Estd. in 2001

tcet CSE ENGINEERS

VOLUME 1 EDITION 1

DECYPHER

CIA- THE TRINITY OF SECURITY

COMPUTER SCIENCE & ENGINEERING DEPARTMENT

VISION

To become a department of high repute by imparting quality education and excel in the field of Cybersecurity.

MISSION

The department of Cyber Security is committed to deliver and nurture students with the knowledge and skill set in the field of Cybersecurity to make them competent professionals and develop in them leadership qualities, ethical attitude, lifelong learning and the mindset to contribute effectively towards industry and society.

OBJECTIVE OF THE COURSE

- To make students acquainted with fundamental knowledge of cybersecurity to protect and predict possible security breaches in to the computer systems and networks.
- To upgrade students in the field of cybersecurity by imparting new technological tools and techniques.
- To make students nationally and globally competent to serve society by helping organizations to overcome security threats.
- To enhance the learning experience with good educational and human values.

PROGRAMME OUTCOMES

OUTCOME 1

To become a department of high repute by imparting quality education and excel in the field of Cybersecurity.

OUTCOME 2

PROBLEM ANALYSIS: Identify, Formulate, Research Literature and Analyze Complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences and engineering sciences.

OUTCOME 3

DESIGN / DEVELOPMENT OF SOLUTIONS: Design solutions for complex engineering problems and design system components or processes that meet specified needs with appropriate consideration for public health and safety, cultural, societal and environmental considerations.

OUTCOME 4

CONDUCT INVESTIGATIONS OF COMPLEX PROBLEMS: Using research based knowledge and research methods including design of experiments, analysis and interpretation of data and synthesis of information to provide valid conclusions

OUTCOME 5

MODERN TOOL USAGE: Create, select and apply appropriate techniques, resources and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of limitations.

OUTCOME 6

THE ENGINEER AND SOCIETY: Apply reasoning informed by contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to professional engineering practice.

OUTCOME 7

ENVIRONMENT & SUSTAINABILITY: Understand the impact of professional engineering solutions in societal and environmental contexts and demonstrate knowledge of and need for sustainable development.

OUTCOME 8

ETHICS: Apply ethical principles and commit to professional ethics and responsibilities and norms of engineering practices.

OUTCOME 9

INDIVIDUAL AND TEAM WORK: Function effectively as an individual, and as a member of leader in diverse teams and in multi-disciplinary settings.

OUTCOME 10

COMMUNICATION: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as being able to comprehend and write effective reports and design documentation, make effective presentations and give and receive clear instructions.

OUTCOME 11

LIFE-LONG LEARNING: Recognize the need for and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

OUTCOME 12

PROJECT MANAGEMENT & FINANCE: Demonstrate knowledge and understanding of engineering and management and leaders in a team to manage projects and in multidisciplinary environments.

Creative Team

SHAREZ SHAIKH
Creative Head

HARSHITA KHANDELWAL

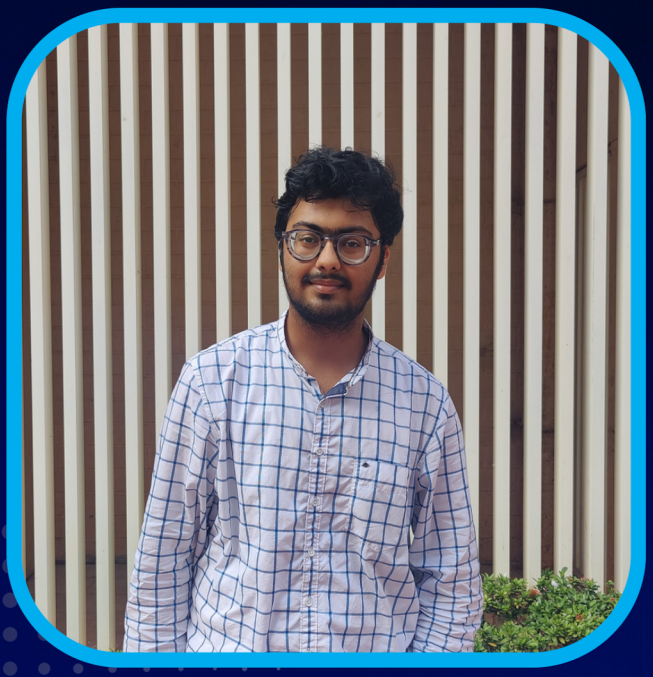
ADITI NIKAM

KESHAV HALDER

MAURWIN BHARDWAJ

Editorial Team

RHEA RAJPUT
Chief Editor



KAUSHAL AGARWAL

STUTI SONI

ANUSHKHA BEHERE


MESSAGES

From the HOD's Desk

Dr. Vidyadhari R Singh

It's an absolute pleasure to introduce to you the premiere issue of "DECYPHER", the first ever magazine to be envisioned from the Department of Cybersecurity. As rightly quoted by Albert Einstein "Creativity is seeing what others see and thinking what no one else ever thought." This magazine reflects the thoughts of creative minds of our budding engineers. With the exponential rise in cybercrime in today's digital age, it becomes a necessity to preserve our privacy and also work towards achieving the three major goals of security, the CIA (Confidentiality, Integrity & Availability). Hence, this magazine will be centering around the theme: CIA: The Trinity of Security.

As the departmental magazine, it an opportunity for students and faculty to present ideas and research into knowledge and motivation for their readers. We have focused on topics ranging from privacy, security breaches and ciphering techniques to the metaverse. We are anticipating readers to engross and absorb all that we wish to convey through this issue, considering the hard work and efforts put in by the stakeholders of the department. I would also like to congratulate the entire team for bringing in fresh thoughts, new ideas, more diversity and work with an inclusive approach. I also thank the committee and the students, faculty, industry experts for their exemplary contribution, their valuable time and effort. I wish you all great success ahead.

Faculty Incharge's Message

"ONE SINGLE VULNERABILITY IS ALL THAT AN ATTACKER NEEDS"

Cyber threats are constantly changing and growing to become more advanced. This causes uncertainty about the privacy of our data. This is why cybersecurity awareness is crucial and is also in great demand nowadays. The advancements in the field, challenge of solving problems, and wide range of career options are making this emerging field more interesting. In today's world, cybersecurity has risen to the top of corporate agendas, as businesses continue to grapple with cyber threats associated with the rise in remote work due to the COVID-19 pandemic.

Ms. Ditixa Mehta

Heightened concerns over security, combined together with a current shortage of cybersecurity professionals, will also drive changes to cybersecurity strategies. As fascinating as the developments in cybersecurity have been, the three security goals have not been altered since. These are CIA - Confidentiality, Integrity, and Availability. These three pillars that are fundamental to data security are the focus of this edition. For cybersecurity professionals, the CIA triad will always remain at the top of their priority list. The DECYPHER 2022 edition 1 strives to ensure that individuals are capable enough to safeguard their own data. We hope to unfold the world of cybersecurity to people and ensure that they remain protected whenever they are on the internet.

It gives me immense pleasure to ensure that this magazine has successfully accomplished its objective. The reflection of the student's creativity is the epitome of the magazine. I take the opportunity to thank all the contributors as their input has made this magazine endearing to our readers.

EDITOR'S MESSAGE

In today's increasingly connected and interdependent world, cybersecurity is an issue that touches virtually every individual, organization, and institutional entity—governmental and non-governmental alike. The main pillars of cybersecurity are CIA - Confidentiality, Integrity, and Availability. Confidentiality is the protection of data from unauthorized access. Integrity is the prevention of unapproved or accidental modification of data. Availability is the accessibility of data to authorized parties on demand.

The introduction of the subject Fundamentals of Information Security was our initiation into the world of cybersecurity. The foremost thing we learnt in this subject were the security goals – confidentiality, integrity, and availability. We believe it encompasses the entirety of the cybersecurity universe, so we chose it as the theme of our premiere magazine.

