



Heritage Institute of Technology, Kolkata

CYBERSPHERE

**Department of CSE (IoT & Cyber Security
including Block Chain Technology)**



Heritage Institute of Technology, Kolkata

CYBERSPHERE



**Department of CSE (IoT & Cyber Security
including Block Chain Technology)**

TECHNOLOGY MAGAZINE

SPIES TECH

AI REVOLUTION

REVOLUTIONIZING
INDUSTRIES,
TRANSFORMING LIVES

CYBER FUTURE

HOW TECHNOLOGY IS
SAFEGUARDING THE
DIGITAL WORLD

GREEN TECH

SUSTAINABILITY MEETS
SMART SOLUTIONS

Unlocking the Potential of
Augmented Reality

Space Tech The New Frontier

Smart Gadgets to Simplify
Your Life

Cybersecurity 2025
Are We Prepared?

TECH GIVEAWAY INSIDE

Win the Latest
Satellite-Enabled
Smartwatch



EXCLUSIVE INTERVIEW

The AI Founder:
Dani Martinez



READER'S CHOICE

Top 5 Breakthrough
Technologies of the Year

June 2025/ Volume 21



1 2 3 4 5 6 7 8 9 0

magazine

GADGET

DEC 2023 | VOL. 32

ON-LINE SHOP

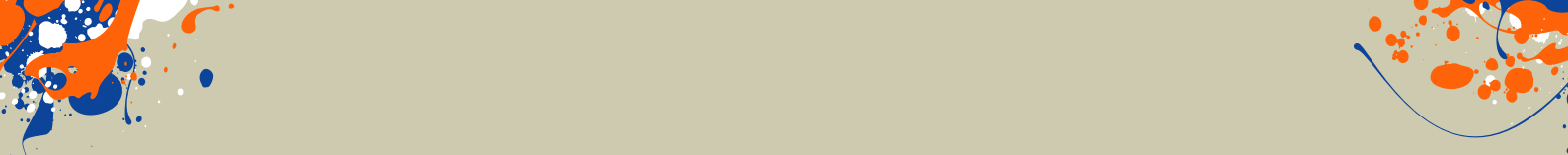
@ reallygreatsite
www.reallygreatsite.com

STORE

123 Anywhere st., Any City,
ST 12345



0 35545 62336 78 1



ART MAGAZINE

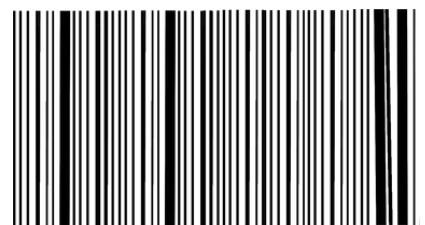
EXPLORING THE SOUL OF CREATIVITY



Unveiling the Latest
in the World of Creativity

Unveiling Creativity
Across the Globe

Easy Painting Techniques
for Beginners



Vol.1 | March 2025





From HOD's Desk

- Dr. Raja Karmakar

Department of CSE (IoT & Cyber Security including Block Chain Technology)

HOD's Message

It is with great pride and a deep sense of responsibility that I share this message on behalf of the Department of Computer Science and Engineering (IoT and Cyber Security including Block Chain Technology). Our department started the journey from the year of 2022, and we have witnessed a transformative journey -- from laying strong academic foundations to emerging as a hub of innovation and interdisciplinary research. We have consistently strived to keep pace with the fast-evolving technological landscape. Our students and faculty have actively contributed to research in critical areas such as secure communication systems, smart environments, and decentralized technologies. Noteworthy achievements include national and international-level project recognitions, publications in reputed conference proceedings, successful industry collaborations, and student-led innovations that address real-world challenges. Looking ahead, our vision is to establish the department as a centre of excellence in IoT and cybersecurity-related emerging technologies. We aim to strengthen our research ecosystem, expand international collaborations, and promote industry-integrated learning. With a strong emphasis on ethical innovation and digital resilience, we are preparing our students not only to excel in their careers but also to become responsible contributors to a secure and connected future.

Professors' Messages

Dear Students, Embracing the dynamic fields of IoT and cybersecurity opens doors to endless opportunities for innovation and impact. These domains are at the forefront of technological advancement, shaping how we interact with the world and protect our digital environments. We encourage you to approach your studies with curiosity, resilience, and a passion for discovery. Innovation thrives when we challenge conventions and pursue research with dedication. Your journey here is not just about acquiring knowledge but about becoming pioneers who will drive the future of technology. Stay motivated, be bold, and never hesitate to explore new ideas. The future belongs to those who dare to innovate.

Questionnaire:

1. What is your vision for the IoT & Cyber Security department in the next 5 years?

My vision is to transform the department into a leading centre of excellence known for cutting-edge research, strong industry collaboration, and nurturing highly skilled professionals. We aim to integrate emerging technologies like Blockchain and AI with IoT and cybersecurity to solve complex real-world problems. We also want to create a vibrant ecosystem where innovation, entrepreneurship, and interdisciplinary learning flourish, preparing our students to be global leaders in technology.

2. How do you see IoT shaping industries and student opportunities?

IoT is revolutionizing industries by enabling smart automation, data-driven decision-making, and enhanced connectivity across sectors like healthcare, manufacturing, agriculture, and smart cities. For students, this translates into diverse career paths ranging from device design and network security to data analytics and system integration. The growing demand for IoT expertise offers exciting opportunities to innovate and contribute to shaping the future.

3. What advice would you give students to stay future-ready in technology?

Stay curious and committed to lifelong learning. The technology landscape evolves rapidly, so building a strong foundation in fundamentals, combined with hands-on experience in emerging areas like IoT, cybersecurity, and blockchain, is crucial. Develop problem-solving skills, embrace interdisciplinary knowledge, and actively engage in research and projects. Also, cultivate soft skills like adaptability, communication, and collaboration. These are key to thriving in any tech career.

4. What are some milestones or proud moments of the department?

We have several milestones to be proud of, including successful research publications in reputed international conference proceedings. For instance, our students won the best paper award for the paper titled "Phone Patrol: An Intelligent Surveillance System for Mobile-Free Environments" in 17th IEEE/ACM International Conference on COMmunication Systems & NETworkS - Systems for the Future of AI/ML (COMSNETS Workshop '25 - SysAI). Our students have won accolades in several hackathons and innovation challenges related to IoT and cybersecurity. Our students participated in IETF 122 Hackathon at Bangkok, Thailand, representing Heritage Institute of Technology, Kolkata, where they were the part of the India Internet Foundation (IIF) team. Establishing specialized labs equipped with advanced tools and fostering partnerships with leading technology companies are other highlights that reflect our commitment to excellence.

5. What role do research and innovation play in a student's journey?

Research and innovation are integral to a student's academic and professional growth. They encourage critical thinking, creativity, and the ability to tackle complex problems. By engaging in research, students gain deeper insights beyond textbooks, develop technical expertise, and contribute original solutions to societal challenges. Innovation drives entrepreneurship and helps students transform ideas into impactful technologies, preparing them to lead in an ever changing world.

6. What inspired you to specialize in IoT and Cybersecurity?

The rapid digital transformation and the increasing interconnectivity of devices fascinated me. IoT's potential to reshape daily life and industries, combined with the critical need for robust cybersecurity to protect these interconnected systems, motivated me to specialize in these fields. Additionally, Blockchain's promise to enhance security and trust in decentralized networks further inspired my pursuit of these areas, aiming to contribute meaningfully to building a secure and intelligent digital future.

A quick personal note for a professor:

What book, idea, or life lesson has influenced your teaching in IoT and Cybersecurity department?

One idea that has profoundly influenced my teaching is the principle of "learning by building." I have always believed that true understanding comes not just from reading or lectures, but from creating, testing, and sometimes failing. Another important principle I always follow is to keep patience.

Any words of encouragement for students working on projects, startups, or research in IoT and Cybersecurity department?

To our students: whether you are building a project, launching a startup, or exploring a research idea -- believe in the process and keep patience. Embrace curiosity, stay resilient in the face of setbacks, and never underestimate the value of small, consistent progress. You are working in one of the most impactful fields of our time. Keep pushing boundaries -- your ideas matter, and your work can shape the future.

Tech Predictions: Professors share “One Big Change” they expect in IoT/CS in the next 10 years.

In the next decade, I believe IoT and Cybersecurity will converge more deeply with AI, leading to autonomous, self-healing security systems. As billions of connected devices become part of everyday life -- from smart homes to smart cities -- the need for real-time, intelligent threat detection will become critical. Future systems would not just respond to cyberattacks – they will predict and prevent them automatically, adapting faster than human response ever could.

Memory Lane: Professors recall a favourite teaching moment or student project.

One of my most memorable teaching moments was guiding a group of students who developed a smart women's safety system using IoT and blockchain for data integrity. What stood out was not just their technical execution, but their passion for solving a real-world problem. Their project won a national-level innovation challenge. Moments like these remind me why I love teaching -- seeing students transform ideas into impact, and watching their confidence grow as they realize their potential.

Advice Corner: One-line tips like “If I were an undergraduate today, I'd definitely...”

If I were an undergraduate today, I would definitely start building small projects – learning by doing is always powerful.



**From Departmental
Coordinator's Desk**

**- Prof. Sudeshna Ghosh
(Departmental Coordinator's message)**

As the Departmental Coordinator of CSE (IoT and Cyber Security with Block Chain Technology), I have the opportunity to witness the growth of a fast-evolving field that combines innovation with responsibility and resilience. Our department is dedicated to training young engineers not only to develop smart and connected systems but also to secure the digital world in which they function. I sincerely appreciate the enthusiasm, adaptability, and dedication of our students and faculty, and I look forward to the positive impact they will create toward a safe and connected future.



From the E-Magazine
Mentor's Desk

Where Technology Meets Imagination and Ideas Shape the Future

- Prof. Palash Dutta
E-Magazine Mentor

Welcome to the new edition of our CSE (IoT & Cyber Security Including Blockchain Technology) e-magazine—where bytes meet brilliance, and every idea has the power to spark innovation. Think of this magazine as more than just an e-book; it's a living tapestry of stories, experiments, and inspirations woven together by our students and faculty members.

Here, technology isn't only about codes and circuits—it's about imagination, creativity, and the human touch behind every breakthrough. Each page you turn is a glimpse into the spirit of our department: curious minds daring to explore, passionate voices eager to share, and a community that thrives on learning together. I feel truly grateful to everyone who made this edition possible. To our students, and faculty members—thank you for lending your ideas and energy. To our Head of Department, a heartfelt thanks for the constant encouragement that fuels our journey. And to my editorial team, your creativity and hard work have turned vision into reality.

Dear readers, this magazine belongs to you as much as it belongs to us. May it spark curiosity, light up your imagination, and remind you that innovation begins with a simple idea waiting to be explored. May each article you explore ignite curiosity, inspire fresh perspectives, and strengthen the sense of belonging within our ever-growing CSE (IoT & Cyber Security Including Blockchain Technology) family.

So, dive in, get inspired, and let's continue to create, innovate, and grow—together.

BIO-CHEMIC WEAPONS AGAINST VIRAL INFECTIONS

**-Dr. Suryadeep Dasgupta
(D.M.B.S., M.D. (BIO), EWH (TKOL))**

Post the global pandemic COVID-19 which brought the world to a standstill and resulted in significant number of casualties all across the world, the common people and medical fraternity came to know about a number of viruses that were either not known or known to a very lesser extent. Names of various viruses and variants such as Alpha, Beta, Delta, Lambda, Omicron, SARS-CoV-2, H3N2, H1N1, Adeno virus made it to our knowledge based upon insights from various sources such as newspapers, television, medical journals, social media and so on. Very recently, the newest version of COVID-19 virus EG.5.1, known as “ERIS” was identified and reported in Pune in May 2023. The same originated from UK but thankfully as of now the WHO assures that there is no cause for panic.

Apart from the variants of COVID-19, now-a-days in our practice, we face two most common type of viruses in our chambers i.e. 1) H3N2-influenza virus & 2) Adeno virus.

1) Symptoms of H3N2 (Influenza) virus :-

- a) Fever,
- b) Body ache,
- c) Running nose,
- d) Cough,
- e) Nausea,
- f) Diarrhoea,
- g) Vomiting

2) Symptoms of Adeno virus :-

- a) Fever,
- b) Common Cold,
- c) Sore Throat,
- d) Conjunctivitis,
- e) Inflammation of the lungs airways,
- f) Inflammation of the intestines or stomach leading to diarrhoea,
- g) Nausea
- h) Vomiting,
- i) Stomach pain

3) Cause:-

These viruses spread through droplets from coughs, sneezes of an infected individual (mainly).

4) Age Group:-

- a) H3N2-(Influenza virus) – Common in all age group.
- b) Adeno Virus – Specially infant less than 2 years or above.

5) Lab Investigation:-

Collecting Swabs from throat or nose in both the cases. An RTPCR TEST is used to analyse the samples.

6) Management:-

- a) Healthy & well-balanced diet to boost immunity.
- b) Drink plenty of fluids & get rest.
- c) Use mask, particularly in crowded areas.
- d) Maintain safe distance from infected individuals.
- e) Avoid Sharing of foods & drinks with infected individuals.

7) Warning Signs:-

- a) High rise of temperature. (103°F-104°F).
- b) Severe Respiratory Distress.
- c) Low Oxygen saturation. (SPO2- below 90).
- d) Breathlessness.

8) Treatment with Bio-Chemic medicines:-

- a) Ferrum Phos
- b) Kali Mur
- c) Kali Sulph
- d) Natrum Mur
- e) Natrum Sulph
- f) Bio-combination 11.

During my experience of dealing with patients suffering from viral infections, I have observed that the above medicines have worked miracles upon the patients in very short periods of time such as only two and three days. In some cases, they have been potent against COVID-19 variants as well as without any side effects.

