C.S.T.S GOVERNMENT KALASALA, JANGAREDDIGUDEM

ELURU DISTRICT

DEPARTMENT OF COMPUTER SCIENCE

RESEARCH PUBLICATIONS

CSTS GOVT.KALASALA :: JRG

Department of Computer Science

JOURNALS / CONFERENCES / AWARDS

This certificate is computer generated and can be verified by scanning the QR code given below. This will display the certificate from the NPTEL repository, https://nptel.ac.in/noc/

Roll No: NPTEL19CS59S42310288

To
DR K SATYA RAJESH
ET3 MYHOME COMPLEX BESIDE SRR COLLEGE
MACHAVARAM
VIJAYAWADA
KRISHNA
ANDHRA PRADESH
520004
PH. NO :9494477497

Score	Type of Certificate
>=90	Elite+Gold
75-89	Elite+Silver
>=60	Elite
40-59	Successfully Completed
<40	No Certificate

No. of credits recommended by NPTEL:1
An additional 1 credit may be awarded if the University deems it fit, based on the actual student effort involved.

NPTEL Online Certification
(Funded by the Ministry of HRD, Govt. of India)

This certificate is awarded to

DR K SATYA RAJESH
for successfully completing the course

Python for Data Science

with a consolidated score of **45** %

Online Assignments	15/25	Programming Exam	6.75/25	Proctored Exam	23.41/50

Total number of candidates certified in this course: 4426

Devendra Jalihal

Prof. Devendra Jalihal
Chairman
Centre for Continuing Education, IITM

Aug-Sep 2019
(4 week course)

Prof. Andrew Thangaraj
NPTEL Coordinator
IIT Madras

Indian Institute of Technology Madras

swayam

Network Database Security in Wireless Sensor Networks with Intellectual Access of using Outlier Detection Techniques

K.Satya Rajesh, N.RaghavendraSai, Ch.Nagamani

ABSTRACT---In the field of information mining, exceptions are likewise alluded to as outliers, variations from the norm, discordant perceptions, or freaks. Other application spaces may utilize terms like exceptions, amazements, or contaminants. Every one of these wordings is catching a deviation from an expected ordinary information demonstration. In this research work, another system that comprises of an Intelligent Agent Based Access Control subsystem and Intrusion Detection subsystem for securing the Web Database has been proposed and actualized. With a specific end goal to give a viable access control framework, new access control variable based math and new arrangements utilizing rules have been proposed and executed. Keeping in mind the end goal to perform interruption and outlier identification successfully, a half and half Intelligent Agent based Intrusion Detection framework has been proposed in this work which enhances the security of the network database.

Keywords: Wireless sensor networks, Intrusion Detection System

Fig. 1 Multi-hop packet transmission in a sensor network

I. INTRODUCTION

Wireless sensor networks (WSN) were develop for a broad range of social and military applications, such as production line, object tracking, infrastructure monitoring, habitat sensing, and frontline surveillance [1], [2]. One basic feature of WSN function is to gather information in between the source station and the target location(s) where the target phenomena were observed. Aforementioned feature usually desire multi-hop packet transmission if the distance from the source to the target phenomena is large. For example, a cluster-based sensor network [3], [4] necessitates a different source of information must travelled single-recipient communication paradigm via multi-hop packet transmission (shown in Figure 1). Further, to decrease communication interference in highly dense wireless networks, the communication range of radios must be decreased. This results in multi-hop transmission as well.
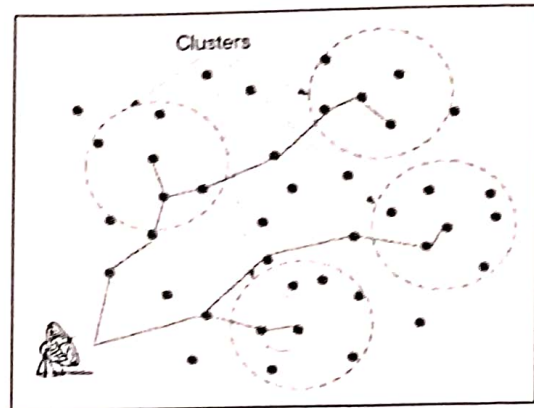
One suitable methodology for reducing the radio power consumption is the so-called modulation scaling [5], which discovers the tradeoff between transmission energy and time duration by that condition, the modulation level to equal the different traffic load. An important examination is that in many coding schemes, suppose w(t) is the energy used for transmitting a packet over units (t) of time, w(t) is a non-negative, monotonically decreasing, and strictly convex function of (t) [6].