Being the editorial team for the first issue of CS&E's departmental magazine, we strived to introduce a variety of topics ranging from confidentiality and privacy to the various cyber threats prevalent nowadays. Through our magazine, we hope to "Decypher" these concepts for the general public.

We had a great time designing and editing this magazine. Everyone has given their best for DeCypher's first edition. We hope you find the 2022 edition interesting and informative. We will meet again for the next publication with more captivating articles.

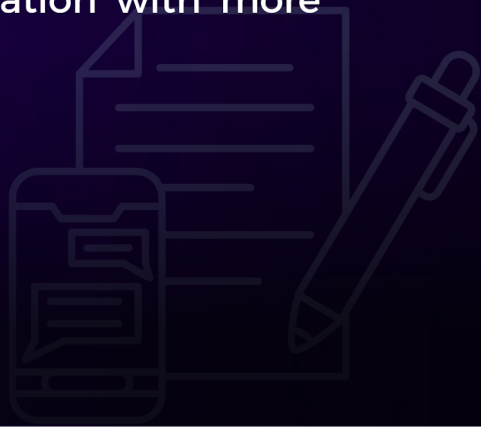


TABLE OF CONTENTS

STUDENT ARTICLES

STUDENT ARTICLES

STUDENT ARTICLES

DIVE INTO CIA

~Shivam Tiwari & Pratik Yadav

Confidentiality is defined as the principle of keeping sensitive data private unless the possessor provides permission to share the data with a third party. Confidentiality measures are designed to help sensitive information from unauthorized access attempts. It's common for data to be distributed according to the type of data and the kind of damage that could be done if it fell into the wrong hands.

Integrity is maintaining the accuracy and ownership of data. Data shouldn't be modified by any third party and steps must be taken to ensure the protection of data from similar third-party threats.

Availability means information should be constantly and readily accessible to authorized parties. This involves duly maintaining hardware, specialized structures, and systems that hold and display the information.

CIA (Confidentiality, Integrity, Availability) is one of the most important triads in the cybersecurity world. To avoid confusion with Central Intelligence Agency, the CIA is also occasionally referred to as AIC (Availability, Integrity, Confidentiality). These three principles together form the "triad" and help guide the development of security programs within the organization.

Securing data confidentiality involves special training to handle sensitive documents. Training can can help familiarize authorized people with threat factors and how to guard against them. Further aspects of training may include strong passwords, password-related styling practices, and data about social engineering to help users from bending data handling rules with good intentions. A good illustration of methods used to ensure confidentiality is requiring an account number when banking online. Data encryption is another common system of ensuring confidentiality. User IDs and passwords constitute a standard procedure; two-factor authentication (2FA) is a growing norm. Different options include biometric verification and security tokens or soft tokens. In addition, users can take precautions to minimize the number of places where information appears and the number of times it's transmitted to complete a needed transaction.

Some precautions include file permissions and admin controls. Admin control may be used to help with incorrect changes or accidental deletion by authorized users from getting into any kind of trouble. Extra measures might be taken in the case of extremely sensitive documents, like storing only on air-gapped computers, disconnected storehouse bias, or for highly sensitive information, in hard-dupe form only. In addition, institutions must put in some means to detect any changes in data that might occur as a result of unusual events like a server crash or natural disaster.

The admin might include cryptographic checksums and different checksums for verification of integrity. Backups must be available readily to restore the affected data to its accurate state.

Best Practices for implementing the CIA triad

An organization should follow the following set of practices to implement the CIA triad successfully.

Confidentiality

- An organization should handle the data, by their privacy policy and no loopholes should be present in their policies.
- Always opt for two-factor authentication (2FA), as it adds an extra layer of security to the devices.
- Permission of apps that are not in daily use should be revoked, as such apps can pose a threat to confidentiality.

Integrity

- Human error should be minimum in handling confidential data.
- Backups should be readily available at any time.
- Admin controls should be with a trusted officer and should be protected on a priority basis.

Availability

- System and software should be up to date as security updates are very important.
- Server monitoring systems should be used effectively.
- In case of data loss, a backup plan should be available.

The conception of the CIA triad was formed over time and doesn't have just a single creator. Confidentiality was proposed in 1976 in a paper by the U.S. Air Force.

Likewise, the conception of integrity was explored in a 1987 paper named “A Comparison of Commercial and Military Computer Security Programs" written by David Clark and David Wilson. The paper honoured that marketable computing required account records and data correctness. It wasn’t easy to find a source, but the concept of availability emerged around 1988.

THE ENCRYPTION LORE

~Keshav Halder & Ankit Das

Ciphering and deciphering messages have been a part of us since the beginning of time. The encoding and decoding of messages was traditionally done using cipher machines or devices.
The first cipher predates back to the Greeks around 400 BC. At that time, they used ciphering methods to send signals or messages to their comrades. The used cipher device, known as the scytale, was made of a tapering baton around which a message-containing piece of paper was spirally wound. When the parchment was unwound, it had a confusing collection of letters, but when it was wrapped around another baton with the same dimensions, the original inscription was once again visible.

Even though the Greeks started it, ciphering of messages became popular because of one roman emperor called Caesar. Around 100 BC Caesar created a cipher that was later named the Caesar cipher. Suetonius employed it in a three-shift configuration to safeguard communications with military import: When he needed to communicate something private, he used ciphers, which is when the letters are arranged in a way that no word can be deciphered. Anyone who wants to decipher them and understand what they mean must replace the letter A with the fourth letter of the alphabet, which is D, and do the same for the remaining letters.

After this, similar methods of ciphering were used by other people to transfer messages.

Then in 1891, Étienne Bazeries invented a more sophisticated cipher device based on principles formulated by Thomas Jefferson of the United States. The ciphertext was created arbitrarily by removing any other row from the discs, which were positioned in a predetermined manner on a central shaft and rotated so that the plaintext's first 20 characters appeared in a row. Then, 20 letters at a time, the remaining letters in the message were handled similarly.

Soon many developments were seen in the world of technology. Radio and electromagnetic communications improved drastically which brought a new revolution in cryptic devices. Although technology was developing really fast, it soon came to a halt when a war began in Europe which ultimately engulfed all the other nations. During this time there were various innovations taking place, not for the betterment of mankind but for its doom. A new type of device came into the picture called the rotor cipher device. One popular rotor method used factors that were basic monoalphabetic substitution ciphers and product ciphers. This machine's rotors were made up of discs with electrical contacts on both sides that were hardwired to allow any number of one-to-one connections (monoalphabetic substitution) between the contacts on opposing sides of the rotor.

Both the Allies and the Axis utilized rotor cipher machines extensively during World War II, with the German Enigma machine being the most known example.

Despite no substantial changes in the fundamental design, the introduction of electronic components in future years led to notable advances in operation speed.

In the 90s, the world of encryption reached a major turning point. SHA Family Hash Ciphers were used for hashing rather than encryption and were published by NIST. The original SHA cipher published in 1993 is now designated SHA-0 in order to fit in with the naming conventions of subsequent versions. Lately, only SHA-2 and SHA-3 were used for hashing. Now, jumping to the current day and age, raw computing power was soaring up in the sky more than ever before. The historical methods were getting outdated, forcing people to come up with better methods to safeguard data from attackers. The ways of encrypting text are only limited by human creativity or intelligence.

Even though the ciphering techniques used today seem incredible, some of the most profound old cases have not been solved yet. One such inhumane case harmed and killed more than seven people within a single year. The name that the person received was The Zodiac Killer. He started terrorizing California in 1966 and his reign ended in 1969. He sent four encrypted messages to challenge the police during that time.

Out of four, the fourth remains unbroken even today. Another unbroken cipher remains on the grounds of the CIA (Central Intelligence Agency) in Virginia. This sculpture bears four encrypted codes.

Among those four codes, only three have been decoded while the fourth code remains one of the most famous unsolved codes on Earth. This shows that effort needs to be put into the world of ciphers.

