

# Study of Cyber Security with Nanotechnology

**Shalini Sharma<sup>1</sup>, Pushpendra Singh<sup>2</sup>, Nagendra Singh<sup>3</sup>, Akshay Sharma<sup>4</sup>**

<sup>1</sup>Assistant Professor, Deptt. of Mathematics, I.E.T., Khandari Campus, Dr. B.R. Ambedkar University, Agra

<sup>2</sup>Assistant Professor, Deptt. of Physics, I.E.T., Khandari Campus, Dr. B.R. Ambedkar University, Agra

<sup>3</sup>Assistant Professor, Deptt. of Mechanical Engineering, I.E.T., Khandari Campus, Dr. B.R. Ambedkar University, Agra

<sup>4</sup>Software Engineer, Plural sight India Pvt. Ltd., Bannerghatta Main Road, Bengaluru, Karnataka  
**Corresponding Author Orcid ID: 0009-0005-5392-6987**

## ABSTRACT

Cyber Security is most important in the field of information technology. Now a days, current world is run by technology and network connections. Securing the systems, important files, data, and other important virtual things and information have become one of the biggest challenges in the present day. At present ‘cyber crimes’ are increasing immensely day by day, therefore the development of the fresh technology in cyber security is necessary. There is a need for modern cryptography to provide protection and to ensure that information that is transmitted in cyberspace remains unbroken and secure. It is required to improve the techniques which make sure the highest possible level of security to internet users. The studies of Nanotechnology include the applications of various fields of science. Nanotechnology applications include new and Powerful bio-detection schemes that will improve intelligent threat at the point of care and unique ways of encoding structures that can be used to secure computer systems. This research paper is centre of attention on challenges faced by cyber security on the latest technologies, ethics and the trends changing the performance of cyber security.

**Keywords— Cyber crime, Cyber Security, Cyber Ethics and Nanotechnology Applications.**

## 1. Introduction

Now a days many latest technologies are changing the lifestyle of the mankind. But Even these latest technologies like mobile computing, cloud computing, net banking, E-commerce etc. also needs high level of security. These technologies hold some important information regarding a person therefore their security has become necessary. Cyber security is most essential because military, government and corporate organizations collect and stock unprecedented quantities of data on PCs and other devices. Increasing cyber security and preserving critical information, infrastructures are essential to each nation's security and economic welfare. Cyber security protects our computer and our company's information from cyber attacks and saves them billions of dollars. For development of new services as well as government policies, it is required to protect Internet users which become integral to the fight against cyber crime. Since technical analysis alone cannot prevent any crime, therefore it is government's responsibility as lawmaker and enforces, to allowed to investigate and prosecute cyber crime effectively. Today's governments are demanding strict laws on cyber securities in order to stop the loss of some important information. Now a days Nanotechnology plays an important role in cyber security by allowing the development of more complex cryptographic schemes. In quantum cryptography the creation of quantum chips are more secure than traditional cryptographic hardware.

## 2. Literature Review:

Cybercrime is a global problem, it poses a bigger threat to large international companies, governments and banks. In a society, the people and tools must all protector to generate a real defence on or after cyber-attacks. Nanotechnology and cyber security relates to the development of brilliant threat detection systems. Many corporations are pursuing research that examines the possible benefits of using nanotechnology to closely resemble biological systems in digital computers. Nano scale AI systems hold much promising for cyber security perspective.

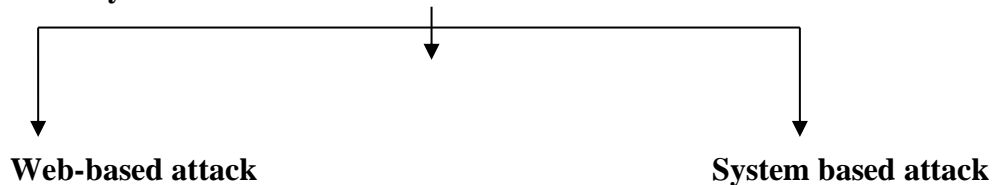
## 3. Cyber-crime:

Cyber-crime may be defined as any illegal activity that uses a computer for the storage of evidence or computer network. The crimes that have been made possible by computers are known as cybercrimes. Cybercrime may harm someone's security or finances. These cybercrimes have become as considerable problem to people and nations. The different types of cybercrimes are email frauds, banking frauds, ransomware attacks, cyber espionage, identity theft, click jacking, spyware, etc. The cyber-crimes will increase along with the technological growth since technology is playing a significant role in a person's life.