So, I would like to state that the BIO-CHEMIC medicines are a blessing for society and mankind. It was invented way back in 1873 by our legend Dr. W.H. Schuessler and to this date and time it continues to serve mankind.



Mr. Sidhartha Mojumdar

History Of
Futura Font

Futura Font History

- Mr. Sidhartha Mojumdar

The Bauer Type Foundry began drawing Futura in 1924 and released it in 1927. It is known as "the fully developed prototype of the century Geometric Sans-serif." Futura was created by Paul Renner as a part of the new Frankfurt concept. It is supposed to have been created in competition with the ground breaking Erbar typeface created in 1926 by Ludwig & Mayer.

We can say about the family from past history that the report is a serif geometric type face with the end of a rounded end, which is a practice worksheet influenced by student handwriting. Austere geometry adhering to the system of font size with temperate readability is done to solve all the font-specific matters. If we want something comprehensive and easily readable, then characterize the style of handwriting practice sheet. We can say that a report is the ideal choice. In InDesign, illustrator and Photoshop are open type applications which feature access of lower-case q with a curly type, lowercase j and f with a tight curl, J with a serif and 9 with a standard stem. (Staff, 2015).

Futura is one of the most famous font families, which evolved from the geometric sans serif in 1927 by Paul Renner. A contribution of the new Frankfurt project was the typeface exactly designed. Bauhaus design style: 1919-1933. The visual element becomes the geometric shape of the font face. The font family was exactly in light, medium, bold and bold oblique font in 1928. The light oblique, medium oblique, demi fold and demi fold oblique font. In 1932, a book font was released. The book oblique font was released in 1939. An extra bold font was after that to come into the dictionary of writing.

Futura light is the most attractive with a thinner type face and is perfect for designing paragraphs and body text. New geometric sans serif from competitive foundries have .

Futura shows more attractiveness and efficiency in its appearance, which makes it a great-looking font. Though Renner was not so much associated with Bauhaus, he shared many of his modern models in modern ways of expressing his feeling toward San serif.

The topography, typeface and the terminology are the main parts associated with the whole practice. Now it has been described in the form of design. A poster is the most common way to associate complete forms of media which communicate vital information about a product and details. As for example, it is so inspirational for a designer to see a blank and white space to think about it and imagine what he could do about it.

Now take about the topographic research paper based on the one given topographers and typeface combination, and it can be broken into the following sections. It should also include a good visual image of good design work that typeface has been used, so by the ensuring information through, correct and good quality. (Paratype, 2016).



No visual effects were undertaken to help inform the topographic direction that the project can take. Adequate research source and included in the book of sketches to help and inspire the visual topographic direction. Adequate quality visual research can be obtained from the topographic system of research. A good range of visual research was sourced and included in the sketchbook. Obviously, it will help the way to influence the poster somewhat. In the sketchbook there is a very good range of visual materials and sources that really help to inspire the topographic and the design ability of the student and the direction of poster in a unique and innovative manner. A wide range of quality research is done which is normally excellent.

This part of research is inspired by the topographic direction of the project, which helps the student to feel more confident about the matter. The quality of design work is being done on the quality of design work. (1001fonts, 2016). In the case of the poster design, we can say that backup of the poster design gives little evidence for the poster design and backup work. Solid and useable ideas are made by the creative nature of such. In the layout and the use of design elements that are appropriate to pass are good done of design. Good creativity of the history of typeface in the design of evidence and layout ideas. The evidence of design ideas which have been created by the topographer is the history of very good creativity.

Technical issues are the main important points that are being considered nowadays. Technical proficiency is poor, with the incorrect software system being used for the work. Also, it is seen that it is not used like a good end-user. So, for that, correct software should be used to get all the error evidence. Adequate presentation is mostly needed for the technical improvement. The final presentation of the poster execution and after correct de bugging, if an error is found, that can be understood. Appropriate software for technical abilities is very creative and very good. It actually helps with the final presentation of any poster presentation. (Ufonts, 2016).



The evolution of San Serif to any other font has been developed to make is more adaptable for writing. Many people worked on this particular part of topography to make it better and clearer in its presentation. Futura was extensively promoted by Bauer and its American division, "die schrift unserer zeit" (translated from German as "the typeface of our time") and referred to as "the typeface of today and tomorrow" in English. It has remained widely used and appears in well-known logos like Volkswagen, Supreme, IKEA, and Party City.

Editor's Page

From late-night brainstorming to final print — here's
CYBERSPHERE 2026

Welcome to the very first edition of CYBERSPHERE 2026, the departmental magazine of IoT, Cyber Security, and Block Chain. This isn't just a magazine — it's a mix of ideas, experiments, stories, and student creativity, all packed into one place. From choosing write-ups to shaping the final look, the process was full of teamwork, learning, and a little bit of fun chaos.

To our juniors: consider this your sign to explore, build, and share. You don't need to be perfect — you just need to be curious.

A heartfelt thank you to our respected HOD and all our teachers for their constant guidance and support.

Now turn the page — and step into CYBERSPHERE.



Arijit Adhikary, 3rd year



Santu Patra, 3rd year



Diya Dey, 3rd year



Soumyajit Acooli, 3rd year

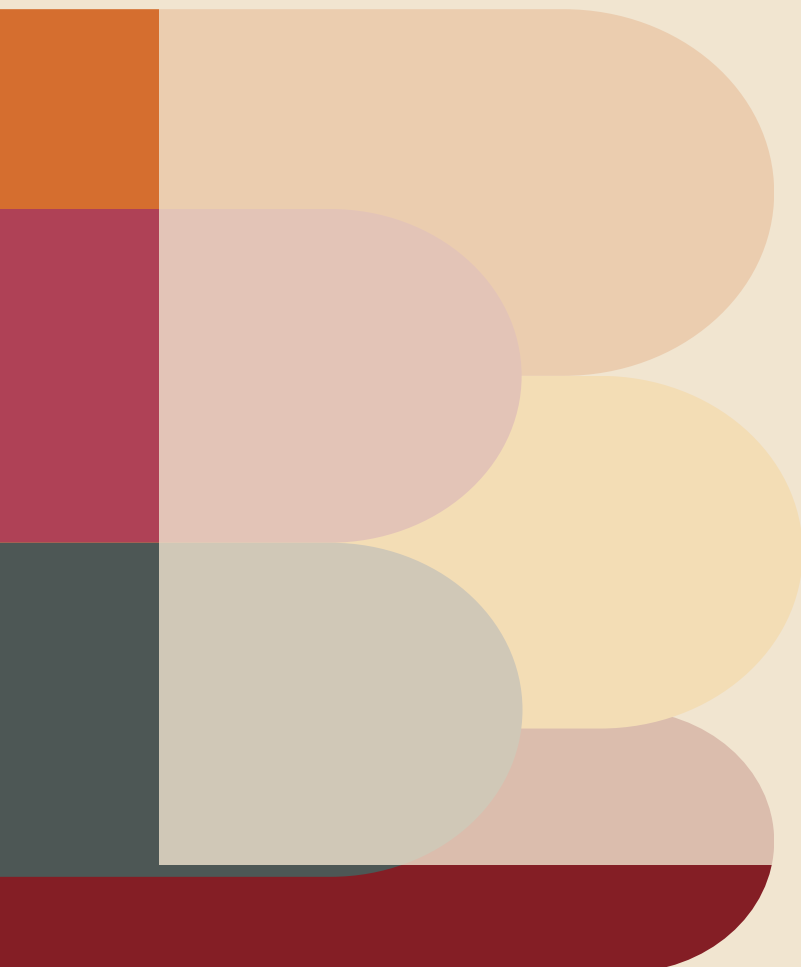


Sutirtha Paul, 3rd year



Voices Unfiltered

INK & INSIGHTS



Song of a Fighter

I have dined with absence,
sat at death's raw table,
and returned with salt in my veins.

The moon ~ my only witness,
bleeds in phases as I do,
waning, waxing,
never whole, never gone.

Loss is my dialect.
I speak in elegies,
my laughter braided with ash.
Each heartbeat is rebellion,
each breath a verdict against despair.

Dostoevsky sits in my silence,
reminding me the abyss is not a stranger,
but a mirror.

Sylvia hums in my ribs,
her candlelight quivering,
teaching me that pain can sing
even as it devours.

The world would bury me
in the quiet of forgotten rooms,
yet I rise, feral, unyielding,
a fighter forged in the cathedral of grief.

Call me ruin,
call me survivor,
but know this,
I am the hymn of the broken,
the song that will not silence,
the flame that teaches darkness
to fear.

- Anushka De
CSE (IoTCS) 3rd year

On The Way Back...Home?

- Avishek Chakroborty
CSE (IoTCS) 2nd Year

...however, the Crown's forced indigo farming on their ancestral farms led to difficult times. Given the soil and climate, the blue yield wasn't promising. Famines were dreaded every summer. People began to fear the collection day.

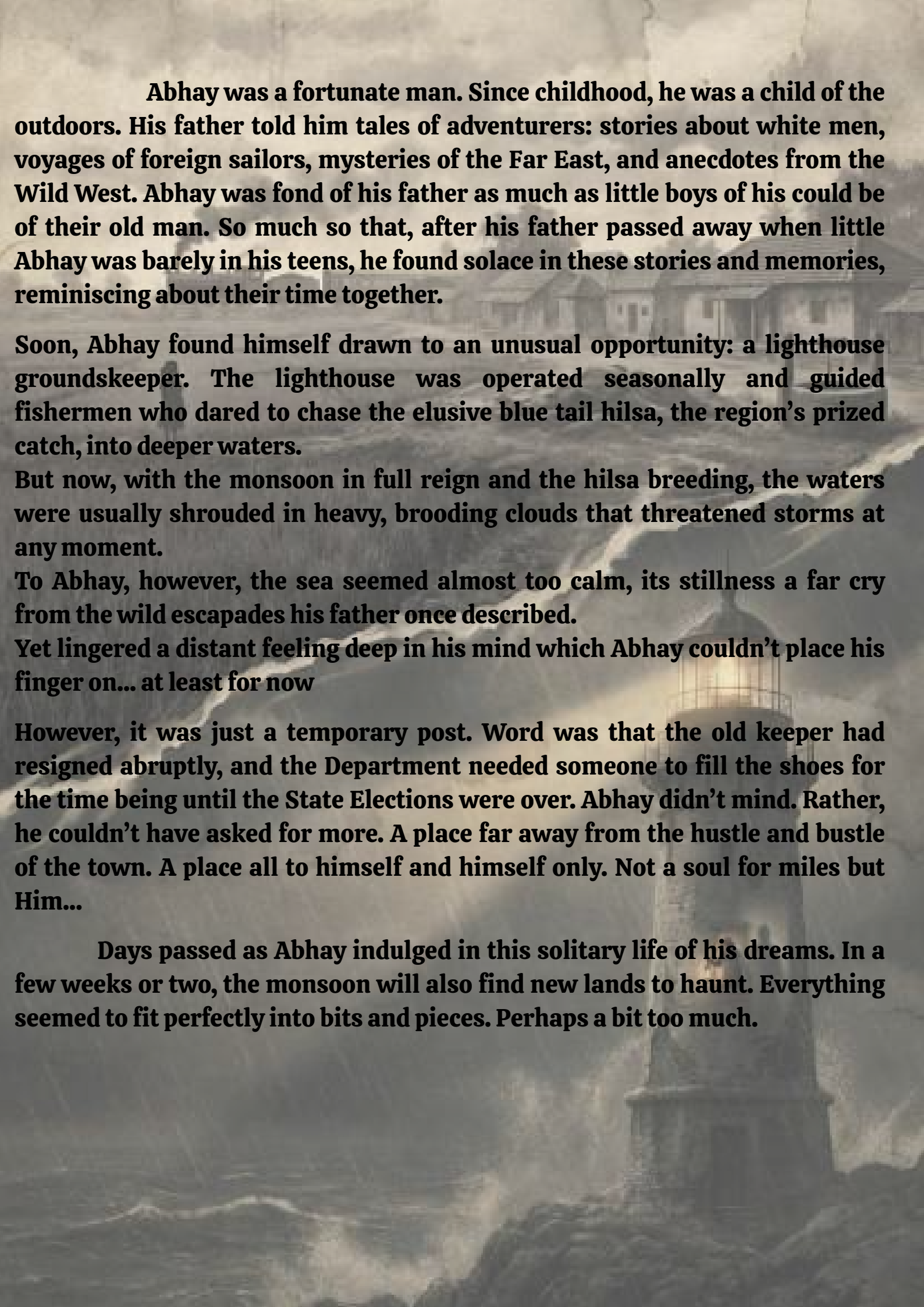
Little Rajyashree, dipped in her childhood folly, was beyond such monumentalities. To her, the biggest worry was the strange occurrence that happened every noon. She would be startled by a sharp, whistling sound which shook her dainty build.

"It's a train car! They run on steel tracks," is what Ma told her.

Words weren't enough; she had to witness more than just remnants of sound and smoke. She knew what she wanted. So one odd, gloomy morning, off she went to the field by the tracks by herself. She sat on the grass...awaiting. After well over an hour, vibrations emanated from the horizon. The thick steam and distant roars etched ever so close. However, in this mystifying moment, a faraway noise also reached her busy ears-loud BANNGGs followed in quick succession...and perhaps...trotting of horses?

Her excitement and fascination knew no bounds on her way back home, where a different sight was awaiting discovery.

The memory Rajyashree would grow to have of her village would be of the big, ominous pile amassed beside the village well. Rajyashree was sure she saw her mother's lifeless eyes that day among dozens other in the mound. The horrors she witnessed that day, an Independent Rajyashree can seldom forget...