Federal agencies today are producing, processing, and moving data at an exponentially accelerating rate. The government must not only deploy the most trustworthy encryption methods available today, but it must also be prepared to adopt future ones in order to keep all that data secure, whether it is at rest, in use, or in transit. The nation's information security will depend on promising new methods of encryption including post-quantum cryptography, quantum key distribution, and homomorphic encryption as adversarial and insider threats intensify. All of this sounds really interesting, but we have to wait and watch how things unfold and what the future has in store for us.

THE ILLUSION OF PRIVACY

~Rhea Rajput

"Attackers want you to give up one of four things: information, access, data, or cash. That's what it is, and it has nothing to do with human stupidity. Not a thing."
– Brett Johnson

The above statement was delivered by a cybercriminal turned security advisor in one of his speeches. In the current digital era, everything we do is being recorded. Even though many platforms claim to keep our information private, there is always some loophole in the terms and conditions that we never really bother to read.

The term **"privacy"** means to protect an individual's critical information like passwords, financial details, etc. Privacy was different in the past when the only public record of ours was an entry in the telephone directory. Nowadays, relationships, engagements, divorces, confessions, and sexual identities are all declared on social media. This global explosion in social media has given Facebook, Twitter, Instagram, and Google unlimited access to data about all the people living in this world. It's a buffet out there for hackers and stalkers. This illusion of privacy is beneficial even to those industries that take advantage from the lack of it.

Now, let's break this illusion. We agree that online privacy isn't something that we have, but do you realise how little privacy you actually have?

All our communications travel across the open air. Some might be encrypted and some are not. This has been the system for a long time, and so everything we say can be collected and used to monitor, steal, and stalk us.

As soon as we go online, our internet service provider can see every single website we are accessing. Be it a home internet connection or mobile data, everything is visible to them. Our mobile carrier may even be tracking and selling our app usage activity.

When we visit a website, the owner can see our IP address and can use it to track us. Tracking scripts can be loaded and used to track our activity across multiple websites. You must have experienced finding ads related to a product you were looking up on a particular website. Moreover, even if we are regularly clearing cookies, there are several other ways of detecting our digital footprint.

The above examples are known, but you might be shocked by the next one. Advertisers can literally tie our in-store visits and purchases back to the ads that are suggested to us. Google actually has a product for this. One of its data sources uses the vague sentence **"transaction data uploaded by the advertiser or aggregated and anonymized data from third parties."** Facebook's advertising services are so advanced and granular that a specific ad can be targeted at a single person only.

Even Gmail, the most trusted mode of communication by many, is not safe. Google employees have access to our emails to delete viruses and remove unsafe or violent emails. The only permission they need is a signed agreement clause from us when we create our account. The same is true for all other email services.

Our GPS is always tracking us. On selecting a destination on google maps and hitting go, even if the phone is put on Airplane mode, it will be seen that the blue dot moves with us. This proves that GPS communications are not turned off when the phone is put on airplane mode. People who are capturing our location with GPS will be able to collect our geo-location long after we have left that range.

Clearing the browsing history doesn't really delete it. Our browsing history is linked to our identity permanently, and is never private, even after going incognito. Pretty horrifying, isn't it? If our name is associated with our computer or installed apps, someone may retrieve information about those things as well as information about installed operating systems and applications. This means that a porn site can extract the user's first and last name, username, cookies, etc. When aiming for active offensive intelligence operations, this frequently occurs. Even though we might not be victims of an offensive attack, having our personal data being collected and sold for marketing and demographics feels invasive.

Ever had a conversation about **"something"** on or near your phone, and later seen an advertisement on Instagram about that same **"something"**?

Or, have you ever said a new singer's name around your Google or Alexa home assistant and then view that singer's song on your YouTube's suggestion? This is all because our devices are spying on us and harvesting every single detail.

So, what can we even do? Private browsing will stop the browser from storing history but our IP address is still visible. Avoiding the use of Facebook is pointless as it has a shadow profile on us anyway. We can use a VPN, but we'll definitely sign into something at some point which will tie us to the VPN, and we can only hope that our VPN doesn't keep logs.

It is quite a hopeless situation. We can't completely abstain from using our devices and apps, so there will always be some data being collected. However, now that there is some awareness, we need to be vigilant while browsing. Understand what you are against, and plan your moves meticulously. Don't get overwhelmed with the perennial data collection, instead take steps to keep your sensitive information private.

IMPACT OF COVID 19 PANDEMIC ON CYBER SECURITY

~Jotiraditya Bhosale

The Coronavirus pandemic has totally changed the working culture of industry. Due to the pandemic when many countries imposed lockdown and made strict norms for people, it was difficult to come out of the house and live a normal life. All industries, government offices, hospitals were closed for an uncertain period, and it created a huge impact on the world's economy. To tackle all these problems created due to Covid-19, companies started to adopt a new working model for their employees, the 'work from home'. Now it has become the new normal. Even after the pandemic is over, employees are choosing to work from home because of the comfort they are getting in this new working model.

But new trends always give rise to new concerns. Although work from home is comfortable, this digital transformation of companies is creating a new problem related to cybersecurity. From big companies like Google and Apple to companies like PepsiCo, Tata Steel and GE India, all are offering their employees work from home option but still many of them are not able to provide their employees a 'Cyber-safe' remote working environment.

Cybercrimes are taking place not only at industry level but also in our surroundings in many forms like:

- **Phishing** – Using a communication medium like a fake email ID to deceive a person into giving personal information.
- Identity Theft - Misusing personal information.
- **Hacking** – Gaining unauthorized access to a party's system.
- Spreading hate and inciting terrorism.
- Distributing child and revenge pornography.
- Body shaming or doxing someone on social media.

The government of India in one of the Lok Sabha sessions informed that till June 2022, total 6,74,021 cybercrimes have been reported according to data tracked by the Indian Computer Emergency Response Team. A total of 11,58,208 and 14,02,809 cybercrimes were reported in 2020 and 2021. Indian government issues alerts regarding the latest cyber threats and is going to operate an automated cyber threat exchange platform to proactively collect, analyse and share alerts with organizations across sectors for fast and effective threat mitigation actions.

While other IT jobs like software engineer, developers are common and well known, after the pandemic cybersecurity jobs are also increasing in number and importance. As the global economy has led to more internet-based computing and connectivity, organizations are now even more vulnerable to cyber-attacks. According to the Data Security Council of India, in 2020, cybersecurity businesses employed around 1.30-2 lakh workers in India. The cybersecurity market is estimated to hire around 10 lakh professionals by 2025.

WHATSAPP
ARE YOUR CHATS PRIVATE?

~Kaushal Agarwal

WhatsApp is a messaging app used by many people to communicate with each other. It is a very simple and effective application to text or send media or documents to someone. But there is always a dark side to everything. WhatsApp is owned by Meta, earlier known as Facebook. Meta is very infamous for its handling of user data and privacy. But first, let us go deep into understanding how WhatsApp keeps our messages private according to the company's official policy.

WhatsApp's biggest highlight of user data protection is E2E Encryption which basically means End to End Encryption. According to them all the messages sent via WhatsApp are encrypted. Once a sender sends a message, it is encrypted for everyone else except the receiver who has the key to unlock the message. They claim no third party can read the messages, even WhatsApp or its parent company Meta cannot read it.

Before a message even leaves the user's device, it's secured with a cryptographic lock, and only the recipient has the keys. The keys change after every single message. Chats between sender and receiver have their own security code which is used to verify that the calls and messages one sends are end-to-end encrypted. Security codes are just visible versions of the special keys and not the actual keys themselves, they're always kept secret.

The sender client creates a pairwise encrypted session with each of the recipient devices in order to enable users of WhatsApp to interact securely and confidentially. The initiator begins to establish the encryption session with each individual device after receiving the keys from the server and authenticating each device's identity.

