Volume 11, Issue 2, February – 2026 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb739

Understanding Cyber Threats Through Human Behavior, Artificial Intelligence, and Cloud Security

Prajakta Vilas Thakar[1]

[1]PDEA Mamasaheb Mohol College

Publication Date: 2026/02/26

Abstract: Staying safe online isn't just a good idea these days—it's essential. We live our lives on the internet, using smart devices and cloud services for just about everything. Sure, that makes things faster and easier, but it also brings big risks. Hacking, stolen data, and scams are everywhere.

This study digs into how cyber protection has evolved and why it's so important for both businesses and personal privacy. Surprisingly, the biggest factor isn't the tech itself—it's us. People keep making the same mistakes. Even with all the warnings, folks still reuse passwords or skip two-factor authentication. We want to believe technology can save us, but honestly, our habits need to change first.

Behind the curtain, artificial intelligence spots threats quicker than ever. These systems are powerful, especially when companies lock down their cloud setups. But old security rules just can't keep up with new threats. That's why "zero trust" security isn't just a buzzword anymore—it's a real approach, where nobody gets a free pass and every login is questioned.

Keywords: *Cyber Threats, Data Protection, Artificial Intelligence, Network Security, Digital Forensics, Privacy, Zero Trust.*

How to Cite: Prajakta Vilas Thakar (2026) Understanding Cyber Threats Through Human Behavior, Artificial Intelligence, and Cloud Security. *International Journal of Innovative Science and Research Technology*, 11(2), 1595-1600. https://doi.org/10.38124/ijisrt/26feb739

I. INTRODUCTION

Tech's everywhere now. It's in your conversations, your bank account, your doctor's office, even how your city works. Pretty much everything runs through a screen or a wire these days, and yeah, it saves time and effort. But tucked inside all that convenience, there's trouble brewing. Information flies around so quickly, and that just makes it easier for hackers to sneak in—stealing data, messing with your identity, setting up scams. That's why protecting computer networks isn't just important—it's urgent. If you don't lock things down, you risk losing more than just a few files. No one's safe. Doesn't matter if you're a huge company, a corner shop, a school, or just a regular person minding your own business—anyone can get hit. Hackers keep getting smarter, and their tools do too. Machines are helping them pull off attacks faster than ever. When threats spread this fast, it makes sense to work together and find defences that are quick and easy to use. So, what's this study actually doing? It boils down to a few clear goals, each one tied to a bigger plan. Everything here is driven by purpose—looking to figure out what happens when technology races ahead of our ability to protect it. Security isn't one-size-fits-all; it keeps shifting as new online threats pop up. We used to rely on locked doors, now we need firewalls. But as soon as we patch one hole, another opens up. It's a never-ending game of catch-up, and staying safe means always being alert—especially in the places nobody's watching. First, the study digs into the most common types of cyber threats and how they hit users. Then, it looks at how new tech—like artificial intelligence and blockchain—are changing the game. These tools don't just keep up with attacks, they're starting to learn, adapt, and hold the line in new ways. Next, it's about the real-life challenges people and organizations face trying to keep their info safe. It's not just about fancy software; it's about habits, choices, and sometimes just plain bad luck. Every layer of protection adds more questions, and the pressure just keeps building until something finally cracks. And last, the study offers up some solid ways to build stronger cyber defences—and points toward where things need to go next.

II. LITERATURE REVIEW

Computers have changed everything, but with all that power comes the job of protecting digital spaces—networks, devices, information, all of it—from online threats. Anderson nailed it back in 2020: the heart of cybersecurity is keeping secrets safe, data solid, and services running. But it's not just

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb739

about fancy code or firewalls. The real defence comes down to rules, routines, and the choices people make every day. When folks stay sharp, keep learning, and actually care about what they're doing, defences get a whole lot stronger. In the end, security isn't just a tech thing—it's everyone's job.

Still, people skip the basics all the time, even when the instructions are right in front of them. This research found three big reasons for that, all tied to how people deal with security rules. One problem comes from daily habits, another pops up when things get stressful, and the last one shows up during the boring, routine stuff.

Take passwords. Most people use the same one for everything. They know they shouldn't, but only a handful ever bother changing them. Then there's two-step login—2FA. It's simple: turn it on, every time. Most hacks happen because someone got hold of a password, yet people still leave the door wide open. Studies say gentle reminders work best. If you nudge folks into using 2FA without making it a pain, they're more likely to stick with it.