A lighthouse stands on a rocky island, its light glowing against a backdrop of a stormy sea with dark, swirling clouds and a bright light source, possibly the sun or moon, breaking through the haze. The lighthouse is a tall, cylindrical structure with a lantern room at the top. The overall atmosphere is dramatic and moody.

Abhay was a fortunate man. Since childhood, he was a child of the outdoors. His father told him tales of adventurers: stories about white men, voyages of foreign sailors, mysteries of the Far East, and anecdotes from the Wild West. Abhay was fond of his father as much as little boys of his could be of their old man. So much so that, after his father passed away when little Abhay was barely in his teens, he found solace in these stories and memories, reminiscing about their time together.

Soon, Abhay found himself drawn to an unusual opportunity: a lighthouse groundskeeper. The lighthouse was operated seasonally and guided fishermen who dared to chase the elusive blue tail hilsa, the region's prized catch, into deeper waters.

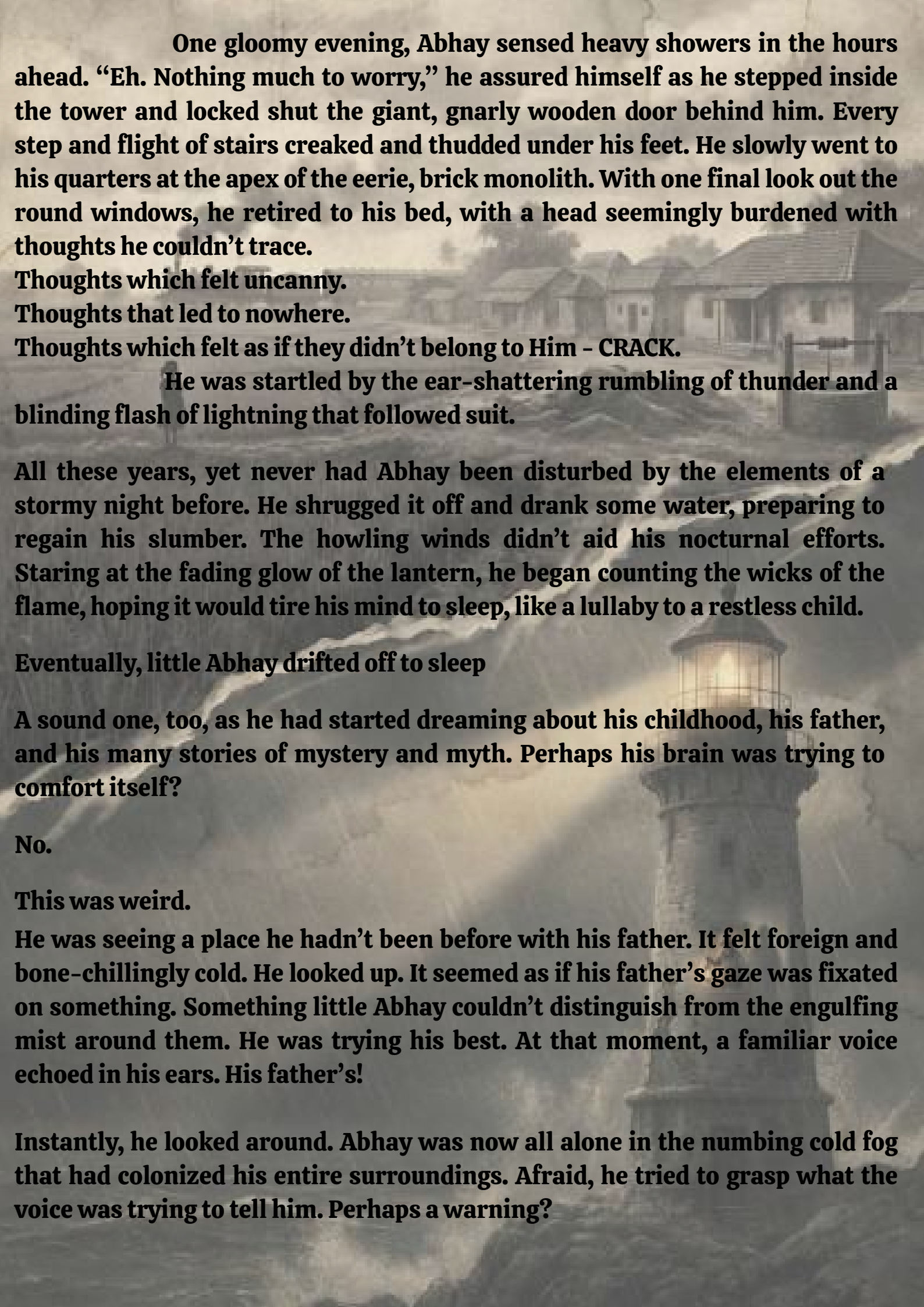
But now, with the monsoon in full reign and the hilsa breeding, the waters were usually shrouded in heavy, brooding clouds that threatened storms at any moment.

To Abhay, however, the sea seemed almost too calm, its stillness a far cry from the wild escapades his father once described.

Yet lingered a distant feeling deep in his mind which Abhay couldn't place his finger on... at least for now

However, it was just a temporary post. Word was that the old keeper had resigned abruptly, and the Department needed someone to fill the shoes for the time being until the State Elections were over. Abhay didn't mind. Rather, he couldn't have asked for more. A place far away from the hustle and bustle of the town. A place all to himself and himself only. Not a soul for miles but Him...

Days passed as Abhay indulged in this solitary life of his dreams. In a few weeks or two, the monsoon will also find new lands to haunt. Everything seemed to fit perfectly into bits and pieces. Perhaps a bit too much.

A lighthouse on a rocky shore with a foggy background and houses in the distance.

One gloomy evening, Abhay sensed heavy showers in the hours ahead. “Eh. Nothing much to worry,” he assured himself as he stepped inside the tower and locked shut the giant, gnarly wooden door behind him. Every step and flight of stairs creaked and thudded under his feet. He slowly went to his quarters at the apex of the eerie, brick monolith. With one final look out the round windows, he retired to his bed, with a head seemingly burdened with thoughts he couldn’t trace.

Thoughts which felt uncanny.

Thoughts that led to nowhere.

Thoughts which felt as if they didn’t belong to Him - CRACK.

He was startled by the ear-shattering rumbling of thunder and a blinding flash of lightning that followed suit.

All these years, yet never had Abhay been disturbed by the elements of a stormy night before. He shrugged it off and drank some water, preparing to regain his slumber. The howling winds didn’t aid his nocturnal efforts. Staring at the fading glow of the lantern, he began counting the wicks of the flame, hoping it would tire his mind to sleep, like a lullaby to a restless child.

Eventually, little Abhay drifted off to sleep

A sound one, too, as he had started dreaming about his childhood, his father, and his many stories of mystery and myth. Perhaps his brain was trying to comfort itself?

No.

This was weird.

He was seeing a place he hadn’t been before with his father. It felt foreign and bone-chillingly cold. He looked up. It seemed as if his father’s gaze was fixated on something. Something little Abhay couldn’t distinguish from the engulfing mist around them. He was trying his best. At that moment, a familiar voice echoed in his ears. His father’s!

Instantly, he looked around. Abhay was now all alone in the numbing cold fog that had colonized his entire surroundings. Afraid, he tried to grasp what the voice was trying to tell him. Perhaps a warning?

He clasped his hands around his ears in an attempt to shut off the penetrating, grainy static of the fog and the desperate thumpings of his heart. He listened hard.

“D-dont ov-en”

“Oven?” he questioned his senses as he focused hard to make out his father’s words.

“Don open thuh fore!”

“Door”. It finally clicked for him.

In that split second, Abhay felt a stinging sensation pricking through his veins. He woke up. Sweating profusely in his bed atop the lighthouse - back in the horrors of the present. He was met with instant rumbling and howling from the skies above.

But wait!

Amid the raging storm, another unfamiliar sound crept into the night.

Taps. Soft, delicate taps on the giant wooden door that led to his quarters. It was masked almost flawlessly by the thunder.

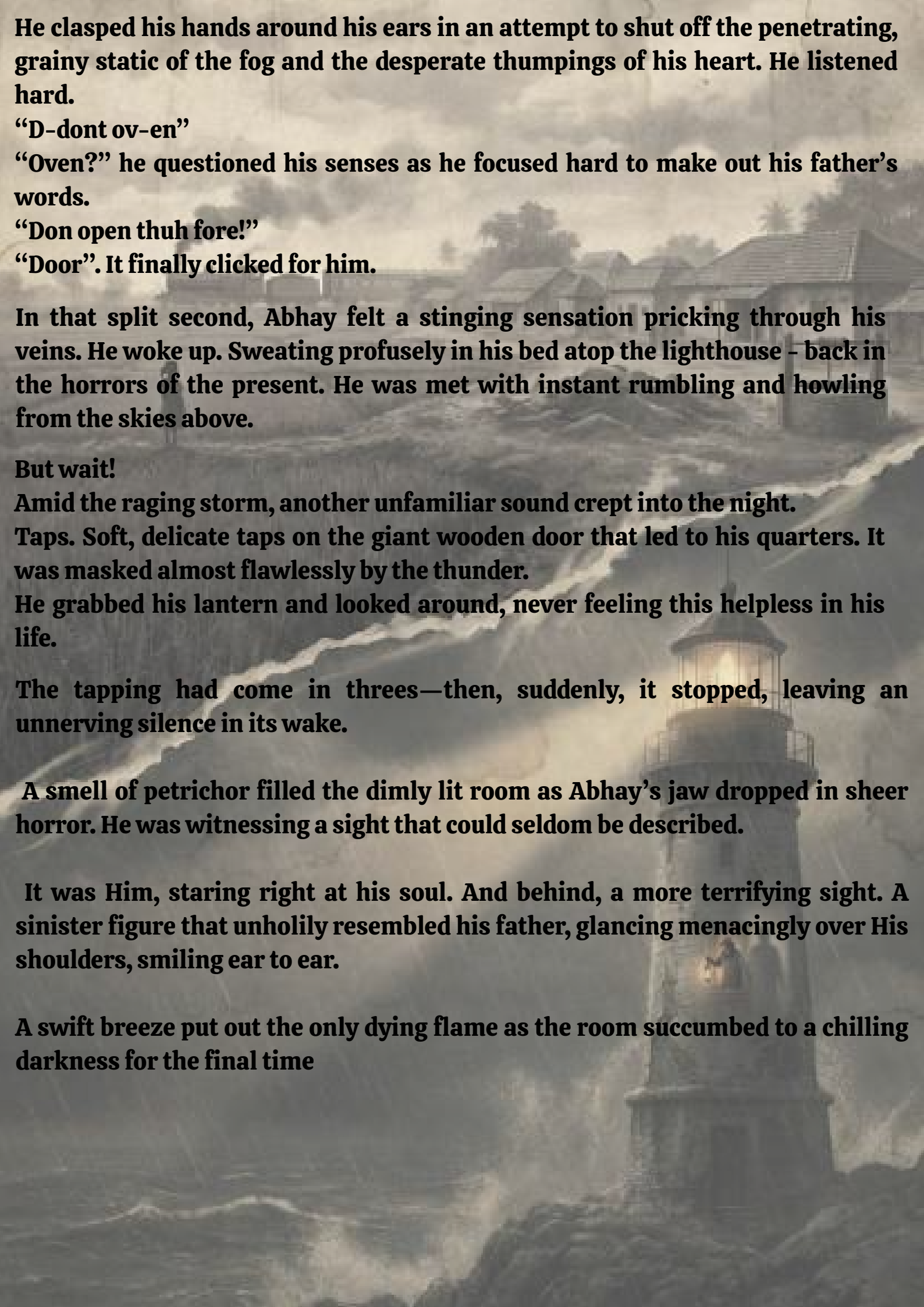
He grabbed his lantern and looked around, never feeling this helpless in his life.

The tapping had come in threes—then, suddenly, it stopped, leaving an unnerving silence in its wake.

A smell of petrichor filled the dimly lit room as Abhay’s jaw dropped in sheer horror. He was witnessing a sight that could seldom be described.

It was Him, staring right at his soul. And behind, a more terrifying sight. A sinister figure that unholily resembled his father, glancing menacingly over His shoulders, smiling ear to ear.

A swift breeze put out the only dying flame as the room succumbed to a chilling darkness for the final time



VOID

In this suffocating fog, I've been lost for so long. My thoughts are a world of tangled threads, and I don't know what to say to calm my restless mind. The ashes of forgotten days cling to me like a ghost.

**"Tukde kaanch ke bikhre zameen par,
chalna chahoon par chhaya hai har qadam.
Yeh dhuan, hai saans lena saza."**

**Glass lies shattered along the path, but I keep strolling,
This smoke is suffocating, each breath a scourge.**

But inside you, there are many secrets. Don't let go of that thread of hope. If you can only listen with your heart, you will find the truth.

"This piece is inspired by the song O Yaara by Kaavish and Abdul Hannan, a melody that holds a very special place deep within my heart..."

