GLOBAL Scientific Research

Journal of Technology Innovations and Energy

Vol. 1 No. 2 (2022)

www.jescae.com

ISSN: 2957-8809

Journal of Technology Innovations and Energy

Vol.1, No.2

June 2022

Chief Editor	Dr. Hayat Khan
Edited by	Global Scientific Research
Published by	Global Scientific Research
Email	thejtie@gmail.com
Website	www.jescae.com
Journal Link:	https://www.jescae.com/index.php/JTIE

CONTENTS

Journal of Technology Innovations and Energy
https://doi.org/10.56556/jtie.v1i2.152
ISSN: 2957-8809

RESEARCH ARTICLE

C++ Software Program for Downdraft Gasifier Design and Development

Aly Radwan[1*], A.S. Abd Ethamid[1], A.khatab[1], M.A.Hamad[1]

[1]National Research Center, Chemical Engineering & Pilot Plant Department, EGYPT

Corresponding Author: Aly Radwan, radwannrc@hotmail.com
Received: 15 January, 2022, Accepted: 27 February, 2022, Published: 03 March, 2022

Abstract
Biomass gasification is an important process of converting biomass into a gaseous fuel through a sequence processes of thermochemical reactions. Prototype of down draft gasifier was designed to generate synthesis gas for house hold applications. C++ Software Program for the design and development of downdraft gasification system was done.

Keywords: Downdraft gasifier; Biomass; Synthesis gas; Software calculation

Introduction

Downdraft gasifiers reactors are the most suitable for rural areas using both small and medium sizes. The system can serve both the household and agriculture applications. The performance of gasification processes in a downdraft gasifier is affected by different factors including residence time, type of reactors, properties of the biomass feed, air to steam ratio and the addition of catalyst. These parameters are affecting on the performance of the gasifier.
The gas produced from gasification processes will be used for different application in rural areas such as drying, domestic cooking, irrigation pump and small scale industrial process. Downdraft gasifier has been applied in China for domestic cooking. Downdraft gasifier of 6-7 kw was designed and constructed in India. Many gasifiers system has been applied in India for heating and small industrial processes (1-8).
The present article deals with software program C++ for design and development of downdraft gasifier .

Processes in downdraft gasifier

In the downdraft gasifier both biomass and air move in the downward direction in the lower part of the gasifier system. Down draft consists from four zones. The zones of gasification process such as drying, pyrolysis, oxidation and reduction is shown in Fig. 1.
The fed biomass is dried in the top of gasifier. The dried biomass moves downward to the upper-middle zone, enabling the pyrolysis and the tar conversion reactions to occur.

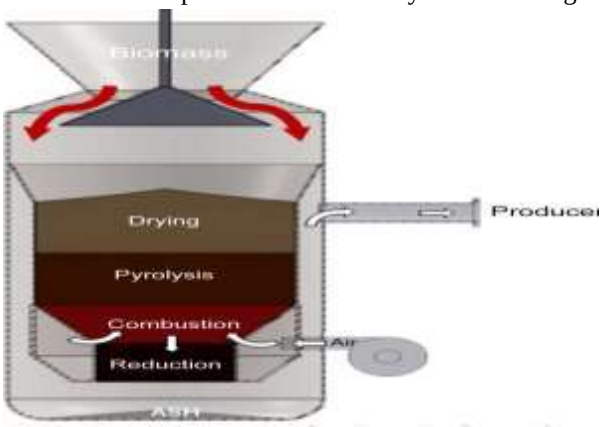


Figure 1. Schematic diagram of downdraft gasifier
The unconverted tars and gases then evolve toward the oxidation zone, where the combustion takes place at higher temperature of 1000-1400 °C.
The chemical species formed finally move through a reduction zone where the H_2 and CO contents are enriched.
The product gas contains a low amount of particulates and tars (~ 1 g/Nm^3) because most of the tars are combusted in the oxidation zone.
The downdraft gasifier is particularly well adapted when a clean syngas gas with a low content of tar and particulates is required.

Advantages & Disadvantages of Downdraft gasifier
Advantages

Downdraft gasifier is very attractive for biomass gasification due to its easy fabrication and operation, and also due to low tar content in producer gas.

Disadvantages

Drawbacks such as grate blocking, channeling, and bridging are found in the downdraft gasifiers, typically for feedstock with low bulk density.
Another disadvantage is that the downdraft gasifiers only suitable for feedstock with low moisture content.

DESIGN OF DOWNDRAFT GASIFIER

The design of the gasifiers is an important parameter that affects their performance. Various works on design improvements have been done for enhancing the performance of the gasifiers (1-12).

Important Parameters in Design

Following parameters must be understood first before starting design of downdraft gasifier.

Equivalence Ratio (ER)

ER is defined as the ratio of oxygen supplied per kg feedstock to the stoichiometric requirement. ER fixes the amount of air supplied for gasification. A value of 0.2-0.4 ER is generally recommended depending on the size of the unit and retaining of heat in the combustion zone. From our studies we recommend, ER 0.25 for medium size gasifier.

Specific Gasification Rate (SGR)

SGR is the volumetric flow rate of gas per unit area based on throat area, the gas volume being measured at the standard conditions. Generally, The recommended SGR value falls in the range of 1920-2640 m^3/m^2 -hr. A mean value of 2000 m3/m3.hr is recommended in our study.

Relative Cylinder Storage Capacity (RCC)

RCC is the mass flow rate of biomass per unit area based on the diameter of the upper cylinder. The recommended RCC value falls in 250-300 m^3/m^2 –hr.

Specific Solid Flow Rate (SSR)

SSR is the mass flow of fuel measured at the throat. It is a derived parameter since it can be obtained from SSR.
As **one kg** of biomass approximately gives **2.4 m^3** of gas, SSR can be related to SSR as SGR/2.4.

$$SSR = \frac{SGR}{2.4}$$

Design Procedure

Some parameters are required to decide first for the design purpose which are as follows:

The capacity of gasifier

Capacity of the gasifier is decided first as **Po kW** thermal output power. While gasifier design procedure is based upon its capacity.

Syngas Yield (Y):

As per literature **1 kg** of biomass will yield **2.4 m^3** of syngas.

High Calorific Value (HCV) of Syngas:

High Calorific Value of produced syngas from most biomass and agricultural residues, is about 4000 KJ / m^3.So, Required syngas generation rate for Qg output thermal power is, $Q_g = \frac{P_o}{HCV} m^3/h$.

Air Flow Rate Calculation:

For the calculation of air flow rate, ultimate analysis of biomass is required. (Tables 1-2) shows the proximate and elemental analysis of biomass residues.
Optimum equivalence ratio is considered as 0.25 from our technical studies.

Table-1. Proximate analysis of biomass samples (wt%).

Biomass type	%Moisture content	%Total volatile matter	%Fixed carbon	%Ash
Cotton stalk	8.9	81.24	14.48	4.28
Rice straw	8.04	69.24	16.7	14.42
Corn stalk	7.96	76.6	19.12	4.27

Table- 2. Elemental analysis of biomass samples (wt%)**.**

Biomass type	C %	O %	H %	N %	S %
Cotton stalk	44.8	43.8	5.8	1.09	0.57
Rice straw	33.86	39.18	4.5	1.045	0.945
Corn stalk	40.3	46.93	4.2	2.3	Nil

The stoichmetric requirement for the combustion of different biomass materials is determined in Table 3.

Table 3. Air requirement for stoichiometric combustion of biomass

Biomass	Stoichiometric oxygen required (Kg/kg)	Stoichiometric air required $m_{a\ comb}$(kg/kg)
Cotton stalks	1.2	5.3
Corn stalks	0.94	4.1
Rice straw	0.86	3.8

Air required for combustion=$Q_{acomb} = m_{acomb}/\rho$

Actual air mass required for gasification$m_{agasification=0.25m_{acomb}}$

From which the air rate required for gasification can be determined

$$Q_{ag\ gasification=-0.25m_{acomb/\rho}}$$

Throat Design

Throat diameter of the gasifier is designed based on specific gasification rate (SGR) value. SGR value of downdraft gasifier falls in between 1920-2640 Nm^3/m^2 -hr. SGR value for downdraft gasifier is taken as SGR = 2000 Nm^3/m^2 -hr.

From the definition of Specific Gasification Rate,

SGR =$\frac{Qg}{A_{th}}$

Where, A_{th}= Area ofthroat

$A=\pi d^2_{th/4}$

So, from which (d_{th}) can be determined

Diameter Combustion Chamber

The combustion chamber is one of the main parts of the gasifier. It should be insulated to retain the heat of combustion. It generally consists of three zones; medium, combustion, higher pyrolysis and the lower is reduction.

The diameter of the combustion chamber is generally taken 2-3 the throat diameter.

In our case we recommend the higher ratio to assist for insulation of the chamber

$d_{Comb=\ 3.0}d_{th}$

Where d_{comb} is the diameter of combustion chamber

Height of Combustion Chamber

There are wide variety of relations for estimation of the height of combustion chamber . The more reasonable is to relate the height to the throat area.

A value of 2-3 is mostly used. For our study we recommend 2

$$H_{Comb=\ 2.0}d_{th}$$

Reduction Zone Height (**H_r**).

The relation between reduction zone height and diameter of the throat is used to calculate reduction zone height below throat. For medium size gasifier.

$\frac{H_r}{d_{th}}$=2.0

Diameter of air distributor

The recommended velocity of air in the distributor is 6-10 m/sec. (Kumar &Ojolo).The cross section area of the air distributor can be obtained based on the volume of air required for gasification

Take the velocity of the air = 6 m/sec

Q_{ag} Gasification =V*A

$$=6*\pi/4\ d^2$$

From which diameter (d) of air distributor can be determined

Determination of number and size of nozzles

The number of nozzles for medium size gasifier (dt 150-300) ranged between 5-8 nozzles.

For even distribution of air we recommend 6 nozzles

Number of nozzles = 6

Diameter of nozzles

The velocity of air in the nozzles should be not less than 30 m/s.In order to have good combustion of the whole cross section but not adjacent to the walls.

V= 30m/s

Using the velocity V= 30 m/sec, and knowing the airflow rate (Q_{ag}) and number of the nozzles n. The area of the nozzlecan be determined from equation.

$V=30= Q_{ag}/(6*A_{nozzle})$

$= Q_{ag}*4/(6*\pi d^2)$

From which diameter of the nozzle (d) can be determined

Fuel Storage Upper Cylinder Diameter ($d_{stoarge}$).

For calculation of diameter of fuel storage upper cylinder, Relativecapacity of cylinder (RCC) is used. Which is 250 kg / hr.$m^2$for downdraft Gasifier.

RCC= $\frac{\dot{m}f}{A_{cylinder}}$ =250 kg / hr. m^2

Where, $\dot{m}_f$= actual mass flow rate of biomass in kg/hr

$\dot{m}_f$= $\frac{Qg}{2.4}$

$A_{cylinder}$ = Area of the upper cylinder for storage of biomass in m^2.

So, the diameter of storage cylinder, $d_{cylinder}$**)** can be determined.

$$A_{Cylinder} = \pi d^2 cylinder\ /4$$

The Height of Upper Cylinder.

The bulk density of pelletized biomass, 300-600 kg/m^3.

Let's take **500** kg/m^3. So, calculating storage of biomass for **3**hrs operation of gasifier, which is sufficient for the consumption of half a day.

Volume required for 3 hrs operations

$V_3=h*\pi r^2$

To calculate height of storage cylinder "upper part"

$\mathbf{V_3=\pi \quad r^2 \quad h_c}$

Where, r = radius of fuel storage cylinder in, m.

h = height of fuel storage upper cylinder in, m.

Mass of fuel = $(Q_g/2.4)$

Volume of fuel = $(Q_g/2.4)*3hr/\rho$

C^{++} Software Program for downdraft gasification design

```
//

//Design calculation of Downdraft Gasifier for Biomass Gasification

//shown in Fig.2

#include <iostream>

#include <math.h>

using namespace std;

int main()

{

float Po, Y, HCV, Qg;

float ma, SGR, rho, Dn, An;

floatAth, Dth, HDR, Hth, Qairg;

floatHr, RCC, Dcy, Acy, vol, Nz;

float W, Vcy, Hcy, Dch, Hch, BD, V;

cout<<
"*********************************************
******" <<endl;

cout<<
"*********************************************
*********" <<endl;

cout<< "******** 1- Calculate Syngas Generation Rate, Qg  **********" <<endl;

cout<<
"*********************************************
**********" <<endl;

cout<< " >> Enter the Capacity of Gasifier(Thermal Output Power,Po = kW)==" <<endl;

cin>> Po;

cout<< " >> Enter Syngas Yield,Y;'1kg biomass will yield 2.4 m3 of syngas' ==" <<endl;

cin>> Y;

cout<< " >> Enter High Calorific Value HCV of Syngas ==== 4000 KJ/m3  ==" <<endl;

cin>> HCV;

Qg = Po*60*60/HCV;

cout<< " 1-  Syngas Generation Rate, Qg = " <<Qg<< "m3/hr" <<endl;

cout<<
"*********************************************
****" <<endl;

cout<<
"*********************************************
****" <<endl;

cout<< "***** 2- Calculate Air Flow Rate, Qair *******" <<endl;

cout<<
"*********************************************
****" <<endl;

cout<<
"*********************************************
****" <<endl;

cout<< " >> Enter the mass air required for combustion (ma) from table according type of biomass)==" <<endl;

cin>> ma;

cout<< " >> Enter air density at stp = 1.29' ==" <<endl;

cin>> rho;

Qairg = 0.25*ma/rho;

cout<< " 2-  Air Flow Rate for gasification, Qairg = " <<Qairg<< "m3/hr" <<endl;

cout<<  "**********************************"
<<endl;

cout<<  "**********************************"
<<endl;

cout<<  "**3-Throat Diamater, Dth **********"
<<endl;
```

```
cout<<        "**********************************"
<<endl;

cout<<        "**********************************"
<<endl;

cout<< " >> Enter Specific Gasification Rate SGR from
1920 to 2640 Nm3/m3.hr" <<endl;

cin>> SGR;

Ath = Qg/SGR;

cout<< " 3-1- Area of Throat, Ath = " <<Ath<< "m2"
<<endl;

Dth = sqrt(4*Ath/3.14);

Dth = Dth * 100;

cout<< " 3-2  - Diameter of Throat, Dth = " <<Dth<<
"cm" <<endl;

cout<<
"******************************************"
<<endl;

cout<<
"******************************************"
<<endl;

cout<<        "**4-Combustion Chamber, Dcb,
Hcb**********" <<endl;

cout<<
"******************************************"
<<endl;

cout<<
"******************************************"
<<endl;

Dch = 3*Dth * 100;

Hch = 2*Dth * 100;

cout<< " 4-1- Diameter of Combustion Chamber, Dch =
" <<Dch<< "cm" <<endl;

cout<< " 4-2- Height of Combustion Chamber, Hch = "
<<Hch<< "cm" <<endl;



cout<<
"**************************************"
<<endl;
cout<<
"**************************************"
<<endl;
cout<<  "** 5-Reduction Zone Height,(Hr)******"
<<endl;

cout<<
"**************************************"
<<endl;
cout<<
"**************************************"
<<endl;
Hr = 2.5 * Dth;
cout<< " 5- Height below Air inlet, Hr = " <<Hr<< "cm"
<<endl;
cout<<
"******************************************"
<<endl;
cout<<
"******************************************"
<<endl;
cout<< " **6-Fuel Storage Cylinder Diameter, Dcy **"
<<endl;
cout<<
"******************************************"
<<endl;
cout<<
"******************************************"
<<endl;
cout<< " >> Enter Relative Capacity Of Cylinder, RCC
250 kg/hr.m2" <<endl;
cin>> RCC;
Acy = Qg /(Y*RCC);
Dcy = sqrt(4*Acy/3.14)*100;
cout<< " 6- Diameter of fuel Storage Cylinder, Dcy = "
<<Dcy<< "cm" <<endl;
cout<<
"******************************************
****" <<endl;
cout<<
"******************************************
***" <<endl;
cout<< " ** 7- Height of Fuel Storage Cylinder, Hcy
****" <<endl;
cout<<
"******************************************
****" <<endl;
cout<<
"******************************************
***" <<endl;
cout<< " >> Enter bulk density (BD) of pelletized
biomass from 300-600 kg/m3" <<endl;
cin>> BD;
cout<< " >> Enter number of operating hour, Hr, take =
3hr" <<endl;
cin>>Hr;
vol = (Qg*Hr)/BD;
Hcy = 4*vol*1000000/(3.14*Dcy*Dcy);
Hcy = Hcy/100 ;
cout<< " 7- Height of fuel Storage Cylinder, Hcy = "
<<Hcy<< "m" <<endl;
cout<<
"******************************************
****" <<endl;
```

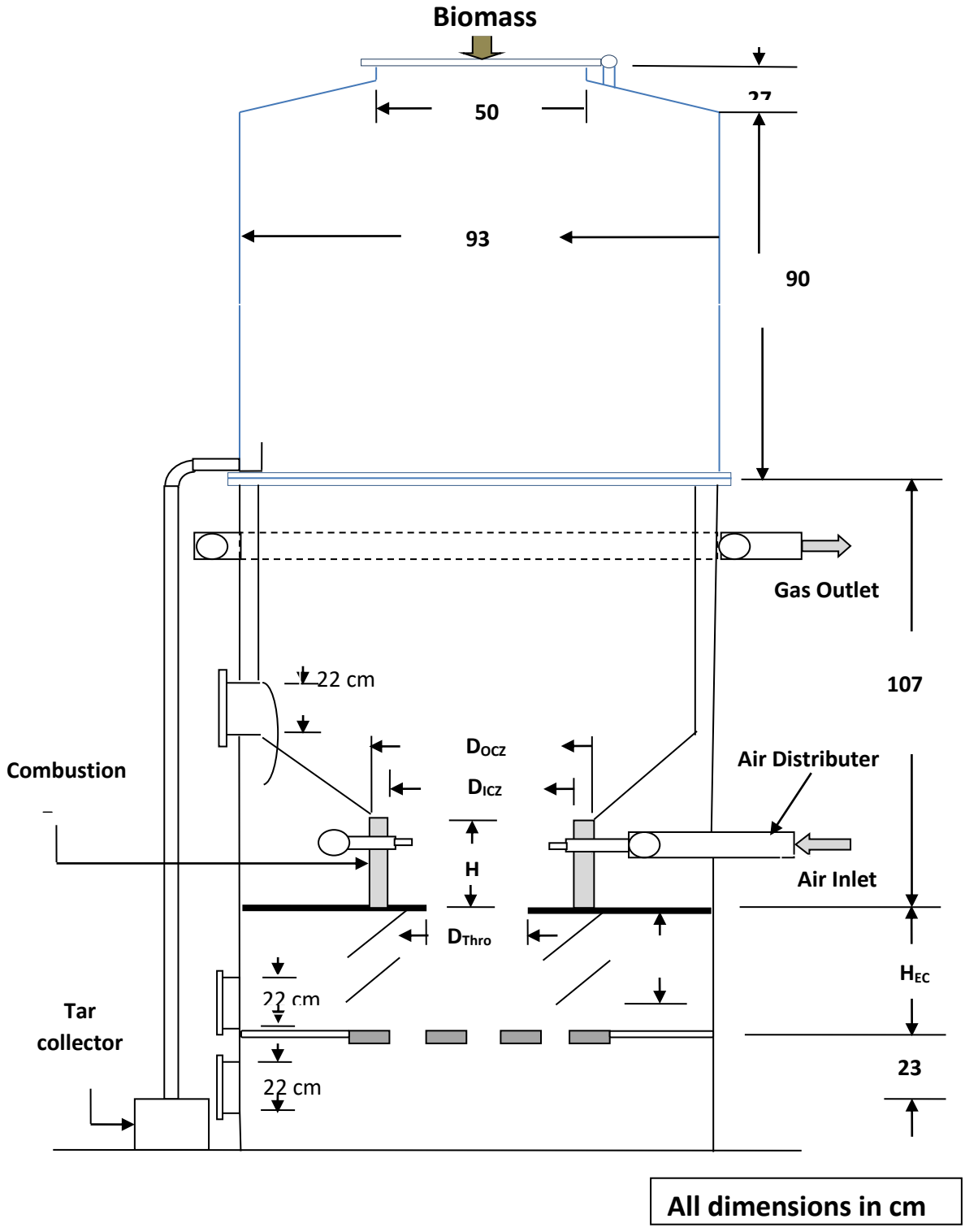


Fig. (2) Gasifier internal details

```
cout<<
"*******************************************
****" <<endl;
cout<< " ********** 8- Nozzle Diameter, Dn
**********" <<endl;

cout<<
"*******************************************
****" <<endl;
```

```
cout<<
"*********************************************
****" <<endl;
cout<< " >> Enter number of Nozzles, Nz" <<endl;
cin>>Nz;
cout<< " >> Enter air velocity, V = 30 m/sec" <<endl;
cin>> V;
      An = Qairg/(Nz*V);
Dn = sqrt(4*An/3.14)*100;
cout<< " 8- Diameter of nozzle, Dn = = " <<Dn<< "m"
<<endl;
return 0;
}
```

Conclusions

1.The following conclusions were drawn:
Downdraft gasification is more suitable processes for converting of biomass for synthesis gas
2.Thermochemical and physical characteristics of biomass together with the optimal design of downdraft gasifier was done.
3.C^{++} Software Program for Downdraft Gasifier Design and Development was established.