## 4. Types of Attack:

A cyber-attack is an unfair advantage of computer systems and networks. Due to the dependency on computer system, the illegal computer activity is increases and changing like any type of crime. Cyber-attacks can be classified into the following two categories as follows:

### Classification of Cyber Attack



**A. Web-based attack:** Web-based attack occurs on a website or web applications.

#### (i) Injection attacks:

Some data will be injected into a web application to manipulate the application and fetch the required information; this type of attack is known as injection attack.

**Example-** SQL Injection, code Injection, XML Injection etc.

#### (ii) DNS Spoofing:

A type of computer security hacking is known as DNS Spoofing. Attacker replace the IP addresses which are stored in the DNS server. In DNS spoofing, attackers steal data of business or private user.

#### (iii) Phishing:

In Phishing the attacker try to steal sensitive information like user login credentials and credit card number etc. Attackers used this technique by taken control of another victim's system.

#### (iv) Brute force:

Brute force attack uses a trial and error method. The criminals to crack encrypted data or security and access to a website, account or network.

#### (v) Denial of Service:

In DoS cyber attack, a server or network resource are unapproachable to the users. DoS attack have two methods: flooding services and crashing services. Single system and single internet connection is using in this system to attack a server.

#### (vi) URL Interpretation:

It is a type of attack where we can change the certain parts of a URL, and attacker who is not authorized to browse, can make a web server to deliver web pages.

**(vii) File Inclusion attacks:**

The files which are available on the web server or to execute malicious files on the web server can be access unauthorized or essential by File Inclusion attack.

**(viii) Man in the middle attacks:**

In this attack an attacker intercepts the connection between client and server and where attackers interrupt an existing conversation or data transfer. Acts as a bridge between them. In this way, an attacker will be able to read, insert and modify the data in the server and client connection.

**B. System Based Attack:**

These are a type of malicious software program inserted by a third party that spread throughout the computer files without the knowledge of a user. Some of the important system-based attacks are as follows:

**(i) Virus:**

Without the knowledge of a user, a type of malicious software program that spread throughout the computer files is known as Virus. It is reproducing itself malicious computer program that reproduce by inserting copies of itself into other computer programs when executed. It can also perform instructions that cause harm to the system.

**(ii) Worm:**

The primary work of worm is to reproduce itself and spread to uninfected computers. It is a type of malware. It works same as the computer virus. Worms often emanate from email attachments that appear to be from trusted senders.

**(iii) Trojan horse:**

It is a type of malware that occurs unpredicted changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intention. It appears to be a normal application but when executed some malicious code will run in the background.

**(iv) Backdoors:**

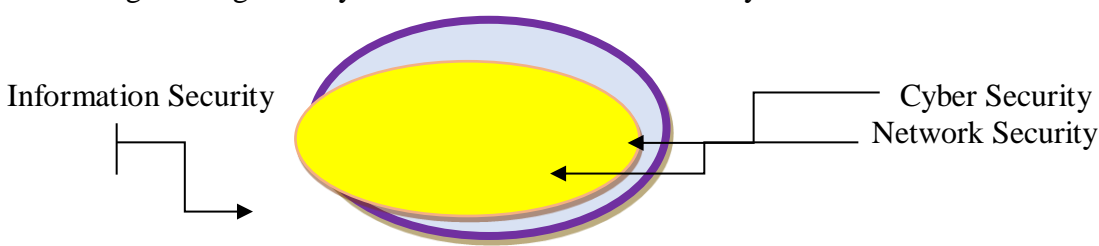
As the name suggest, it is a method in which hackers installing backdoor malware through a fishing email, that bypasses the usual authentication process. A service provider create a backdoor so that an operating system can be accessed.

**(v) Bots:**

A bots is an automatic process that interacts with other network services. When they receive specific input, some bots program run automatically, while others only execute commands. The crawler, chat room bots and malicious bots are common examples of bots program.

**5. Cyber Security:**

Security means the mechanism of protecting anything. Computer systems, mobile devices, servers, electronic networks and data can be protected by practice of cyber security from malicious attacks. In the organizations privacy and security of the data will always be in top priority. Now a day, in this world all the information is maintained in a digital or a cyber form. In the case of home users, cyber-criminals would continue to plan social media sites to steal personal data. It is for all person to take all the required security measures during social networking and bank transactions. Governments must have an outline for how Processes they contract with together attempted and popular cyber attacks. Some well-respected outline can escort for us. It clarifies how we can recognise bouts, protect organisations, notice and reply to threats and improve from successful occurrences. Security means the mechanism of protecting anything. A commercial or society could look a huge damage if they are not sincere about the safety of their online event.