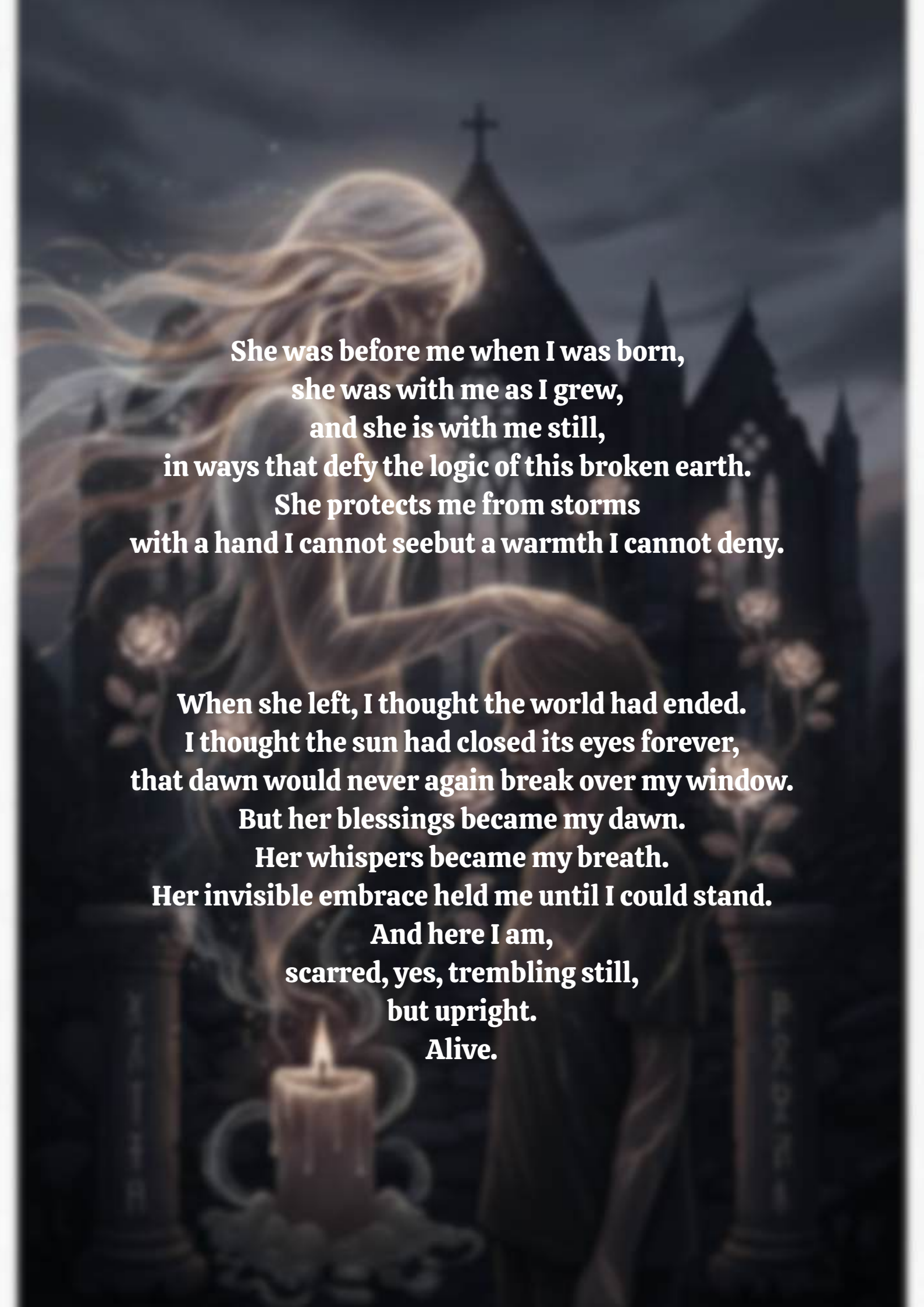
**- Ayush Kumar
CSE (IoTCS)
2nd year**

A Mother Beyond Death

I lost everything,
not in a single stroke, but piece by piece,
like a candle burning itself into absence
First went the certainties,
then the people I loved,
then the little joys I thought would never betray me.
I stood in a room full of ruins,
my heart a collapsing cathedral where echoes of laughter
mocked me with their absence.

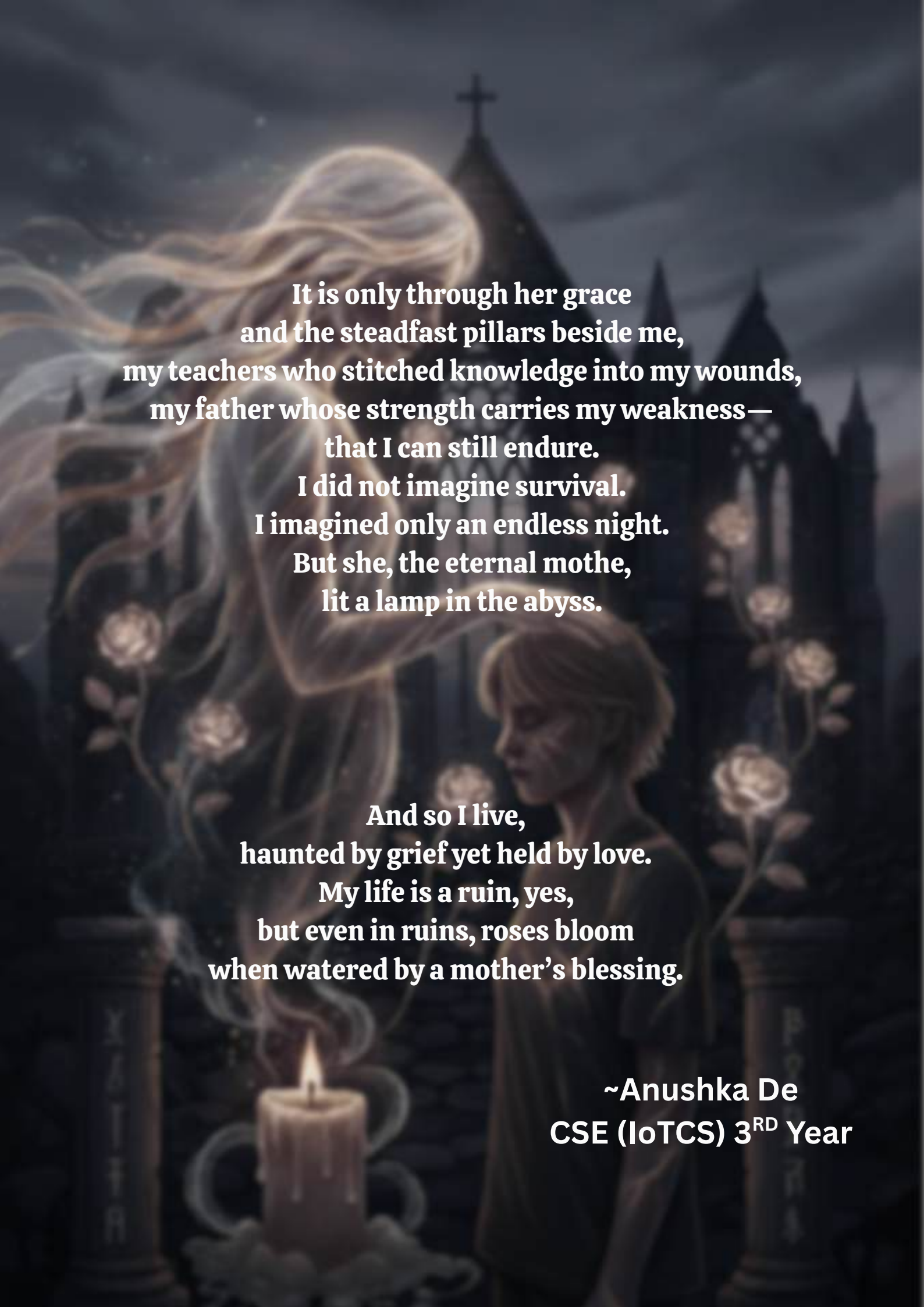
Yet amid this merciless undoing,
one truth refused to die: my mother
Not her body~death was cruel enough to take that,
but her presence, her unyielding tenderness
that clings to me even now.





**She was before me when I was born,
she was with me as I grew,
and she is with me still,
in ways that defy the logic of this broken earth.
She protects me from storms
with a hand I cannot see but a warmth I cannot deny.**

**When she left, I thought the world had ended.
I thought the sun had closed its eyes forever,
that dawn would never again break over my window.
But her blessings became my dawn.
Her whispers became my breath.
Her invisible embrace held me until I could stand.
And here I am,
scarred, yes, trembling still,
but upright.
Alive.**



It is only through her grace
and the steadfast pillars beside me,
my teachers who stitched knowledge into my wounds,
my father whose strength carries my weakness—
that I can still endure.
I did not imagine survival.
I imagined only an endless night.
But she, the eternal mother,
lit a lamp in the abyss.

And so I live,
haunted by grief yet held by love.
My life is a ruin, yes,
but even in ruins, roses bloom
when watered by a mother's blessing.