References

T.B. Read and A. Das, **(1986)**, Handbook of biomass downdraft gasifier engine systems, Fig. 5-3, page 31..

Basu, P.(**2010**.), "Biomass gasification and pyrolysis: practical design and theory. Academic press.

Knoef, H.A.M., **(2005**). Handbook biomass gasification. Meppel, TheNederlands: BTG Biomass Technology Group B.V.

D.K. Vyas, Tarak Dipak, Mendpara Viral, S.H. Akbari (**2014)**" , Design and development of inverted down draft gasifier for cooking purpose" Scholars Journal of Engineering and Technology, SJET,**.**

G Suresh Kumar, AVSSKS Gupta, M Viswanadham,(**2018)**"Design of lab-scale downdraft gasifier for biomass gasification, Material Science and Engineering 455,.

M.A.Chawdhury and K.Mahkamov,(**2011)**"Development of a small downdraft biomass gasifiers for developing countries" J Sci. Res. 3, 51-64,**.**

Md. Ali Azam, MdAbsanullah and Sultana R.Syeda, **(2007**)"Construction of a downdraft biomass gasifier", Journal of Mechanical Engineering, Vol.ME37, June.

Asadullah, M.,(**2014)**" Biomass gasification gas cleaning for downstream applications: a comparative critical review. Renew. Sust. Energy Rev. 40, 118-132.

Jan Venselaar (**1982)** ―design rules for down draft wood gasifiers a short review‖ project JTA-9A - Research Development at the Institute Technologi, Bandung, Indonesia August**.**

D.S Mandwe, S.R Gadge, A.Kdubey, VP Khambalkar,(**2006)**" Design and development of a 20 kw cleaning and cooling system for a wood chip gasifier, Journal of Energy in Southern Africa, Vol.17 No.4**.**

S. J. Ojolo and J.I Orisaleye (**2010)**" Design and development of a laboratory sale biomass gasifier" Journal of Energy and Power Engineering, ISSN 1934-8975, USA, August Volume 4, No. 8.

SinhalSamirkumarNarendrabhai, Mohammad Husain Shaikh, Patel Sachin"(**2018)**" Design , development and experimental studies of downdraft gasifier", International Journal of advanced Research , Ideas and innovations in technology,, ISSN:2454-132X, volume 4, Issue 3..

Campbell, J.M., Gas Conditioning and Processing, Volume 2: The Equipment Modules, 9th Edition, 2nd Printing, Editors Hubbar d, R. and Snow–McGregor, K., Campbell .

Journal of Technology Innovations and Energy
https://doi.org/10.56556/jtie.v1i2.180
ISSN: 2957-8809

RESEARCH ARTICLE

Mobile Technology's Role in Meeting Sustainable Development Goals

Showkat Ahmad Dar[1*], Naseer Ahmad Lone[2]

[1]Department of Political science and Public Administration, Annamalai University Tamil Nadu, India
Address: Handwara, Jammu &, Kashmir-193221
[2]Chandigarh University India

Corresponding author; Showkat Ahmad Dar, darshowkat41@gmail.com
Received: 04 February, 2022, Accepted: 14 March, 2022, Published: 17 March, 2022

Abstract
It has become increasingly important for companies in the twenty-first century to consider environmental sustainability. Various industries have taken varied approaches to environmental protection. Every major cell phone company has gotten behind this great cause at some point. The digital divide exists even in the most remote regions of the world, where there is little or no infrastructure. Cellular technology adoption continues to climb even as prices come down for smart phones and the availability of reliable networks expands. Because mobile devices are so widely available and frequently used, many forward-thinking individuals are turning to them to help eliminate knowledge gaps, alleviate poverty, and enhance the environment. According to the GSMA's sixth annual SDG impact report, the mobile industry's contribution to all 17 Sustainable Development Goals (SDGs) increased in 2020. We are barely half-way to our potential impact on attaining the Sustainable Development Goals because of this worldwide pandemic. Given that the 2030 SDG targets are only 10 years away, progress cannot be taken for granted. There is a strong correlation between mobile phone uses in all the countries of the world. Thus, the purpose of the study is to demonstrate how mobile technology helps achieve long-term sustainable development goals.

Keywords: Mobile Technology; SDGs; Poverty and Contribution etc

Introduction

The mobile sector contributes to a sustainable, robust, and high-quality infrastructure. They are dedicated to using the internet and digital solutions to advance the 2030 Agenda and speed up the SDGs (SDGs). They can make a significant contribution to a global effort that will leave no one behind. According to GSMA, an organization that brings together the world's main mobile operators, connectivity is crucial for meeting the UN's 17 Sustainable Development Goals. In February 2016, at the Mobile World Congress (MWC) in Barcelona, Spain, the mobile sector committed to working toward the UN's Sustainable Development Goals (SDGs). Since then, MWC's contributions to the SDGs have been gathered into the 2017 "Mobile Industry Impact Report." The Sustainable Development Goals (SDGs) were launched in September 2015 as a 17-point plan to achieve equitable and long-term health on all scales, from the planet's biosphere to individual communities (GSMA, 2021). The goal is to alleviate poverty, maintain the environment, and ensure future peace and prosperity. 300 telecoms companies from around the world detail their contributions to the 2030 targets.(GSMA, 2020 Mobile Industry SDG Impact Report, 2020)
The article's findings are based on analyses of mobile industry-sponsored activities. These include using communication to help local companies and creating jobs for the poor. Each Sustainable Development Goal (SDG) is given a score from 0 to 100 based on its importance. An SDG score of 37.5 means the industry is providing 37.5% of what it can to achieving this SDG. The mobile phone sector has been at the forefront of inventing innovative products and surviving in the current climate. These include techniques to(GSMA, 2021) survive in the existing environment. The mobile phone business has produced smaller, lighter phones to lessen their environmental impact (Technology & Environmental Sustainability Initiatives). (GSMA, 2020 Mobile Industry SDG Impact Report, 2020).
Smaller gadgets require less energy during travel, recycling, and reuse, and less raw material and shipping space. Mobile phone manuals are only available digitally. This reduces tree-made paper use. The mobile phone industry uses innovation to establish an eco-friendly ecosystem. Solar-powered phones have also been produced. This forward-thinking innovation reduces reliance on non-renewable energy sources like electricity. Most companies have created energy-efficient and solar-powered mobile phones. These phones last longer without being recharged, saving money and reducing greenhouse gas emissions. Nokia has lowered no-load energy use by 90%, demonstrating its efficiency. This forward-thinking innovation eliminates the need to rely on papers by giving

maps on users' phones to help walkers and travellers find instructions. All components are recyclable and contain no nickel or mercury. Apple's facilities run on renewable energy. This project will minimise carbon emissions, leading to a greener habitat (GSMA, 2020 Mobile Industry SDG Impact Report, 2020).

Mobile phones have enabled connectivity, which has resulted in substantial progress in the fight against inequality. Despite rising mobile data traffic, download speeds improved by 33% in 2020 as a result of greater use of 4G and 5G. These enhancements strengthen the mobile industry's contribution to the SDGs by allowing mobile to be at the heart of a diverse set of services addressing society's global concerns. Last year, 3.3 billion people used their phones to make video calls, allowing for a variety of online activities like e-learning, medical, and remote working. Mobile internet is used by 1.6 billion people to enhance or monitor their health, and 2 billion people utilise it to obtain education for themselves or their children. The mobile sector contributes significantly to all 17 sustainable development goals. Hence the objective of the research is:

To explain and analyse the role and contribution of mobile technology in attaining sustainable development goals is the research objective of the study.

Literature review

Digital inequality in cross-national samples is a rising area of research, although few studies addressed this subject. (Bhandari, A.2019). Mobile technology, gender: International Telecommunication Union access to ICTs by gender (ITU). Women's relative access to mobile phones is overwhelmingly promoted by their wellbeing, as demonstrated by their availability of modern contraception (i.e., reproductive autonomy). The growth imperative and the world polity hypothesis show sporadic correlations along the distribution, but these correlations are inconclusive.

By tackling revolutionary issues, we protect human dignity and the planet. We seek to sustain the gains made on interlinked issues like (CDMA report 2020) climate, health, gender equality, human rights, data and technology, peace, and humanitarian aid.

State of Mobile Internet Connectivity is the Connected Society program's flagship report since 2018. This report offers the mobile industry and other stakeholders a complete overview of global connectivity trends and (Gsma report 2020) main hurdles to mobile internet uptake and use. During the COVID-19 outbreak and economic instability, mobile internet use skyrocketed. More than half of the world's population now uses mobile internet. Coverage grew to 94% of the population by 2020.

Human mobility and inequality are connected throughout modern history, from labour migration to urbanisation. Sustainable Development Goals can now revisit this problem (Hackl, A. (2018) global partnership. This review article proposes a mobility equity framework as part of SDG 10, which aims for reducing disparities within and across nations by 2030. It draws on extensive research evidence and significant disputes.

In rural areas with poor infrastructure, digital gaps persist despite the fast proliferation of mobile phones. The rise of mobile phones is connected to less gender inequality, higher contraceptive use, and decreased maternal and child mortality, with the poorest nations benefiting the most. Micro-level examination shows that mobile phones have improved women's sexual and (Rootandi et. al) reproductive health knowledge and autonomy. Expanding mobile phone access and coverage and narrowing the digital gap have major consequences for sustainable development. Academics and decision-makers interested in how technology affects sustainable development should read the paper.

Methodology

The current study can benefit from both ex post facto and analytical research. Analytical and descriptive methods are used in the investigation. As a result, both primary and secondary sources are used in this study. Secondary data culled from trustworthy sources such books, websites, and newspaper stories, 2020 Mobile Industry Impact Report: Sustainable Development Goals, several international journals and periodicals, was analysed qualitatively.

Discussion and Result

Mobile technology has committed to all 17 UN SDGs five years after they were announced. In order to address global concerns, mobile technology is critical. While half of the world was in lockdown this year, mobile networks were put to the test, and they were able to withstand the unexpected data (GSMA, 2020 Mobile Industry SDG Impact Report, 2020) spikes. Mobile infrastructure is solid and resilient, ensuring continuity and recovery, thanks to years of investment. SDG 9: Industry, Innovation, and Infrastructure is particularly affected by the mobile industry. (GSMA, Mobile Industry Impact-Report SDGs.pdf, 2021).

The mobile technology is ideally positioned to shape future outcomes, support stakeholders, and have an economic impact. We're working on a long-term digital transformation strategy. The SDGs are critical for human development and progress, and the ICT sector's commitment to achieving them reflects the concept of "business as a force for good" (Sunil Mittal 2020). The mobile industry's accomplishments were highlighted in this fifth annual SDG impact report. Individuals all throughout the world rely on mobile technology as their primary – and often only – means of digital access. All 17 SDGs have benefited from greater mobile connectivity and on-demand digital services. Actions and mobilisation after COVID-19 are critical for safeguarding progress

made since 2015 and advancing the 2030 Agenda. In 2019, the mobile services industry's global influence on the SDGs grew. 1.6 billion Mobile members are improving or monitoring their health, up 330 million from last year. Customers use mobile banking services in 2.3 billion, up 620 million from 2018.

The economy, society, and ecology have all benefited from mobile connectivity. Mobile connectivity has increased global GDP by $360 billion, or 4%, since 2015. During that time, the industry supported 30 million people globally, adding 5 million jobs in the process. Mobile technology has cut GHG emissions by ten times the carbon footprint of the mobile industry. The mobile industry's (GSMA, Mobile Industry Impact-Report SDGs.pdf, 2021) ability to achieve SDG 9: industry, innovation, and infrastructure are aided by mobile network coverage.

The mobile sector made the greatest contribution to SDG 4: good education. In 2019, 610 million additional people used mobile to access education for themselves or their children, bringing the total number of people who utilised mobile to 2 billion (equivalent to 40 percent of mobile subscribers). The impact (GSMA, 2020 Mobile Industry SDG Impact Report, 2020) of the SDGs is increased when people use their phones. We estimate that the mobile industry and its partners will only achieve 70% of their entire SDG impact by 2030 unless they move faster.

Dynamics of Mobile Industry in achieving Sustainable development Goals

Mobile technology &SDG 1No Poverty

SDG 1 aims to alleviate poverty, improve economic access, and strengthen poor resilience. In 2019, 8.2 percent of people lived in extreme poverty, down from 15.7 percent in 2010, while the rate of decline has slowed and is likely to climb for the first time in two decades as a result of COVID-19. Mobile technology aids in the emancipation of families from poverty and facilitates humanitarian relief. Since 2015, 200 million additional disadvantaged people have used cell phones. Mobile technology boosts productivity and efficiency. It enables rural and non-rural businesses, particularly SMEs, to grow and create new jobs by reaching out to more customers in non-local markets. Smartphone help to alleviate poverty. Peru's proliferation of mobile phones reduced extreme poverty by 5.4 percent. 59 Nigeria's workforce participation increased by 7%, while extreme poverty decreased by 7% as a result of mobile broadband networks. Families may save money and weather job loss, illness, and environmental (GSMA, 2020 Mobile Industry SDG Impact Report, 2020) and economic calamities with the help of mobile money. Mobile money users in Burkina Faso save three times more than non-users. In Tanzania, 57 mobile money users could totally mitigate the impact of a rainfall on consumption.

Mobile technology &enabling humanitarian assistance

The poor will be less exposed to extreme weather caused by climate change, as well as other economic, social, and environmental shocks and disasters, by 2030. Mobile networks are required for disaster response and risk mitigation. Operators and humanitarian organisations can form partnerships to provide cash relief via mobile money, enhancing resilience and response. Emergency calls, emergency broadcasts, and disaster assistance coordination can all be aided by mobile services (GSMA, 2020 Mobile Industry SDG Impact Report, 2020). Operators and humanitarian organisations work together to give disaster-prone communities early warning signals.

Mobile technology &SDG 2 Zero Hunger

Ending hunger, improving nutrition, and promoting sustainable agriculture are all goals of SDG 2. Agricultural practises, nutritional awareness, and food security are all improved by mobile technology (Ray Walshe1, 2020). Agricultural (GSMA, Mobile Industry Impact-Report SDGs.pdf, 2021) efficiency is improved by mobile devices, satellites, drones, and other high-tech solutions. With rural mobile penetration in LMICs reaching 59 percent in 2019, SDG 2 had the second-highest industry effect in 2019. In 2019, 13% of rural customers used mobile agricultural services, while 27% used mobile finance services. Nutritional information is provided via mobile health services, allowing consumers to make healthier food choices. Dietary knowledge is higher among users of mobile health services than among non-users. 64 Mobile agriculture services provide advice on suitable agricultural techniques and weather forecasts to smallholder farmers, resulting in(GSMA, Mobile Industry Impact-Report SDGs.pdf, 2021) higher per-hectare yields.

Mobile technology &SDG 3 Good Health and Well-being

SDG 3 promotes health and happiness. Despite falling maternal and infant mortality. Mobile technology improves health care funding, delivery, training, the health information system, and early disease detection using analytics. Limited-resource areas need digital health care solutions. Since 2015, SDG 3 has had the second-most impact on business. 32% of mobile users tracked and improved (Rotondi, 2020) their health worldwide in 2019. This is a 900 million increase from 2015. By 2019, there will be 745 million wearables and 500,000 IoT health connections. (Up 45 percent since 2015).

Mobile technology &SDG 4 Quality Education

SDG 4 wants to make sure that everyone can get a good education and keep learning throughout their lives. Even though more children are going to school, there are still 770 million people who can't read or write. Women make up two-thirds of the population. SDG 4 is aided by mobile technology because students, teachers, and employees may learn and teach from anywhere. Tablets, smart phones, and basic phones are increasingly being used for school administration and management (Méndez, 2018). In terms of business, SDG 4 has changed the most since 2015. Educational services are available to over 2 billion mobile consumers. It has increased by 1 billion since 2015. Mobile phone users account for 1.5 billion people who have access to government services (an increase of 958 million users since 2015). Mobile technology can aid education by allowing more people to access the internet. E-learning can aid in the expansion of ICT and the closing of the digital divide. Teachers can profit from mobile technology since it provides new digital tools. During crises like the COVID-19 pandemic, which kept 90 percent of students out of school, e-learning is extremely successful.(GSMA, Mobile Industry Impact-Report SDGs.pdf, 2021).

Mobile technology &SDG 5 Gender Equality

SDG 5 emphasises women's empowerment and equality. Women now have more chances and access to technology thanks to the Beijing Declaration, which was signed 25 years ago. 1.4 billion Girls and women live in countries where they do not have the same rights as males. 1.4 billion People reside in countries that are considered "borderline." By making it easier for women to acquire and utilise mobile technology and by empowering more women, the mobile sector contributes to the achievement of SDG 5. Women benefit economically and socially from smart phones (Bhandari, 2019). There are 90 million more female cell phone users in 2019 than in 2014. More than half of adult females use a mobile device to access the internet (1.2 billion). Most women believe that cell phones make them feel safer, that they help them at work, and that they provide information. For women, their communities, businesses, and the economy, mobile technology fosters social, economic, and political equality. Mobile phones allow people to get health information, financial services, and career opportunities. When 5G and AI arrive, women and girls will not be able to just be online. 90% of today's jobs are digital. To achieve online equality with men, women must use modern technology. Women's digital literacy (GSMA, Mobile Industry Impact-Report SDGs.pdf, 2021) and advanced abilities can aid their job search in the ICT and digital economy.

Mobile technology &SDG 6 & 7 Clean Water and Sanitation & Affordable and Clean Energy

SDGs 6 and 7 strive to provide electricity, water, and sanitation that is affordable, reliable, sustainable, and modern. In 2017, 785 million people lacked access to safe drinking water, and 3 billion lacked hand washing facilities (SDG 7). In 2018, 789 million people were without electricity, with 85 percent of them living in rural areas. By allowing utilities or municipalities to receive client payments via mobile technologies, water delivery and sanitation are improved. It makes remote, low-cost charging for non-sewered sanitation services much easier (Schroeder, 19). PAYG energy options have risen as mobile money and connectivity has increased, allowing households to purchase solar devices with low-cost financing. Africa sold 4.2 million pay-as-you-go solar units in 2019, up 48 percent from 2018. 100 In the areas of clean cooking, agriculture, and water, new PAYG models have evolved. Emerging water and sanitation providers are struggling to recoup expenses and establish a sustainable business model. Every year, $260 billion is spent on water and sanitation challenges. 101 When sales aren't enough to finance upkeep and growth, customers suffer. Data loss is reduced through smart metres and digital payments. These improve service availability, customer service, and willingness to pay.(GSMA, 2020 Mobile Industry SDG Impact Report, 2020)

Mobile technology & SDG 8: Decent Work and Economic Growth

SDG 8 encourages economic growth, employment creation, and decent work. In recent years, both real GDP per capita and labour productivity have increased by 2%. Mobile technology enables MSMEs to reach out to more customers and sell more in non-local markets, resulting in the creation of local jobs. Mobile improves client access to product information and company interaction, boosting trade and competition. Labour and capital are both increased as a result of mobile technologies. According to the ITU, a 10% increase in mobile broadband penetration boosts GDP by 1.5–2.5%. Upgrades from 2G to 3G and 4G boost mobile's economy (Heirman, 2021). In 2019, mobile technology contributed $4.1 trillion to global GDP. The informal economy is formalised and boosted by mobile technologies. By transferring monies into the official system, mobile banking helps to support monetary policy. Using resources from the formal sector improves macroeconomic stability. Mobile carriers directly employed 16 million people in 2019 and supported 14 million jobs indirectly. 112 Mobile internet and mobile-enabled platforms increase productivity, create jobs, and make entrepreneurship easier(GSMA, Mobile Industry Impact-Report SDGs.pdf, 2021).

Mobile technology &SDG 9: Industry, Innovation and Infrastructure

SDG 9 encourages infrastructure resilience, inclusive and sustainable industrialization, and innovation. Its goal is to offer LDCs with widespread, low-cost internet connectivity. Mobile technology contributes to SDG 9 as a crucial infrastructure and a sector accelerator. Industrial operations and production (Tomaselli, 2019) can profit from connectivity-enabled technological advancements. The industry also promotes cutting-edge research and development, as well as the creation of 5G-enabled services with low latency and high bandwidth.(GSMA, 2020 Mobile Industry SDG Impact Report, 2020)

Mobile technology &SDG 10: Reduced Inequalities

SDG 10 reduces inequality within and between nations. 84 countries' figures show that income disparity reduced in 38 and climbed in 25. The world's richest 0.9% holds 43.9% of its wealth, while 56.6% own less than 2%. Mobile technology supports SDG 10 by reducing remittance costs and improving relief distribution. Mobile money remittances climbed to $7.3 billion in 2019 from $5.5 billion in 2018 and are currently available in 184 corridors. 127 Because mobile is so popular, people with impairments and in humanitarian circumstances can access life-changing products and services. 60% of the world's poorest countries128 have mobile phones, up 200 million since 2015(Hackl, 2018). 361 million more impoverished people utilise mobile internet since 2015. PWDs endure more socioeconomic challenges and prejudice than non-disabled people. Disasters affect disabled individuals disproportionately. 130 Assistive mobile devices and services enable people live healthier, more productive, independent, and dignified lives by facilitating access to healthcare, education, labour markets, and civic participation.(GSMA, 2020 Mobile Industry SDG Impact Report, 2020)

Mobile technology &SDG 11: Sustainable Cities and Communities

SDG 11 focuses on safe, resilient, and sustainable cities. One-quarter of city dwellers live in slums and informal settlements due to urbanisation and population growth. 140 3 billion people will need housing by 2030, says the UN. Over 90% of the world's population breathes polluted air, according to the WHO(Leal Filho, 2020). Data analytics, edge computing, and fast connections enable smart traffic and cities, allowing governments to ensure safe, reliable public transit and reduce air pollution. This helps SDG 11. In a disaster or environmental concern, operators provide emergency broadcast systems and emergency communication. In 2019, only half of city residents have reliable public transit. 142 Smart ride-sharing, scheduling, smart traffic signal control, and air monitoring can make transportation systems more eco-friendly.