Look at what's really happening out there. People worry about being caught up in some big, flashy cyber-attack, but that's actually pretty rare. Instead, it's the sneaky stuff—malware infections, phishing emails—that hit way more often. Those are the real troublemakers, and they slip by unnoticed. Ransomware is another beast, especially when there's money involved. Companies take the biggest hit, but weirdly, most don't see it coming. That disconnect? That's a big part of the problem.

A lot of folks don't realize just how risky those widespread device attacks can be, especially scams that trick you into giving up personal info—phishing, for example. And there's something else: data isn't locked up behind office walls anymore. It's everywhere, floating in the cloud, but people still act like it's all sitting on a server in the back room. Some have moved to cloud systems, while others hang onto the old ways.

People talk about online safety a lot, but not many really get how the cloud works. Instead of just dumping all the focus on antivirus software or locking down individual computers, it's time to pay attention to who can get at your data and how your cloud setup is built. These days, it's not just about the device sitting on your desk—it's about where your information lives and who has the keys.

Cyber threats don't stay the same for long. They morph, slip into new shapes, and sometimes hit out of nowhere. One day it's a slow-moving attack hiding in the background, the next it's something loud and messy. Most times, you don't even see the danger until it's already caused trouble. Every day brings some new example. And honestly, each threat acts a little differently. Many don't even look dangerous at first, but every one packs its own risk. As defences get smarter, so do these threats.

When ransomware strikes, it locks up your files and demands a ransom. If you want your stuff back, you have to pay up. Then there's phishing—scammers pretending to be someone you trust, tricking you into handing over private info. These messages might look totally normal, but they're anything but honest. Like thieves at dawn, they sneak in, mess with trust, and steal your secrets before you know what's happened.

Sometimes, attackers flood systems with bogus traffic, jamming up networks so real users can't get through. Everything slows down or just stops as the fake requests pile up. And if there's a weak spot in the design, attackers find it fast. People lose access, and services go offline.

The danger isn't always outside, though. Sometimes someone inside the company—the person you see every day—uses their access in all the wrong ways. Maybe they have clearance, maybe you thought you could trust them, but they cross the line and use their power to harm the organization.

There's also the classic man-in-the-middle move. A hacker slips into the conversation between two people, quietly reading or even changing what gets said. The real chat keeps going, and no one notices the extra set of eyes. It's sneaky—nobody sees the eavesdropper, and private words end up in the wrong hands. This kind of attack lives on trust and silence.

These days, artificial intelligence and machine learning have started to change the game. Instead of waiting for trouble, smart systems spot weird patterns in real time—just like Xu and Li pointed out in 2021. Algorithms pick up on new tricks, learning and reacting way faster than old-school software ever could. When attackers try something new, these systems adapt fast.

As more businesses jump into cloud computing, keeping data safe matters more than ever. Cloud security isn't just the provider's job or the customer's—it's both. Customers protect their own side, vendors handle theirs, and both have to work together. Using things like encrypted transfers, tight permission controls, and real-time monitoring keeps everything locked down. Trust isn't enough—you need teamwork and the right tools to stay ahead.

III. METHODOLOGY

This research digs into real-world experiences by mixing hard numbers from surveys with personal stories. It's not just about the stats — the open-ended questions pull out details about how people actually feel and act when it comes to online safety. Interviews add another layer, showing the habits and worries that don't always show up in the numbers.

First, the study zeroes in on what students and employees really know about staying safe online. Then it shifts to the real-life problems companies face when they try to protect their digital spaces.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb739

The process was pretty straightforward. A random group answered a set of questions on Google Forms. The idea? Keep things organized so it's easier to spot trends in the answers. Each question steered the conversation in a certain direction. After two weeks, all the responses rolled in and landed in spreadsheets. Numbers went one way, comments went another. This made it simpler to line things up and compare. Every answer got checked twice. If something was missing or didn't make sense, it got tossed. The data that made the cut forms the core of what comes next.

So, what did we look for? First, how confident are people in their own online safety skills? Then, how often do they run into cyber issues or close calls? The study tracks habits that put data in danger, like reusing passwords or ignoring software updates. It checks how often people actually fix security problems versus how often they take shortcuts. Turns out, the little things matter. Small good habits today can prevent big disasters later.

Finally, the study digs into how serious people think online threats really are. Comparing what people say they know with how they actually behave, you start to see where there's a gap between confidence and reality.