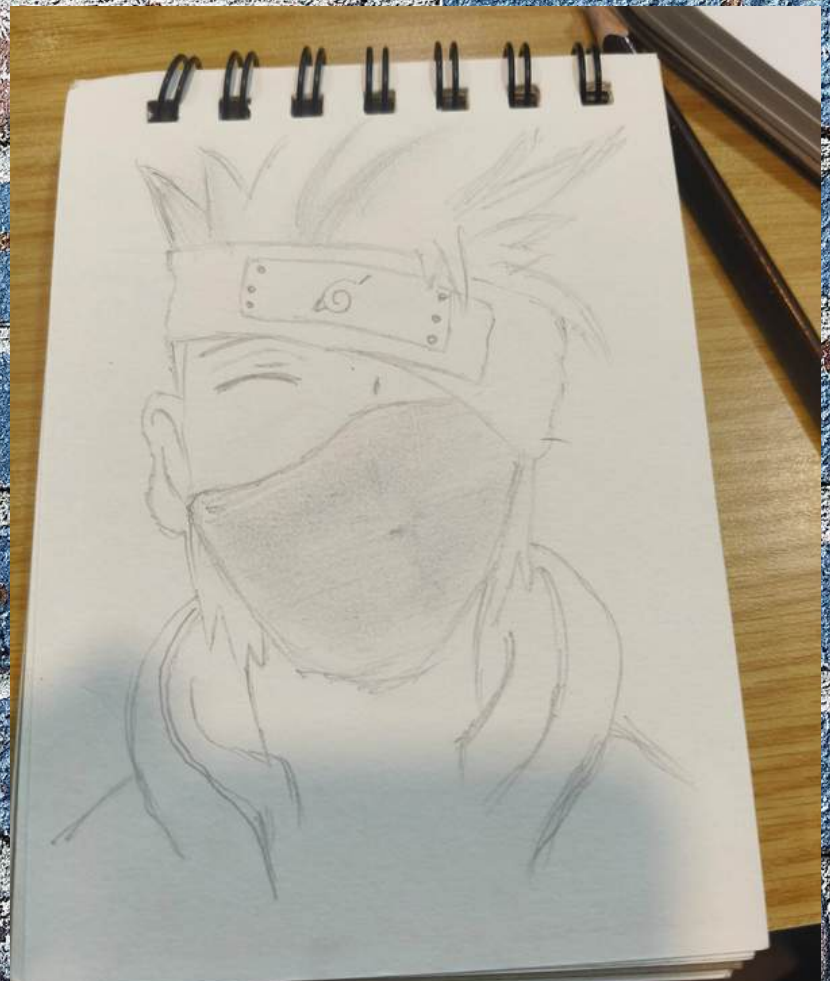
~Anushka De
CSE (IoTCS) 3RD Year



BRUSH STROKES



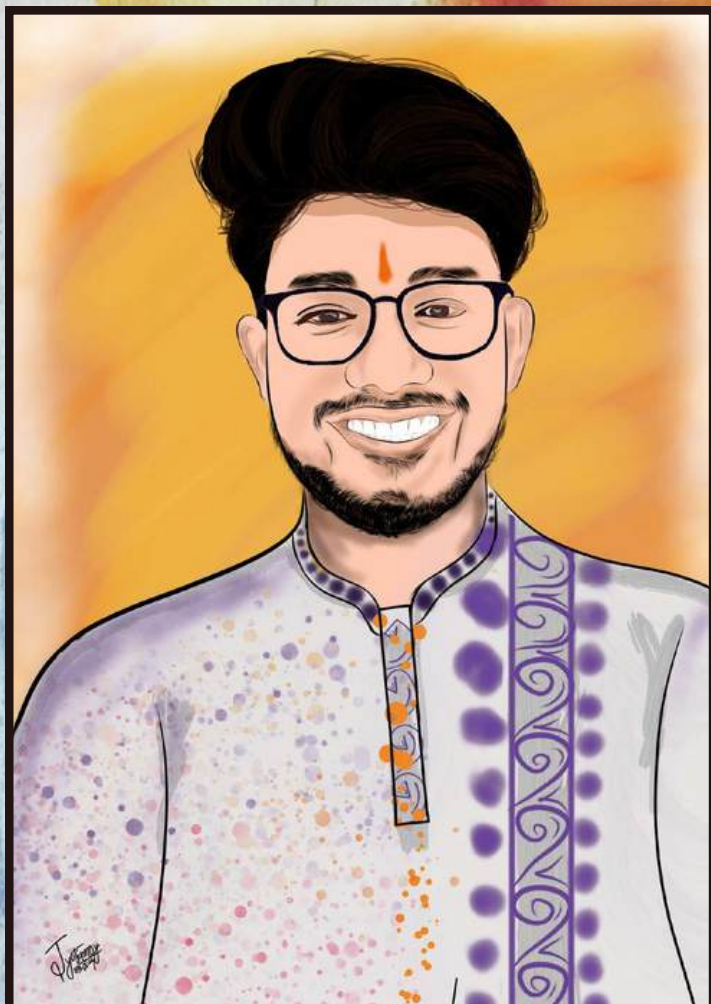
Soumili Paul
CSE (IOTCS)
3rd year



Santu Patra
CSE (IOTCS)
3rd year



Jyotirmoy Karmakar
CSE (IOTCS) 3rd year

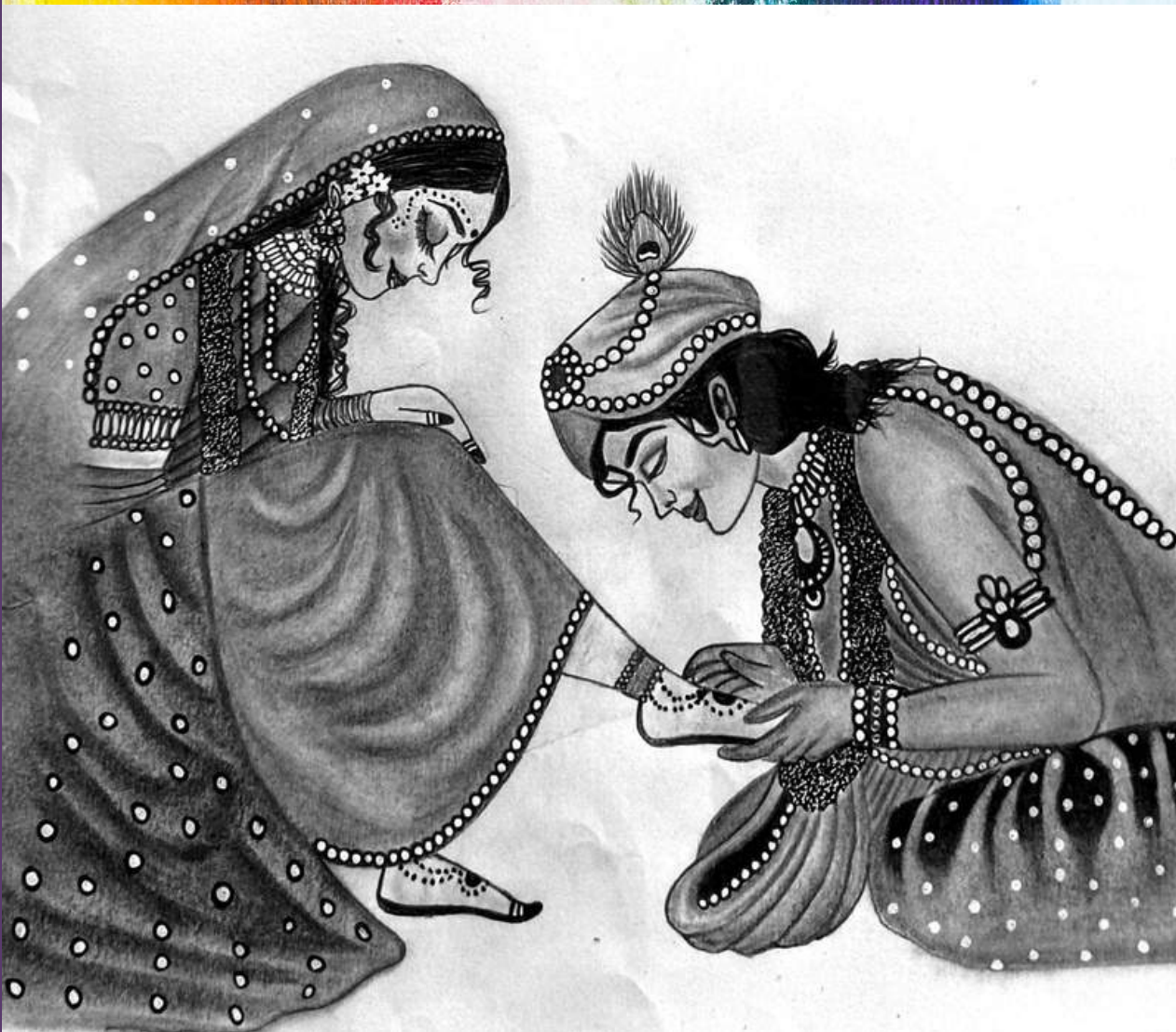




Soumyajit
Acooli
CSE (IOTCS)
3rd year



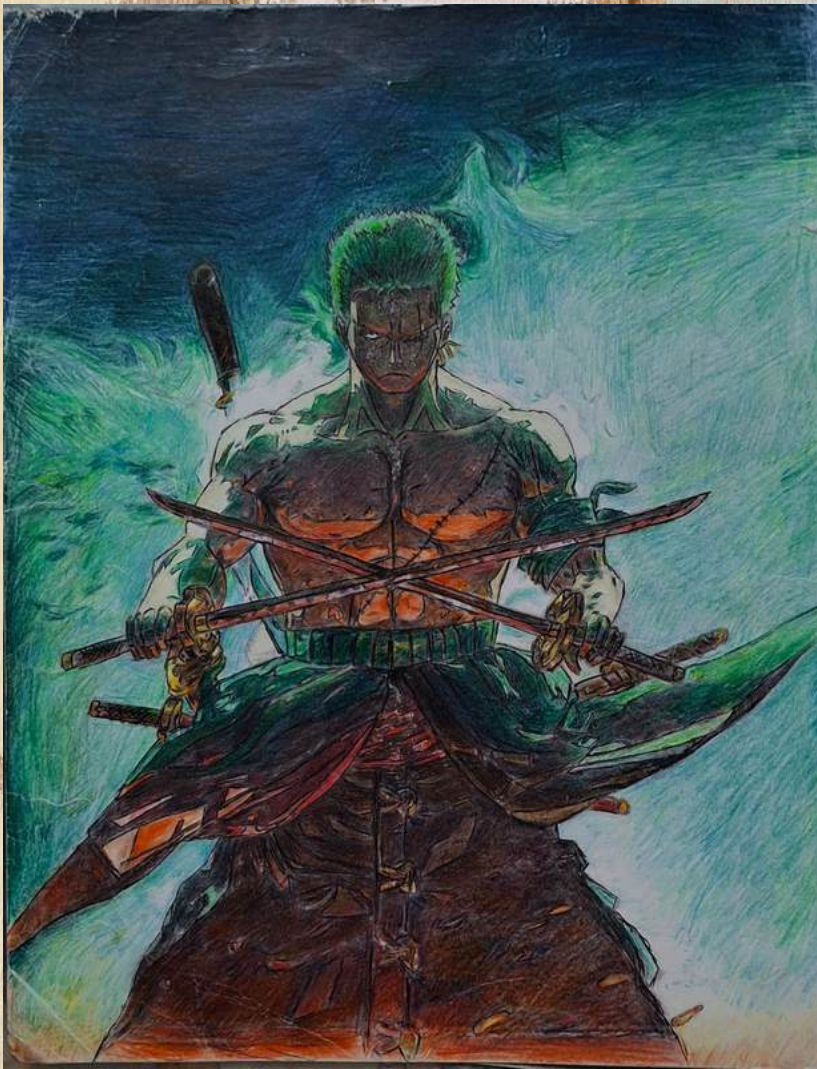
Anurima
Das
CSE (IOTCS)
3rd year





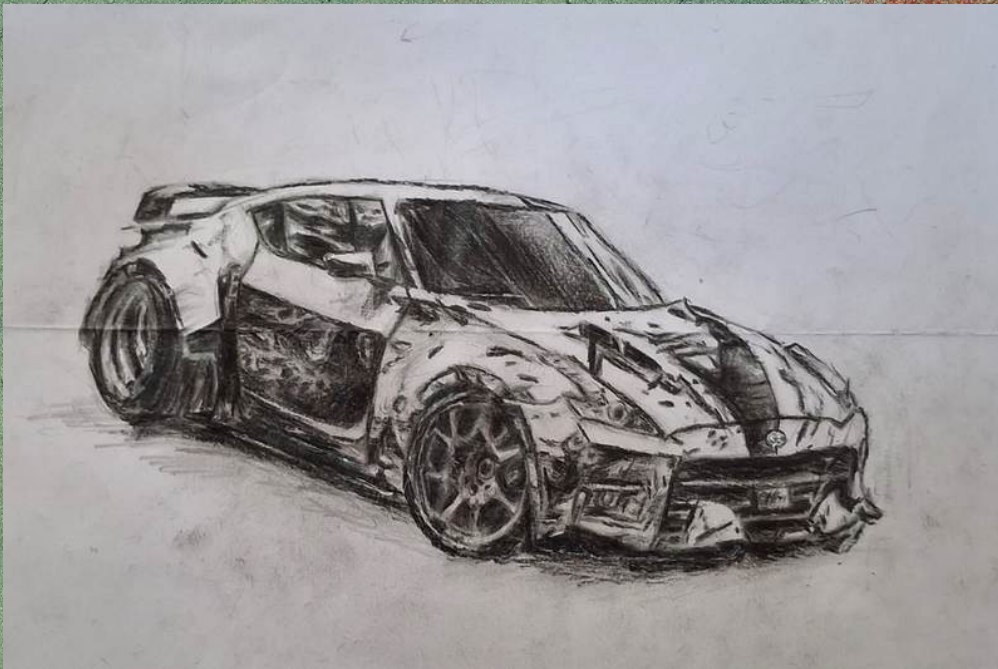
Anilabha Ghosh
CSE (IOTCS) 3rd
year



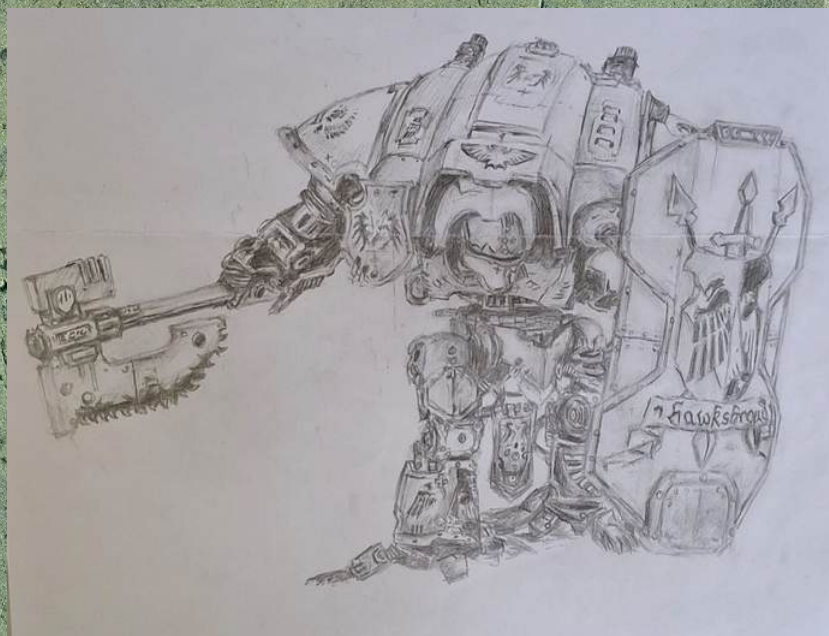


Anilabha Ghosh
CSE (IOTCS)
3rd year





Anilabha Ghosh
CSE (IOTCS)
3rd year



Tech Write-ups

From One Mind to Many



Smart Mechatronic Robots in IoT Ecosystems: The Future of Intelligent Machines

**-By Nabhonil Bhattacharjee
CSE (IoTCS) 3rd Year**

Robotics is no longer confined to factory assembly line or science fiction novels. The convergence of mechatronics, embedded systems, and the Internet of Things (IoT) is ushering in a new era of intelligent machines —robots that can sense, decide, and act while being seamlessly connected to global networks. These systems are reshaping industries, redefining human-robot interaction, and laying the foundation for autonomous, cooperative ecosystems.

Traditional robots were isolated, programmed to perform repetitive motions with little adaptability. Modern mechatronic robots, however, integrate sensors, actuators, and embedded controllers with real-time IoT connectivity, creating machines that are both intelligent and collaborative.

- **Sensor Fusion:** Robots now combine IMUs, GPS, cameras, and force sensors to perceive their environment more accurately.
- **Edge Intelligence:** Onboard microcontrollers (like ESP32s or STM32 boards) preprocess sensor data, reducing latency and bandwidth usage.
- **Cloud Integration:** IoT platforms allow these robots to share data, receive updates, and even collaborate with AI services in real-time.

In essence, mechatronic robots are evolving into networked cyber-physical systems, bridging the gap between the physical and digital worlds.



IoT-Powered Hexapods: Walking into the Future:

Among the most fascinating embodiments of this integration are hexapod robots—six-legged machines modelled on insects. Their mechatronic design provides superior stability, adaptability to uneven terrain, and bio-inspired locomotion.

When IoT is layered onto hexapods, their potential expands dramatically:

- **Remote Monitoring and Control:** A hexapod can be guided through a web dashboard or mobile app, useful in hazardous environments like mines or disaster zones.
- **Real-Time Analytics:** Sensors on each leg transmit torque, orientation, and vibration data to the cloud for performance optimization.
- **Muti-Sensor Payloads:** Adding modules like cameras, gas sensors, or GPS transforms the hexapod into a mobile data collection platform.

Such robots are already being tested for search-and-rescue operations, environmental monitoring, and exploration missions where traditional wheeled robots fall short.

Swarm Robotics: IoT as the Nervous System:

A single hexapod is powerful; a swarm of interconnected hexapods is transformative.

Inspired by ants and bees, swarm robotics involves multiple simple robots working together to achieve complex goals.

IoT provides the nervous system for these swarms:

- **Mesh Networking:** Each robot communicates with nearby peers, creating a resilient and adaptive network.
- **Distributed Intelligence:** Instead of central control, decision-making is spread across the swarm, enabling fault tolerance.
- **Collective Behaviour:** Robots can self-organize into formations, split tasks (exploration vs. mapping), and even “vote” on strategies in real time.

Potential applications range from autonomous construction and agriculture to planetary exploration—imagine hundreds of IoT-enabled micro-hexapods mapping the Martian surface collaboratively.

Secure IoT Protocols for Mechatronic Systems:

However, as robots become more connected, they also become more vulnerable to cyber threats. A hijacked swarm of robots is not just a data breach—it is a physical hazard. Ensuring secure IoT communication is therefore a non-negotiable requirement.