Mobile technology &SDG 12: Responsible Consumption and Production

SDG 12 focuses on sustainable consumption and production. In 2017, the global material footprint was 92 billion metric tonnes. Per capita, this is 1,250 percent more expensive than in low-income countries. 150 Without political action, the UN estimates that by 2060, this will have risen to 190 billion metric tonnes. Through recycling facilities, awareness programmes, and policy initiatives, mobile technology and mobile operators contribute to SDG 12's e-waste management targets(Whitaker, 2020). Circularity as a service is being utilised to complete the loop on end-of-life trash handsets in developing countries, where over 1 billion devices will reach the end of their useful lives without their owners having access to a recycling facility or service. In 40 countries, mobile carriers are leading 67 e-waste management initiatives, with 43 of them setting up collection stations in their offices and customer contact centres. More than simply plastic recycling can be aided by mobile technologies.

Mobile technology &SDG 13: Climate Action

Climate action must be taken quickly, according to SDG 13. The warmest decade ended with the second warmest year on record. The world is not on track to fulfil the 1.5°C or 2°C goals set out in the Paris Agreement. To avoid catastrophic effects, the globe must cut emissions in half by 2030. Despite COVID-19's significant reduction in human activity, the projected 6% reduction in emissions for 2020 is insufficient, and emissions are expected to climb once restrictions are relaxed(Lens, 2021). Connectivity, efficiency, and behaviour are all improved by mobile technology, which also cuts emissions. Decarbonisation necessitates the use of linked devices. 30 percent of worldwide mobile connections are represented by 29 mobile operator organisations. Over 50 mobile operators, accounting for two-thirds of all mobile connections worldwide, disclose data on climate, energy, and greenhouse gas emissions (CDP). In collaboration with the ITU, GeSI, and SBTI, the GSMA developed an ICT decarbonisation strategy. This allows ICT companies to define climate-related scientific goals (SBTs).

Mobile technology &SDG 14 & 15: Life below Water & Life on Land

Oceans, seas, and their resources are included by SDG 14. Oceans are vital to life and have a significant impact on global weather patterns. By 2050, the ocean will have more plastic than fish, and an increase in acidity of 100–150 percent will kill half of all marine species. 166 SDG 15 promotes land use sustainability. It advocates for long-term forest management, as well as the abolition of desertification, land degradation, and biodiversity loss. 100 million hectares of forest have been lost in the last 20 years(Chand, 2021). SDG 14 is aided by mobile

technology because it allows people to record and retrieve information. SDG 15 allows for the rehabilitation of terrestrial ecosystems through sensor-based and machine-to-machine communication services. Underwater life is supported by digital software and smart equipment. Despite weak underwater transmissions, the mobile industry helps coastal ecosystems. It delivers cost-effective biodiversity monitoring platforms. This is necessary for SIDS, LDCs, and hand-fishers.

Mobile technology &SDG 16: Peace, Justice and Strong Institutions

DG 16 advocates for peaceful, inclusive communities, universal access to justice, and effective, accountable, and transparent institutions. Mobile technology helps to achieve SDG 16 by facilitating information access and free speech. For disadvantaged people, a mobile digital ID is a reliable choice. These items make it possible for people to participate in social and economic life while also making themselves visible to governments. In countries where there are few IDs, governments prioritise reforms and investments in identification infrastructure, such as birth registration. Electronic IDs are used in 161 countries(Corneloup, 2021). Mobile network carriers can check user IDs against a government database or credential in 19 of 155 countries with SIM registration (12 percent). Enrolling, locating, and communicating with the poor for cash transfer programmes is tough. Social protection and money transfers are aided by digital tools. The ability to review recipient information is made easier by digital registration, and transparent, targeted funding reduces corruption and expedites aid delivery. In 2018, cash transfers accounted for more than half of all social security funds. Institutions indirectly alleviate poverty. Cash-transfer households escaped poverty in 36% of cases. Authorities can track data traces left by mobile money transfers.

Mobile technology &SDG 17: Partnerships for the Goals

The goal of SDG 17 is to strengthen the global sustainable cooperation. To improve the SDGs, the public and commercial sectors must work together. Through public-private and cross-sector collaboration, the mobile industry contributes more to the SDGs. Mobile phone usage charges contribute to the funding of public initiatives. VAT, corporate tax, income tax, and employee and employer social security payments are all included in most countries. The industry paid $500,000,000,000 in taxes in 2019(Wu, 2018). 186 Governments may use mobile technologies to get more money and spend it more effectively. Taxes, school fees, and traffic fines can all be digitised to help countries become more organised and grow. It creates auditable and transparent spending records. Governments can reach out to more people and save money and time by using mobile money. More people applied to Senegal's Customs School after the costs of the entrance exam were made public online. This is most likely due to rural candidates' desire to save money on travel expenses.

India & SDGs

India's GDP could reach $10 trillion by 2030. According to the World Bank, increasing fixed broadband coverage by 10% will improve GDP by 1.38 percent in developing nations. Telecom can help the United Nations achieve its Sustainable Development Goals (SDGs) (SDGs). Mobile technology (1+ billion mobile connections), biometric identity via Aadhar (1+ billion UID cards), and bank accounts (250+ million Jan dhan accounts) could all help India achieve the SDGs more quickly. India ranks 117th on the Social Progress Index(Srivastava, 2018). BharatNet fibre should be extended to all gram panchayats, internet speeds should be increased (from 512 Kbps to 8 Mpbs, the global average), and millions of Wi-Fi hotspots should be installed, among other things. This could open up a trillion-dollar market for data and video applications in areas such as digital learning, e-health, e-governance, digital banking and payments, agriculture, logistics, smart grids, and water management, among others. Digital India's ambition of a knowledge economy and a digitally enabled society will be realised. India's one-sixth of the world's population is required for the 2030 Agenda. In India's second VNR; subnational and local governments, civil society, local communities, vulnerable persons, and businesses are all involved. Sabkasaath Sabka Vikaas is India's SDG mantra (Collective Efforts for Inclusive Growth). SDGs have been endorsed, implemented, and tracked via mobile devices at the state and district levels. Due to economic advancement and empowerment, 271 million Indians have been lifted out of poverty. Nutrition, child health, education, and sanitation have all benefited from the mobile industry, as have water, power, and housing. Ensure that everyone has access to the same nutrition, health, education, social protection, entrepreneurial abilities, and work skills. JAM has given the poor, including over 200 million women, new ways to obtain credit, insurance, and direct cash transfers (DBT), giving them greater economic power, and mobile technology plays a key part in all of these industries. Renewable energy, disaster-resistant infrastructure, and environmental restoration are among India's climate action priorities. India has reduced CO2 emissions by 38 million tonnes per year and provided clean cooking fuel to 80 million underprivileged people. India's mobile seva effort provides people with effective services at their doorsteps, which are made feasible through mobile technology (GSMA, 2020 Mobile Industry SDG Impact Report, 2020). India's young population and thriving business and innovation ecosystem aid the country's rapid development. By 2025, India seeks $5 trillion. GDP for 2018-19 is $2.72

trillion. It intends to do so through increasing manufacturing, expanding infrastructure, increasing investment, stimulating technical innovation, and encouraging entrepreneurship through mobile technology. The India-United Nations Development Partnership Fund helps developing countries implement the 2030 Agenda. India is confident since it has already conquered challenges. With domestic and foreign partners, India will build a long-term future.

Conclusion

Mobile technology was once a technological marvel, but now it is a user-friendly tool thanks to its multiple functionalities. SMS calls and games were the earliest uses of mobile phones. It's now a digital world, which has simplified life and business; marketers can quickly offer products via mobile devices. Since their development, mobile phones have aided humanity in a variety of ways, including saving lives in accidents and other situations. Safety is ensured by smart phones. While travelling, families can converse. Mobile technology is here to stay, and it will continue to evolve to meet our basic needs and make our lives easier. SDGs in Action are a smartphone app that keeps you up to date on the UN's Sustainable Development Goals. Education and local action are required to accomplish the Sustainable Development Goals (SDGs) by 2030. Because local is global, this article demonstrated how mobile technology can educate and empower individuals to achieve the SDGs in their local communities.

By putting connections in our hands, mobile technology has helped businesses and society develop. Mobile is no longer a luxury for billions of people who want to communicate or access the internet. It is the primary means of obtaining life-improving and life-saving services. It benefits the digital economy by facilitating payments and smart infrastructure, and it supports in the fight against climate change. The COVID-19 pandemic has demonstrated the importance of connectivity. People who do not understand digital technology are falling further behind as a result of COVID-19. To retain recent advancements, the mobile industry must collaborate with governments, other industries, civil society, and the international community. As the Decade of Action begins, the mobile industry and its stakeholders must be prepared to harness mobile's full potential to address the world's most pressing issues.

Declaration of Competing Interest

The authors declares explicitly that he has no known competing financial interests or personal affiliations with third parties that could have influenced the work presented in this study.

Acknowledgements

The author's wishes to convey their heartfelt gratitude to the anonymous reviewers for their insightful remarks and suggestions that helped improve the overall quality of this research.

References

Bhandari, A. (2019). Gender inequality in mobile technology access: The role of economic and social development. Information, Communication & Society, 22(5), 678-694.

CDMA. (2020) the Sustainable Development Goals Repo rt 2020. www.Unstats.Un.Org.https://unstats.un.org/sdgs/report/2020/The Sustainable Development-Goals-Report-2020.pdf rretrievedon 21 April 2022.

Chand, A. A., Lal, P. P., Prasad, K. A., & Mamun, K. A. (2021). Practice, benefits, and impact of personal protective equipment (PPE) during COVID-19 pandemic: Envisioning the UN sustainable development goals (SDGs) through the lens of clean water sanitation, life below water, and life on land in Fiji. Annals of Medicine and Surgery, 70, 102763.

Corneloup, S., & Verhellen, J. (2021). Peace, justice and strong institutions. In The Private Side of Transforming our World UN Sustainable Development Goals 2030 and the Role of Private International Law (pp. 505-540). Intersentia.

Del Cerro Velázquez, F., & Morales Méndez, G. (2018). Augmented reality and mobile devices: A binominal methodological resource for inclusive education (SDG 4). An example in secondary education. Sustainability, 10(10), 3446.

GSMA. (2017) Mobile Industry Impact Report. www.Gs ma.Com. https://www.gsma.co betterfuture/mobil e-industry-impact-report retrieved on 16, May 2022.

Hackl, A. (2018). Mobility equity in a globalized world: Reducing inequalities in the sustainable development agenda. World development, 112, 150-162.

Heirman, K. A., Gill, J. C., & Caven, S. (2021). Decent Work and Economic Growth. In Geosciences and the Sustainable Development Goals (pp. 183-207). Springer, Cham.

Leal Filho, W., Marisa Azul, A., Brandli, L., Gokcin Ozuyar, P., & Wall, T. (Eds.). (2020). Sustainable Cities and Communities. Cham: Springer International Publishing.

Lens, P. N. (2021). RESB: 20 years of environmental science and bio/technology for sustainable development. Reviews in Environmental Science and Bio/Technology, 20(1), 1-3.

R. W. K. C. et. al (2020, April 23). AI and Big Data Standardization: Contributing to

United Nations Sustainable Development Goals. www.Journals.Riverpublishers.Com. https://journals.riverpublishers.com/index.php/JICTS/article/download/2641/1735?inline=1 retrieved on 21, April 2022.

Rotondi, V., Kashyap, R., Pesando, L. M., Spinelli, S., & Billari, F. C. (2020). Leveraging mobile phones to attain sustainable development. Proceedings of the National Academy of Sciences, 117(24), 13413-13420.

Schroeder, P., Anggraeni, K., & Weber, U. (2019). The relevance of circular economy practices to the sustainable development goals. Journal of Industrial Ecology, 23(1), 77-95.

Srivastava, A. (2018). Standardizing evaluation process: necessary for achieving SDGs–a case study of India. Evaluation and Program Planning, 69, 118-124.

Tomaselli, M. F., Timko, J., Kozak, R., Bull, J., Kearney, S., Saddler, J.& Zhu, X. (2019). SDG 9: industry, innovation and infrastructure–anticipating the potential impacts on forests and forest-based livelihoods. Sustainable Development Goals: Their Impacts on Forests and People. Cambridge University Press, United Kingdom, 279-314.

Walshe, R., Casey, K., Kernan, J., & Fitzpatrick, D. images SDG 2: Zero Hunger.

Whitaker, M., & Pawar, P. (2020, April). Commodity Ecology: A Virtual Community Platform for Promoting Responsible Consumption and Production to Achieve SDG# 12. In 2020 IEEE Green Technologies Conference (Genentech) (pp. 59-61). IEEE.

Wu, J., Guo, S., Huang, H., Liu, W., & Xiang, Y. (2018). Information and communications technologies for sustainable development goals: state-of-the-art, needs and perspectives. IEEE Communications Surveys & Tutorials, 20(3), 2389-2406.

Yang, Jie Chi, and Yi Lung Lin. "Development and evaluation of an interactive mobile learning environment with shared display groupware." *Journal of Educational Technology & Society* 13, no. 1 (2010): 195-207.

Journal of Technology Innovations and Energy
https://doi.org/10.56556/jtie.v1i2.113
ISSN: 2957-8809

RESEARCH ARTICLE

The Basic Concept of Cyber Crime

Osman Goni*[1], Md. Haidar Ali[1], Showrov[1], Md. Mahbub Alam[1], Md. Abu Shameem[1]

[1]Computer System and Network Division (CSND), Institute of Computer Science (ICS), Atomic Energy Research Establishment, Bangladesh Atomic Energy Commission, E-12/A, Agargaon, Sher-e-Bangla Nagar, Dhaka-1207, Bangladesh

Corresponding Author: Osman Goni , engr.osmangoni@yahoo.com
Received: 12 March, 2022, Accepted: 27 March, 2022, Published: 01 April, 2022

Abstract
Cyber Crime is a common phenomenon in the world. Cyber Crime is that group of activities made by the people by creating disturbance in network, stealing others important and private data, documents, hack bank details and accounts and transferring money to their own. Cyber Crime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government. Cybercrime**,** also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, Trafficking in child pornography and intellectual property, stealing identities, or violating privacy. The cybercrime and they its impacts over the society in the form of economical disrupt, psychological disorder, threat to National defense etc. Restriction of cyber-crimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society. Now a day's Cybercrime is increasing day by day. People have been greatly suffering for it. It is not only creates human suffering but also put effect on it. So Cyber Crime is one of the major crimes done by computer expert. This paper gives the basic concept of cybercrime.

Keywords: Cyber Crime; Criminal; Child Pornography; Computer Crime; Human Suffering

Introduction

Cyber Crime is not an old sort of crime to the world. It is defined as any criminal activity which takes place on or over the medium of computers or internet or other technology recognized by the Information Technology Act. There are number of illegal activities which are committed over the internet by technically skilled criminals. Taking a wider interpretation, it can be said that, Cyber Crime includes any illegal activity where computer or internet is either a tool or target or both. Cyber Crime is an uncontrollable evil having its base in the misuse of growing dependence on computers in modern life. Usage of computer and other allied technology in daily life is growing rapidly and has become an urge which facilitates user convenience. It is a medium which is infinite and immeasurable. Some of the newly emerged cybercrimes are cyber-stalking, cyber-terrorism, e-mail spoofing, e-mail bombing, cyber pornography, cyber-defamation etc. Some conventional crimes may also come under the category of cybercrimes if they are committed through the medium of computer or Internet (Chaubey, 2012). Cybercrime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial-of-service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity. The Cyber Crime can halt any railway where it is, it may misguide the planes on its flight by misguiding with wrong signals, it may cause any important military data to fall in the hands of foreign countries, and it may halt e-media and every system can collapse within a fraction of seconds (Nayak, October 2013). Cybercrime is growing and current technical models to tackle cybercrime are inefficient in stemming the increase in cybercrime. This serves to indicate that further preventive strategies are required in order to reduce cybercrime. Just as it is important to understand the characteristics of the criminals in order to understand the motivations behind the crime and subsequently develop and deploy crime prevention strategies, it is also important to understand victims, i.e., the characteristics of the users of computer systems in order to understand the way these users fall victim to cybercrime. Current era is too fast to utilize the time factor to improve the performance factor. It is only possible due the use of Internet. The term Internet can be defined as the collection of millions of computers that provide a network of electronic connections between the computers. There are millions of computers connected to the internet. Everyone appreciates the use of Internet but there is another side of the coin that is Cyber Crime by the use of Internet (Hemraj Saini, 2012). Cyber Crime is a bi-product of the ever-increasing development in the

areas of information and communication technology (ICT). The attackers mainly attack the confidential data of the organizations or personal information thereof. The most targeted organizations are hospitals, government offices, police stations, financial. institutions, Research and Development (R&D) organizations and other telecommunication firms etc (Shusmoy Kundu1, 2018).

Literature Review

Cyber Criminal

Cyber criminals are an ever-present menace in every country connected to the Internet. The cyber criminals constitute of various groups or category as shown below;

Children and Adolescents

The simple reason for this type of delinquent behavior pattern in children is seen mostly due to the inquisitiveness to know and explore the things. Other cognate reasons may be to prove themselves to be outstanding amongst other children in their group.

Organized Hackers

These kinds of hackers are mostly organized together to fulfill certain objective. The reason may be to fulfill their political bias, fundamentalism, etc. The Chinese are said to be one of the best quality hackers in the world. They mainly target the other governments' sites with the purpose to fulfill political objectives.

Professional Hackers/Crackers

These kinds of hacker's work are motivated by money and mostly employed to hack the site of the rivals and get credible, reliable and valuable information. Further they are employed to crack the system of the employer basically as a measure to make it safer by detecting the loopholes.

Discontented Employees

This group includes those people who have been either sacked by their employer or are dissatisfied with their employer. Traditionally, internal attacks posed the greatest threat to computer networks, which accounted for about 70 percent of all attempted intrusions (Brigadier General Md. Khurshid Alam).

Cyber Crime

Dr. Debarati Halder and Dr. K. Jaishankar define cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS) (2016)." The oxford Dictionary defined the term Cyber Crime as "Criminal activities carried out by means of computers or the Internet (2016)." "Cyber Crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime (2016)." "Cyber Crime means any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them (2016)." Cybercrime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial-of-service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity. The Cyber Crime can halt any railway where it is, it may misguide the planes on its flight by misguiding with wrong signals, it may cause any important military data to fall in the hands of foreign countries, and it may halt e-media and every system can collapse within a fraction of seconds (Nayak, October 2013).

Categories of Cyber Crime

There are a lot of Cyber Crime categories; these categories include different terminology and iconography that create controversy over the computer attacker terms.

Data Crime

Data Interception, Data Modification, and Data Theft are called Data Crime. An attacker monitors data streams to or from a target in order to gather information. This attack may be undertaken to gather information to support a later attack or the data collected may be the end goal of the attack. This attack usually involves sniffing network traffic, but may include observing other types of data streams, such as radio. In most varieties of this attack, the attacker is passive and simply observes regular communication, however in some variants the attacker may attempt to initiate the establishment of a data stream or influence the nature of the data transmitted. Privacy of communications is essential to ensure that data cannot be modified or viewed in transit. Distributed environments bring with them the possibility that a malicious third party can perpetrate a computer crime by tampering with data as it moves between sites. In a data modification attack, an unauthorized party on the network intercepts data in transit and changes parts of that data before retransmitting it. Data Theft used to describe when information is illegally copied or taken from a business or other individual. Commonly, this information is user information such as passwords, social security numbers,

credit card information, other personal information, or other confidential corporate information. Because this information is illegally obtained, when the individual who stole this information is apprehended, it is likely he or she will be prosecuted to the fullest extent of the law (Nayak, October 2013).

Network Crime

Unauthorized Access and Virus Dissemination are called Network Crime. "Unauthorized Access" is an insider‘s view of the computer cracker underground. The filming took place all across the United States, Holland and Germany. "Unauthorized Access" looks at the personalities behind the computers screens and aims to separate the media hype of the 'outlaw hacker' from the reality (2012). Malicious software that attaches itself to other software. (Virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are examples of malicious software that destroys the system of the victim (Virus Glossary (2006), 2012).

Related Crimes

Aiding and Abetting Cyber Crimes, Computer-Related Forgery and Fraud and Content-Related Crimes are called Related Crime. There are three elements to most aiding and abetting charges against an individual. The first is that another person committed the crime. Second, the individual being charged had knowledge of the crime or the principals' intent. Third, the individual provided some form of assistance to the principal. Computer forgery and computer-related fraud constitute computer-related offenses. Cyber-sex, unsolicited commercial communications, cyber defamation and cyber threats are included under content-related offenses. The total cost to pay by victims against these attacks is in millions of millions Dollar per year which is a significant amount to change the state of un-developed or under-developed countries to developed countries (Legal Info (2009), 2012) (Shantosh Rout (2008), 2012) (By Jessica Stanicon (2009), 2012).