**6. Difference between Network Security and Cyber Security:**

| S. No. | Parameters                | Network Security   | Cyber Security  |
|--------|---------------------------|--|---|
| 1.     | <b>Definition</b>         | Network security is a feature that protects data as it travels through and beyond an organization’s network. As a result, it protects firm data from wicked employees who are not authorized to view specific sensitive information. | Cyber security is a way that protects a company’s device and server data. In other words, it serves as an extra layer of defence against cyber criminals. |
| 2.     | <b>Data</b>               | Network security defend the data flowing over the network. Network security secure the transit data only. It protects anything in the network realm.   | It protects the data stored in the devices and servers. Cyber security secure the entire digital data. It protects everything in the cyber realm.         |
| 3.     | <b>Hierarchy</b>          | Network security is a subset of cyber security.  | Cyber security is a subset of information security.   |
| 4.     | <b>Viruses</b>            | Network security deals with the defence from DOS attacks, viruses, and worms.  | It deals with the protection from cyber-frauds and cybercrimes that includes hacking and pre-texting.   |
| 5.     | <b>Strikes against</b>    | Network Security strikes against Trojans.  | Cyber Security strikes against cyber frauds and cyber attacks.  |
| 6.     | <b>Security</b>           | It secures the data travelling across the network by terminals.  | It deals with the protection of the stored data.  |
| 7.     | <b>Examples</b>           | Example of Network security are Multi-factor authentication, software updates, and rigorous password regulations.  | Examples of cyber security precautions are to secure sensitive data, online authentication, and up-to-date information.                                   |
| 8.     | <b>Popular job titles</b> | Two popular job titles are Network Security Engineer and Network Security Architect.   | Two popular career titles are Cyber Security Architect and Cyber Security Analyst.  |
| 9.     | <b>Job role</b>           | In network security the job role of professional lies in safeguarding an organization’s IT infrastructure.   | A cyber security specialist is skilled in the protection, detection, and recovery of cyber security threats.  |

**7. What is Nanotechnology?**

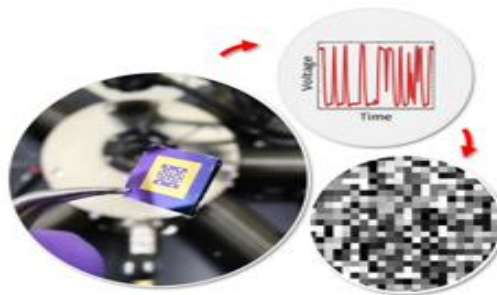
Nanotechnology is unite the field of physics, chemistry, and engineering. From the last few years, scientists and engineers have done some considerable research on designing and engineering materials down at the small groups of atoms. Because this technology is involves on microscopic level, it is called nanotechnology. Nanotechnology is one of the burning fields in science, business and news these days. The word ‘Nano’ has a big potential and is speedy intimate into the world’s consciousness. Nano, mean something is very small. The size of a Nanometer is one billionth of a meter which is about 100,000 times smaller than the human hair’s width. Nanotechnology involves elaboration and application of materials at a Nanoscale. Nanotechnology can be applied to a variety of applications including industrial and military applications

## 8. Nanotechnology Applications in Cyber Security:

Now a day scientists designing materials. These materials are layering one by one to create with super properties, like ultra strength and flexibility.

### (i) Nanotechnology in Cryptography:

The use of Nanotechnology is to improve cyber security with development of Nanoscale chip technology. Cryptographic keys are generated in computers using pseudorandom number generators (PRNGs). Pseudorandom number generators is an algorithm for generating a sequence of numbers whose properties approximate the properties of sequences of random numbers. Bangalore-based Indian Institute of Science (IISc) has developed a True Random Number Generator (TRNG) device; random numbers are generated using the random motion of electrons. TRNG device consists of an unnatural electron trap set up by thin layers of matter of black phosphorus and Graphene. When an electron is trapped, the current measured from the device increases, and decreases when it is released. Electrons move in and out of the trap in a irregular manner, the measured current also changes randomly. The generated random number is determined by the timing of this change. Nano-scale allow the creation of non-leaky quantum chips that are much more secure, while the standard chips based on CMOS transistor can currently leak information. They are designed to be unbreakable in case of data breach attack. Quantum cryptography is already applied by banks for Nano-scale architecture.



The image of the fabricated electronic chip that generates the random number

### (ii) Nanotechnology Influence on threat detection:

IT leaders gave the opinion on 21 July 2020 that Cyber security and nanotechnology can cross over satisfactorily in the field of threat detection. Nanotechnology is useful for creating computers that more closely imitate the human brain. Field of Artificial Intelligence is the simulation of human intellect processes by computer system.