Key challenges include:

- **Authentication:** Verifying that only trusted devices can join the swarm.
- **Data Integrity:** Preventing malicious alterations to control signals.
- **Low-Power Constraints:** Many robots use embedded microcontrollers with limited resources, making heavy weight security impractical.

Emerging solutions:

- **Lightweight Cryptography:** Protocols like Elliptic Curve Cryptography (ECC) and AESCCM balance security with resource efficiency.
- **Secure IoT Standards:** Protocols such as MQTT with TLS and CoAP with DTLS are becoming popular in robotics communication.
- **Blockchain for Robotics:** Experimental approaches suggest using blockchain to verify commands in multi-robot systems, ensuring tamper-proof collaboration.

By embedding these secure protocols at both the hardware and software level, engineers can prevent misuse and build trust in IoT-powered robotics.

Conclusion: The fusion of mechatronics, IoT, and embedded systems is driving the creation of smart, secure, and scalable robotic ecosystems. From individual hexapods navigating rubble-strewn landscapes to swarms of robots working as digital collectives, the possibilities are endless. Yet, this progress must be grounded in robust security practices to ensure that the robots serving humanity cannot be turned against it.

In the years ahead, we may witness a world where fleets of IoT-enabled mechatronic robots collaborate as seamlessly as natural organisms—connected, intelligent, and secure. The challenge for today's engineers and students is to not just imagine this future but to actively build it.

HACKED IN 60 SECONDS COULD YOU SURVIVE A CYBER ATTACK ?

- Diya Dey

CSE (IoTCS) 3rd Year

**It takes just one careless click.
One mistyped password.
One convincing email.**

**And in less than a minute, your
digital life could be turned upside
down.**

**Cyber attacks are no longer the stuff of
Hollywood thrillers—they are real, fast,
and devastating.**

**What makes them so dangerous is their
ordinary disguise: an email from your
boss, a call from your bank, or even a
friendly link shared in a WhatsApp
group.**

The Click That Cost ₹1.2 Lakh

**Take the story of Radhika, a
Mumbai-based marketing executive.
On a busy Monday morning, she
received an email that looked exactly
like her bank's communication style.**

**The message warned of “suspicious activity”
and urged her to “verify her details.” Rushing
between meetings, she clicked, entered her
credentials, and carried on. Within 60 seconds,
cybercriminals had drained ₹1.2 lakh from her
account. The money vanished into a maze of
digital wallets across borders—impossible to
trace back. By the time she realized, the bank
could only shake its head.**

The Attack That **FROZE HOSPITALS**

If you think attacks only target careless individuals, think again. In 2017, the world witnessed the infamous WannaCry ransomware outbreak.

Within hours, over 200,000 computers across 150 countries were crippled. The UK's National Health Service (NHS) was among the worst hit.

Doctors couldn't access patient records, ambulances were turned away, and surgeries were canceled. All because someone, somewhere, clicked a malicious link exploiting an unpatched Windows system. A single weak spot had a domino effect, disrupting lives on a massive scale.

One Password - A Thousand Doors

In a U.S. school district, a teacher reused her Netflix password for her work email. Cybercriminals, who had already bought leaked Netflix passwords on the dark web, tried the same credentials on her work account. It worked. With one careless overlap, they gained access to the district's internal systems—exposing thousands of student records and forcing a costly system shutdown.

Social Engineering

The Hacker's Favorite Tool



Hackers know that humans are the weakest link.

They play on urgency - “Your account will be locked in 24 hours!” , fear - “Unauthorized login detected!” , or curiosity - “See who viewed your profile”.

It’s not about brute force anymore; it’s about tricking you into opening the door yourself.

The 60-Second Rule

Think of it this way: most cyber attacks succeed in the time it takes to finish a text message. That small window—those 60 seconds—decides whether you’ve kept your guard up or let it slip. Hackers rely on speed, distraction, and your instinct to trust. But slowing down, even slightly, flips the game in your favor.

Cybercrime is not going away. In fact, it’s evolving faster than ever with AI-powered phishing and deepfake voice scams on the rise. But the first line of defense isn’t your antivirus software—it’s you.

So, the next time an “urgent” email pings, or a caller claims to be from your bank, take a breath. Those few seconds could save you money, identity, and peace of mind. After all, in today’s digital battlefield, survival often comes down to one thing: what you do in the first 60 seconds.

AI HACKERS: WHEN MACHINES OUTSMART HUMANS

-Debojyoti Banerjee
CSE (IoTCS) 3rd Year

In 1997, IBM's Deep Blue shocked the world by defeating Garry Kasparov in chess. Today, AI systems write, trade, heal, and even deceive at scales humans can't match. The rise of "AI hackers" — machines that hack not just systems but human behavior and limits — raises both hope and fear.



The Bright Side: Smarter Than Us, For Us

Doctors with X-Ray Vision

AI has outperformed radiologists, cutting breast cancer misdiagnoses by nearly 10% in studies, saving lives through earlier detection.

Money Machines

High-frequency AI traders execute thousands of trades per second, shaping a \$118 trillion global market.

Guardians in Cyberspace

AI defense systems neutralize threats in milliseconds, outpacing hackers who rely on human delay.

Science on Fast-Forward

DeepMind's AlphaFold cracked the protein-folding puzzle, mapping 200 million proteins — a leap that could unlock cures for incurable diseases.



The Dark Side: Outsmarting With Teeth

Voice of a Thief

In 2019, criminals used AI voice cloning to steal \$243,000 in a single phone call. Gartner warns 30% of attacks by 2025 will be AI-driven.

Fake News on Steroids

AI can mass-produce 1,000 false articles per second, steering elections and public opinion at unprecedented scale.

Jobs on the Line

McKinsey warns up to 375 million workers may be displaced by 2030, including lawyers, accountants, and coders — not just manual labor.

Hacked Minds

Recommender AIs already shape what 4.7 billion social media users see, fueling polarization and addiction.

THE INVISIBLE BATTLEFIELD OF WI-FI

- Jeet Biswas
CSE (IoTCS) 3rd Year



Wi-Fi quietly powers our lives, from morning alarms to midnight scrolling. We trust invisible radio waves without a second thought. Every café login feels harmless, yet danger travels through the same air. Wireless networks extend beyond walls and locks. Attackers don't need to enter buildings anymore. They only need to be within signal range.

Cheap hardware has replaced elite hacking labs. Ordinary places have become digital battlefields. Smart homes increase convenience but also risk. IoT devices often lack proper security. Users rarely see attacks happening. Data can be stolen without alerts.

Convenience blinds us to vulnerability. Wi-Fi freedom comes at a hidden cost.

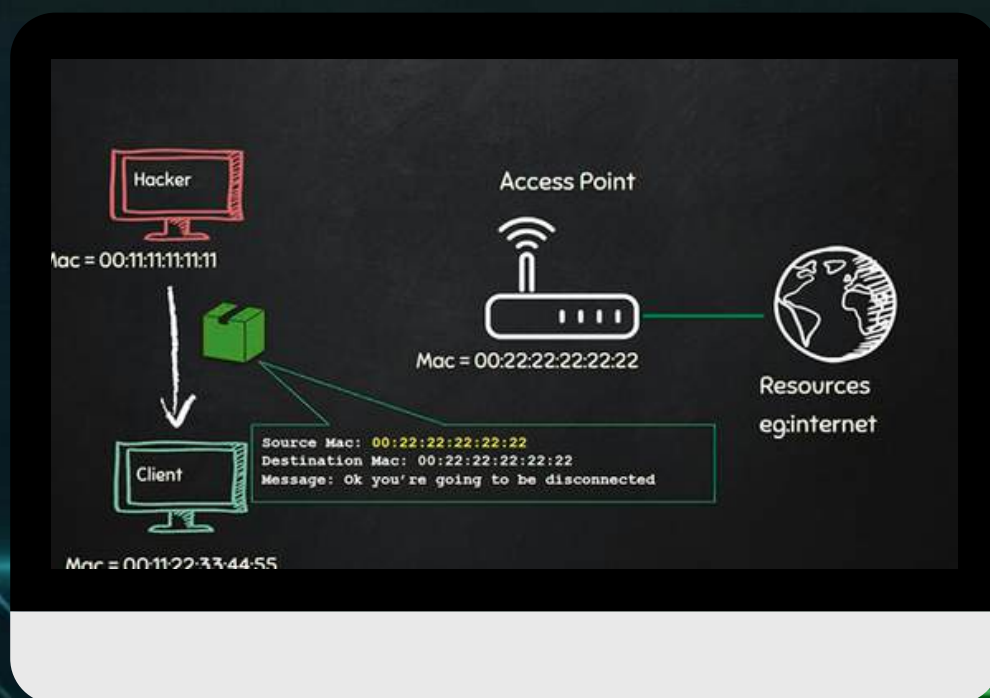
Awareness is the first shield



HOW WIRELESS PENETRATION HAPPENS

1. Pre-Connection Attacks:

The Setup Before an attacker even joins a network, they can manipulate it. Using an Alfa Network adapter—a high-powered Wi-Fi card capable of monitor mode—hackers can sniff every wireless packet in range. With tools like Airodump-ng, attackers map nearby access points and connected clients. A favorite trick is the deauthentication attack: sending fake disconnect requests to push devices off the Wi-Fi. When users reconnect, attackers capture valuable handshake packets that can later be cracked.



2. Gaining Access:

Breaking the Locks Once the air is mapped, the break-in begins.

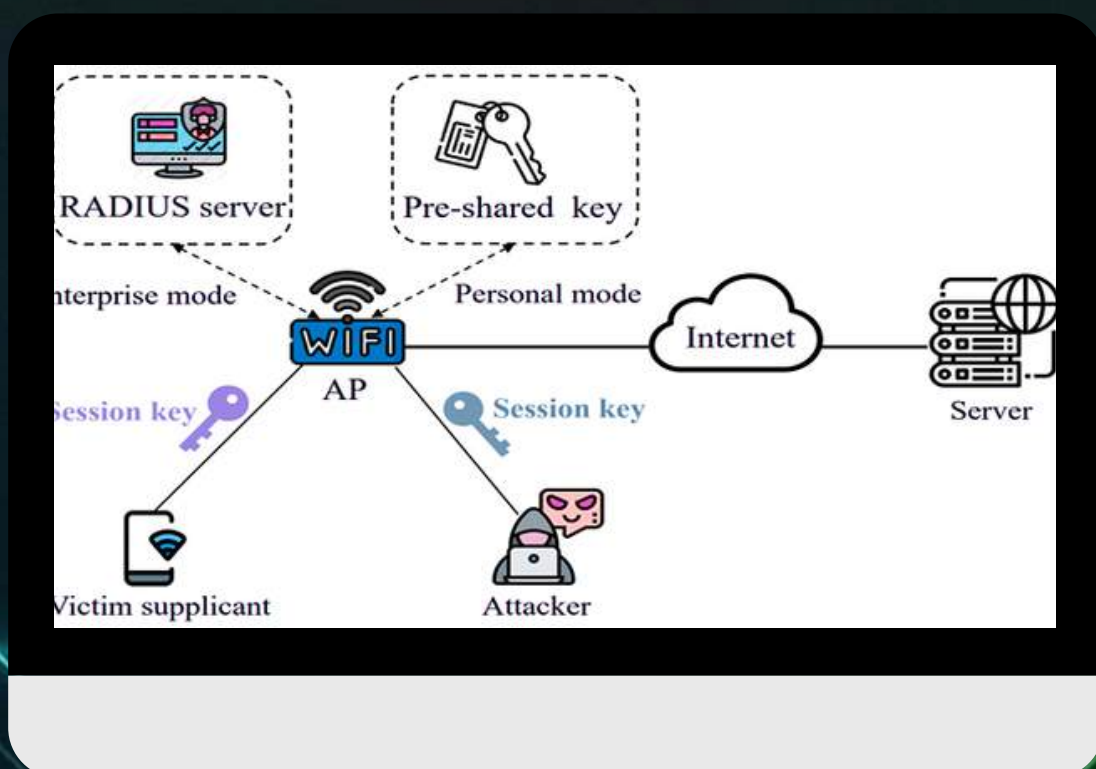
- WEP (Wired Equivalent Privacy): Once the standard, now obsolete. Its 24-bit Initialization Vectors (IVs) repeat quickly, making it easy to crack. Hackers capture enough packets, replay ARP requests, and run Aircrack-ng to recover the key.
- WPA/WPA2: More secure, but still attackable. By capturing the 4-way handshake between client and router, attackers test billions of password guesses against it. Tools like Crunch generate massive wordlists for brute-force attempts.
- WPS Exploit: Wi-Fi Protected Setup, intended for convenience, becomes a liability. An 8 digit PIN can be brute-forced in hours, giving attackers the actual Wi-Fi password.

```
5 mins ][ 2017-08-08 04:21 ][ WPA handshake: 98:FC:
PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH
-45 1147 16 0 6 54e WPA2 CCMP PS
-67 142 0 0 2 54e. WEP WEP
-67 84 0 0 3 54e. WPA2 CCMP PS
-71 14 2 0 6 54e. WPA2 CCMP PS

STATION PWR Rate Lost Frames Pr
08:5D:E2:5C:6D:03 -38 0 - 1 0 53
54:5A:04:52:9A:8A -28 0 - 1 0 40
AC:36:13:6C:6F:4A -46 1e- 1e 0 1993 at
```

