એક બની રહ્યું છે, આ પરિસ્થિતિ ને સુધારવા ભારત સરકાર ઘણી યોજનાઓ ચલાવી રહી છે. સાથે સાથે સરકાર દ્વારા ભારત દેશમાં માહિતી અધિનિયમ, 2000(IT ACT 2000) કાયદો બાર પાડવામાં આવ્યો છે. આ યોજનાઓ મોટે ભાગે ગ્રામ્ય વિસ્તાર માટે જરૂરી છે કારણ કે હાલ ગ્રામ્ય વિસ્તારોમાં પણ મોટા ભાગના લોકો ઇન્ટરનેટનો ઉપયોગ કરે છે, પરંતુ ગ્રામ્ય વિસ્તારોમાં સાયબર જાગૃતિના અભાવે સાયબર ગુનાનો શિકાર બને છે, ઉદાહરણ તરીકે, ૨૦૨૪-૨૫માં સાયબર ગુનાઓમાં

 ISSN: 2349-6002

૪૬% વધારો થયો છે. આ આકડા ને ઘટાડવા માટે લોકો ને ડિજિટલ સાક્ષર કરવા ખૂબ જરૂરી છે, તેમ પણ કહી શકાય કે સાયબર સુરક્ષા વગર ડિજિટલ વિકાશ ટકાઉ બની સકતો નથી. આ પેપરમાં સાયબર સુરક્ષા અને ડિજિટલ સાક્ષરતા વચ્ચેના સબંધનું વિશ્લેષણ, તેનું મહત્વ અને સરકારી પગલાંની ચર્ચા કરવામાં આવશે, જેમાં ઉદાહરણો અને આંકડાઓનો સમાવેશ કરવામાં આવ્યો છે.

II. સાયબર સુરક્ષાનો અર્થ અને મહત્વ

સાયબર સુરક્ષા એટલે ડિજિટલ માધ્યમો એટલે કે મોબાઈલ, ઇન્ટરનેટ, લેપટોપ, કોમ્પ્યુટર, નેટવર્ક જેવા માધ્યમો દ્વારા ડેટા ચોરી, સાયબર હુમલાઓ, ડિજિટલ સંપત્તિમાં અનુમતિ વગર પ્રવેશ તથા નાણાકીય ફ્રોડ જેવી સાયબર ઘટનાઓથી સુરક્ષિત રાખવાની પ્રક્રિયા. હાલના આધુનિક સમયગાળામાં ભારતના લોકો બહોળા પ્રમાણમાં ડિજિટલ સેવાઓનો ઉપયોગ કરે છે જેમ કે બેન્કિંગ, શિક્ષણ, વ્યાપાર વગેરે જેવી બાબતોમાં પણ ડિજિટલ માધ્યમનો ઉપયોગ કરવામાં આવી રહ્યો છે. આમ નાણાકીય બાબતો અને દેશની સુરક્ષામાં ડિજિટલ માધ્યમનો ઉપયોગ થતો હોવાથી સાયબર સુરક્ષા એ રાષ્ટ્રની સુરક્ષા નો એક મહત્વપૂર્ણ ભાગ બની છે.

III. ડિજિટલ સાક્ષરતાનો અર્થ અને મહત્વ:

ડિજિટલ સાક્ષરતા એટલે માત્ર મોબાઇલ, ઇન્ટરનેટ તથા કમ્પ્યુટરનો ઉપયોગ પૂરતી સીમિત નથી. લોકો અત્યારે ડિજિટલ માધ્યમનો બહોળા પ્રમાણમાં ઉપયોગ કરી રહ્યા છે પરંતુ તેમને ડિજિટલ માધ્યમની પૂરી જાણકારી તથા ઉપયોગ કરવા માટેની યોગ્ય પદ્ધતિની આવડત ન હોવાથી ઘણીવાર લોકો ભૂલ કરી બેસે છે અને સાઇબર ગુનાનો ભોગ બને છે, આમ લોકોને સાયબર ગુના નો ભોગ બનતો અટકાવવા માટે ડિજિટલ સાક્ષર બનાવવા ખૂબ જ જરૂરી બને છે. તેમજ તેમને ડેટા સુરક્ષાની સમજ તથા ઇન્ટરનેટ પરની માહિતીનો યોગ્ય ઉપયોગ અને તેમને વિશેની જાણકારી આપવી તે આવશ્યક બને છે. આમ લોકોને યોગ્ય માહિતી હોય તો તે છેતરપિંડી કરતી લિન્ક તથા ફિશિંગ જેવી ઘટના થી બચી શકે છે, તથા મજબૂત પાસવર્ડ બનાવવા સક્ષમ બને છે, સોશિયલ મીડિયા પર પ્રાઇવસી સેટિંગ્સ તથા ફેક અકાઉંટ ને ઓળખી શકે આમ લોકો ડિજિટલ સાક્ષર બને તો આવા ફ્રોડથી બચી શકે છે.