- The initiator saves the recipient's Identity Key, Signed Pre Key, and One-Time Pre Key as Irecipient, Srecipient, and Orecipient respectively.
- An ephemeral Curve25519 key pair called Einitiator is generated by the initiator.
- The initiator loads its own Identity Key as Iinitiator.
- The initiator calculates a master secret by :

master_secret = ECDH(Iinitiator, Srecipient) || ECDH(Einitiator, Irecipient) || ECDH(Einitiator, Srecipient) || ECDH(Einitiator, Orecipient).

The final ECDH is omitted, if there is no One Time Pre Key.

- The initiator uses HKDF to compute a Root Key and Chain Keys from the master_secret.

Following the establishment of a session, clients communicate by exchanging messages that are encrypted with AES256 in CBC mode and authenticated with HMAC-SHA256. For all messages transmitted, the client uses client-fanout, which encrypts each message for each device with the corresponding pairwise session.

The Message Key is ephemeral and changes for every message sent, making it impossible to recreate the Message Key used to encrypt a message from the session state after a message has been sent or received. The Message Key is derived from the sender's Chain Key which "ratchets" forward with every message transmitted. Each message roundtrip also results in the performance of a new ECDH agreement, which produces a new Chain Key.

Whenever a new Message Key is needed by a message sender, it is calculated as:

1. Message Key = HMAC-SHA256(Chain Key, 0x01).
2. The Chain Key is then updated as Chain Key = HMAC-SHA256(Chain Key, 0x02).

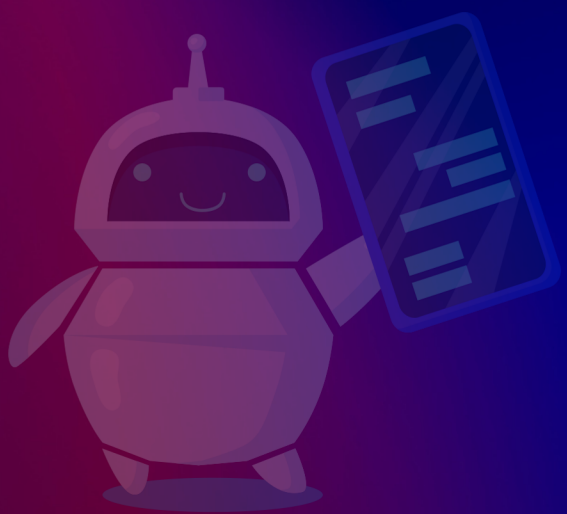
An ephemeral Curve25519 public key is advertised along with each message that is sent. A new Chain Key and Root Key are computed once a response is received as:

1. ephemeral_secret = ECDH(Ephemeralsender,Ephemeralrecipient).
2. Chain Key, Root Key = HKDF(Root Key, ephemeral_secret).

Even after all this complex encryption, news of WhatsApp chats getting leaked is still heard. How does this happen? If the chats are encrypted and secure and no third party can access it, still somehow or the other user data is getting leaked. Mostly it was due to a loophole in WhatsApp's backup policy.

All E2E encrypted chats can be backed up to third party applications like iCloud or Google Drive. These backups were not encrypted or protected under E2E policy. So, an attacker can try to attack user's cloud storage to get the user data. But WhatsApp has now given the user the choice to encrypt the backup data. This is kept OFF by default but user can turn it on by going to Settings>Chats>Chat Backup>End-to-end Encrypted backup and then turning it ON. WhatsApp is also introducing some new features over time to make chats more private between users. They have recently added the option to send photos for one time view only. Users are now also given the option to open the app using their fingerprint or Face ID in case their device is in wrong hands. Also, two step verification has been introduced while signing up on a new device.

With all this said, it is better to not share sensitive information via WhatsApp and always practice caution while on internet. Remember, your data is very precious to these companies.
"Once you lose your privacy you realise you have lost an extremely valuable thing."



SCAM ALERT!

~Vaibhav Walunj

Cybercrime is a criminal activity that attacks on systems, networks, and information and its aim is to compromise their confidentiality which is one of the major security goals. In simple words, we can say that cybercrime means to interfere with or to hamper someone's privacy or secrecy knowingly or unknowingly. Due to cybercrime, an individual or an organization can lose their confidential information or data which can affect them a lot in terms of finance and reputation. In India, almost 65% of the population has mobile phones which is expected to increase in upcoming years, but they don't have adequate knowledge about the threats or vulnerability of the smartphone they are using. Due to this, cyber criminals take advantage and steal confidential data which can be their personal information or their financial information that is available on their mobile phones.

According to the cybercrime portal of India, due to an exponential increase in smartphone users in India cybercrime is also expected to increase further. Some of the major cyberattacks that take place in India are email fraud, social media fraud, banking fraud, ransomware attacks, etc. Have you ever got a call from your bank seeking your debit card details? It is most likely that the call is from Jamtara.

Jamtara is a district in Jharkhand which is known as the "phishing capital of India." It is infamous for OTP frauds, looting a huge amount from credulous people, followed by frauds in credit and debit cards, KBC, and lottery frauds among others. The most common fraud is OTP fraud where the scammer offers to update KYC details of the person by asking them for their card details, CVV, and the OTP they receive on their mobile phone. The victim ends up losing a large sum of money.

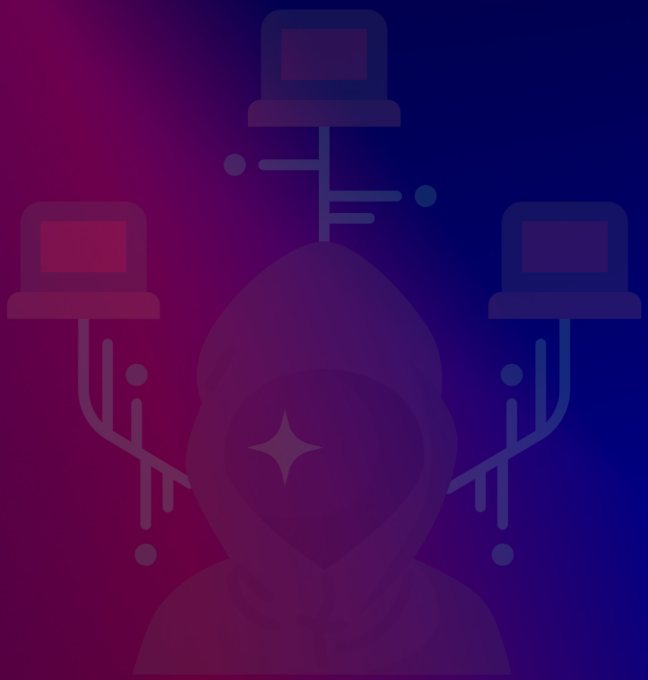
One of the latest scams that took place in Jamtara was the KBC scam where they would send an image or a video on WhatsApp claiming that they have won a large amount of money but to claim that money they first need to pay 5- 10% as tax, and without thinking twice people fall into the trap and end up losing money. The situation in Jamtara is such that the youngsters are taught different languages for doing such frauds. They have taken these frauds as their job which they do daily. They neither regret their actions nor consider this as a crime. A web series has also been made on this named Jamtara which is available on Netflix.

As the 5G industry is blooming in India, a new scam has been started in which the phisher offers 5G SIM upgradation to the customers. Scammers have been posing as customer service representatives from reputable telecom service providers, promising clients assistance in upgrading their SIM cards.

Their strategy is to send phishing links to victims to compel them into providing personal and

financial information. When customers are trapped by these scammers, they share their personal information and thus compromise their confidentiality. Not only is their confidentiality compromised but they also they lose their integrity which can be done by modification and masquerading of the data. Majority of the attacks on systems and the data stored therein are crimes committed for financial gain. These crimes may manifest themselves in a disruption to a particular financial service or a violation of the confidentiality, integrity, or availability of financial data.