Therefore, the challenge is to identify patterns in data that do not align with the behavior predicted. Outlier detection is commonly used in various applications, for example credit card fraud detection, insurance and healthcare, cyber safety intrusion detection, defense critical systems malfunctioning and enemy military surveillance. Outer identification is important because outliers in data often mean interesting (and often critical) actionable information in a wide variety of fields of operation.

II OUTLIER LOCATION IDENTIFICATION METHODS

In numerous data processing tasks, a large amount of data is being collected and processed. One prime step in procurement a coherent analysis is the detection of anomalous observations. Outlier detection refers to the problem that trends are observed in data are not consistent with the normal expected behaviour. Outlier detection involves the process of identifying data objects that do not

compromise with the remaining objects in the data set. Such irregular patterns also involve outliers, deviations, exceptions, discordant findings, faults, aberrations, failures, sounds, accidents and errors as well as surprises, novelties, toxins, etc. In spite of the terms noise or error, these are also considered to carry important information.

For a number of applications, additional detection procedures have been proposed, such as credit card fraud detection, clinical trials, irregularity analysis of the voting system, data cleaning, weather intrusion, geographic information systems, sport performance analyzes and other datamining assignments. Detecting outliers is of utmost importance as they might lead to model misspecification, biased parameter estimation and improper results. This process of detecting outliers should be done prior to analysis and modeling.

III. NETWORK OUTLIER DETECTION SYSTEM ALGORITHM

The proposed Network outlier detection system(NODS) algorithm will effectively identifies the anomalies in the network database system and enhances the security of the network database.

- x is the initial record from dataset.
- R is the Record set.
- K is the distance from one node in network to other node.
- A is the cluster set created from K with all records
- Identify() function is used for detecting outliers in the network with R Records.

```
Function NODS()
Let   { x_i ∈ R^4, i=1,...,N } be the data vectors in the training set;
Calculate the distance   K(x_i, x_i) to origin for each data vector x_i;
Obtain
A = {K (x_i, xi), i=1,...,N};
return R = Identify (A, 1, n, [v_n]+1)
Function Identify (list, l, r, n)
if
l=r
return list  [l]
anomaly =   l + floor (rand () • (r−l+1))
anomaly = Outlier(list,   l, r, anomaly)
if   n = anomaly
return list [n]
else if   n < anomaly
return Identify(list,    l, anomaly − 1, n)
else
return Identify (list, anomaly + 1, r, n)
```

In the proposed method, Let R is the Data vectors considered in the trained data set. Distance K is calculated between hubs in the network. Identify() function is called which is used for detecting outlier IDs in the considered network. Outlier() function considers for the highlighting of identified outliers from the network so as to take necessary action on the network for secure data transmission. The identify() is called in any one of the three cases i.e. if all anomalies are identified, then the list will be returned. If

specified anomalies are not identified, then again Identify() is called otherwise other anomalies are identified till all records are monitored.

IV RESULTS

The productivity of the proposed Network Based Outlier Detection calculation is likewise contrasted with Nested Looping calculation utilizing the informational indexes. The new proposed calculations are nearly tried utilizing different informational collections. The execution of the above said calculations are pictorially represented.

It likewise demonstrates the different execution time of the above said calculation against the quantity of information focuses. The execution time is appeared in seconds. This diagram is drawn by taking the quantity of information focuses in X-hub and the execution time in Y-pivot.
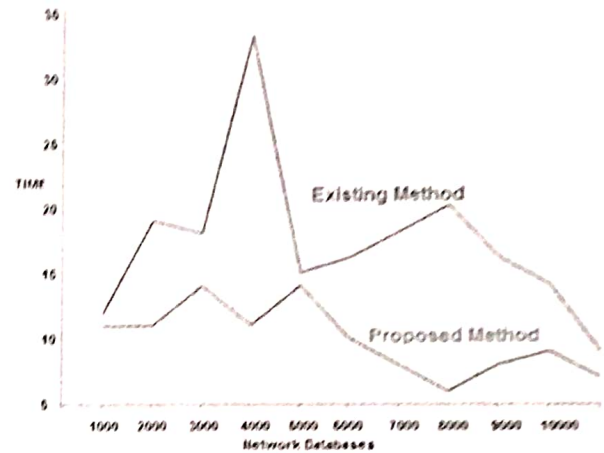