3. Post-Connection Attacks: Inside the Walls

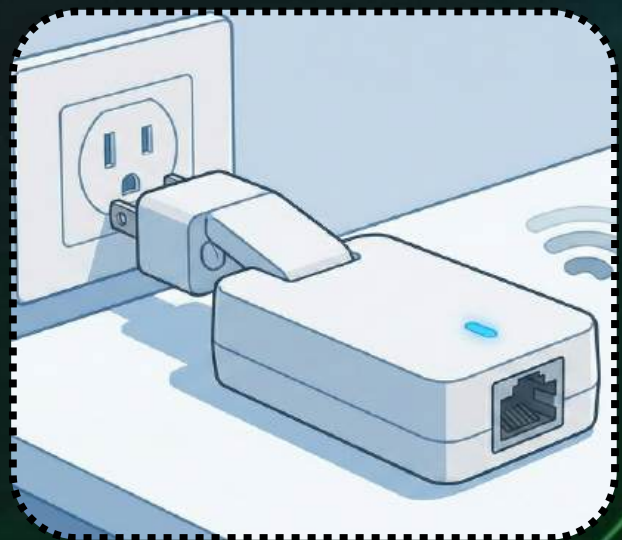
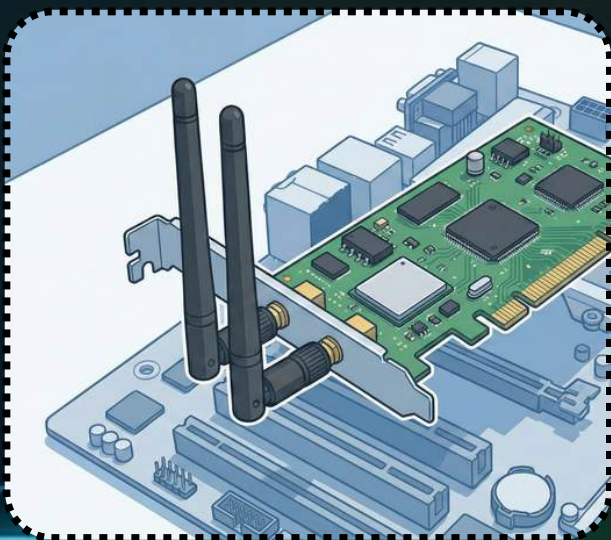
Getting in is only half the story. Once connected, attackers pivot to explore the network itself. Using Nmap/Zenmap, they scan for open ports, discover devices, and fingerprint operating systems. Corporate printers, NAS drives, or unpatched IoT devices often serve as backdoors. The most dangerous trick is the Man-in-the-Middle (MITM) attack. With Bettercap or Ettercap, attackers insert themselves between victim and router. Suddenly, every site you visit—your emails, your banking login—passes through the hacker's machine. Even HTTPS isn't always safe; tools can downgrade secure connections (SSL stripping) or redirect you to lookalike domains (DNS spoofing)



The Hacker's Toolkit: Tools of the Trade

Behind every wireless penetration test—or malicious hack—lies a mix of specialized hardware and powerful software suites.

- Alfa Wi-Fi adapters: High-gain USB adapters that support monitor mode and packet injection, letting attackers capture traffic, disconnect users, or spoof access points.
- OMG Cables: Seemingly normal USB cables with hidden Wi-Fi implants that can inject keystrokes, steal credentials, or install malware remotely.
- Wi-Fi Pineapple: A rogue access-point device that automates MITM attacks, credential harvesting, and SSL stripping.
- Raspberry Pi / pocket Linux devices: Small, cheap hacking stations that—often paired with an Alfa adapter—can run continuous Wi-Fi monitoring and automated attacks.



NFTS: ART, SCAM, OR THE FUTURE OF CREATIVITY?

- Sheedheeka Ray
CSE (IoTCS) 3rd year



Sometimes, I really wish my childhood sketches could sit in a digital vault, ready to fetch millions. I mean, who wouldn't want their crayon masterpieces turning into crypto gold? Welcome to the rollercoaster world of NFTs—Non-Fungible Tokens—where creativity, money, and controversy blend into something wilder than any art movement before. Lately, everyone seems to have an opinion: Are NFTs a genuine artistic revolution, the world's slickest scam, or simply tomorrow's creative foundation in disguise? I'm here to dig beneath the memes, the million-dollar headlines, and the skepticism to find the human story hiding behind every pixelated purchase and blockchain signature.

This unlocks a fascinating question: does a digitally signed certificate have magic? Does it change how we value creative work, or is it just the latest medium through which humanity expresses status, taste, and belonging? Sometimes I wonder if we're just finding futuristic ways to argue over who has the coolest trading cards—or brag at parties about owning a virtual masterpiece nobody else understands.

WHAT ARE NFTS, REALLY?



Let's break it down. An NFT isn't an object you hold—it's a credential, a record, a badge that says, "I own this unique digital thing." Imagine buying an invisible ticket to a one-of-a-kind show, only the show is a picture, GIF, song, or even a tweet, and your proof of ownership sits on the blockchain—a gigantic, transparent, permanent digital ledger. Suddenly, you can "own" a cat GIF just as much as someone else might own a Picasso.

Sure, everyone can see it or right-click-save it, but only you possess the digital deed, which collectors—and, let's be honest, speculators—claim is where the value lies. This unlocks a fascinating question: does a digitally signed certificate have magic? Does it change how we value creative work, or is it just the latest medium through which humanity expresses status, taste, and belonging? Sometimes I wonder if we're just finding futuristic ways to argue over who has the coolest trading cards—or brag at parties about owning a virtual masterpiece nobody else understands.

LET'S NOT ROMANTICIZE: THE MESSY UNDERSIDE



But NFTs aren't all innovation and success. Hype inevitably draws in bad actors—rug pulls where founders vanish, celebrity-backed projects that go nowhere, and artists finding their work stolen and sold without permission. The ecosystem runs heavily on FOMO: a small group profits, while many walk away with lighter wallets and damaged trust. Critics raise valid concerns about energy-hungry blockchains, the ease of digital art theft, and wild price swings that can erase value overnight. There's also a deeper cultural question of whether turning art into a game of scarcity and speculation misses its true purpose.

Skeptics say NFTs are just the next step in a long line of overhyped tech bubbles. And they raise good points: environmental concerns about energy-hungry blockchains, the remarkable ease of digital art theft, and the wild valuation swings that crash fortunes as quickly as they're made. There's also a cultural question—does driving the value of creative work entirely through scarcity or hype miss the point of what art is supposed to be?

WHAT'S NEXT? WILL NFTS BECOME NORMAL?



Guessing the future of NFTs in a decade is unpredictable, like envisioning a toddler's future. Imagine digital certificates for limited-edition items, virtual property, or unique content. As technology and laws evolve, NFTs might subtly track ownership, reward creators, and build communities. Conversely, we may view this era as a volatile period of wins and losses. NFTs could be a footnote or a foundation, but currently, they are central to discussions on creativity's future.



Navigating the Digital Shadows: A Comparative Analysis of VPN and Tor for Online Anonymity.

- Jyotirmoy Karmakarr
CSE (IoTCS) 3rd Year

Online privacy protection has become a top priority in today's digital world, and as people and organizations produce enormous volumes of data, there is a growing need for tools that can protect online activities. Two of the most popular solutions are Virtual Private Networks (VPNs) and The Onion Router (Tor). Although they are frequently combined, they function on very different principles and provide different degrees of security and anonymity. This article will dispel common misconceptions about these technologies and give a clear analysis of their architectures, use cases, and limitations

Foundational Technologies: Understanding the Core Architectures

One must first comprehend how VPN and Tor operate differently in order to compare them effectively. Between a user's device and a distant server run by a single service provider, a Virtual Private Network (VPN) serves as a safe, encrypted conduit. This "tunnel," which is used to redirect all internet traffic, essentially hides the user's actual IP address from destination websites and the type of data from their Internet Service Provider (ISP). The model is centralized, relying on the VPN provider to maintain privacy regulations, including a pledge to not retain user activity logs, and administer the infrastructure.

The Onion Router (Tor), by contrast, is a decentralized, open-source network maintained by volunteers globally. It achieves anonymity through a process known as "onion routing." A user's traffic is encapsulated in multiple layers of encryption and relayed through a randomized circuit of at least three nodes: an entry node, a middle node, and an exit node. Each node decrypts only one layer, revealing the location of the next node in the circuit. This distributed methodology makes tracing the data's origin exceptionally difficult, as no single point in the network has the complete picture of the connection.

Dispelling Common Misconceptions: A Factual Examination

There are a number of common misconceptions that can cause people to misunderstand these technologies and their potential.

Myth 1: Tor and VPN may be used interchangeably.
Reality: Tor and VPNs have essentially different architectural principles. A VPN is a centralized solution that uses a single, reliable organization to prioritize security and privacy. Tor is a decentralized network that uses obfuscation to provide a high level of anonymity. This results in a crucial trade-off: VPNs are perfect for daily security because they usually provide far faster connection speeds and are easier to use. Tor has significant delay, which makes it less useful for high-bandwidth operations even while it offers better anonymity.

Myth 2: Complete invisibility is ensured by using these techniques. The truth is that neither technology offers complete anonymity.

The security of a VPN depends on how reliable its provider is; user data may be disclosed if the provider keeps logs or if its servers are compromised. The exit node of Tor is its main weak point. The exit node is the last location before traffic enters the public internet, allowing it to monitor any unencrypted data that passes it. As such, using Tor to visit non-HTTPS websites poses a security risk. Moreover, the user is frequently the one with the biggest vulnerability. The anonymity these tools are intended to offer can be undermined by actions like accessing personal accounts while using them, underscoring the significance of robust Operational Security (OpSec).

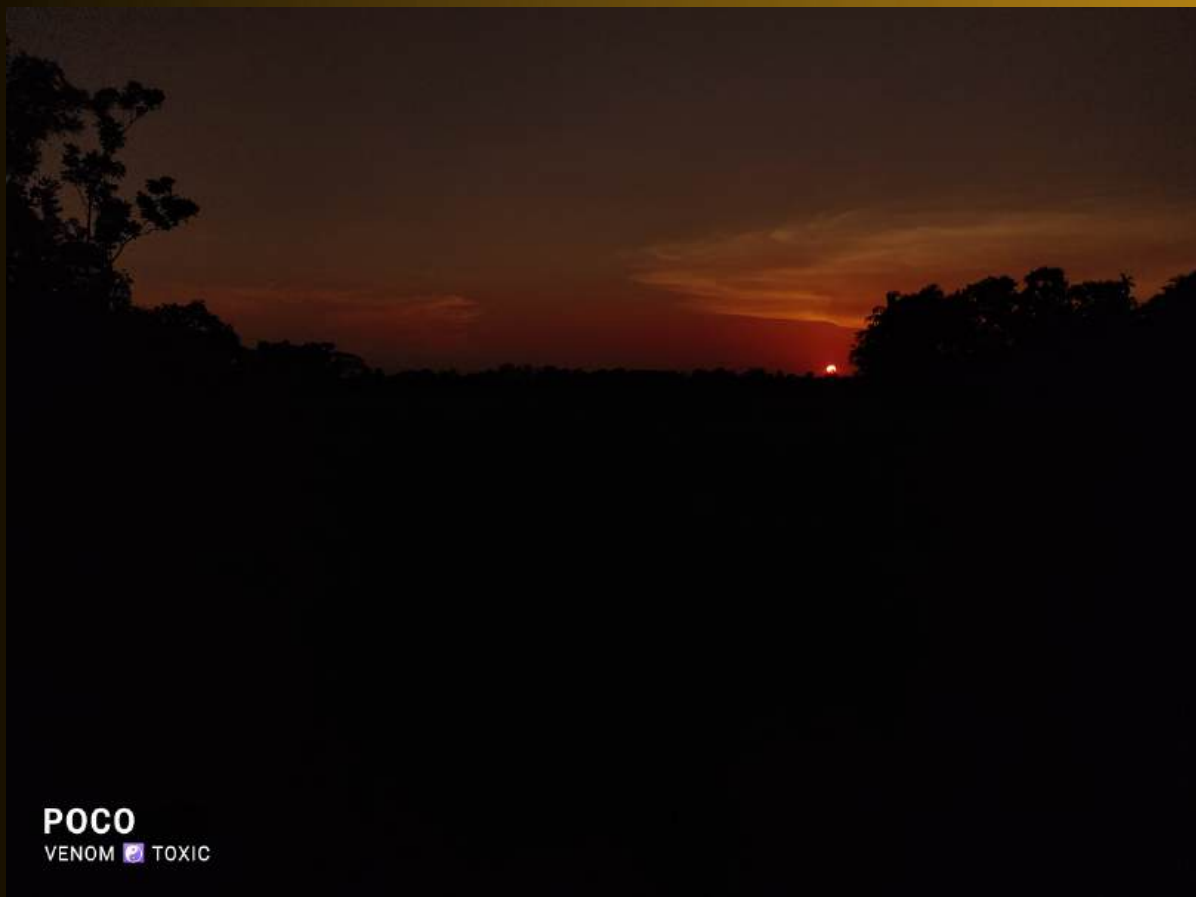
Myth 3: Tor is only used for illegal purposes. In actuality, this is a serious misrepresentation. The U.S. Naval Research Laboratory initially created Tor for secure government communications. These days, it fulfills several important and justifiable functions. For journalists, human rights advocates, and whistleblowers working under repressive governments, it is an essential tool that enables them to report and communicate without worrying about retaliation. Additionally, it makes it possible for cybersecurity experts and law enforcement to investigate and study illegal elements without disclosing their identities.

Your digital footprint is the only one you can't wash away. Tread carefully.