To conclude we can say that “touch your phone like you are touching a live wire.” Because if you click at the wrong place, you may end up losing a lot of your personal and financial information. The biggest reason for a large number of these scams is human greed, the entire Indian attitude of getting more for less, and so on. These cyber criminals do not have the brightest minds, but they have realized how to defraud others. Now, you can also report any financial cyber fraud to the helpline number- 1930. Hence, you must report your financial fraud regardless of how small the amount is. Beware of such scams and frauds and never disclose your personal and financial information to any unauthorized person.



METAVERSE OR METACURSE?

~Sharez Shaikh

In the novel "Snow Crash" released in 1992, Neal Stephenson gave everyone the idea of a futuristic world that everyone demanded for. Many innovations took place from then, trying to mimic this master plan by Neal. On October 28, 2021, Mark Zuckerberg emphasized his vision by launching Facebook's metaverse and also rebranding it to **"Meta"**. This got people excited as the term Metaverse portrayed the imagination of Neal Stephenson. But this metaverse isn't what Neal thought about.

It is said that **"The more data you put online, the bigger digital footprint you have, so you end up with more risks"**. Everything that is free on the internet isn't actually free! Such organizations make money by collecting users' data and selling it to third-party clients. This huge amount of data is available for these clients to exploit, making it a vulnerability for the users whose data was collected. Since the metaverse is going to be so vast, way beyond our imaginary boundaries, it will not be possible for a single organization to manage and moderate this world. This is where third-party companies come into the picture. They will have access to the metaverse and ultimately, the users' data. It will be up to the organization and third-party companies how they want to collect and use the data.

Every time we think that we have reached the peak of privacy invasion, a new challenge emerges.

Stepping into the metaverse requires some accessories like AR - VR headset and VR gloves. These gears collect users' biometric data to ensure that the user-experience is as per their expectations. As the metaverse continues to evolve, there might be a possibility that IoT devices may be used for a better experience, resulting in the collection of even more data by companies and organizations. By using these devices, users get a stimulating experience in exchange for their biometrics and daily routine. Fair trade, isn't it?

Metaverse will play an important role in encouraging cybercrimes. Evolution of technology always creates a loophole for attackers to exploit. It is expected to witness new forms of phishing, deepfakes, crypto, and NFT scams. The greed of Bitcoin drowned many people who logged in with their credentials and lost everything. India itself witnessed more than 18 million cyberattacks within the first quarter of 2022 and more than 5% of it was due to phishing attacks. Imagine getting routed to an attacker's vault which is the exact same replica of your world and depositing your credentials in his database. That's it, you've been phished! A typing mistake may cost you everything you have in your virtual world. Influencers are significant in spreading information to a large group of people. Most of the attackers target these official channels to share scam links or malware with innocent people who trust these official channels.

Not even Twitter was able to protect its official handle and a crypto wallet address was shared by attackers asking for donations. If no one is safe in this world where everything is stable and running smoothly, how can we ensure safety in the metaverse?

It is less fascinating and more sobering that technology collides head-on with morals and ethics. Before gearing up with our virtual goggles and jumping with both of our virtual feet into the **“metacurse”**, it is worth considering the risks. We are the youth and we have the power to decide what is good for the people and the broader world, rather than being a script kiddie and connecting to a device that will make it all happen.

DATA BREACH

HOW VULNERABLE IS YOUR DATA?

~Anushka Behere

Website hacked! Millions of data leaked! It seems like we hear about a new data breach daily. So, what does it mean? Speaking in laymen's terms, a data breach happens when sensitive data falls into the hands of someone who has no business handling it. So, if a hacker extracts your credit card information, it's a breach. However, the leak of data can also be unintentional. Like if you forget your USB drive in a coffee shop and someone finds it and sees your photos - it's a data breach.

Whenever you enter your personal information such as your passwords or credit card details on a website, is there a feeling of hesitation? Fear of getting exposed is due to thousands of headlines about data breaches. Even then, you probably push those feelings deep down and hit that submit button, because, well, you need to shop, apply for that loan, file a complaint, or do any sensitive activity that happens on the internet.

Usually, we hear about breaches when a company fails to keep its data secure. Unsurprisingly, it causes more trouble for us. This is because we leave a lot of information online like where we live, what we like, how much we earn, and what we buy. This data is precious to any company. That's why various websites and apps collect it, making hackers' lives much easier. Now, in one single attack, they can steal an enormous amount of data.

If you regularly enter your personal information online, there are chances that your data could have been stolen at some point. On May 22, 2021, it was revealed that Dominos India, a division of Jubilant FoodWorks, had experienced a cyberattack and that order information, contact information, and credit card information for 18 crore orders had been exposed on the dark web.

For some good news, not all breaches are the same. There are steps you can take to protect yourself. Below listed are some threats to your online data, what cybercriminals do with your stolen data, and what you can do about it.

- Think carefully about the risk you will be taking

Not all personal data is the same. For example, if the stolen data was your shopping history, maybe that won't harm you but if it was your credit card details then it's a different story. So, give out only that information which, even if leaked, will not be harmful.

- Market of your stolen data

Hackers generally don't use the stolen data themselves. Instead, they sell it on the infamous dark web for other criminals to use. For example, a stolen PayPal account goes for $30. According to Ravi Sen, an associate professor of information and operations management at Texas A&M University, stolen credit card numbers and security codes can be used to create clone cardsfor making fraudulent transactions.

- Don’t make it easy for thieves

Besides using strong passwords, encryption, VPN, and avoiding malware, you have to be stingy with your personal data. If you use a free service then it’s probably not free—you’re just paying for it in another way. If it’s not worth, do not use it and stay safe!

ENCIPHER TO DECIPHER

~Shivam Mishra

For starters, you don't need to know what cipher, encipher, and decipher is. Now let's focus on the story. Every one of us can relate to this, and if not then today is the day to do so.

Let us consider a case where, a teacher conducted a class test and the test grades possible were A, B, C, F, where A is the best and F is for fail. You managed to score a good grade B but your brother failed the test and got F.

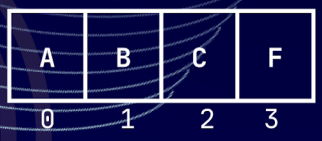
You made a deal with your brother that, if your father asks what your grades are in the test then you will say that we both got B.

At this point, you must be thinking how this story is connected to encipher or decipher, but it's directly connected. Now let's understand some terminology used in the above analogy.

Plaintext: The original message. In our analogy, it was the brother's grade F.
Cipher: Algorithm to convert plaintext into ciphertext.
Ciphertext: Plaintext is transformed into some other text using an algorithm. In our analogy ciphertext was the grade of the brother that you told your father and i.e, B.
Key: Mutually decided value for encryption and decryption, used in cipher. In analogy, the key was '2'.
Encipher: Conversion of plaintext into ciphertext.
Decipher: Conversion of ciphertext into plaintext.

In analogy you converted plain text B into cipher text F by using key 2. Grades were A, B, C, F. Initialize values of A=0, B=1, C=2, F=3 and key=2. To encipher or decipher we use an important concept called circular increment, but here the question arises why circular and not linear?

Linear VS Circular Increment
Consider below array of grades and marking the index of array from 0 to 3.



I can access this array using its index value.

Suppose we have the index value 0 which is for grade A and we want to encipher it using key 2, so we will add 2 in 0 (index of A).
CT = 0+2= 2 where CT=ciphertext
We can see 2 is the index of grade C. Plaintext is A its ciphertext is C. It's correct, no problem, but what if plaint text was F (index=3)?
CT= 3+2= 5
In array there is nothing with index 5 so it's not enciphered.
Here, increment of index goes: 0,1,2,3,4,5,6,7,8,9,10…
Now, consider the same array with same index values as above but let's change the representation.