Types of Cyber Crime

There are many types of Cyber Crime. 1. Hacking, 2. Virus dissemination, 3. Logic bombs, 4. Denial-of-Service attack, 5. Phishing, 6. Email bombing and spamming, 7. Web jacking, 8. Cyber stalking, 9. Data diddling, 10. Identity Theft and Credit Card Fraud, 11. Salami slicing attack, 12. Software Piracy, 13. Cyber Pornography, 14. Sale of illegal articles, 15. Pharming 16.TOR Network

Hacking

In simple words, hacking is an act committed by an intruder by accessing your computer system without your permission. Hackers (the people doing the ‘hacking’) are basically computer programmers, who have an advanced understanding of computers and commonly misuse this knowledge for devious reasons. Hacking is the technique of finding the weak links or loopholes in the computer systems or the networks and exploiting it to gain unauthorized access to data or to change the features of the target computer systems or the networks. Hacking describes the modification in the computer hardware, software or the networks to accomplish certain goals which are not aligned with the user goals. In contrast, it is also called breaking into someone's security and stealing their personal or secret data such as phone numbers, credit card details, addresses, online banking passwords etc. (Aman Gupta, 4 April 2017).
Now the methodology or the path followed by the Hackers is as follows:

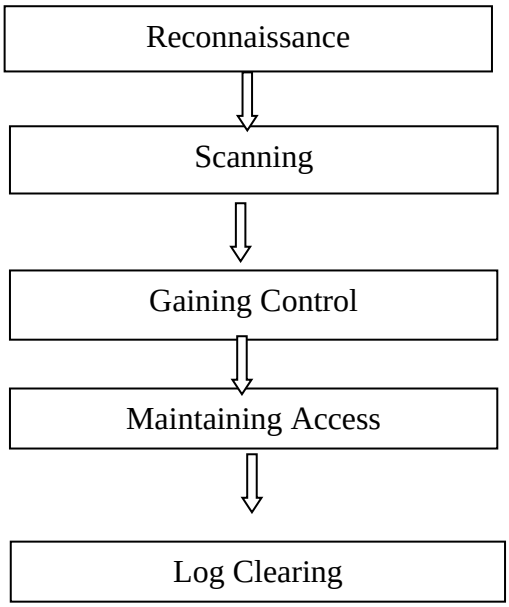


Figure:1. Block Diagram of the methodology or the path followed by the Hackers

Virus dissemination

Viruses are computer programs that attach themselves to or infect a system or files, and have a tendency to circulate to other computers on a network. They disrupt the computer operation and affect the data stored – either by modifying it or by deleting it altogether. "Worms" unlike viruses don't need a host to cling on to. They merely replicate until they eat up all available memory in the system. The term "worm" is sometimes used to mean self-replicating "malware" (MALicious softWARE). These terms are often used interchangeably in the context of the hybrid viruses/worms that dominative current virus scenario. "Trojan horses" are different from viruses in their manner of propagation.

Figure:2. A simple diagram to show how malware can propagate

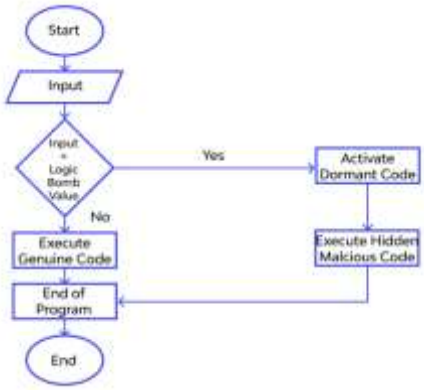
Logic bombs

A logic bomb, also known as "slag code", is a malicious piece of code which is intentionally inserted into software to execute a malicious task when triggered by a specific event. It's not a virus, although it usually behaves in a similar manner. It is stealthily inserted into the program where it lies dormant until specified conditions are met. Malicious software such as viruses and worms often contain logic bombs which are triggered at a specific payload or at a predefined time. The payload of a logic bomb is unknown to the user of the software, and the task that it executes unwanted. Program codes that are scheduled to execute at a particular time are known as "time-bombs". For example, the infamous "Friday the 13th" virus which attacked the host systems only on specific dates; it "exploded" (duplicated itself) every Friday that happened to be the thirteenth of a month, thus causing system slowdowns.

There's another use for the type of action carried out in a logic bomb "explosion" – to make restricted software trials. The embedded piece of code destroys the software after a defined period of time or renders it unusable until the user pays for its further use. Although this piece of code uses the same technique as a logic bomb, it has a nondestructive, non-malicious and user-transparent use, and is not typically referred to as one.

A logic bomb is a piece of malicious code that lies dormant and hidden within a legitimate software until a condition is satisfied to trigger its payload. This malware is normally embedded by developers into genuine software. A logic bomb has a flaw that it only works for a software for which it has been designed, it doesn't replicate on other applications. Presence of Logic bomb in system poses great risks to its security and integrity (Palash Sandip Dusane1, May - June 2020). Working of logic bomb code in a genuine code is shown in figure:

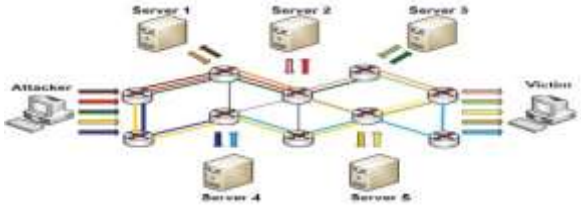
Figure:3. Working of Logic Bomb (Palash Sandip Dusane1, May - June 2020).



Denial-of-Service attack

A Denial-of-Service (DoS) attack is an explicit attempt by attackers to deny service to intended users of that service. It involves flooding a computer resource with more requests than it can handle consuming its available bandwidth which results in server overload. This causes the resource (e.g. a web server) to crash or slow down significantly so that no one can access it. Using this technique, the attacker can render a web site inoperable by sending massive amounts of traffic to the targeted site. A site may temporarily malfunction or crash completely, in any case resulting in inability of the system to communicate adequately. DoS attacks violate the acceptable use policies of virtually all internet service providers.

Figure:4. RDoS Principle (Obaid, March-2020).

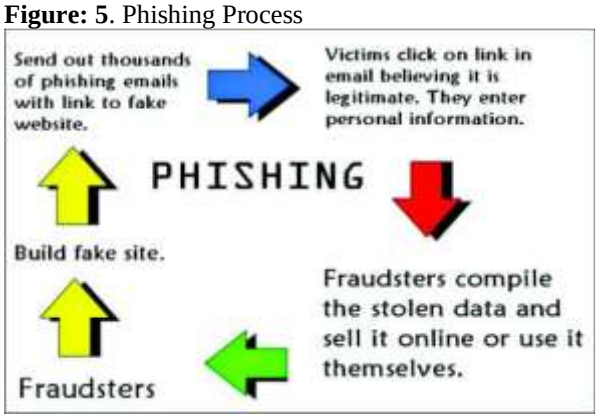


Another variation to a denial-of-service attack is known as a "Distributed Denial of Service" (DDoS) attack wherein a number of geographically widespread perpetrators flood the network traffic. Denial-of-Service attacks typically target high profile web site servers belonging to banks and credit card payment gateways. Websites of companies such as Amazon, CNN, Yahoo, Twitter and eBay! are not spared either.

Phishing

This a technique of extracting confidential information such as credit card numbers and username password combos by masquerading as a legitimate enterprise. Phishing is typically carried out by email spoofing. You've probably received email containing links to legitimate appearing websites. You probably found it suspicious and didn't click the link. Smart move.

Figure: 5. Phishing Process



The malware would have installed itself on your computer and stolen private information. Cyber-criminals use social engineering to trick you into downloading malware off the internet or make you fill in your personal information under false pretenses. A phishing scam in an email message can be evaded by keeping certain things in mind.

Email bombing and spamming

Email bombing is characterized by an abuser sending huge volumes of email to a target address resulting in victim's email account or mail servers crashing. The message is meaningless and excessively long in order to consume network resources. If multiple accounts of a mail server are targeted, it may have a denial-of-service impact. Such mail arriving frequently in your inbox can be easily detected by spam filters. Email bombing is commonly carried out using botnets (private internet connected computers whose security has been compromised by malware and under the attacker's control) as a DDoS attack. This type of attack is more difficult to control due to multiple source addresses and the bots which are programmed to send different messages to defeat spam filters. "Spamming" is a variant of email bombing. Here unsolicited bulk messages are sent to a large number of users, indiscriminately. Opening links given in spam mails may lead you to phishing web sites hosting malware. Spam mail may also have infected files as attachments. Email spamming worsens when the recipient replies to the email causing all the original addressees to receive the reply. Spammers collect email addresses from customer lists, newsgroups, chat-rooms, web sites and viruses which harvest users' address books, and sell them to other spammers as well. A large amount of spam is sent to invalid email addresses.

Web jacking

Web jacking derives its name from "hijacking". Here, the hacker takes control of a web site fraudulently. He may change the content of the original site or even redirect the user to another fake similar looking page controlled by him. The owner of the web site has no more control and the attacker may use the web site for his own selfish interests. Cases have been reported where the attacker has asked for ransom, and even posted obscene material on the site.

Web jacking can also be done by sending a counterfeit message to the registrar controlling the domain name registration, under a false identity asking him to connect a domain name to the webjacker's IP address, thus sending unsuspecting consumers who enter that particular domain name to a website controlled by the webjacker.

Figure 6: Detailed Overview of Web Jacking

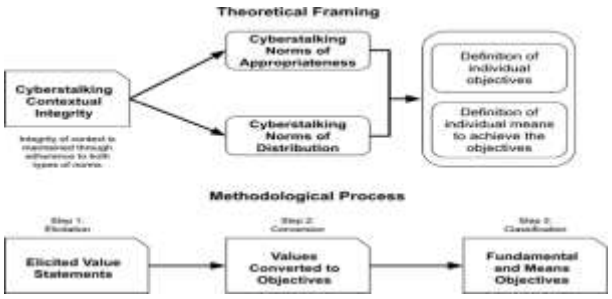
The purpose of this attack is to try to harvest the credentials, usernames, passwords and account numbers of users by using a fake web page with a valid link which opens when the user is redirected to it after opening the legitimate site.

Cyberstalking

Cyber stalking is a new form of internet crime in our society when a person is pursued or followed online. A cyber stalker doesn't physically follow his victim; he does it virtually by following his online activity to

harvest information about the stalkee and harass him or her and make threats using verbal intimidation. It's an invasion of one's online privacy.

Figure:7. Objectives for preventing Cyberstalking



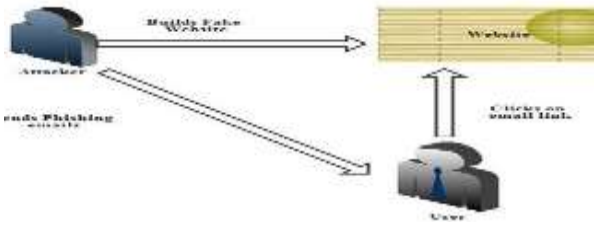
Cyber stalking uses the internet or any other electronic means and is different from offline stalking, but is usually accompanied by it. Most victims of this crime are women who are stalked by men and children who are stalked by adult predators and pedophiles. Cyber stalkers thrive on inexperienced web users who are not well aware of netiquette and the rules of internet safety. A cyber stalker may be a stranger, but could just as easily be someone you know.

The Internet has literally become a fertile breeding ground for an entirely new and unique type of criminal offender hereafter known as the cyber stalker. The cyber stalker is one who uses the Internet as a weapon or tool of sorts to prey upon, harass, threaten, and generate fear and trepidation in his or her victims through sophisticated stalking tactics, which for the most part, are largely misunderstood and in some cases, legal (Pittaro1, 2007).

Data diddling

Data Diddling is unauthorized altering of data before or during entry into a computer system, and then changing it back after processing is done. Using this technique, the attacker may modify the expected output and is difficult to track. In other words, the original information to be entered is changed, either by a person typing in the data, a virus that's programmed to change the data, the programmer of the database or application, or anyone else involved in the process of creating, recording, encoding, examining, checking, converting or transmitting data.

Figure 8: Data Diddling Attack

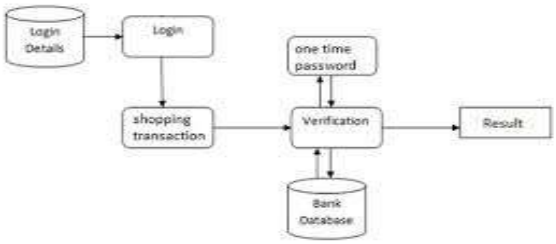


This is one of the simplest methods of committing a computer-related crime, because even a computer amateur can do it. Despite this being an effortless task, it can have detrimental effects. For example, a person responsible for accounting may change data about themselves or a friend or relative showing that they're paid in full. By altering or failing to enter the information, they're able to steal from the enterprise. Other examples include forging or counterfeiting documents and exchanging valid computer tapes or cards with prepared replacements. Electricity boards in India have been victims of data diddling by computer criminals when private parties were computerizing their systems.

Identity Theft and Credit Card Fraud

Identity theft occurs when someone steals your identity and pretends to be you to access resources such as credit cards, bank accounts and other benefits in your name. The imposter may also use your identity to commit other crimes. "Credit card fraud" is a wide-ranging term for crimes involving identity theft where the criminal uses your credit card to fund his transactions. Credit card fraud is identity theft in its simplest form. The most common case of credit card fraud is your pre-approved card falling into someone else's hands.

Figure 9: Credit Card Fraud System hidden Markov Model (Nabha Kshirsagar1, 2015).



With rising cases of credit card fraud, many financial institutions have stepped in with software solutions to monitor your credit and guard your identity. ID theft insurance can be taken to recover lost wages and restore your credit. But before you spend a fortune on these services, apply the no-cost, common sense measures to avert such a crime.

Salami slicing attack

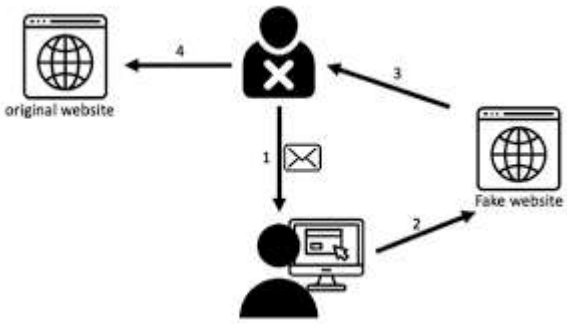
A "salami slicing attack" or "salami fraud" is a technique by which cyber-criminals steal money or resources a bit at a time so that there's no noticeable difference in overall size. The perpetrator gets away with these little pieces from a large number of resources and thus accumulates a considerable amount over a period of time. The essence of this method is the failure to detect the misappropriation. The most classic approach is "collect-

the-round off" technique. Most calculations are carried out in a particular currency are rounded off up to the nearest number about half the time and down the rest of the time. If a programmer decides to collect these excess fractions of rupees to a separate account, no net loss to the system seems apparent. This is done by carefully transferring the funds into the perpetrator's account.

Attackers insert a program into the system to automatically carry out the task. Logic bombs may also be employed by unsatisfied greedy employees who exploit their knowhow of the network and/or privileged access to the system. In this technique, the criminal programs the arithmetic calculators to automatically modify data, such as in interest calculations.

The attackers steal resources or money a little at a time in the salami technique. The important thing here is to make the change meaningless and no one will notice it completely. For example, an employee of bank installs a software into the servers of the bank, which takes a small amount of money from each customer's account. Every account holder isn't likely to notice this illegal deduction, but every month the attacker will make a substantial amount of money. The attacker installs malware on the server so that it performs a specific purpose, such as installing malware on the bank' server and its purpose is to deduct small values of money and send it to the attacker without giving an alert (Asalah F Altwairqi, December, 2019).

Figure:10. Salami Slicing Attack and Phishing Attack (Asalah F Altwairqi, December, 2019).



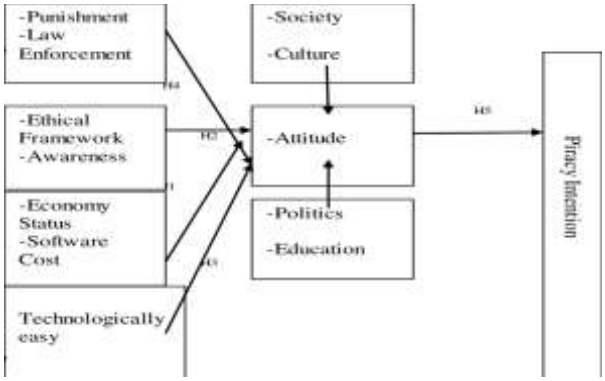
Stealing money electronically is the most common use of the salami slicing technique, but it's not restricted to money laundering. The salami technique can also be applied together little bits of information over a period of time to deduce an overall picture of an organization. This act of distributed information gathering may be against an individual or an organization.

Data can be collected from web sites, advertisements, documents collected from trash cans, and the like, gradually building up a whole database of factual intelligence about the target. Since the amount of misappropriation is just below the threshold of perception, we need to be more vigilant. Careful examination of our assets, transactions and every other dealing including sharing of confidential information with others might help reduce the chances of an attack by this method.

Software Piracy

We can find almost any movie, software or song from any origin for free. Internet piracy is an integral part of our lives which knowingly or unknowingly we all contribute to. This way, the profits of the resource developers are being cut down. It's not just about using someone else's intellectual property illegally but also passing it on to your friends further reducing the revenue they deserve.

Figure:11. Software Piracy ((PhD, October 2013).



Software piracy is the unauthorized use and distribution of computer software. Software developers work hard to develop these programs, and piracy curbs their ability to generate enough revenue to sustain application development. This affects the whole global economy as funds are relayed from other sectors which results in less investment in marketing and research.

Cyber Pornography

Pornography' is "describing or showing sexual acts in order to cause sexual excitement through books, films, etc." This includes pornographic websites; pornographic material produced using computers and use of internet to download and transmit pornographic videos, pictures, photos, writings etc. There are more than 420 million individual pornographic webpages today. Child pornography is a very unfortunate reality of the Internet. The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide (Vadza, 2013).

Child Sexual Abuse is more severe than any form of exploitation a girl child can encounter. This is because it can leave a severe and lasting impact on a girl child for the rest of their life. Further, Child pornography is considered to be different from adult pornography due to

intricacies involved. In child pornography, children are harmed not only in production process but also after publication of such pornography on internet, or via any other media. It attaches a taint on the future of children depicting them in bad light and characterizing them on social networking sites belonging to children who are below 18 years of age. Publication of their nude photos, either with their consent or fraudulently, affects the prospects of their development and it also affects their mental health .Therefore, in a country like India and Bangladesh where a considerable portion of the population consists of women and children, laws made in this regard must be essentially stringent and must at the same time cater to the varied social and cultural scenario pertinent .Moreover, the available statutory measures along with regulatory enforcement mechanism to churn out cyber pornography must be articulated keeping in light the rapid development of the internet and its ill-effects on the society and the innocent minds of the children (Joshi, 2021).

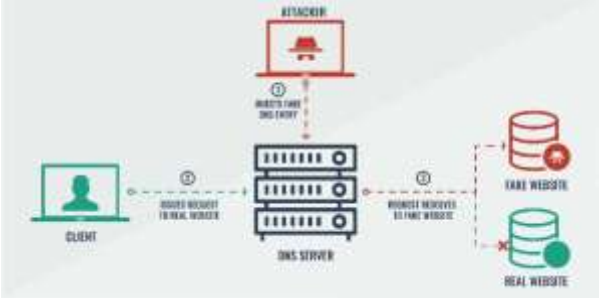
Sale of illegal articles

This would include trade of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication. Research shows that number of people employed in this criminal area. Daily peoples receiving so many emails with offer of banned or illegal products for sale (Vadza, 2013).

Pharming

Pharming is an attack expected to divert your site traffic to another, presumably false site. Pharming isn't effectively discernible on PC. Pharming is normally done by infecting DNS servers which is beyond control and stays undetectable for a large part. The main way pharming could have been done on your PC is by altering the host's file. In the event that the record contains false entries, at that point some program has attempted to perform pharming on your PC. Some site blocking software use the hosts file to map addresses to the localhost (Cyber Crime: Rise, 2020).

Figure:12. Pharming Attack.