Fig 5.1 Comparison of Execution Time amongst proposed and existing calculations

The outlier detection rate analysis based on node longitude location value and the degree of the node is illustrated in the below graph.
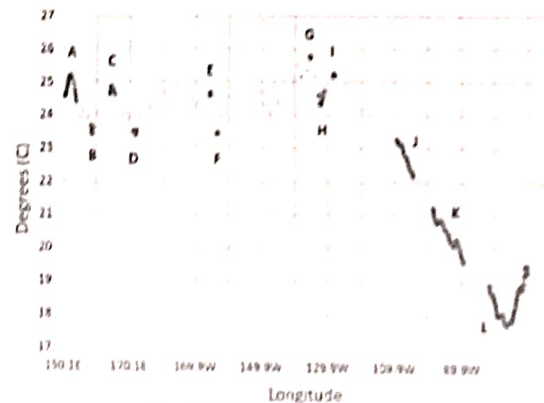

Fig 5.2 Outlier Detection Rate

V CONCLUSION

The proposed framework introduced a two-level half and half interruption location technique in light of directed and anomaly strategies. This technique shows extraordinary execution in perceiving remarkable characterization ambushes and likewise tremendous scale attacks new and presented strikes when attempted with a NSL KDD datasets. In furthermore considers, this system will attempt to influence a more suitable social affair to approach in light of speedier and profitable classifiers with a specific end goal to make a basic duty in the examination of the outlier acknowledgment. In this research work, another system that comprises of an Intelligent Agent Based Access Control subsystem and Intrusion Detection subsystem for securing the Web Database has been proposed and actualized. With a specific end goal to give a viable access control framework, new access control variable based math and new arrangements utilizing rules have been proposed and executed. Keeping in mind the end goal to perform interruption and outlier identification successfully, a half and half Intelligent Agent based Intrusion Detection framework has been proposed in this work which enhances the security of the network database.

Ch.Nagamani, Research Scholar, Department of Computer Science, AcharyaNagarjuna University, Guntur, A.P, India.Pursing Ph.D. from Nagarajuna University. Here interested areas are Data warehousing and Data mining, Data Analaytics Computer Networks.

REFERENCES

1   D. Estrin. L. Girod. G. Pottie, and M. Srivastava. "Instrumenting the world with wireless sensor networks," in *The International Conference on Acoustics, Speech and Signal Processing*, May 2001.

2   G. J. Pottie and W. J. Kaiser, "Wireless integrated network sensors," *Comunications of the ACM*, vol. 43, no. 5, pp. 551–558, May 2000.

3   M. Singh and V. K. Prasanna, "A hierarchical model for distributed collaborative computation in wirelss sensor networks," to appear on 5th Workshop on Advances in Parallel and Distributed Computational Models.

4   Y. Yu, B. Krishnamachari, and V. K. Prasanna, "Cluster-based lightweight middleware for a class of wireless sensor networks," submitted to IEEE Network Magazine.

5   C. Schurgers, O. Aberhome, and M. Srivastava, "Modulation scaling for energy-aware communication systems," in *ISLPED*, 2001, pp. 96–99.

6   B. Prabhakar, E. Uysal-Biyikoglu, and A. E. Gamal, "Energy-efficient transmission over a wireless link via lazy packet scheduling," in *INFOCOM*,

7   2001.

8   W. Ye, J. Heidemann, and D. Estrin, "An energy-efficient MAC protocol for wireless sensor networks," in *Proc. of INFOCOM*. New York, June 2002, pp. 1567–1576.

AUTHORS PROFILE

1. ***Dr K. Satya Rajesh*** received Ph.D Degree from Rayalaseema University, Kurnool. He received Master's degree M.C.A from ManonmaniamSundarnar University in 2003. He received Master's degree M.Tech in Computer Science & Engineering from AcharyaNagarjuna University in 2010. He is currently acting as a Head of the Department of Computer Science in C.S.T S Govt. Kalasala, Jangareddygudem, W.G Dist A.P., India. His research interests are Computer Networks & Sensor Networks. He had published several papers in National and International Conferences & International Journals. He is a member of IACSIT, IAENG and also review member of many Journals.

N.RaghavendraSai. Assoc. Prof. Dept of CS &Engg, KoneruLakshmaiah Education Foundation, Vaddeswaram, AP, India. His interested areas are Data warehousing and Data mining Computer Networks.