❖ સાયબર સુરક્ષા અને ડિજિટલ સાક્ષરતા વચ્ચેના સબંધ

સાયબર સુરક્ષા અને ડિજિટલ સાક્ષરતા એક બીજા સાથે પરસ્પર રીતે જોડાયેલા ખ્યાલો છે. ડિજિટલ સાક્ષરતા લોકોને ડિજિટલ સાધનો, મોબાઈલ, ઇન્ટરનેટ તથા ઓનલાઇન સેવાઓનો સમજદારીપૂર્વક ઉપયોગ કરવા સક્ષમ બનાવે છે, જ્યારે સાયબર સુરક્ષા આ ડિજિટલ માધ્યમો દ્વારા થતી ડેટા ચોરી, ઓળખચોરી તથા ઓનલાઇન છેતરપિંડી જેવી ઠગાઇથી સુરક્ષિત રાખવા મદદરૂપ થાઈ છે. જો કોઈ વ્યક્તિ ડિજિટલ સાક્ષર ન હોય તો તો સાયબર સુરક્ષા હોવા છતાં છેતરપિંડી તથા ઓળખ ચોરી જેવા કિસ્સાઓ નો ભોગ બને છે. તે જ રીતે, ઘણી વાર એવું પણ બને છે કે ડિજિટલ સાક્ષરતા હોવા છતાં ટેકનિકલ રીતે સાયબર સુરક્ષા મજબૂત ન હોય, ઘણા કિસ્સા માં ડિજિટલ સાક્ષરતા પ્રથમ રક્ષણ પૂરું પાડે છે જ્યારે સાયબર સુરક્ષા તકનીકી સ્તરે મજબૂત સુરક્ષા પૂરી પાડે છે, બન્નેના સંયોજનથી જ ડિજિટલ મધ્યમમાં અસરકારક સુરક્ષા શક્ય બને છે.

❖ ભારત સરકારના સાયબર સુરક્ષા માટે લીધેલા પગલાઓ

ભારત સરકારે સાયબર સુરક્ષાને મજબૂત બનાવવા અને લોકો સાયબર ગુનાનો ભોગ ન બને એ માટે ઘણા પગલાંઓ લીધેલા છે જે નીચે મુજબ છે.