TOR Network

This section depicts the noxious business activities recognized in the profound web, especially commercial centers and merchandise cyber-criminal exchange. In spite of the way that the entirety of the previously mentioned systems can possibly bolster unlawful exchanges of each sort, until now, the main system that appears to have increased some footing for underground commercial centers is TOR. The explanation for this might be connected to the way that TOR is relatively more experienced and more created than the opposition and has been endorsed by associations, like the Electronic Frontier Foundation as the first choice among hostile to restriction instruments, putting it under the spotlight as of late. The Deep Web and malware are consummately appropriate for one another, particularly with regards to facilitating order and-control (C&C) system. It is the idea of concealed administrations and destinations like TOR and I2P to shroud the area of servers using solid cryptography. This makes hard for forensic researchers to investigate using conventional methods like looking at a server's IP address, checking enlistment subtleties, etc. What's more, using these locales and administrations isn't especially troublesome. It is then to be expected to see various cybercriminals use TOR for C&C. We've seen the administrators behind predominant malware families use TOR for certain pieces of their arrangement. They basically group the authentic TOR customer with their installation package. Another major malware family that utilizes the Deep Web is Crypto Locker. Crypto Locker alludes to a ransom ware variation that encrypts victims very own reports before redirecting them to a site where they can pay to recover access to their documents. Crypto Locker is likewise keen enough to consequently alter the payment page to represent a victim's local language and means of payment. It shows why the Deep Web bids to 16 cybercriminals who are eager to make their foundations increasingly powerful to potential takedowns (Cyber Crime: Rise, 2020).

Conclusion

The future of the Internet is still up for grabs between criminals and normal users. Our reliance on networks will only continue to grow in the years ahead. This paper concludes with basic information of our privilege society which should aware about Cyber Crime. Based on an analysis of existing cyber-Crimes and privacy issues targeting about Cyber Crimes, a comprehensive framework is developed that provides an overview of possible security and privacy threats along with the ways of attacks and countermeasures. In the future, we are planning to apply the proposed framework in Cyber Crime to analyze the impact of the proposed approach in mitigating cyber privacy and security issues. Having identified and understood in clear terms the various cyber-Crimes to cyber security, caution is a watchword

for whoever is on the internet. Nevertheless, cyber security is potentially under the mercies of some common factors as explained in this journal article.

References

(2016, January 4). Retrieved January 4, 2016, from http://www.ripublication.com/irph/ijict_spl/ijictv4n3spl_06.pdf

(PhD, M. S.-T. (October 2013). Software Piracy: Some Issues. *Columbus State University, University Ave, Columbus.* 4225 University Ave, Columbus, GA, 31907.

(2012, January 28). Retrieved January 28, 2012, from http://www.imdb.com/title/tt0373414/

(2016, January 4). Retrieved January 4, 2016, from http://www.oxforddictionaries.com/definition/english/cybercrime

(2016, January 4). Retrieved January 4, 2016, from www.naavi.org/pati/pati_cybercrimes_dec03.htm

(2016, January 4). Retrieved January 4, 2016, from http://cybercrime.org.za/definition

Aman Gupta, A. A. (4 April 2017). Ethical Hacking and Hacking Attacks. *International Journal Of Engineering And Computer Science, 6*(4), 21042-21050.

Asalah F Altwairqi, M. A.-A. (December, 2019). Four Most Famous Cyber Attacks for Financial Gains. *International Journal of Engineering and Advanced Technology (IJEAT), 9*(2), 2131-2139.

Brigadier General Md. Khurshid Alam, n. p. (n.d.). CYBERCRIME IN BANGLADESH: IMPLICATIONS AND RESPONSE STRATEGY.

By Jessica Stanicon (2009). (2012, January 28). Retrieved January 28, 2012, from http://www.dynamicbusiness.com/articles/articles-news/one-in-five-victims-of-cybercrime3907.html

Chaubey, P. R. (2012). An Introduction to Cyber Crime and Cyber law. In P. R.K.Chaubey, *An Introduction to Cyber Crime and Cyber law.* Kamal Law House.

Cyber Crime: Rise, E. a. (2020, July 1). Retrieved July 1, 2020, from https://www.researchgate.net/publication/344349620

Hemraj Saini, Y. S. (2012). Cyber-Crimes and their Impacts: A Review. *2*(2).

Joshi, D. M. (2021). CYBER PORNOGRAPHY: AN INTERDISCIPLINARY STUDY OF TECHNOLOGY LED CRIME AGAINST WOMEN AND CHILDREN. *International Journal of Creative Research Thoughts (IJCRT), 9*(12), b297-b301.

Legal Info (2009), C. O. (2012, January 28). Retrieved January 28, 2012, from http://www.legalinfo.com/content/criminal-law/crime-overview-aiding-and-abetting-or-accessory. html

Nabha Kshirsagar1, N. P. (2015). Credit Card Fraud Detection System using Hidden Markov Model and Adaptive Communal Detection. *(IJCSIT) International Journal of Computer Science and Information Technologies, 6*(2), 1795-1797.

Nayak, S. D. (October 2013). IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES. *6*(2).

Obaid, H. S. (March-2020). Denial of Service Attacks: Tools and Categories . *International Journal of Engineering Research & Technology (IJERT), 9*(03), 631-636.

Palash Sandip Dusane1, Y. P. (May - June 2020). Logic Bomb: An Insider Attack. *International Journal of Advanced Trends in Computer Science and Engineering, 9*(3), 3662-3665.

Pittaro1, M. L. (2007). Cyber stalking: An Analysis of Online Harassment and Intimidation. *International Journal of Cyber Criminology. This work is licensed under a under a creative commons Attribution-Noncommercial-Share Alike 2.5 India License, 1*(2), 180–197.

Shantosh Rout (2008), N. I. (2012, January 28). Retrieved January 28, 2012, from http://www.santoshraut.com/ forensic/ cybercrime.htm

Shusmoy Kundu1, 2. K. (2018). Cyber Crime Trend in Bangladesh, an Analysis and Ways Out to Combat the Threat. Dhaka-1216, Bangladesh: International Conference on Advanced Communications Technology(ICACT).

Vadza, K. C. (2013). Cyber Crime & its Categories. *3*(5).

Virus Glossary (2006), V. D. (2012, January 28). Retrieved January 28, 2012, from http://www.virtualpune.com/citizen-centre/html/cyber_crime_glossary.shtml

Journal of Technology Innovations and Energy
https://doi.org/10.56556/jtie.v1i2.185
ISSN: 2957-8809

RESEARCH ARTICLE

Estimation of the Global Solar Radiation in Anyigba Kogi State Using Hargreaver And Samani

Ayodele S. Abdullateef*[1], Ohiani O. Alexander[1], Adeyemi O. John[1]. Papa M.A

[1]Department of Physics, Kogi State University, Anyigba, Kogi State-Nigeria

Corresponding author:Ayodele S. Abdullateef, ayabdullateef2020@gmail.com
Received: 03 March, 2022, Accepted: 03 April, 2022, Published: 04 April, 2022

Abstract
This work estimates the global solar radiation in Anyigba with latitude 7.498 using Hargreaves and Samani model. The average monthly global radiation for Anyigba was found to be 32 MJ/m^2 /day with a MBE of 15.6333 MJ/m^2 /day and RMSE OF 5.985 MJ/m^2 /day.

Keywords: Hagreave and Samani; Global Solar Radiation; Extraterrestrial Solar Radaiation; Clear Sky Index

Introduction

Having adequate information of the global solar radiation and other meteorological factors is important both in the field of solar energy and agriculture. Empirical models such as Angstrom-Prescott and Hargreaves and Samani model can be used to estimate global solar radiation. This is because many locations in developing countries do not have weather stations that record this meteorological factors such as temperature, humidity and global solar radiation (Abdu and Ayodele, 2016).
Solar radiation data is important in architectural design, solar energy design and irrigation system and crop growth (Okogbue and Adedokun, 2002). Most empirical models uses sunshine meteorological factor for the estimation of global solar radiation (Abdu and Ayodele, 2016). Temperature factor based models like Hargreaves and samani can also be used were temperature data is available.
Some related work includes the research conducted by Bernadetta, *et al* 2017, which involves testing of the performance of some empirical models. The model tested includes Garcia's model. This research was conducted in Makurdi using weather data between 1990-1991 and 1995 to 2003 (Jegede *et al*, 2017) where the global solar radiation month variation for the location was estimated.
Ayegba *et al*, used Hargreaves and Samani model to estimate the global solar radiation for Abuja using minimum and maximum temperature data between February 1-29, 2016, obtained from weather online limited . The maximum global radiation was estimated to be 29.60.609 MJ/m^2 / day.
Jegede *et al* 2017, estimated the monthly global solar radiation on Ida campus of Ida Federal polytechnic in Kogi State using maximum and minimum temperature data between July 1998 to June 30, 2015. It was observed that Hargreaves and Samani's model has their values of maximum global solar radiation more than Angstrom model's estimated global solar radiation. Therefore there is need to extend the use of Hargreaves and samani model beyond Ida and ascertain its suitability for other locations.

Aim

Aim of this study is to evaluate the global solar radiation in Anyigba, Kogi state, using Hargreaves and Samani Model, by obtaining the solar radiation data from the Centre for Atmospheric Research, determine the variability of solar radiation in Anyigba using Hargreaves and Samani then have better understanding of how solar radiation changes in different months of the year using this model.

Scope of the study

This study will be carried out in the geographical area of Anyigba with altitude of 420metres above sea level. Five (5) years solar radiation data (2011-2016) would be used for this work. The availability and variability of solar radiation will be analyzed using Hargreaves and Samani model.

Materials and method

In order to estimates the global solar radiation using Hargreaves and Samani model, solar radiation data from 2011 to December 2016 was obtained from the Centre for Atmospheric Research Centre (CAR), in Kogi State University Anyigba with coordinate 7.498 ^{0}N, 6.829^0 E. The data collected was recorded using Campbell weather station. Campbell weather station is powered using a solar panel and designed to work automatically unmanned for a longer time. It comes with an enclosed data logger,

pressure sensor and a 12 volt battery. Campbell weather instrument has a sensor which records the meteorological factors such as the solar radiation, wind speed, wind direction and soil temperature. The weather instrument records meteorological data automatically for 24 hours every day, and resolution of five minutes. The data was recorded in Watt per meter square (W/m^2). The solar radiation data obtained was sorted from hourly data to a monthly data solar radiation, a six year data of minimum and maximum temperature was obtained for the year 2011 to 2016. The minimum and maximum data of the temperature was used to obtained the global solar radiation using Hargreaves and Samani model as shown in equation one(1). Muhammad J.Y.,(2018).

$$H/H_0 = a\,(T_{max} - T_{min})^{1/2} \quad (1)$$

Where a is set at 0.16 for interior region

Hargreave and samani after more research took the coefficient of the Model as a=0.16 for interior region and a=0.9 for costal region.

Where H_o is the extraterrestrial radiation (radiation intensity outside the earth's atmosphere) measure in joule per day.

The value of H_o can be calculated using the equation given by Abdu and Ayodele, 2016 as:

$$H_o = \overline{H_O} = \frac{24\times3600}{\pi} I_{sc}\left[1 + 0.033cos\frac{360d}{365}\right] \times \left(cos\varphi\ cos\delta\ sin\omega s + \frac{\pi}{180}\omega s\ sin\varphi\ sin\delta\right) \quad (2)$$

Where:

w_s = sunset hour angle in degree defined as:

$$w_s = cos^{-1}(-tan\varphi tan\delta) \quad (3)$$

δ = declination angle given as:

$$\delta = 23.45 \sin\left(360 \times \frac{[284+75]}{365}\right) \quad (4)$$

ø = the latitude of the location;

ḍɳ = day number of the year starting from the first of January;

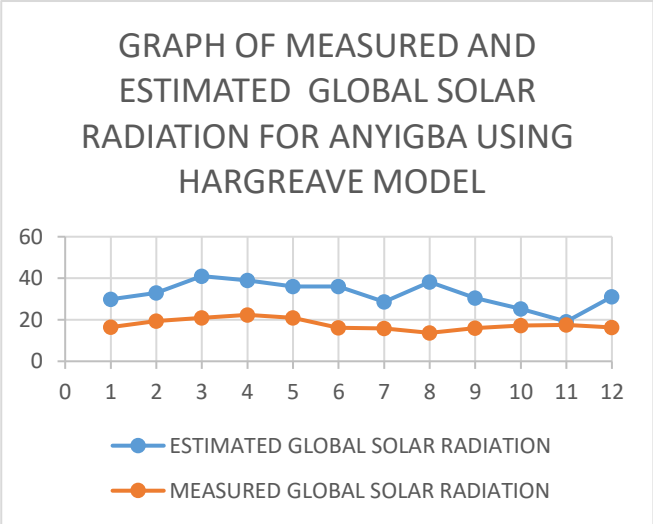
I_{sc} = Solar constants given as 1367 (Wm^{-2});

Result and discussion

Table 1: Average solar radiation from 2011 to 2016

A_{MODEL} = 0.16

MONTH	T_{MIN} (^{O}C)	T_{MAX} (^{O}C)	$\overline{Ho}$ (MJ/day)	$\bar{H}_{icalculated}$ A_{model} (MJ/day)	$\bar{H}_{measure}$ (MJ/day)
January	5.25	37.34	32.9788	29.8900	16.4020
February	8.20	42.34	35.2930	32.9953	19.4216
March	8.63	56.10	37.2209	41.03139	20.9286
April	7.63	49.43	37.7024	39.0012	22.3609
May	8.24	45.42	36.8846	35.9849	20.8980
June	9.20	48.05	36.1095	36.0114	16.1654
July	9.80	34.73	36.3333	28.6273	15.1654
August	3.51	44.75	37.1392	3816 03	13.6800
September	8.70	35.10	37.1568	30.5464	16.0092
October	7.77	27.45	35.6608	25.3118	17.2066
November	6.51	19.35	33.3857	19.1409	17.5666
December	9.60	46.00	32.1839	31.0669	16.2436



Discussion

From Table 1, it shows the month of March to be the month with the highest global solar radiation which corresponds with the measured global solar radiation. Fromm table 1, it can be seen that the month of November recorded the lowest global solar radiation while the month with the lowest global solar radiation in the measured data happens to be the Month of August. This is an anomaly as the pattern of the estimated data is supposed to correspond with the measured data, from the graph in figure 1, it can be seen that as the global solar radiation of the measured global solar radiation increases and decreased , there is a corresponding increase and decrease in the estimated global solar radiation except for the month of August and December, in the month of August the estimated increase while the measured data decrease. In December estimated data increase abruptly whereas the measured data decreases, this is as a result of errors in the minimum and maximum temperature data used and the suitability of the model for the estimation of the global solar radiation

Conclusion

In areas where there are no solar radiation data but minimum and maximum temperature data, the temperature data can be used with Hargreaves and samani model to estimate global solar radiation. The global solar radiation for Anyigba was estimated using Hargreaves and Samani model. The average monthly global solar radiation was found to be 32MJ/m^2 /day with a RMSE of 15.633314MJ/m^2 /day and MBE of 5.9805 MJ/m^2 /day . This implies that comparing the measured and estimated global solar radiation for Anyigba using the model, the estimated global solar radiation shows an overestimation of about 15.6314 MJ/m^2 /day , which is above acceptable range. Therefore the global solar radiation estimated does not show a good agreement with the measured global solar radiation. This may be as a result of inaccurate temperature data.

Recommendation

There is need for further investigation of suitability of Hargreaves and Samani model for Anyigba using data from different weather stations.

References

Abdu G., and Ayodele A.S., (2016). Empirical Model for the Estimation of Monthly Global Solar Radiation in Zaria Nigeria. International journal of physics and mathematical science. Vol 6(4). pp 57-62

Ayegba A., Olu J.J., and Odoma A.N.,(2017). ‘’A Study of the Global Solar Radiation of Makurdi, Benue state , Nigeria . American International journal of research in science, Technology Engineering and Mathematics’’ Vol 18(1). Pp 70-75.

Bernadetta I. Salisu, D., and Moses, a.,(2007) **’’**Testing the Performance of Solar Empirical Models for Estimating Global Solar Radiation over Makurdi Nigeria ‘’Journal of Natural science research Vol3(5). Pp. 165-170

Jegeda J.O., Ale F., Abdullai, A., and Aboola A.O., ’’ The Analysis of the Monthly Global Solar Radiation on the Campus of the Federal polytechnic Ida, Kogi State , Nigeria’’ International Journal of Engineering and Applied Science (IJEAS) Vol.4(7). Pp6-10

Okogbue E.C. and Adedokun J.A., (2002). ‘’Characterization of Sky Condition Over Ile Ife, Nigeria’’ Metorol Z (Germany) vol14. 97-99

Journal of Technology Innovations and Energy
https://doi.org/10.56556/jtie.v1i2.134
ISSN: 2957-8809

RESEARCH ARTICLE

Analytical Framework of Cloud Homomorphic Encryption / Cryptographic Logic Obfuscation for Cyber Health Hygiene

Akhigbe-mudu Thursday Ehis[1*]

[1]Africa Institute of Science Administration and Commercial Studies Lome-Togo

Corresponding author: Akhigbe-mudu Thursday Ehis, akhigbe-mudut@iaec-university.tg
Received: 01 January, 2022, Accepted: 02 April, 2022, Published: 15 April, 2022

Abstract
Hacking and the resulting disaster have become so dangerous that developers and organizations are taking extra precautions to reduce their incidence and impact. A drift is any gap between the code and the cloud. Ad hoc adjustments can, of course, result in environment instability, deployment challenges, unpredictably high costs, and security or compliance gaps. The risk of configuration drift becoming a permanent fixture is one of the most important considerations on this study. One such strategic strategy to mitigate these behaviors and render it unavailable to tracking, interpretation, and use by hackers is logic obfuscation. This study presents two strategies for combating piracy and overbuilding attacks. First, the proposed algorithms, then the logic obfuscation develop to hide the functionality and implementation of a design by inserting gates onto the original design. The attackers can use circuit extraction from the gate-level netlist but they won't be able to deduce the obfuscated logic functions. As a result, the proposed obfuscation technique in this brief not only resists image processing but also incurs low area and power overhead.

Keywords: Cloud Encryption; Cryptographic Algorithm; Cyber hygiene; Data at Rest; Homomorphic Encryption, Logic Obfuscation

Introduction

For many individuals and businesses, security is a key consideration when selecting a public cloud provider. Encryption in transit and at rest, which ensures that data can only be accessed by authorized roles and services with proven access to encryption keys, is at the heart of many security strategies. This document appears to capture the fundamental understanding of encryption and cryptographic primitives, which sounds intriguing. Rich theory started to emerge, establishing cryptography as a discipline and a mathematical study. This point of view has influenced how researchers think about computer security in general. Designing and employing codes that permitted two groups to communicate while keeping those messages hidden from eavesdroppers who could monitor communication between them was the old cryptography.
The hard drive acts as a communication channel through which the attacker can listen and read the contents if he or she has access to it. Although "sharing" a key is simple, the user requires a secure and reliable method of remembering / storing the key that will be used over time. In order to write a legal definition, one must consider what is vital in the current crisis and what external structures are necessary (Jonathan and Yehuda, 2020). This section introduces a skewed view of computer privacy as a starting point for a study of current encryption. It demonstrates how this definition may be used to achieve perfect privacy while avoiding the unlikely consequences mentioned earlier, and how a short key can be used to encrypt numerous large communications. An explicit binding of the high chance of success of an enemy running for a certain period of time or, more precisely, investing a specified amount of computational work gauges the security of a cryptographic system. Any definition of security has two parts: a description of what constitutes a system "break" and a description of the adversary's capabilities. Computer secrecy presents two complete secrets: first, confidentiality is guaranteed exclusively to victorious opponents; second, the secret has a small possibility of "failing." This is how to ensure message integrity by detecting any fraudulent messages or disruptions sent over an unprotected communication channel using cryptographic techniques (Gamma et al., 2021). It's easy to believe that encryption addresses the message verification problem. This is for odd, erroneous reasons, such as the opponent being unable to alter the secret message in any logical way because ciphertext totally masks the message content. The message verification code's aim is to prevent the enemy from altering or inserting a new message into a message sent from one person to another unless the recipient notices that the message is not from the intended recipient (Lama Alhathally et al., 2020). What's important to remember is that what defines a good message is entirely dependent on the application. This chapter explores the cryptographic primitive with numerous applications in addition to the existing secure communication problem: Cryptographic hash functions are a type of cryptographic hash function. There are numerous applications for non-conflict hash algorithms expanding the message code verification with

another approach – a standard like Hash Based Message Authentication (HMAC). Between the private writing fields and the public key, hash operations can be seen as a duplicate. Hash functions are increasingly widely utilized in cryptography, and they're frequently used in situations where far stronger structures are required than collision resistance. Hash functions are simple jobs that condense long, unfocused input into short, focused output. In the air, non-collision hash functions are the same; the purpose is to avoid conflict. A explicit collision resistance policy is built into cryptographic hash functions. Because it is impossible to encrypt solid code of every potential key using the necessary amount of memory, hash key functions overcome this technological challenge (Kotsiopoulo et al., 2021).

What is Code Obfuscation?

Hacking and the resulting disasters have become so dangerous that developers and organizations are taking extra precautions to reduce their incidence and impact. The use of code obfuscation is one such strategic strategy that keeps administered codes out of the hands of malicious actors. Code obfuscation comprises remodeling certain characteristics of at-work codes in order to make them inaccessible to tracking, interpretation, and usage by cybercriminals while remaining functional for the developers. The changes to metadata/instructions can be made without affecting the final output that the targeted code provides for application development. Using this method, developers can make the application/program more resistant to hacking attempts. This method performs admirably on all available code kinds.

What is Encryption

Encryption is a process that takes legible data as input (often called plaintext), and transforms it into an output (often called ciphertext) that reveals little or no information about the plaintext. The encryption algorithm used is public, such as the Advanced Encryption Standard (AES), but execution depends on a key, which is kept secret. To decrypt the ciphertext back to its original form, you need to employ the key. At Google,for instance, the use of encryption to keep data confidential is usually combined with integrity protection; someone with access to the ciphertext can neither understand it nor make a modification without knowledge of the key. In this paper, we focus on encryption at rest. By encryption at rest, we mean encryption used to protect data that is stored on a disk (including solid-state drives) or backup media (Sarigiannidis et al., 2021).