DK International Research Foundation

FACULTY AWARDS
DKIRF - 2019

This is to certify that

Dr. K. Satya Rajesh

**Department of Computer Science,
C.S.T.S Government Kalasala, Jangareddigudem,
West Godavari, Andhra Pradesh**

is conferred a special recognition under

Best Researcher

for the year 2019. This award endorses or concedes a vivid researcher to continue their work, assure accessible and congruous technology in the application of education.

Date   : 29th December 2019
Venue : DS Hotel, Perambalur

C. Ashok Kumar
Founder & Chairman

ADIKAVI NANNAYA UNIVERSITY
RAJAMAHENDRAVARAM

Certificate of Appreciation

The services of Dr./Prof. _K. Satya Rajesh_

for delivering an expert lecture in the Workshop on "DATA ANALYSIS AND ANALYTICS"
held at Department of Computer Science & Engineering, University College of
Engineering, Adikavi Nannaya University, Rajamahendravaram on 22nd February 2020.

CONVENER
Prof. P Suresh Varma
CONVENER
DAA-2020

ADIKAVI NANNAYA UNIVERSITY

RAJAMAHENDRAVARAM

Certificate of Participation

This is to certify that Dr/ Mr/Ms/Mrs __K. Satya Rajesh__

has participated in the Workshop on "*DATA ANALYSIS AND ANALYTICS*", organized by

Department of Computer Science & Engineering, University College of Engineering,

Adikavi Nannaya University, Rajamahendravaram on 22nd February 2020.

CONVENER
Prof. P Suresh Varma
CONVENER
DAA-2020

3rd International Conference on Multidisciplinary Research Trends in Arts, Science, Engineering & Technology

ICMRTASET-2019

Certificate of Presentation

This is to certify that DR K.SATYA RAJESH

bestowed paper titled NETWORK SECURITY ISSUES USING ANT COLONY OPTIMIZATION TECHNIQUES

at the 3rd International Conference on Multidisciplinary Research Trends in Arts, Science, Engineering & Technology (ICMRTASET-2019) at Dhanalakshmi Srinivasan Hotel, Perambalur, Tamilnadu on 29th December, 2019.

Chairman / DKIRF

President / IACRD

President / SMCRAC

Organized by

DKIRF
DK International
Research Foundation

IACRD
International American Council
for Research & Development

SMCRAC
Saint Martin's Centre for Research &
Accreditation Commission

Oral Presentation Certificate

International Conference On Recent Challenges & Explorations In Engineering Technology & Science

Organised By

RAMACHANDRA College of Engineering

Accredited by NAAC B++, NBA (ME, ECE & CSE), Approved by AICTE, NewDelhi and
Permanently Affiliated to JNTUK, Kakinada, An ISO 9001:2015 Certified Engineering College

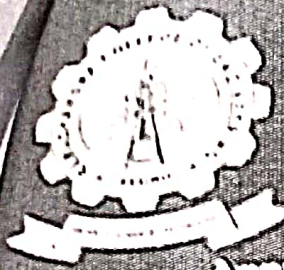Vatluru (V), Pedapadu (M), Eluru - 534007, W.G.Dt., AP

ISO 9001:2015

ELSEVIER SSRN   Google scholar   ROAD   DOAJ DIRECTORY OF OPEN ACCESS JOURNALS

This is to certify that the paper entitled ..Network...Database...Security...In..Wireless..Sensor..Network.. With..Intellectual...Accessing..Using..Public..Relation..Technique..With authors(s) ...K...Satya...Rajesh.......... At..Raghavendra..Sai.,......Ch.Nagamani..was presented by............. K..Satya...Rajesh............................ in the ICRCEETS-2k19 International Conference On Recent Challenges & Explorations In Engineering Technology & Science, held on 21st December 2019 at Ramachandra College of Engineering.

Paper was presented infront of Panel Members of IJIEMR and Standard Solutions.