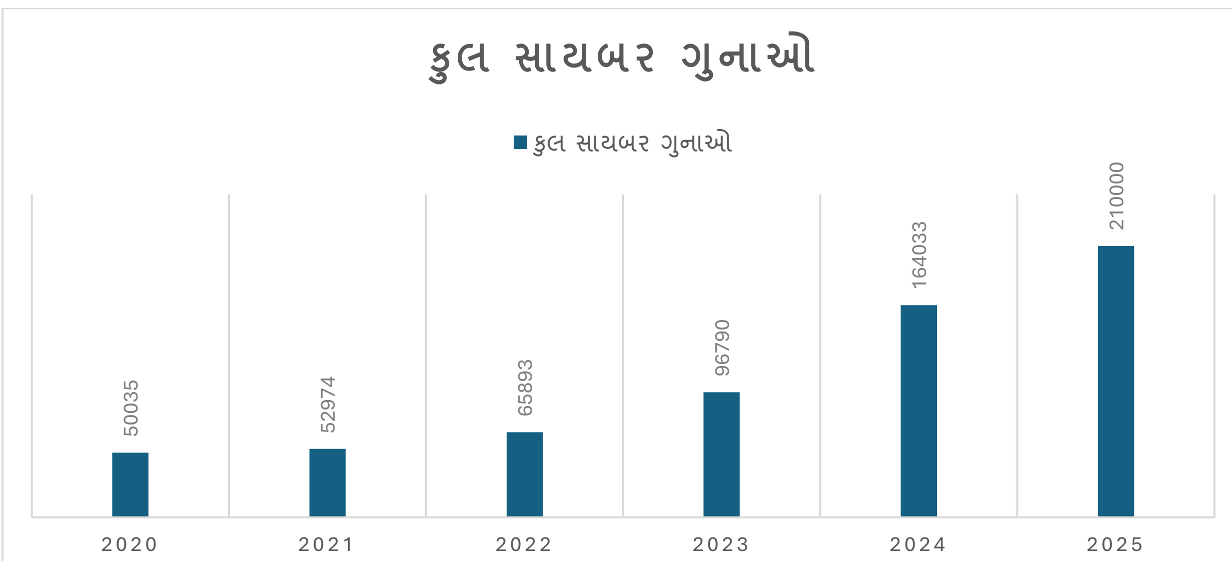
 ISSN: 2349-6002

- સાયબર સુરક્ષા માટે:
  - National Cyber Security Policy 2013- સાયબર સુરક્ષાની ક્ષમતામાં વધારો કરવા.
  - Cyber Surakshit Bharat- સરકારી કર્મચારીઓ માટે તાલીમ
  - ૨૦૨૫માં સ્માર્ટફોન પર પ્રીલોડ સંચાર સાથી એપનો આદેશ:
- ડિજિટલ સાક્ષરતા માટે:
  - PMGDISHA: ગ્રામીણ વિસ્તારોમાં ૬ કરોડ લોકોને ડિજિટલ તાલીમ
  - Project BharatNet: ગ્રામ પંચાયતોમાં બ્રોડબેન્ડ
  - Digital India

ભારત સરકારે લીધેલા સાયબર સુરક્ષા અને ડિજિટલ સાક્ષરતા માટેના પગલાઓ અને સુરક્ષા નીતિઓ ઉપર મુજબ સે જેનો અમલ કરી સરકાર લોકો ને સાયબર સુરક્ષા વિશે જાણકારી અને તેના થી બચવા કરવા માટે સક્ષમ બનાવે છે.

❖ ભારતમાં સાયબર ગુનાઓ ના કેસો માં થતો વધારો(2020 થી 2025)

ભારત જેમ જેમ આધુનિકતા તરફ આગળ વધી રહ્યું છે તેમ તેમ ભારતમાં સાયબર ગુનાઓ ના કેશમાં મોટા પ્રમાણમાં વધારો થતો જોવા મળે છે. ગુનાઓના આંકડા અને ટકાવારી પ્રમાણે વધારા ની માહિતી નીચે મુજબ છે.



નોંધ:વર્ષ ૨૦૨૫ ની જાણકારી અંદાજ મુજબ છે.NCRB (NATIONAL CRIME RECORDS BUREAU)ના સંપૂર્ણ રેકોર્ડ હજી આવેલ નથી

આમ ઉપરની માહિતી પરથી જાણવા મળે છે કે ભારતમાં સાયબર ગુનાઓની સંખ્યામાં મોટા પ્રમાણમાં વધારો જોવા મળી રહ્યો છે. આ વધારાની સ્થિતિને નિયંત્રીત કરવા માટે લોકોને ડિજિટલ સાક્ષર કરવા ખૂબ જરૂરી છે.

❖ સાયબર કાયદાઓ:

સાયબર કાયદાઓ એટલે ઇન્ટરનેટ, કોમ્પ્યુટર, મોબાઈલ અને ડિજિટલ ટેકનોલોજી સાથે જોડાયેલા ગુનાઓ અને નિયંત્રિત કરતો કાયદો. હાલના આધુનિક યુગમાં બેન્કિંગ, સોશિયલ મીડિયા, ઈ-કોમર્સ નું પ્રમાણ

ખૂબ વધ્યું છે, એના માટે સાયબર સુરક્ષા ખૂબ જરૂરી બને છે. સાયબા કાયદાઓ ઓનલાઇન ફ્રોડ, હેકિંગ, ડેટા ચોરી અને વાઇરસ ફેલાવાને અટકાવવા માટે બનાવવામાં આવ્યા છે. ભારતમાં માહિતી ટેકનોલોજી અધિનિયમન 2000 (IT Act 2000) સાઇબર કાયદા નો મુખ્ય આધાર છે. આ કાયદા દ્વારા ડિજિટલ સહી, ઓનલાઈન વ્યવહારોને, કાનુની રીતે માન્યતા આપવામાં આવી છે. સાયબર કાયદો એ નાગરિકોનું ડિજિટલ રીતે રક્ષણ કરે છે. અને આવા ગુનેગારોને સજા આપવાનું કાર્ય સાયબર કાયદો કરે છે. આથી સાયબર કાયદા ની સમજ દરેક નાગરિકો અને વિદ્યાર્થીઓ માટે ખૂબ જરૂરી છે. જેથી આપણે સુરક્ષિત અને જવાબદાર રીતે ઇન્ટરનેટનો ઉપયોગ કરી શકીએ.

❖ હેતુઓ:
- ➢ સ્કૂલ અને કોલેજ લેવલ માં ડિજિટલ સાક્ષરતા નો અભ્યાસ ફરજિયાત કરવો.
- ➢ પછાત વિસ્તારો તથા સાક્ષરતાનું પ્રમાણ ઓછું હોય તેવા વિસ્તારમાં તાલીમ આપવી.
- ➢ મહિલાઓ અને વૃદ્ધોને ખાસ સાયબર સુરક્ષાનું મહત્વ સમજાવવું.
- ➢ સાયબર સુરક્ષા વિશે લોકોને જાગૃત કરવા.