IV. RESULTS AND DISCUSSION

➢ *Cybersecurity Knowledge Levels*

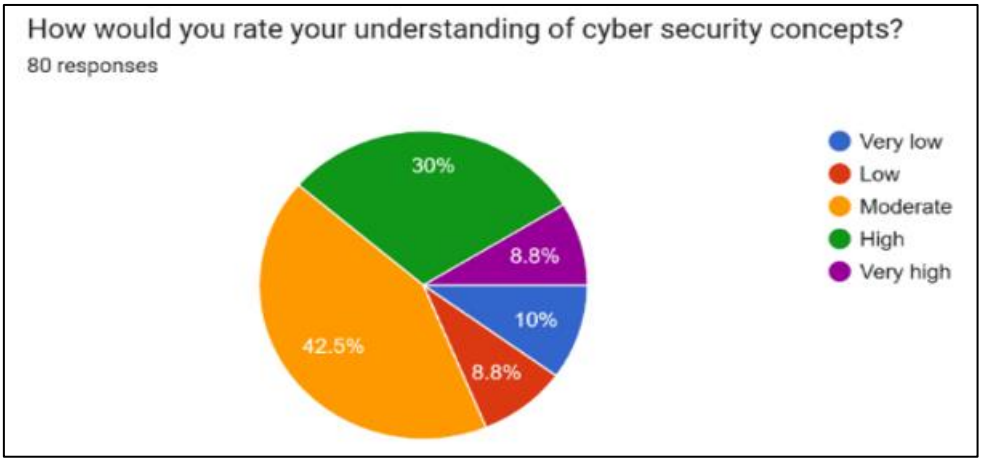

Fig 1 Cybersecurity Knowledge Levels

➢ *Cyber Threat Awareness*

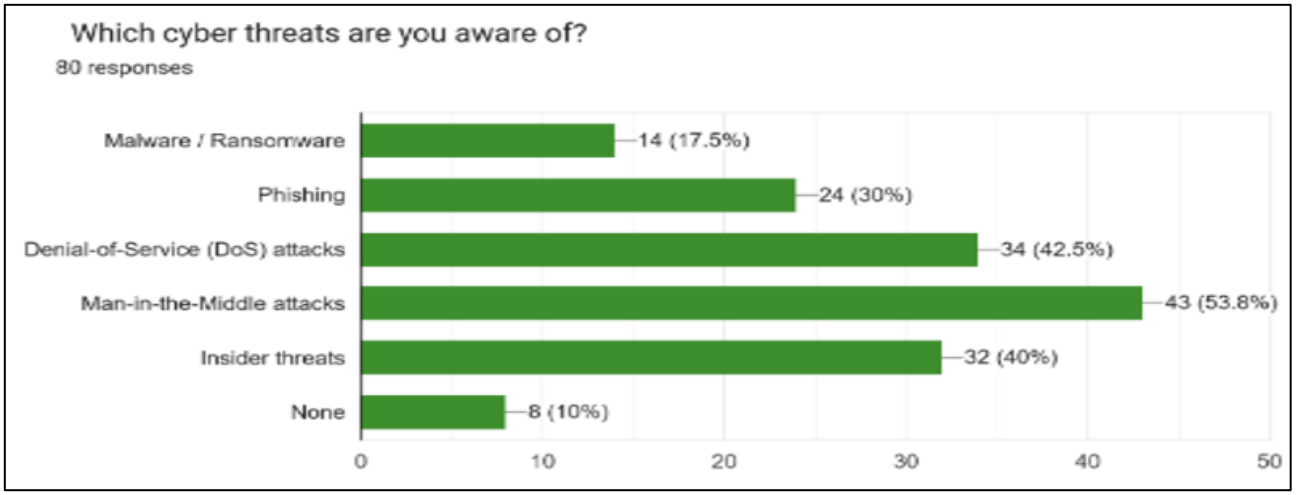

Fig 2 Cyber Threat Awareness

Most people—about 42.5 percent—say they know a decent amount, while around three out of ten feel pretty confident about what they know. Still, it's more common to know a little than to know a lot. There's a solid chunk—about 18.8 percent—who barely understand the topic at all. So, plenty of folks could really use some basic cyber safety lessons. When you dig into what people actually said, there's a clear gap. Sure, they claim to know things, but that doesn't always show in how they act. Over and over, you see the same thing: just because someone knows about online safety doesn't mean they do what they should. Half of the people surveyed said they knew enough about staying safe online. But if you look at what they actually do, the story changes. More than half admitted they keep reusing the same password. Even though everyone hears about two-factor authentication, lots of people still skip it. Some even said they don't bother with it at all. Cloud services are everywhere now, so it's no surprise people use them all the time. Some folks

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb739

store their stuff in the cloud, but others only bother with security tools every now and then. Honestly, that sounds like people are reacting after something happens instead of thinking ahead and staying safe from the start.