Organising Secretary

Convener

Principal

RAMACHANDRA
College of Engineering

Accredited by NAAC B++, NBA (ME, ECE & CSE)
Approved by AICTE, New Delhi, Permanently affiliated by JNTUK
An ISO 9001:2015 Certified Engineering College
Vatluru(V), Pedapadu (M), Eluru 534007,
W.G.Dt., A.P

IN ASSOCIATION WITH
IJIEMR, STANDARD SOLUTIONS

9 781675 714706

Index

Network Database Security In Wireless Sensor Networks With Intellectual Access Of Using Outlier Detection Techniques

K.Satya Rajesh *, HOD, Dept. of Computer Science, C.S.T.S Govt, Kalasala, Janagreddygudem, W.G. Dist, A.P ksatyarajeshcsc@gmail.com

N.Raghavendra Sai, Assoc. Prof, Dept. of CS & Engg, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP

Ch.Nagamani, Research Scholar, Department of Computer Science, Acharya Nagarjuna University, Guntur, A.P

Abstract

In the field of information mining, exceptions are likewise alluded to as outliers, variations from the norm, discordant perceptions, or freaks. Other application spaces may utilize terms like exceptions, amazements, or contaminants. Every one of these wordings is catching a deviation from an expected ordinary information demonstration. In this research work, another system that comprises of an Intelligent Agent Based Access Control subsystem and Intrusion Detection subsystem for securing the Web Database has been proposed and actualized. With a specific end goal to give a viable access control framework, new access control variable based math and new arrangements utilizing rules have been proposed and executed. Keeping in mind the end goal to perform interruption and outlier identification successfully, a half and half Intelligent Agent based Intrusion Detection framework has been proposed in this work which enhances the security of the network database.

Keywords

Wireless sensor networks, Intrusion Detection System

A BRIEF STUDY ON VULNERABILITY IN CYBERSECURITY

J. RAJA SRIKANTH, M.TECH(CSE)

Dept. of Computer Science, CSTS Govt. Kalasala, Jangareddigudem, Eluru Dt.
Email: rajasrikanth.jallipalli@gmail.com

Abstract : A vulnerability in cyber security is referred to as a flaw or weak point in the hardware, software, internal controls, technical controls, physical controls, or any other safeguards that could allow the system's security policy to be violated through either accidental activation or purposeful exploitation. In cybersecurity, similar terms such as risk, threat, vulnerability, etc., might sound similar but have very different meanings, which will be covered further. Various types of cybersecurity vulnerabilities are also covered. An area or platform where information on computer security flaws is gathered, kept up to date, and shared is known as a vulnerability database. Vulnerability databases are very often referred to patch known vulnerabilities and prevent exploitation.

I INTRODUCTION

In simple terms, vulnerability means the state of being open or susceptible to getting attacked and hurt. So how does this relate to cybersecurity? In cybersecurity, a [1] vulnerability is defined as a flaw or weakness in the hardware, software, internal controls, technical controls, physical controls, or any other safeguards that could allow the system's security policy to be violated through either inadvertent activation or deliberate exploitation.

Hackers and attackers exploit these vulnerabilities to cause damage to the systems and data. Various types of vulnerabilities can be classified into six broad categories.

Cybersecurity vulnerabilities are weaknesses in systems, networks, applications, or processes that can be exploited by attackers to gain unauthorized access, steal data, or disrupt operations.

II VULNERABILITIES FACTORS

a) **Software flaws**: Software bugs can allow attackers to execute malicious code, steal data, or take control of systems.

b) **Misconfigurations:** Improper configuration of systems and networks can create security gaps that attackers can exploit.

c) **Weak passwords:** [2] Poor password management practices can make it easy for attackers to gain unauthorized access to systems and accounts.

d) **Human error:** Human mistakes, such as clicking on phishing links or opening malicious attachments, can lead to security breaches.

III TYPES OF CYBERSECURITY VULNERABILITIES

There are many different types of cybersecurity vulnerabilities, but some of the most common include:

a) **Zero-Day Vulnerabilities:** These are vulnerabilities that are unknown to the software vendor and have not yet been patched. Zero-day vulnerabilities are often exploited by sophisticated attackers to launch highly targeted attacks.

b) **Remote code execution (RCE) vulnerabilities:** These vulnerabilities allow attackers to execute malicious code on a victim's system without requiring any user interaction. RCE vulnerabilities can be exploited to steal data, install malware, or disrupt operations.

c) **Injection vulnerabilities:** These vulnerabilities allow attackers to inject malicious code into legitimate applications. Injection vulnerabilities can be exploited to steal data, execute arbitrary commands, or disrupt operations.

d) **Broken authentication and session management vulnerabilities:** These vulnerabilities allow attackers to steal user credentials or hijack user sessions. This can allow attackers to gain unauthorized access to systems and data.

e) **Data exposure vulnerabilities:** These vulnerabilities allow attackers to access sensitive data that is not properly protected. This data can include customer records, financial information, or trade secrets.