What is Data at Rest?

Data at rest refers to data in any digital form that is stored in a computer. This data type is now dormant, as it is not being transmitted between devices or between network points. This information is not actively used by any app, service, tool, third-party, or employee (Panagiotis et al., 2021). At rest isn't a data state that lasts forever. When someone requests a file, the data is transferred across a network and becomes in-transit data. The data enters the in-use state once someone (or something) starts processing it. Both structured and unstructured data can be found in data at rest. The following are some examples of places where a firm can store data at rest: (i) Hard drives and solid-state drives (SSDs) in PCs and laptops. (ii) Database servers. (iii) The cloud, (iv) In a colocation facility operated by a third party and so on. Unlike individual in-motion packets travelling via a network, static data storage often has a logical structure and meaningful file names. Data at rest often contains the company's most sensitive and confidential information, such as: (i) financial documents (past transactions, bank accounts, credit card numbers, etc.). Intellectual property (ii) (product information, business plans, schematics, code, etc.). (iii) Contacts, (iv) Marketing information (user interactions, strategies, directions, leads, etc.). (v) Personal information about employees and customers. (vi) Information on healthcare. Companies frequently replicate files in virtualized environments at rest, backup drives to off-site facilities, allow employees to take laptops home, and communicate data via portable devices, among other things. Data encryption should be used to protect the privacy and security of data at rest. Encryption is the process of translating a piece of data into seemingly meaningless text an unauthorized person (or system) cannot decipher (figure 1).

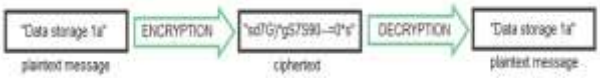


Figure 1: Encryption of Data at rest

Encrypting data at rest is critical for data security, and it reduces the risk of data loss. In most circumstances, symmetric cryptography is used to encrypt data at rest. Unlike asymmetric encryption, where one key scrambles data (public key) and the other decrypts files, the same key encrypts and decrypts the data (private key). When speed and responsiveness are important, as they are with data at rest, security teams commonly use symmetric cryptography. Unfortunately, data encryption isn't just a precautionary measure. At-rest encryption is an important part of cybersecurity since it ensures that data is not easily accessible to hackers. As cybercriminals develop more sophisticated methods for gaining access to and stealing corporate information encrypting data at rest has become a mandatory measure for any security-aware organization (Manuel et al 2018).

What is Cyber Hygiene?

Cyber hygiene refers to the habits and activities that computer and other device users take to keep their systems healthy and secure online (Miamantou et al., 2021). These procedures are frequently followed as part of a routine to protect one's identity and other personal information from

being stolen or tampered with. Cyber hygiene, like physical hygiene, is practiced on a daily basis to protect against natural deterioration and common dangers.

WHAT IS CLOUD ENCRYPTION?

The technique of encoding or modifying data before it is sent to cloud storage is known as cloud encryption (Felix and Isaac, 2021). You're probably already aware that encryption employs mathematical techniques to convert simple data (plaintext), such as a text, file, code, or image, into an unreadable form (ciphertext) that can be hidden from unauthorized or harmful users. It's the simplest and most important technique to ensure that your cloud data isn't hacked, stolen, or viewed by a bad party. Cloud storage companies encrypt data and offer customers with encryption keys. When necessary, these keys are utilized to safely decrypt data. Decryption is the process of converting encrypted data into readable data. There are six distinct areas of the cloud computing environment where equipment and software require significant security attention, as indicated in Figure 2. (Alexandria 2021). These six aspects are: (1) data security at rest, (2) data security in transit, (3) user/application/process authentication, (4) robust data separation between customers, (5) cloud legal and regulatory challenges, and (6) incident response. Cryptographic encryption technologies are unquestionably the finest solutions for safeguarding data at rest. Hard drive manufacturers are currently releasing self-encrypting drives that follow the trustworthy computing group's trusted storage standards (Degabriele and Paterson 2010). These self-encrypting disks have encryption technology, allowing for automated encryption at a low cost and with minimal performance impact. Although software encryption can be used to protect data, it slows down the operation and makes it less secure because an adversary may be able to take the encryption key from the machine without being detected.

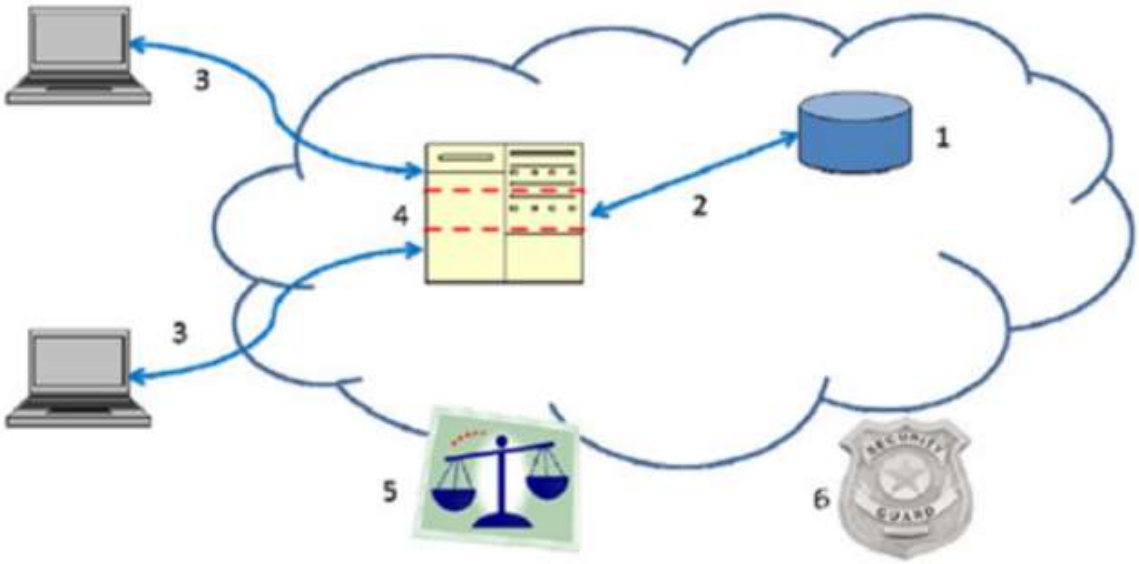


Figure 2: Shows six specific Areas of the Cloud Computing Environment Where equipment and Software Require Security Attention

Statement of the Problem

Most experts agree that encryption is the most effective method for protecting data in the cloud, but it is difficult to implement. For as long as software developers have been writing software, organizations have been working to eliminate misconfigurations in their environments. Configuration drift in the cloud is unavoidable. Even businesses with the best of intentions, who have worked through cloud adoption scenarios and built their infrastructure on well-architected frameworks, frequently encounter deviations from their baseline. When the actual known state of the infrastructure differs from the previous defined configuration, configuration drift happens. Drift can be caused by manually adding or removing resources, as well as making modifications to existing resource definitions. It can also be caused by a variety of automation techniques. Drift isn't inherently bad in and of itself, but given the different severity of effects and the speed of the cloud, awareness is critical, as is having a mechanism in place to resolve unintentional, costly cloud misconfigurations.

Drift can be defined as any code-to-cloud gap, but it doesn't mean all out-of-state configuration changes expose your infrastructure. Ad hoc adjustments can, of course, result in environment instability, deployment challenges, unpredictably high costs, and security in compliance gaps or annoyances to catastrophic production failures.

The risk of drift becoming a permanent fixture is one of the most critical factors on this study. Not understanding why and where a configuration was updated can result in unmanaged blind spots when it comes to evaluating an account's trust boundaries, such as locking its networking

settings or identity-based rights. In a large scale, this can lead to rifts in such borderlines, resulting in catastrophic data breaches and losses. Consider intentionally opening a port to the internet to troubleshoot DNS issues, or providing role administrative privileges to complete a complex database transfer process. There's a chance that those settings established ad hoc using CLI and never reverted after the project or bug was fixed, and they'll become a permanent fixture.

Those are the types of drift that an adversary intending to infiltrate an unprotected cloud asset could take advantage of. On the other hand, not all drifts provide a genuine or exploitable risk; in fact, some drifts may be planned. It's crucial to understand the types of drift that can occur as a result of dynamic infrastructure resource creation or modification to fulfill scalability needs, especially before automating your drift detection.

Literature Review

(Marain et al., 2021) Said that a lot of modern cryptography is now built on solid mathematical underpinnings. However, this does not negate the fact that the field is still a work of art. The rigorous method allows for innovation in establishing definitions that are appropriate for today's applications and surroundings, proposing new mathematical assumptions or inventing new primitives, and constructing and demonstrating secure schemes. Of all, even if cryptosystems are proven secure, there will always be the art of attacking them. Modern cryptography's approach has revolutionized the industry and helps to ensure that cryptographic systems applied in the real world are secure. However, it is critical not to exaggerate what a demonstration of security entails. A proof of security is always conditional on the definition and assumption(s) that are utilized (Mladenav et al., 2020). The evidence may be meaningless if the security promise does not match what is required, or if the threat model fails to represent the adversary's genuine capabilities. Similarly, if the underlying premise proves to be incorrect, the proof of security is useless. The takeaway lesson is that a scheme's proved security does not always imply its security in the real world (Jonathan and Yehuda 2020). While some have seen this as a disadvantage of provable security, we see it as a positive sign of the approach's robustness.

To attack a provably secure scheme in the actual world, all that is required is a focus on the definition (that is, determining how the idealized definition differs from the real-world context in which the scheme is deployed) or the underlying assumptions (i.e., to see whether they hold). Cryptographers, on the other hand, must constantly revise their definitions to make them more realistic, as well as investigate their assumptions to see if they are correct. Provable security does not eliminate the age-old conflict between attacker and defender, but it does provide a framework that helps the defender win.

One of the most often used integrated circuit (IC) protection approaches is logic obfuscation. (Simiosoghlou et al., 2020) Obfuscates IC designs by randomly inserting additional key gates, according to a conventional combinatorial logic obfuscation method proposed (XOR or XNOR). The design's functional input is one of the inputs to a key gate, while the other is a 1-bit key input. To prevent attackers from accessing the proper key, it will be placed in a tamper-evident memory within the design. The obfuscated design will function correctly if you apply the correct key. The IC can be protected from piracy and overbuilding by using logic obfuscation. An opponent could derive the key from the type of inserted gates if the IC was purchased via image processing-based RE (Jonathan and Yehuda 2020).

To circumvent this issue, the authors advocated replacing an XOR gate with an XNOR gate and an inverter, and similarly replacing XNOR gates with XOR gates and inverters, and using de Morgan's law to relocate inversions further up or down. Due to the logic redesign created by de Morgan's rules, this solution has large area and power overheads.

(Mladenov et al. 2020), (Diamantou et al., 2021), and (Yufei and Abhari, 2022) give overviews of a wide range of obfuscation and categorization strategies. On the theoretical side, (Kotsiopuolo et al., 2021) is working on a mathematical model for obfuscation. The most basic strategies substitute equivalent expressions for sections of expressions. Many of the tactics in Hacker's Delight can be useful for obfuscation. Smart equivalences that are difficult to discern are particularly intriguing (Stauch et al., 2022). However, because they are used by popular obfuscators, tools have been developed to precisely remove them (Chaschatzis et al., 2022). Because some algorithms may be identified simply by the presence of constant values (Dimiros et al., 2022), strategies for encoding them have been devised. Mixed-Boolean-Arithmetic and their algorithmic creation are among them (Chausainov and Moscholio 2021), and they look at efficient techniques of constructing various equivalences and encodings that use both logic and arithmetic operations. (Jilian Zhang 2016) suggest opaque predicates to make program analysis more difficult by making it difficult to tell which pathways in a program are taken. Flattening the control flow graph (Radiglou et al., 2021) is another way that has been considered. (Boursiannis et al., 2021) Worked really hard to improve this strategy. The effectiveness of the strategies is assessed using symbolic execution (Felix and Isaac 2021), which is used in the evaluation. It can be used to attack disguised code automatically (Illia Siniosoghu et al., 2021). Not only must implementors be careful to accomplish correctness and speed, but they must also avoid timing and other side-channel leakage.

(Yufei and Abhari 2022) software, it will very certainly struggle with post-quantum cryptographic software's latency. Space and time constraints have always created significant research obstacles for cryptographers, and they will continue to do so for post-quantum cryptographers. On the plus side, cryptography research has yielded numerous impressive speedups, and further research efforts in post-quantum cryptography should continue to yield impressive speedups. Despite substantial cryptanalytic efforts, the (Alexandria, 2021) hash-tree public-key signature system and (Felix and Isaac, 2021) code public-key encryption

scheme were both proposed thirty years ago and remain essentially unchanged. Many other hash-based and code-based cryptography candidates are much more recent; multivariate-quadratic cryptography and lattice-based cryptography provide even more new post-quantum cryptography candidates. There have been several specific suggestions that have been broken. Perhaps a new system will be broken the moment a cryptanalyst takes the time to examine it. One may insist on employing tried-and-true systems that have stood the test of time. However, many users cannot afford traditional systems and must instead examine newer, smaller, faster systems that take advantage of more recent cryptographic technology. To maintain trust in these systems, the community must ensure that cryptanalysts have spent time looking for vulnerabilities. These cryptanalysts, in turn, must learn post-quantum cryptography and get experience with post-quantum cryptanalysis.

The RSA public-key cryptosystem began as a one-way trapdoor function called "cube modulo n." (An interesting historical note: Rivest, Shamir, and Adleman employed huge random exponents in their initial paper (Paisias et al., 2021). Small exponents, such as 3, are hundreds of times faster, as (Radoglou et al., 2021) pointed out.) Unfortunately, a trapdoor one-way function cannot be used in the same way as a safe encryption function. Modern RSA encryption must first randomize and pad a message modulo n before cubing it modulo n (Pliatso et al 2021).

Furthermore, it encrypts a short random string instead of the message to accommodate large communications, and then uses that random string as a key for a symmetric cipher to encrypt and authenticate the original message. It took many years to build the infrastructure around RSA, and there were numerous disasters along the way.

Research Methodology

This paper addresses the fundamentals of cloud computing with its challenge: “Security” in two folds:

(i) It proposes an algorithm for encrypting data at rest before transmitting it for storage in the cloud.

(ii) Logical Obfuscation: Logic Obfuscation hides the functionality and the implementation of a design by inserting additional gates into the original design.

PROPOSED ALGORITHM

The proposed algorithm is to encrypt the data on the client side before transferring it to be stored in the cloud. This will translate the obvious text into ciphertext and prevent data theft by the intruder. That is, even if the attacker is unable to block the data, he will not be able to read the actual data or get a logical explanation from it. The algorithm is equipped with a table of ASCII Codes and Binary Representation codes with zero Padded for easy calculation

Table 1a: ASCII Codes

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

1. Convert the letter to its ASCII code

Encryption Algorithm

2. Convert ASCII code to its 8-bit binary number. If it does not equal 8 bits, add the previous 0s.
3. Find 1 complement to the last 4 pieces.

4. Convert the generated binary code to the ASCII character and transfer it to the cloud.
Example: Suppose we want to send a 'C' over the cloud. First, we convert the plain text 'C' to its ASCII code i.e., 67 uses (table 1). Then we convert 67 to its 8-bit binary number. 67 in binary says 1000011 but since it is not equal to 8 bits, add 1 preceding 0 to get 01000011. This is indicated by (Included Binary Representation Codes No zero). Then we get the completion of 1 of the last 4. This will give us 01001100. Finally, we convert this 8 binary number into its ASCII code letter, 'L'.

B. Decryption Algorithm

1. Get the ASCII code for the character.
2. Convert ASCII code to binary. Add the previous 0s if they are not equal to 8 bits.
3. Subtract the last 4 bits from the 8-digit binary generated.
4. Convert binary generated value to ASCII code.
The real character (blank text) is a letter similar to the ASCII code. Using the example above to convert cipher text into plain text:

First, convert the cipher 'L' text to ASCII code which is 76. 76 and then convert it to binary to get 1001100 but since it does not equal 8 bits, add the previous 0 to get 01001100. Then we undo the last 4 bits. to get 01000011 and convert this binary number to its ASCII equivalent. The original character or plain text is a character similar to the generated ASCII code.

ASCII table

ASCII stands for American Standard Code for Information Interchange. Computers can only understand numbers, so the ASCII code is a numerical representation of a character such as 'a' or '@' or an action of some kind. Below the tables (Tables 1a and 1b) are ASCII characters tables and this includes descriptions of the first 32 unpublished characters. ASCII was actually designed to be used with teletypes so the definitions are unclear. When someone says you want your CV but in ASCII format, all this means you are looking for 'blank' text that has no formatting such as tabs, bold or highlighting - a raw format that can be understood by any computer.

Table 1b: Extended ASCII Codes

128	Ç	144	É	160	á	176	▒	192	└	208	╨	224	α	240	≡
129	ü	145	æ	161	í	177	▒	193	┴	209	╤	225	ß	241	±
130	é	146	Æ	162	ó	178	▓	194	┬	210	╥	226	Γ	242	≥
131	â	147	ô	163	ú	179	│	195	├	211	╙	227	π	243	≤
132	ä	148	ö	164	ñ	180	┤	196	─	212	╘	228	Σ	244	⌠
133	à	149	ò	165	Ñ	181	╡	197	┼	213	╒	229	σ	245	⌡
134	å	150	û	166	ª	182	╢	198	╞	214	╓	230	µ	246	÷
135	ç	151	ù	167	º	183	╖	199	╟	215	╫	231	τ	247	≈
136	ê	152	ÿ	168	¿	184	╕	200	╚	216	╪	232	Φ	248	°
137	ë	153	Ö	169	⌐	185	╣	201	╔	217	┘	233	Θ	249	∙
138	è	154	Ü	170	¬	186	║	202	╩	218	┌	234	Ω	250	·
139	ï	155	¢	171	½	187	╗	203	╦	219	▉	235	δ	251	√
140	î	156	£	172	¼	188	╝	204	╠	220	▄	236	∞	252	n
141	ì	157	¥	173	¡	189	╜	205	═	221	▌	237	φ	253	²
142	Ä	158	₧	174	«	190	╛	206	╬	222	▐	238	ε	254	■
143	Å	159	ƒ	175	»	191	┐	207	╧	223	▀	239	∩	255	

Source: www.LookupTables.com

Zero-Padded Binary Representation
Convert an integer to a binary string of a specific length in Java

This post will discuss how to convert a number into a binary character unit of a certain length in Java. The solution should attach to the left the binary string with the leading zero. There are several ways to convert a whole number into a binary format in Java:

```
community category NumberFormatUtils {
Public static String longToBinString (val ende) {
  char [] buffer = new character [64];
  Arrays.fill (buffer, '0');
  because (int i = 0; i <64; ++ i) {
    long mask = 1L << i;
    uma ((ival & imaski) == imaski) {
      buffer [63 - i] = '1';
    }
  }
  replace new String (buffer);
```

```
}
public static void main (String ... args) {
   long term =
0b0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
   System.out.println (total);
   System.out.println (Long.toBinaryString (value));
   System.out.println
(NumberFormatUtils.longToBinString (value));
}
}
Output: 5,
101 :
0000000000000000000000000000000000000000000000000000000000000101
```

3.15 (1). Using the String.format () method

To find a binary string of a specific length with leading zeros, we can use the String () class formatting method as follows:

```
Public class Numberformatutils {
Public static string longTobinstring (long val) {
Arrays fill (buffer;'0');
For (int i=0; i<64; ++i){
Long mask =iL<<I;
If (val & Mask )==mask){
Buffer[63-i]='I';
}
```

2. Using StringBuilder:

```
class Main
{
   public static String toBinary(int x, int len)
   {
      StringBuilder result = new StringBuilder();

      for (int i = len - 1; i >= 0 ; i--)
      {
         int mask = 1 << i;
         result.append((x & mask) != 0 ? 1 : 0);
      }
      return result.toString();
   }
   public static void main(String[] args) {
      System.out.println(toBinary(1000, 16));
   }
}
Output: 0000001111101000
```

3.16 (2). Using StringBuilder:

```
class Main
{
   Public Binary Stable (int x, int len)
   {
      StringBuilder Result = New StringBuilder ();
      because (int i = len - 1; i> = 0; i--)
      {
         int mask = 1 << i;
         result.put ((x & mask)! = 0? 1: 0);
      }
      return result.to String ();
   }
   public static void main (String [] args) {
      System.out.println (toBinary (1000, 16));
   }
}
Output: 0000001111101000
```

Drift Detection Manually

The drift detection scan is operational from time to time, depending on the interval set in the description. (Default 1800 seconds, or 30 minutes.) There may be times when you know that files in the directory have changed and you need a summary to be created quickly, but you do not want to change the intermission permanently. Just use manual detection scanning (Figure 3).