Smart computer systems based on nanotechnology offered the intelligent threat detection efficiency, monitor complicated systems like energy and weapons. Intelligent threat detection could quickly recognize and isolate security threats.

Many of the applications of these "intelligent" systems help organizations monitor energy or weapons systems that require software so complicated that it exceeds a human's ability to write and verify the software and its performance.

### (iii) Nanotechnology with National Security:

Nanotechnology could also miniature sensors and devices. In terms of security, ingested devices could also be used to prepare assured authentication and encryption. With the help of high sensitivity of Nano sensors, the work erect for public use can be routinely tested and small amounts of contaminants can be detected.

Many another promising area of crossover for nanotechnology and cyber security relates to the development of truly intelligent threat detection systems. The researcher examines benefits that may be reasonable for using nanotechnology to replicate biological system in digital computers are pursuing by several organization.

Block chain technology is an advance database mechanism which reduces weakness, implements robust encryption and more efficiently validates data and integrity. It can even eliminate the need



for specific passwords; often consider the weakest link in cyber security. In the network, transaction is recorded with every node, making it challenging for hackers to steal data, except in cases where platform-level vulnerability exists.

From a cyber security view, nanoscale AI systems hold much promise. They quickly identified emerging threats and isolate them, they could also be programmed to take proactive measures to shut down incoming threats. thus, nanotech and AI provide strength to solve the skills shortage that curse the cyber security industry.

## 9. Conclusion:

Nanotechnology has been already accepted by industrial sectors, such as the information and communications sectors, food technology as well as in cosmetics/ medical products and medicines. Nano materials may also provide new opportunities for the depletion of environmental pollution. Cyber security is one of the most important feature of the developing very quickly digital world. It is impossible to deny the threats of it, so it is extremely important to learn how to defend from them and educate others how to do it too.

## References:

1. Sheth Ashwini, Bhosale Sachin, Bukhari Adnan. "A Survey on Cyber Security" Contemporary Research in India, pp.15-20, April, 2021
2. Vidhya P.M. "Cyber Security -Trends and Challenges" International Journal of Computer Science and Mobile Computing, pp.586 – 590, February, 2014,
3. Upadhyay Veenoo, Yadav Suryakant. " Study of Cyber Security Challenges Its Emerging Trends: Current Technologies" International Journal of Engineering Research And Management (IJERM), pp.48-52 July 2018
4. Singh Reetu. "A review on cyber security" International Journal of Advance and Innovative Research, Volume 8, Issue 2 (V) April - June 2021
5. Raman Smrutha. "Cyber Security: An challenge in itself" Hult International Business School, Published June 2, 2021
6. Shruti M.. "Types of Cyber Attacks You Should Be Aware of in 2023" In Simplilearn, May 5, 2023.( [Types of Cyber Attacks You Should Be Aware of in 2023 | Simplilearn](#))
7. Natarajan Megana. "Cybersecurity Strategies Influenced by Nanotech" In Itsecurity Wire. July21 2020
8. Khaled Salem Ahmad Amayreh; Ahmad Taufik Hidayah Bin Abdullah. "Conjunction in Expository Essay Writing by Jordanian Undergraduate Students Studying English as a Foreign Language (EFL)". International Research Journal on Advanced Science Hub, 4, 02, 2022, 24-30. doi: 10.47392/irjash.2022.006
9. Mohammadibrahim Korti; Basavaraj S. Malapur; Smita Gour; Rajesh M. Biradar. "Shuchi 1.0: Robotic System For Automatic Segregation of Waste & Floor Cleaning". International Research Journal on Advanced Science Hub, 4, 02, 2022, 31-37. doi: 10.47392/irjash.2022.007
10. Bhuneshwari Nayak; Rachana Choudhary; Roymon M. G.. "Isolation, Screening and Morphological characterization of Laccase producing fungi". International Research Journal on Advanced Science Hub, 4, 02, 2022, 38-43. doi: 10.47392/irjash.2022.008
11. Kotte Sowjanya; Munazzar Ajreen; Paka Sidharth; Kakara Sriharsha; Lade Aishwarya Rao. "Fuzzy thresholding technique for multiregion picture division". International Research Journal on Advanced Science Hub, 4, 03, 2022, 44-50. doi: 10.47392/irjash.2022.011
12. Mohammadibrahim Korti; Girish B. Shettar; Ganga A Hadagali; Shashidhar Shettar; Shailesh Shettar. "Voice-based direction control of a robotic vehicle through User commands". International Research Journal on Advanced Science Hub, 4, 03, 2022, 51-56. doi: 10.47392/irjash.2022.012
13. Nagendra Singh; Manoj Kumar Agrawal; Sanjeev Kumar Verma; Ashish Kumar Tiwari. "A Review on Effect of Stress and Strain Distribution on the AA5083 With Respect to Different