Here, increment of index goes: 0,1,2,3, 0,1,2,3, 0,1,2,3…

We can observe that when the index of the last element is incremented it again restarts the array. If we add 1 in index value 3 then it gives 0. To make this possible we use the modulus operator (%). Here, the size of the array is 4 since it contains 4 elements.

Formula for encipher: Index of CT = (index of PT + KEY) % (size of array)
Procedure: F with key = 2, where F is plaintext.
Index value of F = 3, Key = 2.
Index of CT = (3+2) % (4)
= 5 % 4
= 1
We got the index value of CT as 1. In array, you can see 1 is the index of element B, so grade F is enciphered to grade B.
Plaintext = F, Ciphertext = B, when key =2.

Formula for decipher: Index of PT = (index of CT - KEY) % (size of array)
Procedure: B with key = 2.
Index value of B = 1, key = 2
Index of PT = (1-2) % 4
= -1 % 4
= -1
Since the answer can't be negative, we will add the size of the array in it.
Index of PT = (-1+4) = 3
3 is the index of element F.
Ciphertext = B, Plaintext = F, when key =2.

Here the cipher method we learned was Additive cipher or shift cipher or Caesar cipher. It is the simplest mono-alphabetic cipher. Since this cipher uses single key, it comes under symmetric key cipher. There are different types of ciphers.

In this article we have learned cipher, encipher, decipher, additive cipher, difference in linear and circular increment. This circular increment concept is also used in DSA topic called circular queue. At end we learned algorithm to encipher and decipher using additive cipher.

KEEP IT CONFIDENTIAL

~Stuti Soni

An organization's efforts to ensure the security of the user's data or its secret data is guided by the CIA Triad. Cybersecurity is based on three principles: confidentiality, integrity, and availability. These principles are important in running a business since they form the basis of a security framework.

The triad can be used to analyse the security procedures of any business.
The main aim of security is to give authorized users access to control the data and prevent unauthorized activities from taking place, thus maintaining confidentiality. For example, in the employee salary database, the information of all employees is stored but only a few authorized employees can access this database. In addition, the information shown to this particular group is not the same for everyone and further restrictions may be placed on the information shown.
Compromise in confidentiality can be seen in many ways.

The following are some common threats:

- Hackers
- Masquerades
- Unauthorized user activity
- Unprotected downloaded files
- Local area networks (LANs)
- Trojan Horses

Some of the day-to-day activities like registering ourselves with the car insurance company or the mobile billing company can be proven to be a useful asset to the companies for scamming us.

Multiple small gangs are backed by an insidious web of bank accounts, digital wallets, and mobile phone SIM cards that have been opened using fraudulent KYC paperwork. These accounts also identify game-changing trends early in the country's future criminality. As per Ish Kumar, director of the NCRB, " the total number of cybercrimes is less than 0.1% of the total IPC (Inter-Process Communication) and SSL (SSL stands for Secure Sockets Layer. SSL is Netscape's protocol for creating an encrypted connection between a web server and a web browser) incidents in a year (in India), criminals are using mobile phones for communication in 30-35% of all crimes."

Jamtara is a locality where cybercrime is at its worst. The majority of phishing fraud occurrences involve phone calls, and the information obtained comes from the provider of the SIM cards or is being purchased by scammers. The fight against cybercriminals and Jharkhand's efforts to dispel the perception that it is the home of India's cybercrime capital is being led by a cyber cell established in Jamtara in the beginning of 2019.
Initial results look encouraging, with local police saying crimes have halved, but can they stop the threat altogether? All of this raise questions about the privacy protection of data collected from users.

All this data is being used somewhere without the user's knowledge, which can be seen as a big threat to them.

To counter this problem the industry uses some models to protect confidentiality. The usage of security techniques to achieve the appropriate level of confidentiality can be outlined in these models. The Bell-LaPadula model is the one that is most frequently used to explain how secrecy is enforced. In this model,

- There is a distinct relationship between objects (i.e., the equipment that contains or receives information) and subjects (i.e., the person, processes, or devices that cause the information to flow between the objects).
- The relationships are described in terms of the subject's assigned level of access or privilege and the object's level of sensitivity.

The access control model is yet another popular model type:

- It organizes the system into objects (i.e., resources being acted on), subjects (i.e., the person or program doing the action), and operations (i.e., the process of interaction).
- A set of rules are set over here and according to that further process is done.

Ways to Put Confidentiality into Practice for an Organization:

- Categorize data and assets being handled based on their privacy requirements.
- Ensure data encryption and two-factor authentication are basic security protocols.
- Ensure that access control lists, and file permissions are monitored and updated regularly.
- Train employees about privacy considerations both at a generic organization-wide level and as per the nature of their role.

In essence, cyber law is designed to supervise human activities on the internet. In India, The IT Act, 2000 as amended by The IT (Amendment) Act, 2008 is known as Cyberlaw. So, in the future, one should be aware of scam calls and think twice before sending information like OTPs or Aadhar card numbers to strangers or suspicious people.

DATA FRAUD

~Saad Khan

We all are unsafe in a way that we might feel oblivious or unbothered about. Data privacy is of serious concern today. People only take this seriously to the extent of having a conversation about it. They like to discuss about various companies stealing their data and they can't do anything to stop this. Everyone is guilty of doing this and it is the ugly truth. But, to be honest, there isn't much that a normal consumer can do about it except playing the role of a victim. If you ask about this issue then a general consumer will probably respond by saying that the whole world uses these applications or that they're not that great a deal to let these huge companies spy on them. But due to these mishaps, a great deal of new threats are advancing in the cyber world. India alone saw crime rates increasing by 10 folds in the past couple of years.

Our data can be used in several fascinating yet dangerous ways that might be difficult for our brain to comprehend. The purpose of this article is not to scare you but to enlighten you about the vulnerabilities in your personal life that can be catastrophic if exploited. There is no complete way to prevent this but we do have some informational tips that will help lower the risk. One way to protect yourself from data breach is to avoid putting your personal data on an unknown or unprotected website. This ultimately protects you from befalling victim to any scam that includes data breach.

A good practice would be to use applications that are fully transparent about their policies or even open source.

Your browsing might be the parasite that you were afraid of all along. In order to prevent your browser from stealing your data you can use a VPN to visit informative sites. Your data might be stolen from you and used against you in such a way that will be difficult to tell. We know about the increase in number of cyber-attacks or scams that are going on in the country, few ways that you may get scammed are:

- The scammer may ask you for your bank details. This is a well-known scam but it can be very convincing at some point.
- Giving threats about terminating electricity supply. This is a new type of scam which is self-explanatory.
- Posing as an online shopping platform to extort money.

The list goes on and on and on, but these were few scams that are increasing drastically. Stay alert and spread awareness about these malpractices.

FACULTY ARTICLES

FACULTY ARTICLES

1. Securing Digital Payments
2. Cloud Encryption in Cybersecurity
3. Data Privacy in Cybersecurity

SECURING DIGITAL PAYMENTS

~Dr Vidyadhari R Singh

Digital Payments have seen a drastic change in India at a much faster pace as compared to markets across the globe. The pandemic has surged the usage of digital payments. The electronic payments are expanding very fast. Payments are becoming increasingly cashless. The main challenge is to safeguard these payment systems. It has become extremely important to secure these payment transactions as there has been a rise in the number of Digital frauds related to the Digital Payments. Digital fraud is when cybercriminals use emails, websites and malicious software to gather personal details and trick you into paying them.

As per the Reports by The Hindu, it has been said that: "The e-commerce market in India is expected to grow to $200 billion by 2026 from $50 billion in 2018. UPI transactions in India have crossed 149 crore in volume and $41 billion in transaction value, in July 2022." The Reserve Bank of India (RBI) has predicted the number of digital transactions to increase to 4 times by the end of this year. There has also been an increase in Debit and Credit cards issued in India, which is second in this across the globe.

Indians consider digital payments as secure as traditional payments because from a regulatory perspective, there is a lesser risk of money (in cash) being lost or stolen and digital payment platforms are encrypted for better security. Fraud detection is also easier since transaction history can be checked in no time.