1. Click the Inventory tab in the top menu.
2. Search the app.
3. Click the Drift tab.
4. Select the drift definition to use for scanning.
5. Click the Get Now button

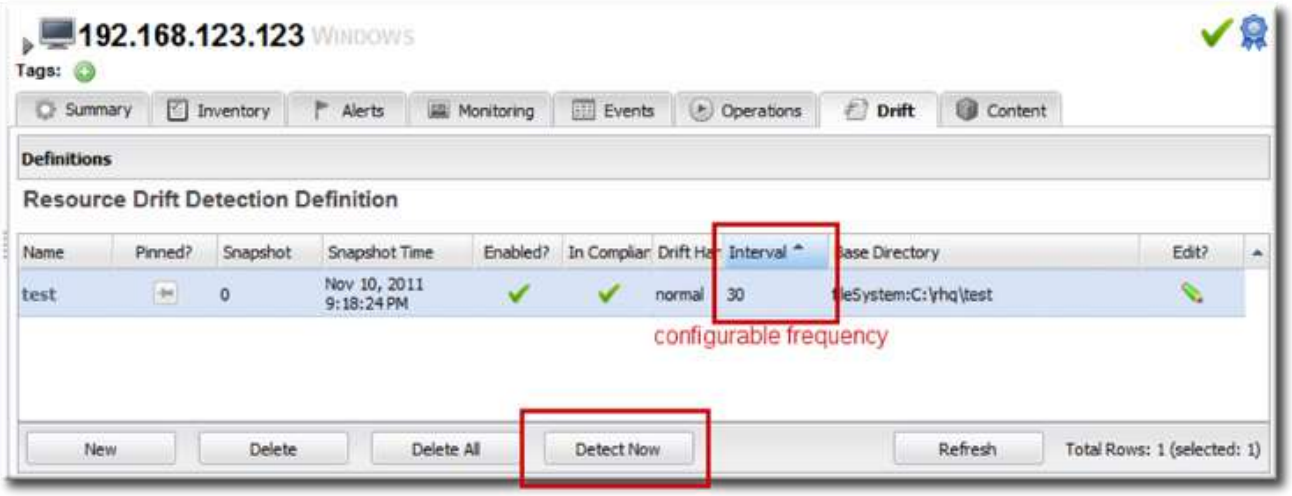


Figure 3: Manual Configuration Drift Detection.

Mathematical Operation Encoding

The simplest method of obfuscation is to integrate mathematical operations by inserting equally strong solid terms that are not visible. Using consistent terminology makes it easy to evaluate the overhead he will appeal to, and by attaching it to unwanted words of the same size, the cost of each shift becomes constant. Because the switch expression will be used instead of the first term, the operating time title is equal to the maximum size and can also be calculated using the above (Figure 4a & 4b). Not all changing words contain not only mathematical words but may also introduce constants, depending on the gross calculation. This may need to be considered in padding. Book (Stauch et al., 2022) provides a rich list of such changes. In Chapter Additive Addition and Logical Performance, many equals of arithmetic integration, subtraction, and denial and all logical operations are clearly presented and proven.

$x + y = x - (\neg y + 1)$

$x + y = (x \vee y) + (x \wedge y)$

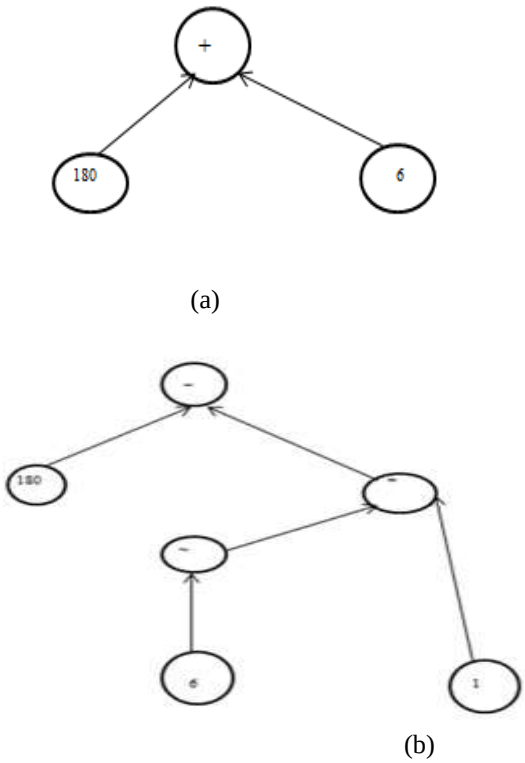
$x + y = (x \oplus y) + (x \wedge y) \bullet 2$

All these changes are the same in that the same complex versions contain both logical and arithmetic functionality. This is common among complex strategies, as it is often difficult to reverse logical expressions and statistics without building a value table. To replicate the same dynamic expressions that complement these mixing conditions can also be found:

$x * y = (x \vee y) \bullet (x \wedge y) + (x \wedge \neg y) \bullet (y \wedge \neg x)$

$x * y = (x \vee y) \bullet (x \wedge y) + \neg (\neg x \vee y) \bullet (x \wedge \neg y)$

The dynamics of these changing expressions depend on the known equations in the analytical tools and development strategies used. By using equilibrium that mixes logical and arithmetic words, this is achieved to some degree. However, because all of these expressions are fixed, this equation can be easily facilitated by using pattern matching methods.



Figures 4a & 4b: Example of Operation Encoding: Encoding of 180 + 6 to the equal Equation $180 - (\neg 6 + 1)$

Logic obfuscation

Logic obfuscation hides performance and application design by adding additional gates to the original build. In order for the design to reflect its correct function (i.e., produce the correct output), a valid key must be assigned to the incomprehensible design. Blurred gates are key gates. When you use the wrong key, the blurred design will show the wrong performance (i.e., the wrong output). Consider the cycle shown in Figure 5 using the " B_1 " and " B_2 " key gates. I0 - I5 input is active and Gate1A and Gate2B are the key connected to the key gates. Using the correct key values (Gate1A = 0 and Gate2B = 1) the design will produce the correct; otherwise, it will produce the wrong output.

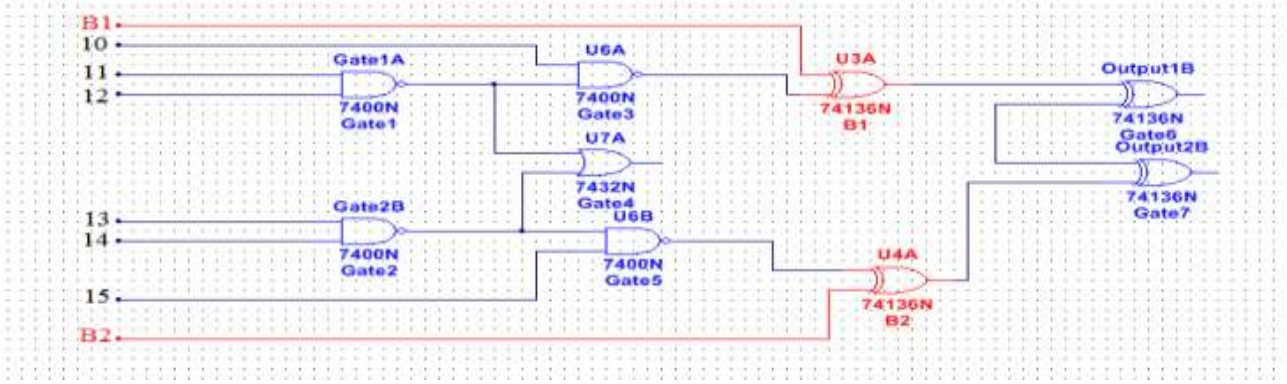


Figure 5: A Circuit Obfuscated Using two keys –gates Gate 1A and Gate 2B, based on the technique proposed (Jilian Zhang, 2016).

By using the 100000 input patterns, the attacker can notify the Gate1A and Gate2B key pieces in Exit B_1 and Output B_2 and view their values.

Definition (attack):

Consider the Gate1A key input in Figure 5. It will be notified on the output of Output1B if the value in one of the G6 input is 0 (uncontrolled gate value OR). This can be achieved by setting input (I1 = 1, I2 = 0 and I3 = 0). As the attacker has access to the active IC, one can use this pattern and determine the value of Gate1A in Output1B. For example, if the Output1B value is 0 in that input pattern, then Gate1A = 0, otherwise Gate 1A = 1. This problem is similar to the problem of reporting errors in the presence of unknown values — X can prevent / hide the spread of error (Alexandria 2021). Key bits Gate 1A and Gate 2B are equal to X sources, as in Figure 5. Similarity and error difference between keystrokes and key distributions: Both purposes require an input pattern that alerts the effect / error key by blocking the result in some or all sources of X / other key fragments, and to prevent their interference.

Result and discussion

Consider the effective cycle illustrated in Figure 5 with two key gates, B_1 and B_2 in different locations. Here, if the attacker has to broadcast the result of any key, then one has to force `0 '(uncontrolled number of gates NOR) in one of the Gate 4 inputs. To force this number, one has to control the main input, which is inaccessible. So one cannot distribute the key effect of the output, failing to determine the key values. Depending on the location of the key gates, different strategies should be used to propagate the key effect. This is the case with a combination of logic obfuscation, as mentioned earlier, when XOR / XNOR gates are introduced to hide design performance (Caspar et al., 2021). Obfuscation is also performed by inserting memory elements (Sariagiannidis et al., 2021). A circuit only works properly if these elements are properly aligned. However, using memory features will add even more important functionality.

Conclusion

In this brief, we have thoroughly analyzed current computer security strategies and developed an effective and efficient way to integrate intelligence to prevent theft, over-construction, and RE attacks. Although attackers may not be able to extract a gate-level netlist with a circuit-based release of retractable engineering tools (RE), they cannot predict obscure logical operations. The only way is to fully evaluate the entire OC configuration with an unreachable brute-force attack. Therefore, our proposed obfuscation process in this brief not only contradicts RE-based image processing but also encapsulates lower space and higher power.

Acknowledgement

Having an idea and turning it into writing is as hard as it sounds. The experience is both internally challenging and rewarding. I especially want to thank the individuals that helped make this happen. Complete thanks to Mrs Josephine Ohens and Mrs Omonigho Akhanolu Casey for their financial support. I will always welcome the chance to represent you.

Thank you to everyone who strives to grow and help others grow. It is the business version of the Lion King Song, “Circle of Life”.

I want to thank God most of all, because without God I wouldn’t be able to do any of this.

Declaration of interests

The author declare that he has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Caspsar Chorus; Sander Van Cranenburgh; Aemiro Melkamu Daniel; Erlend Dancke Sandof’ Anae Sobhani; Teodora Szep (2021): “ Obfuscation Maximization Based Decision Making : Theory, Methodology and First Empirical Evidence”. *Journal of mathematical Social Sciences 109 (2021) 28 - 44.* https://doi.org/10/1016/mathsocsci.2020.10.002

V. Mladenov; V. Chobanov; P. Sarigiannidis; P.I. Radohlou- Grammatikis; Hristov A. and P. Zlatev (2020): “Defense Against Cyber Attacks on the Hydro Power Plant Connected in Parallel with Energy System”. *Jounal (2020 12th Electrical Engineering Faculty Conference, BULEF 2020, Publisher: IEEE*

Siniosoghlou; G. Eftstathopoulos; D. Pliatsios; I.D. Moscholos; A. Sarigiannidis, G. sakellari and Loukas G and P. Sarigiannidis (2020): “ Neuralpot: An Industrial Honeypot Implementation Based on Deep Neural Networks.’ *Proceedings –IEEE Symposium on Computers and Communications.* https://doi.org/10.1109/ISCC.50000.2020.9219712.

Jonathan Katz; Yehuda Lindell (2020); “Introduction to Modern Cryptography. *(3rd ed) chapman and Hall {CRC},* https://doi.org/10.1201/9781351133036

Alexandria V.A (2021): "The Cyber Defense Review, *2019 International Conference on Cyber Conflict U.S { CYCON U.S } Volume 5, No. 1, Spring 2020*

Felix Bentil; Isaac Lartey (2021): "Cloud Cryptography – A security Aspect. International *Journal of Engineering Research and Technology (IJERT) Volume 10, Issue 05, May 2021, pp. 448-450*

Illias Siniosoglou; Panagiotis Rodoglou-Grammatikis and Georgios E; Efstathopoulos; Panagiannids Fouliras and Panagiotis Sarigiannidis (2021): "A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments". *IEEE Trabsaction Networks and Service Management (2021), Volume 1, No. 1, 2021,*
https://doi.org/10.1109/TNSM.2021.3078381

T. Kotsiopoulos; P. Sarigiannidis; D. Ioannidis and D. Tzovaras (2021): "Machine Learning and Deep Learning in Smart Manufacturing: The Smart Grid Paradigm. *Journal of Computer Science Review, Volume 40, page 100341*. https://doi.org/10.1016/j.cosrev.2020.100341

I. Siniosoglou ; V. Argyriou; S. Bibi, T. Lagkas and P. Sarigiannidis (2021): " Unsuspervised Ethicak Equity Evaluation of Adversarial Federated Networks." *The 16th International Conference on Availability, Reliability and Security. Pages 1-6*
https://doi.org/10.1145/3465481.3470748

P.Diamantou Lakis ; P. Bouzinis; P. sarigiannidis; Z. Ding and G. Karagiannidis (2021): " Optimal Design and Orchestration of Mobile edge Computing with Energy Awareness. *IEEE Journals of Transaction on Sustainable Computing. Volume 1, No. 1, 2021.*
https://doi.org/10.1109/TSUSC.2021.3103476

Yufei Ding, M. Javadi- abhari (2022): "Quantum and Post-Moore's Law Computing. *IEEE Internet Computing, Vol. 26, pages 5*-6. https://doi.org/1o/10.1109/mic.2021.3133675

M.Stauch; P. Radoglou-Grammatikis; P. Sarigiannidis; G. Lazaridis; A. Orosu; I. Nwankwo; and D. Tzovaras (2022); " Data Protection and Cyber Security Activities and Schemces in the Energy Sector. *Journal of Electronics. Volume 11, No.06*.
https://doi.org/10.3390/electronics.11060965

C. Chaschatzis; C. Karaiskou; E. Mouratidis; E. Karagiannis; P. Sarigiannidis (2022); " Detection and Characterization of Stressed Sweet Cherry Tissues Using Machine Learning. *Journal of Drones. Volume 6, No. 3, (2022), https://doi.org/10.3390/drones6010003*

Dimirios Pliatsios; Sotitios K. Goudos, Thomas Lagkas ; Vasileios Argyriou; Alexandrias Apostolos; A. Boulogeorgos and Panagiotis Sarigiannidis (2022); " Drones Based station for Next Generation Internet of Things; A comparison of Swarm Intelligence Approaches. *IEEE Open Journal of Antennas and Propagation. https://doi.org/10.1109/OJAP.2021.3133459*

I.A Chausainov and I. Moscholios and P. sarigiannidis and M. logothetis (2021): "Multi Service Loss Models for Cloud Radio Access Networks. *IEEE Journal of Access.*
https://doi.org/10.1109/ACCESS.2021.3105946

P. Radoglou- Grammatikis; P. sarigiannidis; E. Iturbe; E. Rios ; S. Martizez ; A. sarigiannidis and G. Eftsathoupoulos and I. Spyridis and A. Seis and N. Vakalis and D. Tzo Varas and E. Kafetzakis and I. Giannidis and M. Tzifas and A. Giannoulakis and M. Tzifas and A. Giannakoulias and M. Tzifas and A Giannakoulis and M. Angelopoupous and F. Tamos (2021): " SPEAR SIEM: A Security Information and Event Management System for the Smart Grid. *Journal of Computer Networks 2021, pages 108008,*
https://doi.org/10.1016/j.comnet.2021.1080008

A.D Boursiannis; M.S. papadopoulou; J. Piaezon; V.C. Mariani; l.S. Coelho and P. Goudos (2021): "Multiband Patch Antenna Design Using Nature Inspired Optimization Method. *IEEE Open journal of Antennas and Propagation, Volume 2, pp. 151 – 152, 2021.*
https://doi.org/10.1109/OJAP.2020.3048490

A. Paisias, T. Kotsiopoulos; G. lazaridis; A.drosu; D. Tzovaras. P. Sariagiannidis (2021): Enabling Cyber- Attacks Mitigation Techniques in a Software Defined Networks. *Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilence. (CSR 2021) PP. 497 – 502. https://doi.org/10.1109/csrs1186.2021.9527932*

D. Pliatsios; P. Sarigiannidis; k. Psannis; S.K. Goudos; V. Vitsas; I. Moscholios (2021): "Big Data Against Security Threats: The SPEAR Intrusion Detection System*," 2020 3rd World symposium on Communication Engineering [WSCE] 2020. Pages 12-17.*
https://doi.org/10.1109/wsce.51339.2020.9275580

Jiliang Zhang (2016): "A Practical Logic Obfuscation Technique for Hardware Security." *IEEE Transactions on Very Large Scale Integration (VLSI) Systems 24(3), 1193 - -1198*.
https://doi.org/10.1109/TVLSI.2015.2437996.

J. P. Degabriele and K.G. Paterson (2010). "On the (in) security of IPsec in MAC-then-encrypt configurations". *In 17th ACM Conf. on Computer and Communications Security, pages 493–504. ACM Press, 2010.*

Manuel Cheminod; Luca Durante; Lucia Seno; Adriano Valenzano (2018): "Performance Evaluation and Modelling of an Industrial Applications Layer Firewall". *IEEE Transactions on Industrial Informatics. Volume 14, No.5, pp. 2159-2170. May 2018.*
https://doi.org/10.1109/TII.2018.2802903.

Panagiotis Radoglou-Gammaliks; Panagiotis Sariagiannidis, Eider Iturbe; Erkuden Rios, et al., (2021): Spear Siem: A security Information and Event Management System for the Smart Grid". *Computer Networks".Volume193, July 2021,108008, pages1-26.*

https://doi.org/10.1016/j.comnet.2021.108008

Marcin Wojnakowski; Remiguisz Wisniewski; Grzegorz Bayzydio and Mateusz Poplawskwi (2021): " Analysis of Safeness in a Petri Nets Based Specification of the Control Part of Cyber-physical systems. *International Journal of Applied Mathematics and Computer Science 2021, Volume 31, No.4, 647-657.* *https://doi.org/10.34768/amcs-2021-0045*.

Lama Alhathally; Mohammed A. Alzain; Jchad Al-Amri; Mohammed Baz; Mehedi Masud (2020): Cyber Security Attacks: Exploiting Weaknesses. *International Journal of Recent Technology and Engineering (IJRTE) ISSN:2277-3878, Volume 8, Issues-5, January 2020, pp.906-913.*

Gammal E.I Selim; Ezz El-Din Hemdan; Ahmed M. Shehatta; Nawal A. El-Fishawy (2021): "An Efficient Machine Learning Model for Malicious Activities Recognition in Water-Based Industrial Internet of Things. *Journal Security and Privacy, Volume 4, pp.1-14, Issue 3, May/June 2021.* *https://doi.org/10.1002/spy2.154*.

Frederick Weigang Pan and Matthew Caesar (2016): Salmon: Robust Proxy Distribution for Censorship Circumvention. Proceedings on Privacy Enhancing Technologies". 2016(4): 4-20. https://doi.org/10.1515/popsets-2016-0026.

Journal of Technology Innovations and Energy
https://doi.org/10.56556/jtie.v1i2.201
ISSN: 2957-8809

RESEARCH ARTICLE

Emerging Cyber Security India's Concern and Threats

Aadil Ahmad Shairgojri[1*], Showkat Ahmad Dar[2]

[1]Research scholars of Political Science & public administration Annamalai University Tamil Nadu, India

Corresponding Author: Aadil Ahmad Shairgojri, aadilhassan1995@gmail.com
Received: 08 April, 2022, Accepted: 13 June , 2022, Published: 18 June, 2022

Abstract
Cybersecurity has developed into a challenging and constantly changing security issue in today's information, communication, and technology-driven world (ICT). Cyberattacks are expected to grow more widespread as the global economy and infrastructure become more dependent on information and communications technology (ICT). As a result of a growing reliance on computers and the Internet, there has been an increase in cyber attacks globally. The main targets of these attacks have all been people, organisations, and governments. Information and communication technologies (ICTs) are increasingly viewed by some countries as a battlefield where strategic warfare should be fought, even as a strategic asset to be leveraged for national security. This is essential because the national security is at risk. The significance of cybersecurity in the ongoing discussion about security concerns is examined in this essay. The authors examine cybersecurity from the viewpoint of India in order to gain a better knowledge of it.

Keywords: Cyber Security; Threats; ICT; Infrastructure and Framework etc

Introduction

In international relations, security is a major concern. It was previously thought that threats from foreign states and government responses to those threats were responsible for state security. A shift in focus from state-centric security to personal security occurred after the end of the Cold War. The fear of external aggression has given way to the threat of internal conflict as a result of civil wars, environmental degradation, economic hardship, and human rights violations. This definition of national security encompasses challenges like resource scarcity, industrial competitiveness, educational crises, environmental risks, drug and human trafficking, and poverty as well as defence of the homeland. From email to social networking to satellite communications to the Internet, everything about human life has changed. This has led to new national security problems, which we will discuss below.

In the digital age, a state's technology infrastructure is exposed to challenges to national security. As a critical piece of digital infrastructure for governments, businesses, and society as a whole in today's globalised world, the internet and other ICTs are necessary for social and economic progress. Because of its inherent openness, the Internet carries a high level of danger. Defending critical infrastructure from cyberattacks is just one aspect of cybersecurity, which also include dangers like cyberterrorism, data breach, and other forms of cybercrime and terrorism.