❖ ઉત્કલ્પના:
- ➢ જો લોકો ડિજિટલ સાક્ષર હોય, તો તે ઓનલાઇન છેતરપિંડી થી બચી શકે.
- ➢ જો વ્યક્તિ મજબૂત પાસવર્ડનો ઉપયોગ કરે,તો એકાઉન્ટ હેક થવાની સાંભાવના ઘટી જે.
- ➢ જો ડિજિટલ સાક્ષરતા ઓછી હોય, તો વ્યક્તિ ઓનલાઈન ફ્રોડનો શિકાર વધુ બને.

❖ સાંસોધન પદ્ધતી:
આ સંસોધન પેપર ગૌણ માહિતી પરથી તૈયાર કરવામાં આવ્યું છે, જેમ કે સરકારી રેપોર્ટ્સ, વેબસાઈટ તથા હાલમાં બનેલા કિસ્સાઓ વિશે લેખ અને વધારેમાં વધારે 2024-25ના આંકડા અને ઉદાહરણ નો ઉપયોગ કરીને તૈયાર કરેલું છે.

તારણો અને સૂચનો

➢ તારણો:
1. મોટા ભાગના લોકોને પાસવર્ડ મેનેજમેન્ટની યોગ્ય જાણકારી નથી.
2. સોસિયલ મીડિયા પાછળ પાગલ યુવા પેઢીમાં ખાનગી માહિતી શેર કરવાની ઘેલછા.
3. સરકારી હેલ્પલાઇન 1930 વિશે ખૂબ ઓછા લોકોને જાણકારી.
4. યોગ્ય જાણકારી ન હોવાને લીધે કોઈપણ લિન્કને ખોલી ડિજિટલ અરેસ્ટનો શિકાર બને.

➢ સૂચનો:
1. સાયબર સુરક્ષાને પ્રાથમિક શિક્ષણનો ભાગ બનાવવો.
2. ડિજિટલ સાક્ષરતાની તાલીમ માતૃભાષામાં આપવી.
3. સ્ત્રીઓ અને વૃદ્ધો માટે ખાસ સાયબર સુરક્ષામાટેના વર્કશોપ યોજવા.
4. સ્માર્ટફોનમાં પ્રિલોડ સાયબર સુરક્ષા એપ 'સંસારસાથી' ને વધારે પ્રોત્સાહન આપવું.

❖ નિષ્કર્ષ:
આમ હાલની પરિસ્થિતિને જોતા ભારતમાં સાયબર સુરક્ષા અને ડિજિટલ સાક્ષરતા બન્નેનો વિકાસ કરવો ખૂબ જરૂરી છે. કારણ કે ભારતના ડિજિટલ વિકાસને ટકાઉ બનાવવા માટે સાયબર સુરક્ષા અને ડિજિટલ સાક્ષરતા વચ્ચે સંતુલન હોવું ખૂબ જરૂરી છે. જેથી વધતા સાયબર ગુનાઓની સંખ્યામાં ઘટાડો કરી શકાય. તથા

સાયબર સુરક્ષા માટેની યોજનાઓ અને પહેલોમાં વધારે ધ્યાન આપવું જેથી ડિજિટલ અસાક્ષર લોકોમાં સાયબર સુરક્ષાની જાણકારી અને તેનાથી બચાવ શક્ય બને. સરકાર દ્વારા ભારત દેશમાં માહિતી અધિનિયમ, 2000(IT ACT 2000) કાયદો બાર પાડવામાં આવ્યો છે જેથી ગુનેગારોને સજા મળે.આમ આ સંશોધન પેપરમાં ભારતમાં સાયબર સુરક્ષા અને ડિજિટલ સાક્ષરતા વચ્ચેનો સંબંધ વિશે વિસ્તૃત જાણકારી રજૂ કરેલ છે.

સંદર્ભસૂચિ

[1] https://gujaratcybercrime.org/#accordion1

[2] https://www.pib.gov.in/PressReleasePage.aspx?PRID=2176254&reg=3&lang=2

[3] NCRB – Crime in India Report 2023

[4] Information Technology Act, 2000, Government of India.

[5] https://en.wikipedia.org/wiki/National_Cyber_Security_Policy_2013

[6] https://vajiramandravi.com/current-affairs/crime-in-india-2023-ncrb-report-highlights-surge-in-cybercrime-in-india