A report states that the top concerns Indians face while making digital payments are vulnerability to fraud (54 per cent) followed by risk of failed transactions (42 per cent). This validates the need for increased financial literacy- to help consumers protect themselves as we move into an increasingly digital world.

Security is paramount. Digital payments are not only authorized but they must be authenticated as well. A strong customer authentication, from a regulatory perspective, using two or more factors should be adopted around the globe. Many frauds have been reported like phishing attacks, frauds using online sales platforms, frauds due to the use of unknown/unverified mobile apps, frauds compromising credentials, impersonation on social media, etc.

The key challenge is to safeguard from these frauds and many more which are excessively prevailing day by day. Future fraud possibilities include exploiting the risk transfer controls and spoofing the current prevention mechanisms. Therefore, it is required to make people aware of these frauds from time to time using various platforms to build a secure digital payment ecosystem. The upcoming technologies like AI/ML, Computer Vision, Natural Language Processing are potential rescuers for stakeholders involved to build a secure digital platform.

CLOUD ENCRYPTION IN CYBERSECURITY

~Ms Ditixa Mehta

When a user stores data on a cloud, he doesn't have control over that data and this is a big challenge in data security. Cloud storage is not only used to store, access, and manage the data but it is also used for cost reduction and easy management of various organizations. In today's era of Internet of Things (IoT), a large volume of data is generated and needs to be stored on the cloud. In IoT, smart devices and sensors generate the data which is transmitted to the clouds.

Encryption as a Service (EaaS) can be accessed by cloud entities based on their data rights. EaaS also provides encryption on the cloud.

Because of the encryption method, the information is unreadable to everyone except the ones who are authorized users for decryption. EaaS also plays an important role in end-to-end security to provide data transmission to authorized clouds and restrictive access from the third-parties. EaaS or Encryption-as-a-Service obstructs cyber criminals or any unauthorized party from stealing or snooping information like the unencrypted passwords on the portal sent over WANs to collect information.

Meeting Regulatory Compliance In addition to traditional physical security, authentication, and authorization methods, various customized cryptographic techniques are used in EaaS such as:

- Identity-based encryption
- Attribute-based encryption
- Homomorphic and searchable encryption
- Isolation of encryption and decryption
- Combination of symmetric and asymmetric algorithms

Benefits of EaaS

- EaaS reduces the cost of maintenance and support for certain applications.
- It results in more efficient use of resources by minimizing underutilized tools.
- Project cycle time is lower, resulting in software features becoming available earlier.
- Access to the final product is ready sooner, giving consumers a better perception of your application.
- It gives you more flexibility in making future changes to your application.

EaaS Applications

- All-time security assurance
- Shield sensitive information
- Meeting Regulatory Compliance
- 24/7 devoted crypto experts and techniques
- Appropriate tools and resources

The main challenge in EaaS is to generate and manage the key. Because of the data in the central location, the symmetric method to generate the key is not feasible. If one of the users loses the symmetric key, unauthorized users can access the data on the cloud. So, there is a need for a scalable asymmetric key management solution for an IoT-based cloud storage setting, where the keys are bound to the identity of entities.

DATA PRIVACY

~Ms Kiran Babar

Data privacy is associated with the proper handling of personal data or personally identifiable information (PII), such as names, addresses, social security numbers and credit card numbers. The main idea is the protection of valuable or confidential data, including financial data, intellectual property and personal health information. All sensitive information that businesses handle, including that of their clients, shareholders, and staff, is primarily the focus of data privacy. This data is essential for the development, management, and finances of businesses. Data privacy enables the restriction of access to sensitive information to authorized parties. It shields data from malicious use by thieves and aids in making sure enterprises abide by legal standards.

Cloud computing has now emerged as a way of storing data on a virtual computer that is used for running processes like software over the internet and cloud storage as a virtual hard drive for storing files on servers to make it accessible over the internet. This is one of the reasons why cyber security and data protection should be prioritized.

The most essential cyber security measures for data protection are as follows:

- **Use Strong passwords:** Strong passwords work well for online security. Make your password difficult to guess.
- **Control access to data and systems:** The individuals can only access data and services for which they are authorized.

Controls on physical access to buildings and computer networks, limitations on access for unauthorized users, restrictions on access to data or services through application controls, limitations on what can be copied from the system and saved to storage devices, and restrictions on the sending and receiving of specific types of email attachments should all be in place.

Install a firewall: A firewall serves as a barrier between your computer and the internet. They serve as a barrier to stop the spread of malware and other cyber threats. Firewall devices must be configured correctly, and their software and firmware must be kept up to date for them to be fully functional.

Use security software: Make use of security software. If dangerous code infiltrates your network, we should utilize security software such as anti-spyware, anti-malware, and anti-virus products to help discover and remove it.

Monitor for intrusion: Intrusion detectors should be used to keep an eye out for suspicious network behavior and systems.

- Based on the sort of behavior it has detected, a detection system that detects a potential security breach may generate an alarm, , such as an email alert.

- **Regularly update systems and programs:** Because our systems or software aren't completely up to date, there exist vulnerabilities that allow for cyber attacks.

As a result, it makes sense to spend money on a patch management system that will oversee all software and system upgrades and maintain your system secure and current. People will depend on enterprises that efficiently use cybersecurity for privacy of data as they become more reliant on it.

Data encryption involves encoding information, often known as cipher text, from raw data. Only a specific decryption key can be used to unlock the encrypted data. The key can be created either before or during encryption. Data integrity is ensured through encryption, which prevents unauthorized changes to the information. By confirming the origins of the material, encryption lowers the risk of accessing it from such sources.

Building awareness and promoting ethical data collecting, privacy, and protection methods are the goals. Data privacy is important because people who want to exist online need to believe that their information is being treated appropriately. The Data Privacy Act safeguards people from the illegal handling of private, non-public personal information.

INDUSTRIAL SECTION

Industrial Visit

INTELLINBLOCK TECHNOLOGIES, ANDHERI, MUMBAI

Intelliblock Technologies is an India-based blockchain start-up company. It is a team of brilliant people with more than 300 man years of IT technology experience. Their solutions covered major blockchain protocols like Ethereum, Hyperledger, Solana, Polygon, BSC, Polkadot, and many more. They are up to date with the latest market technologies and bespoke solutions and other customized solutions best suited for an esteemed organization.

Neha Jain ma'am introduced herself as the founder and CEO of the company. Then she stated her company's goal which is to become the best in blockchain industry, expand themselves globally, and make blockchain technology simpler for everyone. Then she told us about their company's achievements. They have 5+ domestic and international clients, 20+ projects in blockchain, and 6+ international collaborations. She also explained the services that her company provides.

Later on, she explained about various categories in blockchain development services like - Private Blockchain Development, POC Development, Smart Contract Audit, DApp Development, Blockchain Payment Remittance Blockchain, Consulting Blockchain, and many more. She also mentioned that cryptocurrency services and metaverse are two major branches that are growing rapidly and can provide many opportunities for engineers like us. Crimes not only happen in real life but have also started in the metaverse and she explained about a recent case that happened in metaverse.

Overall, it was a very informative and knowledgeable experience. We were able to understand our field more and learned about the basic requirements that one should have to survive in the software world.

Industrial Visit

APAAR INFOSYSTEMS, MAHAPE, NAVI MUMBAI

Apaar Infosystems is an India based technology solutions consulting company. It is a talented group of individuals having over 25-man years of experience in IT technology domains like Big Data, Analytics, Robotics, Artificial Intelligence & Advisory services. They are up to date with latest market technologies and bespoke solutions and other customized solutions best suited for any esteemed organization.

Firstly, Mr. Nilesh Shinde, the founder and CEO, introduced us to Apaar Infosystems, their mission, vision, and objectives. He briefly discussed the methodologies which are used more nowadays to keep our data and system updated and secured.