- Channel Angle of ECAP". International Research Journal on Advanced Science Hub, 4, 03, 2022, 57-66. doi: 10.47392/irjash.2022.013
14. Pravin T, M. Subramanian, R. Ranjith, Clarifying the phenomenon of Ultrasonic Assisted Electric discharge machining, "Journal of the Indian Chemical Society", Volume 99, Issue 10, 2022, 100705, ISSN 0019-4522, Doi: 10.1016/j.jics.2022.100705
15. R. Devi Priya, R. Sivaraj, Ajith Abraham, T. Pravin, P. Sivasankar and N. Anitha. "MultiObjective Particle Swarm Optimization Based Preprocessing of Multi-Class Extremely Imbalanced Datasets". International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems Vol. 30, No. 05, pp. 735-755 (2022). Doi: 10.1142/S0218488522500209
16. T. Pravin, C. Somu, R. Rajavel, M. Subramanian, P. Prince Reynold, Integrated Taguchi cum grey relational experimental analysis technique (GREAT) for optimization and material characterization of FSP surface composites on AA6061 aluminium alloys, Materials Today: Proceedings, Volume 33, Part 8, 2020, Pages 5156-5161, ISSN 2214-7853, <https://doi.org/10.1016/j.matpr.2020.02.863>.
17. Rajashekhar, V., Pravin, T., Thiruppathi, K.: A review on droplet deposition manufacturing a rapid prototyping technique. Int. J. Manuf. Technol. Manage. 33(5), 362–383 (2019) <https://doi.org/10.1504/IJMTM.2019.103277>
18. V.S. Rajashekhar; T. Pravin; K. Thiruppathi , "Control of a snake robot with 3R joint mechanism", International Journal of Mechanisms and Robotic Systems (IJMRS), Vol. 4, No. 3, 2018. Doi: 10.1504/IJMRS.2018.10017186
19. Nusrath Unnisa A; Manjula Yerva; Kurian M Z. "Review on Intrusion Detection System (IDS) for Network Security using Machine Learning Algorithms". International Research Journal on Advanced Science Hub, 4, 03, 2022, 67-74. doi: 10.47392/irjash.2022.014
20. Jyotshana Upadhyay. "Digital Marketing Practices Adoption in Micro, Small and Medium Businesses for Inclusive Growth". International Research Journal on Advanced Science Hub, 4, 04, 2022, 75-80. doi: 10.47392/irjash.2022.021
21. Arti Maurya; Kartick Chandra Majhi; Mahendra Yadav. "One Pot Synthesis of Lanthanum Doped Cobalt Selenate Electrocatalyst for Oxygen Evolution Reaction (OER)". International Research Journal on Advanced Science Hub, 4, 04, 2022, 81-87. doi: 10.47392/irjash.2022.022
22. Palash Mondal; Hritik Dey; Sreetama Paul; Shamik Sarkar; Apurba Das; Amit Karmakar. "Additively manufactured porous titanium alloy scaffolds for orthopaedics: An effect of process parameters on porosity". International Research Journal on Advanced Science Hub, 4, 04, 2022, 88-93. doi: 10.47392/irjash.2022.023
23. Kousik Bhattacharya; Avijit Kumar Chaudhuri; Anirban Das; Dilip K. Banerjee. "A Data Mining based study on Dengue Fever: A Review". International Research Journal on Advanced Science Hub, 4, 04, 2022, 101-107. doi: 10.47392/irjash.2022.025
24. Bharathi M; Senthil Kumaran S; Edwin Samson P. "Influence of Nano Silica Particles on Quasistatic Mechanical and Low Velocity Impact Properties of Carbon-Glass-Sunn Hemp/Epoxy in Intra-Inter Ply Hybrid Composites". International Research Journal on Advanced Science Hub, 4, 05, 2022, 120-133. doi: 10.47392/irjash.2022.032
25. Anukriti Sharma; Navdeep Singh. "Hybrid Modulation for Reduced Switches AC-AC Multi Frequency Converter". International Research Journal on Advanced Science Hub, 4, 05, 2022, 134-142. doi: 10.47392/irjash.2022.033
26. Lonescu Adrian M. "Nanotechnology and Global Security" JSTOR, pp.31-47 spring 2016