IV CYBERSECURITY VULNERABILITY DIFFERENT FROM A CYBER SECURITY THREAT

A flaw[3] or weakness in the hardware, software, internal controls, technological controls, physical controls, or any other safety measure that could allow the system's security policy to be broken by accidental activation or intentional exploitation is referred to as a vulnerability.

A threat can be described as an act or intention to cause damage. A cybersecurity threat can range from malware to targeted denial-of-service attacks. These threats use vulnerabilities and exploit them. The potential of a successful cyberattack is another way to characterize threats.

V DIFFERENCE BETWEEN VULNERABILITY AND RISK

A risk implies uncertainty or the possibility of something terrible happening. Risk is the likelihood or potential for harm, injury, loss, or any

other undesirable event brought on by vulnerabilities either within or out and preventive measures can prevent that. It is impossible to eliminate risk, Risk management can be done to prepare and deal with threats. Not fixing vulnerabilities results in increased risk.

Risk[4] is directly proportional to the number of threats on the system, which is dependent on the number of vulnerabilities. Risk can be of two types that are external and internal. When the risk is caused by external factors such as attackers. When the risk is caused by internal factors such as mal intent of an employee, etc.

VI CAUSES VULNERABILITIES

There are numerous causes for vulnerabilities in cybersecurity which include outdated software, design flaws, security misconfiguration, [6] personnel involved in the design, testing, and usage process, bugs in the software, and unexpected errors such as buffer overflows.

The software systems can be complex, thus resulting in vulnerabilities due to misconfigurations.

Sometimes, the end user falls into the trap of social engineering attacks, causing much more damage.

The end-user not updating the software can also result in causing vulnerability for the system.

Sometimes unintentional bugs and flaws remain in the product when there are design issues and the product is not adequately tested, causing a vulnerability.

Not taking into account errors such as memory errors, including buffer overflow, causes the vulnerability.

VII MITIGATE CYBERSECURITY VULNERABILITIES

There are a number of steps that organizations can take to mitigate cybersecurity vulnerabilities, including:

a) **Regularly patch software:** Software vendors regularly release security patches to fix known vulnerabilities. Organizations should install these patches as soon as possible to protect their systems.

b) **Implement strong password policies:** [5] Organizations should implement strong password policies that require users to create complex passwords and change them regularly.

c) **Educate employees about security best practices:** Employees should be educated about security best practices, such

as how to identify and avoid phishing emails and malicious attachments.

d) **Use security solutions:** Organizations should use security solutions, such as firewalls, intrusion detection systems, and antivirus software, to protect their systems and data.

VIII CONCLUSION

Cybersecurity vulnerabilities are a serious threat to organizations of all sizes. By understanding the different types of vulnerabilities and taking steps to mitigate them, organizations can help to protect themselves from cyberattacks.

CONCLUSION

Cybersecurity has evolved dramatically over the centuries, from the early days of telegraphy to the complex digital landscape of today. Threats have grown in sophistication, necessitating continuous innovation in defense mechanisms. As technology advances, the future of cybersecurity remains uncertain, but one thing is clear: the importance of protecting our digital world is paramount.

References

[1] Lun, Y.Z., D'Innocenzo, A., Malavolta, I., Di Benedetto, M.D.: Cyber-physical systems security: a systematic mapping study. arXiv preprint arXiv:1605.09641 (2016).

[2] Razzaq, A., Hur, A., Ahmad, H.F., Masood, M.: Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. In: Autonomous Decentralized Systems (ISADS), 2013 IEEE Eleventh International Symposium on 2013, pp. 1-6. IEEE

[3] Von Solms, R., Van Niekerk, J.: From information security to cyber security. computers & security 38, 97-102 (2013).

[4] Benson, V., McAlaney, J., Frumkin, L.A.: Emerging Threats for the Human Element and Countermeasures in Current Cyber Security Landscape. In: Psychological and Behavioral Examinations in Cyber Security. pp. 266-271. IGI Global, (2018)

[5] Bada, M., Sasse, A.M., Nurse, J.R.: Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672 (2019).