Cyberthreats are on the rise in the 21st century. Despite the fact that foreign governments and political organisations with a variety of goals are increasingly using this technique. It is still a criminal enterprise. Stuxnet, political "hacktivism," destabilising activities, and military operations are all examples of cyber espionage, sabotage, and destabilisation (OECD 2012). It appears as if cyberattacks are getting more planned and professional due to the increasing sophistication of cybercriminals, the rise of cyber espionage, and the operations of hacker collectives. States are now aware that cybercrime is a significant security concern to the country. Cybersecurity is currently a national policy issue that touches on the economy, society, education, legislation, law enforcement, technology, diplomacy, military, and intelligence, among other things. The concept of "sovereignty" is gaining in importance (OECD 2012).

The vast majority of political and financial organisations, military organisations, businesses, hospitals, and other industries store and process a great deal of sensitive information on computers, making network outages, virus infections, and hacker data disastrous. As cyberattacks become more common and sophisticated, the need to secure private information, sensitive commercial information, and national security grows. 3 In order to safeguard and secure the cyber environment and the assets of the organisation and its users, a number of tools, regulations, guidelines, training, activities, security concepts, and protections, risk management techniques, assurance, and technology are employed (ITU 2009). By protecting computer programmes, networks, and data, cybersecurity strives to keep information technology safe from unauthorised access and unforeseen damage or

destruction. Cybersecurity is essential to the development of IT and Internet services (UNODA 2011). National security and economic development depend on the protection of critical information infrastructures. Safeguarding the Internet is now a standard prerequisite for new services and government policy in many nations. Against the backdrop of this new threat, we examine India's response.

Research Objectives

Cybersecurity is crucial since it guards against theft and destruction to many types of data. It is a collection of tools, procedures, and techniques created to safeguard programmes, networks, and systems. As digital technology advances, the number of devices and users rises, the global supply chain becomes more complicated, and data becomes more vital in the digital economy, the system in the cyber space has become susceptible and will continue to be so as attacks increase in number. After conducting a thorough examination of the literature, the paper sets out to examine the crucial areas that are vulnerable to cyberattacks and to highlight the difficulties involved. Additionally, the paper illustrates India's cyber security strategies.

Material and method

The majority of the content in this research paper comes from secondary sources, such as articles, books, and official documents that were acquired from the official portals of the Indian government. The facts and relationship have been rigorously examined and explained using an empirical methodology. Qualitative information was acquired and utilised to arrive at a fair conclusion. Direct methods, such as scientific observation and expert interviewing, have also been utilised for this research project. Empiricism, observation, critical analysis, and exploratory approaches have been highlighted in order to contextualise the study's topic. These methods have added fresh, logical information to the body of literature that is supported by empirical data.

Discussion and results

Cybersecurity in India: Background

As a result of their neglect of cybersecurity, India's authorities are unable to meet the country's expanding demands. Anti-malware programmes like Stuxnet, Flame, and Black Shades make India's lack of cybersecurity capabilities even worse. India has fewer cybersecurity projects than other developed countries. In India, a lot of government initiatives are still just on paper. Two approved projects, the National Critical Information Infrastructure Protection Center (NCIPC) and the National Cyber Coordination Centre (NCCC), have not been carried out to their full potential. Adding insult to injury, India's 2013 National Cyber Security Policy has not been properly implemented, resulting in invasions of privacy and human rights abuses.

India must safeguard not only its financial institutions but also its satellites, automated power grids, and nuclear power facilities from cyberattacks. The Indian government has acknowledged the rise in cyberattacks on financial institutions. Cybercrime in India can take many forms, from viruses to hacking to identity theft to spamming to email bombing to website destruction to cyberdefamation. Internet access in the country is ranked 85th, yet cyberattacks are placed 7th (Express News Service 2014). There were 62,000 cyberattacks in the middle of 2014, up from 23 in 2004. Security threats to government organisations rose by 136 percent in 2013, while those to Indian financial services corporations rose by 126%. 69 percent of all assaults target large organisations of some kind (IANS 2014). According to Symantec, four out of every five attacks in 2014 were aimed at commercial, hotel, and personal services. India requires a cybercrisis management strategy to address these and other issues.

Cyber Security in India: In-Depth

India's IT sector has developed to play a key part in the country's economy and governance. Living standards, job prospects, and cultural diversity are all enhanced in some way as a result of the industry's presence among Indians. Thanks to information technology, India is emerging as a prominent participant in commercial services and technological solutions. There is a growing need to protect the digital environment and enhance the sector as a result of the advent of technology (DEITY 2012). Having included IT into their operations, the vast majority of financial institutions and banks are now vulnerable to cyberattacks as a result of routine business processes. Having no mechanisms in place to deal with these concerns is worrying. For example, the UIDAI and NeGP programmes have been promoted by the government, which has also built out a substantial IT infrastructure and increased industry involvement. In the public sectors of defence, banking, energy, telecommunications, and transportation, computer networks are essential for commercial transactions, information sharing, and communication. Computer networks. Advances in telecommunications, online and e-commerce are high priorities for the government. Indian Prime Minister Narendra Modi's claim that the "Digital India" plan, which aims to connect every gram panchayats to broadband internet, boost e-governance, and transform India into a connected knowledge economy, has been approved by the cabinet is typical. A high level of safety. Since Indian military and intelligence agencies are increasingly reliant on IT, they are more vulnerable to cyberattacks. In the event of an attack on government infrastructure, military and government secrets could be taken.. As a result, the Indian Ministry of Defense has delegated responsibility for cyber defence to a slew of organisations. The Indian Army's Cyber Security Establishment was founded in 2005 to protect divisional

networks and conduct cybersecurity audits. The Military College of Telecommunications Engineering in Madhya Pradesh now has a cybersecurity lab for officers to learn about signal and data transmission network security. In March 2011, India's Ministry of Communications and Information Technology (MCIT) drafted a national cybersecurity policy that prioritised infrastructure, development, and public-private partnerships (DEITY 2012). In June of that year, the National Security Council decided to establish the National Center for the Protection of Critical Information Infrastructure. National Technical Research Organisation (NTRO) The state's critical infrastructure was to be safeguarded through the use of CERTs at the national and sectoral levels (CERTs). In May of that year, the Defense Research and Development Organization developed a national cyber defence system to protect network sectors. Project completion reached a half-way point in May 2012. United Nations Development Program (UNIDIR). The Technical Intelligence Communication Centre and the National Defense Intelligence Agency developed a joint team to raise public awareness of cyber vulnerabilities.

Energy and Cybersecurity

India's non-traditional security challenge is the safety of the country's energy sector. The country is fourth in the globe despite its low energy use per person (TERI 2013). Information about cyberattacks and equipment vulnerabilities in the Indian energy sector is scarce because of inadequate regulation and governance. As India ties itself to contemporary technology to address its expanding energy needs, the industry is becoming a target of increasingly sophisticated attacks. A variety of cybersecurity concerns for India's critical infrastructure have surfaced as a result of the power sector's reliance on ICT. 60 percent of all cyberattacks on India's power grid occurred between 1994 and 2004. (2013) The 30th and 31st of July, 2012, saw a huge blackout in Northern India that affected 670 million people and slowed down train and road travel. Traffic lights and related equipment failed, and police were unable to maintain control of the situation. A number of large refineries were damaged by flames and explosions, resulting in numerous deaths, while oil supply was impeded by pipeline breaks (IDSA 2012).

Defence and Cybersecurity

India's armed forces rank third in the world, and the country's defence industry is robust (KPMG 2010). As a result of its reliance on modern technologies and network integration in its defence industry, it has put the country in danger. In 2012, hackers targeted the eastern command computer systems of the Indian Navy, which control missile submarine tests and maritime action in the South China Sea. Infected navy computers sent sensitive documents and data to Chinese IP addresses. In addition to the NSA and Air Force, Indian officials have not said what data was accessed. The NSA and other computers used by the Indian Air Force were breached by hackers in 2010 and 2012, allowing private information and papers to be accessed. Military personnel, the PMO, the defence, home, and external affairs departments, as well as intelligence organisations were all targeted in the same year. Politically aspirant actors endanger India's defence industry, putting national security, public safety, and the country's economy in jeopardy. Real-time cyber defence is necessary to protect the advancements and capabilities of the defence industry (DEITY 2011). "The DRDO is building India's own operating system in partnership with several top institutions in response to 8 the growing concern over cyberattacks as we are mostly dependent on operating systems," said former DRDO director-general V. K. Saraswat.

Finance and Cybersecurity

India's economy is growing at one of the fastest rates in the world because of its reliance on information technology. New concerns have been introduced because of the increased reliance on technology. According to statistics, the majority of hackers are motivated by financial gain (KPMG 2014). In modern banking and financial services, both state-sponsored and non-state assaults are possible since they are so complicated. Fraud, theft, and other wrongdoings have become easier to commit as a result of the modern technology's link (Bamrara et al. 2013). According to former Indian Telecom Minister Kapil Sibal, "Cybersecurity is vital for economic security and failing to ensure it will lead to economic destabilisation. India's financial sector has seen an upsurge in network security breaches, data loss, and other white-collar crimes, putting the banking industry at danger of large losses. In 2013, over $4 billion was lost by Indian firms as a result of cyberattacks. A year later, the cost of such assaults had risen by 30%. Among India's top five cybercrimes are identity theft (11%), ransomware (11%), and phishing (9 percent). Also, the RBI has released data on how commercial banks are targeted for fraud, such as through Internet banking and ATM (debit/credit) cards. In 2010, there were 4,049 million cases, which grew to 5,267 million cases in 2012. India needs a comprehensive cybersecurity policy to protect its banking sector under these circumstances.

Telecommunications and Cybersecurity

Telecommunications have fuelled India's economic and social growth. Indians have 943 million phone lines as of February 2012. In the same month, 9 911 million mobile phone connections and 160 million Internet users—of whom half used social media—were registered. India is expected to have 600 million internet connections by 2020. Cyberattacks have accompanied this industry's rapid expansion. Some argue that cybercrime is the greatest danger to the telecom industry. As of August 7, 2013, BSNL's database was infiltrated with spyware by hackers. On the 12th of October, BSNL's Office Domain suffered a significant data breach (Dilipraj 2014). A DDoS attack on MTNL's website was launched by unidentified hackers

on June 9, 2013, in an attempt to bypass Internet filtering. Referring to Reddy (2012): Passwords, emails, and other contact information are all stored separately on mobile phones. Consumers can now use Paytm, MobiKwik, and other point-of-sale payment methods, thanks to recent advancements in mobile commerce." Networks that are open and profitable are more vulnerable (Ruggiero and Foote 2011). In 2014, 7.9 percent of mobile devices were infected, which ranked the United States in second place in the world.

Cyber security in India issues and challenges

The protection of computer systems and electronic devices from malevolent cyberattacks, opportunist malware, and the unintended installation of malware by users themselves is what we mean when we talk about cyber-security. The breadth of cyberthreats is constantly expanding on a global scale. In the modern world, attempts are made yearly to divulge information for political or financial gain by hacking data and/or sensitive, private, or classified records. India's population comes from a diverse spectrum of social and economic origins. Depending on their financial situation, people employ a variety of technology, from expensive, highly secure electronic gadgets to low-cost mobile phones. This makes it difficult to establish a single set of legislative and technological standards controlling data protection. Additionally, there is a low level of digital literacy and familiarity among the general populace. Governments, companies, and individuals are all concerned about cyber security, which is becoming more and more of a problem. Maintaining the security of our personal data has become a top priority as more and more aspects of our life are being captured online, including our credit card details, vacation journals, and cute kitten videos. Ransomware, phishing, virus attacks, and other dangers are only a few of the many that exist for cyber security. With 2,299,682 instances of local cyberattacks already in Q1 2020, India is placed 11th globally.

Cyber attacks and India's response

In order to reach a $5 trillion economy, it is rumoured that the Indian government will announce its cybersecurity strategy policy in January 2020. A recent analysis by Recorded Future, a U.S. business that studies worldwide cyber threats, detailed RedEcho's attack on India's power infrastructure. From the middle of 2020 onward, ten organisations in the power industry and two Indian seaports were planned as targets. At an SKOCH event, Rajesh Pant, the national cybersecurity coordinator for India, said: "India's cybersecurity strategy policy would enable the government to secure all of India." This endeavour will help the government achieve its $5 trillion economic growth goal. Few efforts have been made to advance the Indian economy. In September 2020, Minister Sanjay Dhotre will inform the legislature that ZTE and Huawei provide the mobile network equipment for BSNL. Huawei was being looked at in 2014 over allegations that it had hacked BSNL. In this sense, the electric power industry is akin to other sectors of the economy. China supplied 21,000 crore of the 71,000 crore worth of power sector equipment that India imported in 2018–19. The government has taken major decisions since the year's beginning. Indian businesses would need government authorisation to import Chinese power supply equipment from July 2020. Before using any equipment other than approved equipment for network updates, telecom businesses must obtain Department of Telecommunications approval.

In order to strengthen our cyberdefenses and safeguard us against cyberattacks, a deterrence plan must be put into place. Some claim it's difficult to prevent cyberattacks. The United States is under attack from China, Russia, Iran, and North Korea despite having the strongest military and cyber capabilities in the world. We have nuclear and conventional deterrence because we are aware of the capabilities and financial burden of our enemies. Cyberwarfare's precise nature is yet uncertain. It is challenging to link cyberattacks to a state actor since we have no way of knowing what the other side is capable of. Deterrence will therefore be challenging to implement. According to a Business Standard analysis, one of the nation's most frequently targeted by cyberattacks in 2021 would be India. It was anticipated that every year, the number of cyberattacks will rise by a factor of two. India is expected to see 1.16 million cyber breaches in 2020, a threefold increase over 2019. This prediction is made by the Computer Emergency Response Team (CERT). 2021 and 2022 are expected to see more breaches. As of June 2021, official sources had identified 6,07,220 cybersecurity weaknesses in total. Is this a condition that the Indian government is aware of? The amount of money spent on cybersecurity is the subject of a wealth of information. Business Standard reports that in 2021–2022 the government overspent on cyber security for the first time in eight years. Recently, the government budgeted 515 crore rupees for cyber security for the years 2022–2023.

The steps India has taken and the progress it has made in creating its cybersecurity plan for 2020.

- **CERT-In** The Indian Computer Emergency Response Team (CERT-In) has made major strides in thwarting cyberattacks on government networks. The Indian government faces a serious problem with cybercrime, but anti-phishing and cybersecurity training have made a difference. CERT-In also releases alerts and advisories to let the public know about the most recent cyberthreats and countermeasures.
- **Cyber Surakshit Bharat** A initiative called Cyber Surakshit Bharat, created by MeitY, is intended to improve the cybersecurity landscape in India. This event was made possible by a grant from the National e-Government Division. (NeGD). Given the effects of digitization on government, good governance is more crucial than ever. Such a programme would increase awareness of cybercrime and make CISOs and frontline IT

personnel more secure. Officials will receive cybersecurity health toolkits and training on best practises as part of this first public-private partnership.

- **National Critical Information Infrastructure Protection Centre** The federal government established the National Center for Immunization and Immunization Programs (NCIIPC) to safeguard crucial data that impacts public health, economic development, and national security. This was modified by Section 70A of the Information Technology (IT) Act, 2000. This organisation has no issues conducting routine cybersecurity exercises to check on the state of readiness and posture of the government and other important sectors.
- **Appointment of Chief Information Security Officers** Greater digitization calls for greater safety considerations. If even the slightest error is found, the entire federal system might collapse. Every government organisation should have a Chief Information Security Officer (CISO) who can determine and record the security needs for every technology innovation. The Indian government has provided CISOs with instructions on how to safeguard apps, infrastructure, and compliance from online attacks.
- Training & Mock Drills The government has also evaluated the cybersecurity of businesses by running mock drills. MeitY reports that 44 drills have been held by CERT-In this year. Reliable sources report that 265 organisations representing various states and industry participated. Attacks will be made against telecommunications, finance, defence, and energy. Cyberattack readiness is a perennial worry for CISOs and network or system administrators. 515 persons had participated in 19 of these trainings as of October 2019.
- Malware Protection The central government has also introduced a malware analysis and detection tool called Cyber Swachh Kendra. Additionally, you can utilize the free tools provided to delete or omit them from your website or online application. As part of the Cyber Swachh initiative, the government has established a department in addition to the National Cyber Coordination Centre to educate the public about existing and potential cybersecurity hazards (NCCC).
- Personal Data Protection Bill Last but not least, the union government of India has approved the Personal Data Protection (PDP) Bill, which aims to localize data and protect Indian users from breaches that may occur anywhere in the globe. According to the bill, all personal data must be processed and maintained in India. Private and confidential information about an individual must be kept locally, however processing abroad is permitted under certain circumstances. The measure also makes an effort to make social media companies more accountable and to compel them to address issues with the dissemination of objectionable content. And they will.

Conclusion

Cyberattacks against India's critical infrastructure, which includes the energy, financial, defence, and telecommunications sectors, have the potential to have a detrimental impact on the country's economy as well as public safety. In accordance with the procedures used by other digital nations, the safeguarding of crucial informational infrastructure has been elevated to a position of great importance in the context of the nation's overall security (DSCI 2013). Indians shouldn't wait to build a national security plan that incorporates cybersecurity as a substantial component of the plan, as has been done by other nations across the world. Other nations have done this successfully.

Acknowledgement

We'd like to thank everyone who contributed to this article. We'd want to express our gratitude to everyone whose suggestions and inspiration helped us create this piece. The authors and specialists who have written on similar issues are also to be thanked for their citations, which helped us to correctly conclude our work.

Conflict of interest and funding

The authors declare no conflict of interest

References

Aiyengar, S. R. R. (2010). National Strategy for Cyberspace Security. New Delhi: KW Publisher

Alık, N. A. H. A. (2022). Emerging Cyber Security Threats: India's Concerns and Options. International Journal of Politics and Security, 4(1), 170-200.

Alsaibai, H., Waheed, S., Alaali, F., & Wadi, R. A. (2020, June). Online fraud and money laundry in E-Commerce. In ECCWS 2020 20th European Conference on Cyber Warfare and Security (p. 13). Academic Conferences and publishing limited.

Bagga, R. (2018). The National Cyber Security Policy of India 2013: An Analytical Study. Indian JL & Just., 9, 164.

Bajwa, L. G. J., George, M. G. N., & Sinha, B. D. (2016). Makeover of Rainbow Country.

Bamrara, D., Singh, G., & Bhatt, M. (2013). Cyber attacks and defense strategies in India: An empirical assessment of banking sector. Gajendra and Bhatt, Mamta, Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector (January 1, 2013).

Buzan, B. (2008). People, states & fear: an agenda for international security studies in the post-cold war era. ECPR press

Devi, S. (2019). Cyber Security In The National Security Discourse. World Affairs: The Journal of International Issues, 23(2), 146-159.

Dilipraj, E. (2013). India's Cyber Security 2013: A Review. Centre for Air Power Studies, 97(14), 1-4.

Dunn Cavelty, M. (2012). The militarisation of cyber security as a source of global tension. Center for Security Studies.

Ebert, H. (2020). Hacked IT superpower: how India secures its cyberspace as a rising digital democracy. India Review, 19(4), 376-413

Ghate, S., & Agrawal, P. K. (2017). A literature review on cyber security in indian context. J. Comput. Inf. Technol, 8(5), 30-36.

Kovacs, A. (2021). Cybersecurity and Data Protection Regulation in India: An Uneven Patchwork. In CyberBRICS (pp. 133-181). Springer, Cham

Kshetri, N. (2016). Cybercrime and cybersecurity in India: causes, consequences and implications for the future. Crime, Law and Social Change, 66(3), 313-338.

Kshetri, N. (2016). Cybersecurity in India. In The Quest to Cyber Superiority (pp. 145-157). Springer, Cham.

Kumar, A. (2020). Securing digital sovereignty: In context to present day challenges of cyber space (Doctoral dissertation, Full Text-IIPA, New Delhi).

KUMAR, G. Cyber Security System and Policy of India: Challenges and Prospects. Soc. Sci, 6(7), 1937-1943

Pandey, S. (2020). Cyber Peace and Security.

Pandey, S. (2020). New Emerging Security Threats and Global Cyber Security Index.

Parmar, S. D. (2018). Cybersecurity in India: An evolving concern for national

Patil, S. (2022). India's Cyber Security Landscape. In Varying Dimensions of India's National Security (pp. 75-90). Springer, Singapore

Poornima, B. (2022). Cyber Threats and Nuclear Security in India. Journal of Asian Security and International Affairs, 23477970221099748.

Prasad, S., & Kumar, A. (2022). Cyber Terrorism: A Growing Threat to India's Cyber Security. In Nontraditional Security Concerns in India (pp. 53-73). Palgrave Macmillan, Singapore

Relia, S. (2016). Cyber warfare: its implications on national security. Vij Books India Pvt Ltd.

Selby, J. (2017). Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both? International Journal of Law and Information Technology, 25(3), 213-232.

Shackelford, S. J., & Craig, A. N. (2014). Beyond the new digital divide: Analyzing the evolving role of national governments in internet governance and enhancing cybersecurity. Stan. J. Int'l L., 50, 119.

Venkatraman, B., & Gupta, K. (2016). Cybersecurity-Its Effects on National Security and International Relations. Indian JL & Pub. Pol'y, 3, 75..