Further, he discussed more about Software Development Life Cycle (SDLC). He started explaining the two methods which are used in the system development life cycle. These are - Waterfall Model and Agile Methodologies.

Agile methodologies are practiced more since agile encourages the team to work simultaneously on different phases of the project and produces highest quality product within the constraints of the budget.

Later on, he switched to the cyber security part in which he discussed the meaning of cybersecurity and what is the need, and how the demand for cyber security is going to increase in the future. Lastly, he concluded the presentation by saying that cyber security is one of the most important aspects of the fast-paced growing digital world but at the same time threats are hard to deny, so it is crucial to learn how to defend ourselves and others too.

Overall, the session was very informative and knowledgeable and every one of us enjoyed and learned new terms and things related to the software and cybersecurity.

Interview

Rashmin Shinde,
Sr. Technical Lead,
Apaar Infosystems

Q: What was your company's most challenging project?
A: The most challenging project that we worked on recently is MunichRe integration.

Q: What are the challenges or risks associated with IoT?
A: Below listed are few of challenges that IoT has:

- Software and firmware vulnerabilities
- Insecure communications
- Data leaks from IoT systems
- Malware risks
- Cyber attacks

Q: How do you think IoT will contribute to the field of cybersecurity?
A: IoT security refers to the methods of protection used to secure internet-connected or network-based devices. IoT security is the family of techniques, strategies and tools used to protect these devices from becoming compromised. Ironically, it is the connectivity inherent to IoT that makes these devices increasingly vulnerable to cyber attacks.

Q: What are the activities involved in the security testing of IoT products?
A: The checklist should include:

- Test your software for common vulnerabilities
- Remove all unnecessary services and components from your software/app
- Include only required & well known third-party libraries in your software
- Monitor these libraries for known vulnerabilities
- Periodically update your software once it has been shipped

Q: Managing data is a challenging task, how do you manage data efficiently?
A: Follow below outlined best practices to manage the data efficiently:

- Prioritize data protection and security
- Focus on data quality
- Reduce duplicate data
- Ensure your data is readily accessible to authorized users only
- Create a data recovery strategy
- Use a quality data management software

Interview

Q: What will be some tips you will give to students who are new to data management and cyber security?
A: Major Cyber Security Tips:

- Learn About Phishing Attacks
- Set up Two-factor or Multi-factor Authentication (MFA)
- Use Firewalls and Anti-viruses
- Make Your Data Backup Regularly
- Secure Your Data
- Don't Use Public WiFi without a VPN
- Check CERT-In Updates on a Regular Basis.
- Keep Your Systems Updated
- Use Strong and Varied Passwords
- Use a Password Manager Tool
- Avoid Unfamiliar Websites
- Stay Cautious on Social Media

Q: During the pandemic when companies switched to a work from home model, how challenging was it to provide cloud services tailored to their respective needs?
A: It was very challenging as we had to bridge the skill gaps. There were concerns around security. Initially there was hesitancy in cloud adoption. Despite the challenges for which organizations are finding comprehensive solutions, cloud services offer a goldmine of opportunity for every industry.

Q: What suggestions would you give to second-year students to get started with app development?
A: The app should have a well designed UI-UX. The flow of the app should allow the user to comfortably move from feature to feature and make transactions as required for the course material.
Incorporate Security and Trustworthiness at the Outset. There should not be any compromise on security and authorization.
It's always better to use latest technologies for App Development. Thoughtful, Timely Notifications are Essential.

ACKNOWLEDGMENTS

"Self believe and hard work always earn us success."

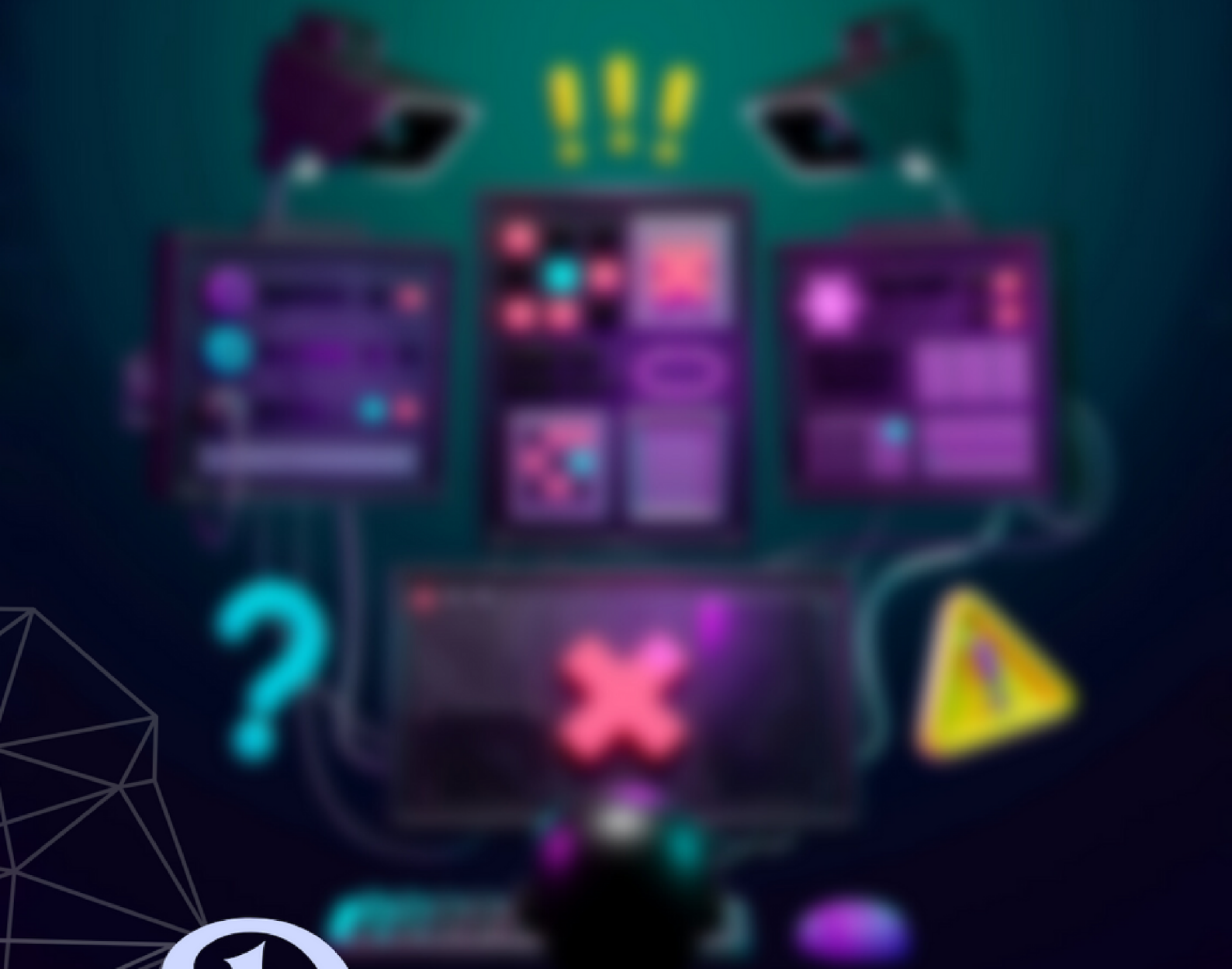
Our team has worked with great enthusiasm and dedication to put up this debut magazine. We would like to express heartfelt gratitude to the Principal Dr. B.K. Mishra and the Vice-Principal Dr. Kamal Shah.

We are extremely grateful to our HOD Dr. Vidyadhari Singh and Faculty In-charge Ms. Ditixa Mehta for giving us this opportunity and being our pillars of support. Thank you for guiding us from concept to completion.

Estd. in 2001

SECURE tcet CSE ENGINEERS

VOLUME 1 EDITION 2 COMING SOON.....



DECYPHER