[6] Floyd, D.H., Shelton, J.W., Bush, J.E.: Systems and methods for detecting a security breach in an aircraft network. In: Google Patents, (2018)

ADVANCEMENTS IN PLANTS BIO-TECHNOLOGY FOR CROP IMPROVEMENT.

K.V.V.Sirisha
(Dept of commerce)
C.S.T.S Govt Kalasala
Jangareddygudem

V. Hanumantha Rao
(Dept of Economics)
C.S.T.S Govt Kalasala
Jangareddygudem

J. Raja Srikanth
(Dept of ComputerScience)
C.S.T.S Govt Kalasala
Jangareddygudem

1. Introduction

→plant biotechnology is a powerful tool-for the development of new plant traits and varieties
→ such new varieties must be produced on a large scale to achieve commercial Success and to satisfy the demand from se growers.
→Traditionally, new varieties were achieve d by the seed propagation Method
. →The improvement of woody fruit species by traditional plant breeding techniques has several limitations.
→ Developments in genetic engineering and Molecular biology techniques allowed the production of improved 7 and few agricultural products.
→ production of artificial seeds, bio- technology, plant made pharmaceuti- cals,
→ The current plant-tissue culture industry is estimated.

plant biotechnology can be defined :
→ Agricultural" biotechnology has been ways used to protect crops from devastating diseases
→Biotech crops can make farming more Profitable by increasing crop quality and yields Moy income cases increase

Plant physiology and environmental stress, mechanisms and adaptations:
→ plant physiology is the study of how different of plants function
→. Father philology Julius Sachs.
→It is broach it Geology that studies anatomy, biological molecules
→ The study of physiology is the study of life".

Environmental Stress:

→ Environmental stress refers to "Factors in person surrounds"
→ Environmental that Con cause emotional on mental strain in their lives.
→ Environmental stress is the deviation in environmental Conditions from species optima
→ Environmental stress refers to
→ physical, chemical, and biological
→ Environmental stresses External,

→ These are internal and they can increased levels of discomfort
→ adoption to the biological mechanics by which organisms environment to charges to their current environment .
→Adaption mechanism refers to modification that an individual organisms or individual in the new environment.
→ physiological adaptive mechanisms are observed behavior
4 main environmental stress:

1. catalysnic events

2.stress full life events

Plant Physiology and Environmental stress, Mechanisms and adaptations

* Plant physiology is a branch of study in botany dealing with the physiological processes or functions of Plants Plant physiology is a branch of study in Botany dealing with the physiological Processes or functions of plants.

*Plant Physiology is the study of how different parts of plants function

*Julius sects (1862): The father of plant Physiology

*The study of how living beings normally work

Father of physiology

Claude Bernad--The father of Physiology.

The branches of plant phisiology :

Plant Physiology is branch of botany that studies how plants work on their physiology.

plant Morphology (shape). Plant Ecology Interactions with the Environment) Phytochemistry (biochemistry of Plant Cell biology, genetic,biophysics, and Molecular biology

Class is plant physiology CBSE class

* determines plant growth development and Economic Production

* The Concept of structure and function, also referred to form and function

* father of Crop: Swaminathan

* father of Indian plant: Jagadish chandra Bose.

* Chlorophyll is a pigment that gives plants Their green color, and It helps Create Their own food Through photosynthesis

* Environmental stress refers to factors in a person's surroundings Can Cause Emotional Their lives or Environment that mental strain in

* 4 main In Environmental stresses

1.cataclysmic events

2. stress full life events.

3. daily hassler and

4.Ambient stressors

* Stress in Economics denotes, both human and naturally induced pressure on the Environment.

Plant physiology and Environmental stress. mechanisms and adaptations:

* Environmental adaptation involves improving aspects of information (Eg. signs clocks) objects (eng furniture positioning), condition's (noise) in the environment.

* Plant physiology is a branch of "study in Botany

→ destroy the ion balance conder Salt stress, it is necessary Otomatically. To Adjust and establish the ion balance in cells fon plan to living.

References :

https://www.routledge.com/Crop-Improvement-Biotechnological-Advances/Kumar-Thakur/p/book/9780367567095

https://www.sciencedirect.com/book/9780128185810/advancement-in-crop-improvement-techniques

https://www.vedantu.com/biology/biotechnology-in-agriculture

https://www.tandfonline.com/doi/abs/10.1080/15427520903584555

https://www.universitiespress.com/details?id=9788173716164

J. Ryshilath

Principal
CSTS Govt. Kalasala
angareddigudem - 5344