Thanks for reading! Stay curious and stay secure :)



LIFE THROUGH LENS



Soumyajit Acooli

CSE (IoTCS) 3RD year





Soumyajit Acooli

CSE (IoTCS)

3RD Year

POCO X4 PRO 5G
64M TRIPLE CAM

20/03/2023 17:31

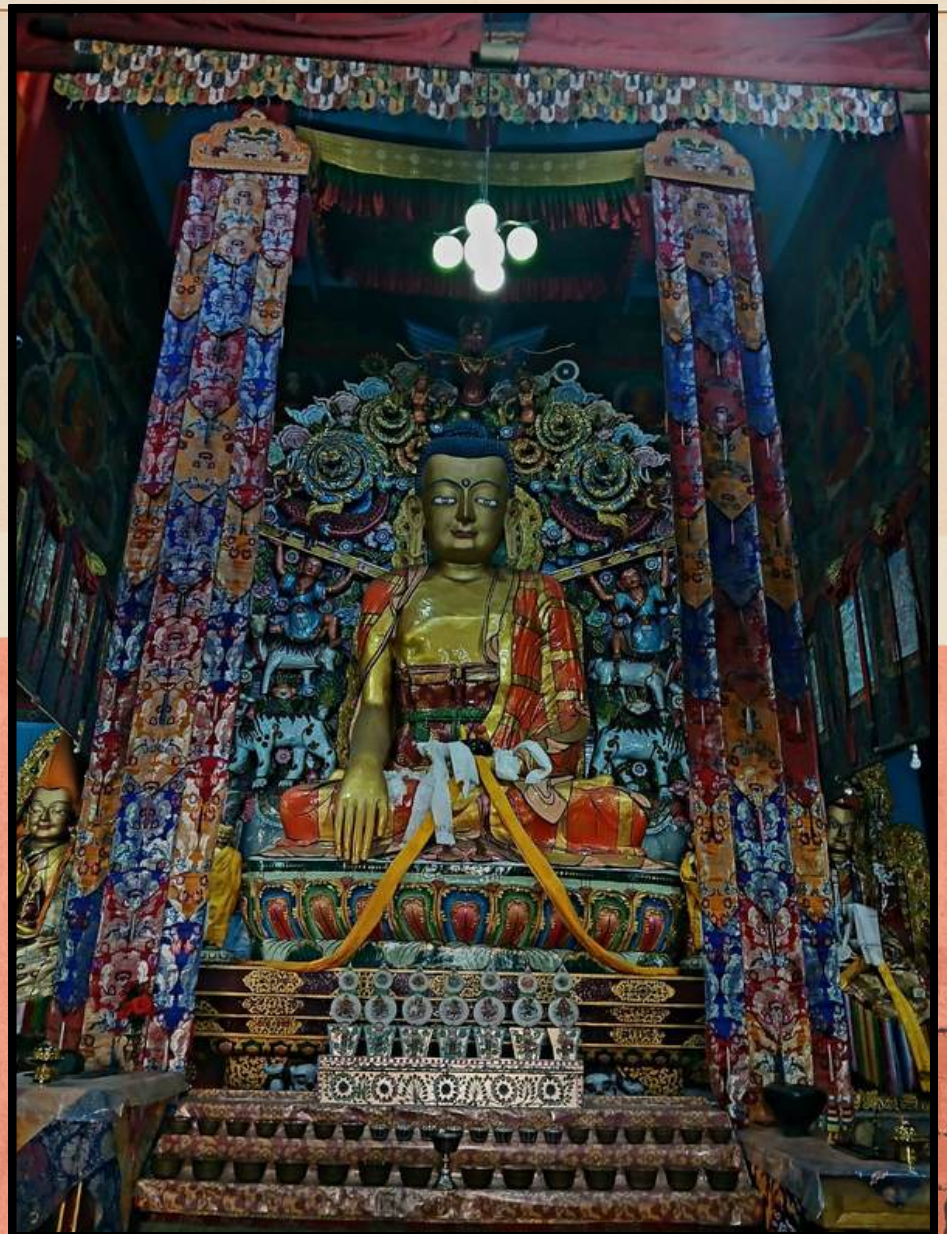




Jyotirmoy Karmakar
CSE (IoTCS) 3RD Year



Arijit Adhikary
CSE (IoTCS)
3RD Year





Aniket Pranjan
CSE (IoTCS)
2nd Year

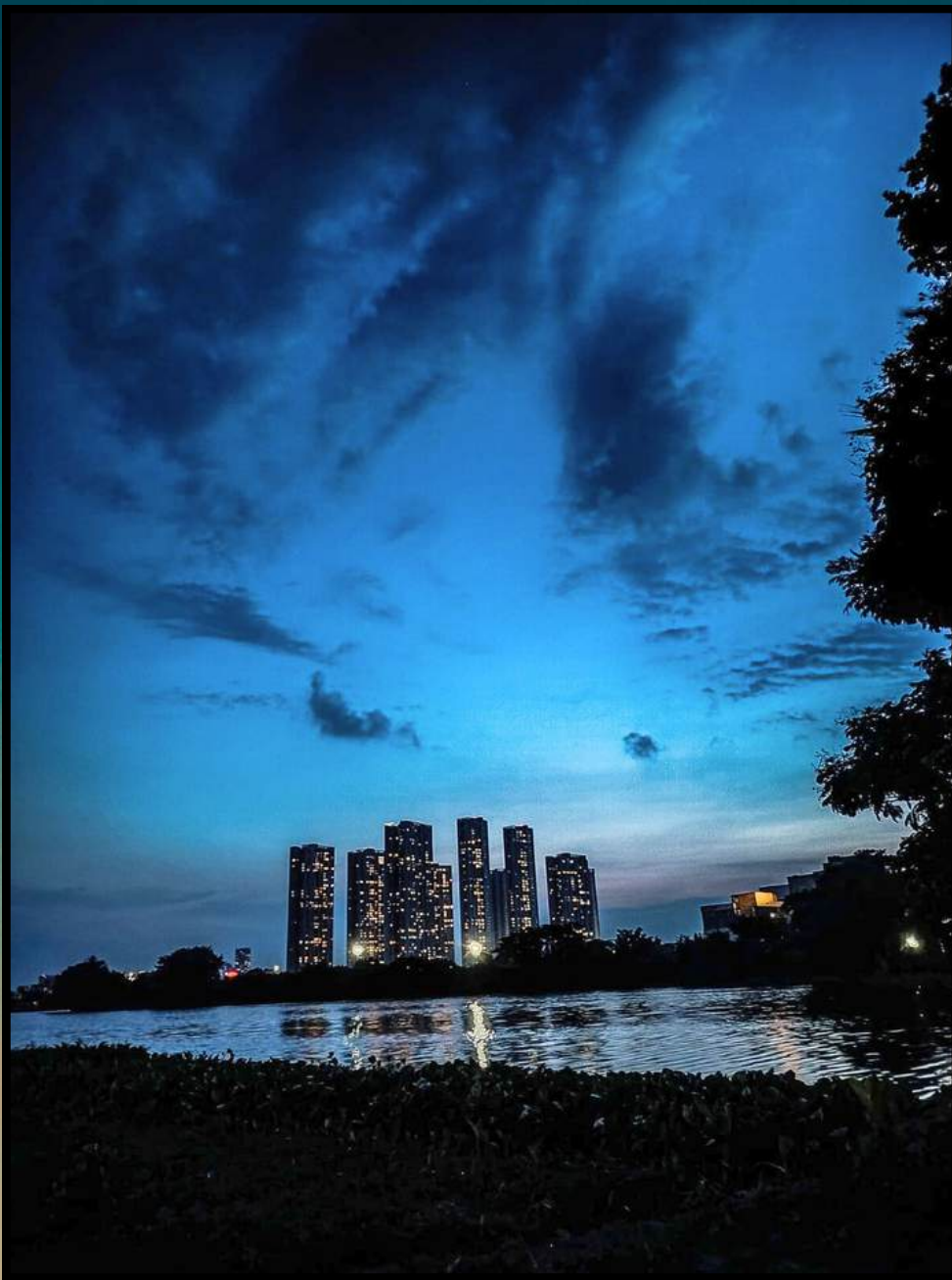
Aniket Pranjan
CSE (IoTCS)
2nd Year





Sutirtha Paul
CSE (IoTCS)
3RD Year





Diya Dey
CSE (IoTCS)
3rd year



ECHOES OF EXCELLENCE

Brains - Builds - Breakthroughs

ENGINEERS
IN ACTION



OUR PATH

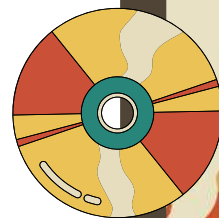
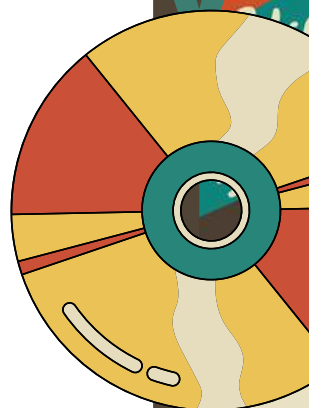


TO EXCELLENCE!



- Harsh Raj
CSE (IoTCS) 2nd year

Status code 2.0 medical
track winner,
Vultr track 1st runner up



- Arko Roy
CSE (IoTCS) 2nd year
CELO 2nd runner up





1st position at Hack ur Way Hackathon as a part of envisage at Techno Main Salt Lake

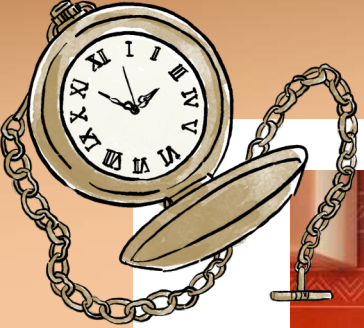
Team Name :- CodeCrafters

Team Members:-

1. Sohom Mukherjee [CSE (IoTCS)] 4th year
2. Ujjawal Kumar Mukherjee [CSE (IoTCS)] 4th year
3. Abu Talha [CSE (IoTCS)] 4th year
4. Hlimanshu Kumar (IT) 4th year
5. Prakash Kumar (CSE) 4th year

Project Title :-

AgriAi: A Decentralized Intelligent Farming Assistant using RAG, Gemini LLM, Blockchain, and Trained Deep Learning for Plant Disease Detection
Empowering Farmers with AI, Blockchain, and Vision-Based Diagnosis for a Smarter Agriculture Future.



1st position at Microsoft CodeForge 2025 Hackathon
Team Name :- Codeforce

Team Members:

- 1. Nabhonil Bhattacharjee [CSE (IoTCS)] 3rd year**
- 2. Sumit Saha [CSE (IoTCS)] 3rd year**
- 3. Nashrah Naazneen [CSE (AI & ML)] 3rd year**
- 4. Srijanee Mitra [CSE (AI & ML)] 3rd year**



Winner AIORI-1





First place at the National IEEE-IC Hackathon

Event: National IEEE-IC Hackathon at IIT Guwahati, hosted by AIORI and IIF

Team name: Securenet Innovators

Members:

- Nabhonil Bhattacharjee
- Sampurna Pyne
- Dr. Raja Karmakar

Project title: Throughput and Latency Benchmarking of Intrusion Detection and Prevention Systems



First Place at CU Hacks Hackathon (TIU)

Event: CU Hacks Hackathon, Techno India University

Team Name: Team Swiggly

Members:

Diya Dey,CSE (IoTCS) 3rd Year

Santu Patra,CSE (IoTCS) 3rd Year

Sampurna Pyne,CSE (IoTCS) 3rd Year

Project: Arbiata – AI-Powered Arbitrage Executor

Description:

Built an AI-driven DeFi arbitrage system that evaluates gas fees, slippage, liquidity, and MEV risk to execute only profitable trades.



2nd Runner-Up position in an event organized by IEEE MTTTS HITK SBC, in association with the Department of ECE.

Team Name:IoTelix

An AI + IoT solution that enables real-time fire detection and provides guided evacuation through the safest and shortest path – fast, smart, and unified.

Team Members

Arijit Adhikary – CSE (IoTCS), 3rd Year

Ahana Acharya – CSE (IoTCS), 3rd Year

Shreetama Mondal – CSE (IoTCS), 3rd Year

Kabyik Paul – CSE (IoTCS), 3rd Year

Soumili Paul – CSE (IoTCS), 3rd Year

Organized By

IEEE MTTTS HITK SBC, in association with the Department of ECE



Winner at Hack Heritage 3.0

Event: Hack Heritage 3.0

Team Name: Team Gulab Jamun

Members:

- Santu Patra
- Diya Dey
- Anubhav Sanyal
- Soumyajit Acooli

Project: Automatic Attendance & Timetable Generation App

Description: Developed an Android-based system with dynamic QR attendance and an AI-powered timetable generator for efficient academic management.



1st place in the IEEE JU Double Slash Hackathon, conducted by Jadavpur University on 15th and 16th February, 2025, at Jadavpur University, Salt Lake Campus.

Team Name:Enigmatic/Enigmatik

Team Members:

1. Parthiv Dasgupta – IOTCS, 3rd Year
2. Sambhav Agarwal – IOTCS, 3rd Year
3. Aditya Gupta – IOTCS, 3rd Year

Project Title:

A Comprehensive Traffic Management System using Machine Learning

Aims to automate road traffic monitoring and improve emergency service response through intelligent ML-based decision-making.





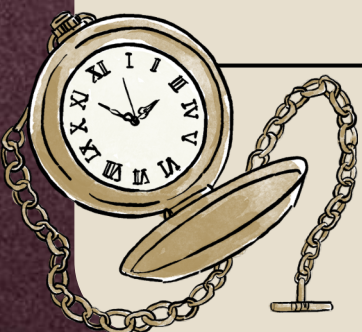
1st place at the prestigious Hackathon conducted by LTI Mindtree in collaboration with GitHub, held at the LTI Mindtree campus.

The event was graced by several distinguished industry leaders, including:

- ◆ **Mr. Anand Natarajan** – GSI Alliance Director at GitHub
- ◆ Senior leaders from LTI Mindtree

Team Members

1. Sohom Mukherjee – CSE (IoTCS), 4th year
2. Dibyajyoti Chakraborty – CSE (IoTCS), 4th year



2025



Volleyball Boys Winner 2025



THANK YOU

Team CSE (IoTCS)