Picture a long rectangle chopped into bars, each one showing what eighty people actually know about online dangers. Out of all of them, forty-three recognized Man-in-the-Middle attacks — that's 53.8 percent, if you like numbers. Funny thing is, malware and ransomware, which pop up all the time, only got noticed by 17.5 percent. That means most people missed them. And get this: one in ten couldn't name a single threat. So even though these risks are everywhere, a lot of folks just don't see them at all.

Almost six out of ten people admit they reuse their login details sometimes. Some own up to it right away, while others just kind of shrug and avoid eye contact. Either way, that's more than half of us taking way too many chances with our security. When passwords leak online, hackers don't waste time—they try them everywhere, like they're waving around a skeleton key. Reusing passwords isn't just a shortcut. It's asking for trouble.

➢ *Password Reuse Habits*

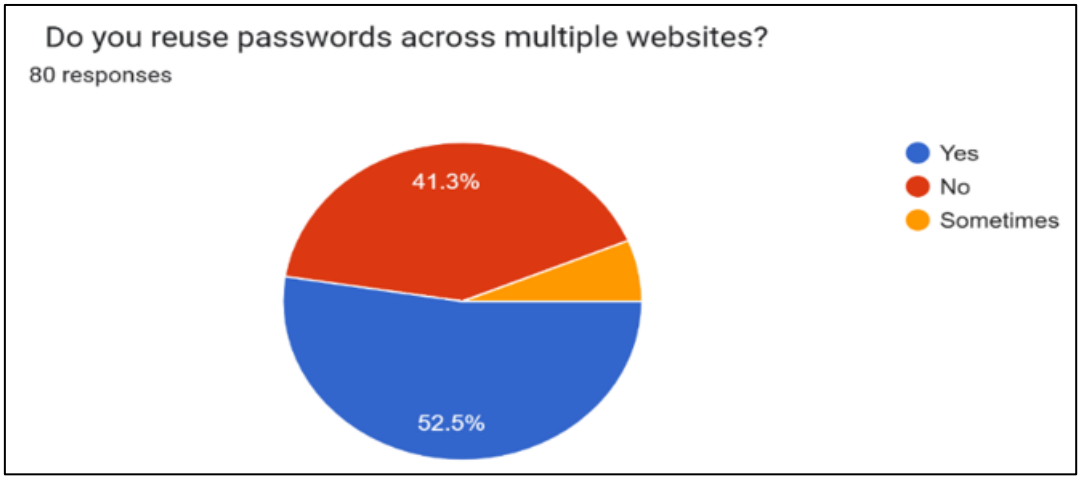

Fig 3 Password Reuse Habits

A lot of folks know what a DoS attack is—about 42.5%. But when it comes to malware or ransomware, barely anyone's paying attention. Only 17.5% recognize those threats, even though they hit more often. Big, flashy cyber-attacks get all the headlines, but honestly, it's those everyday dangers sneaking by that cause the most headaches.

➢ *Awareness of AI in Security*

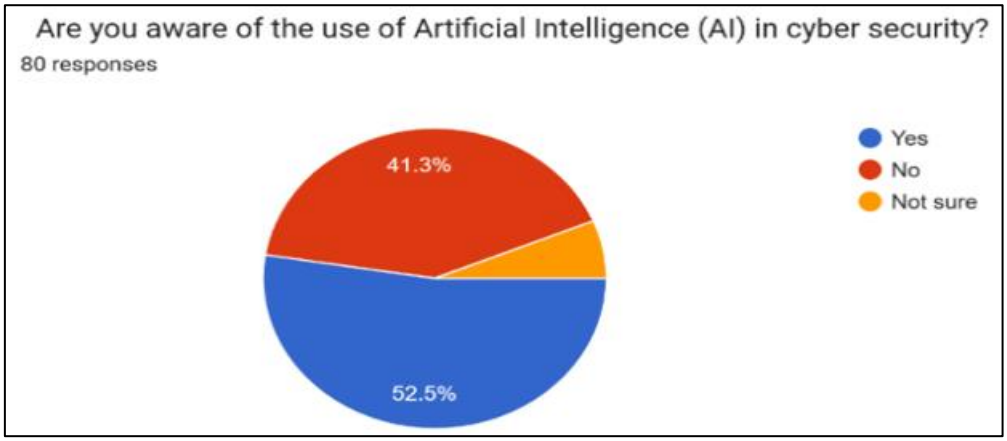

Fig 4 Awareness of AI in Security

About half—52.5 percent—say they know AI is being used for online security. But, here's the kicker: the same group admits they use the same passwords across different sites, even though that's risky. What stands out most? Interception attacks. Over half—53.8 percent—recognize those. Then there's a drop-off. Fewer than one in five see malware and ransomware as real threats, even though those spread all the time.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb739

So, even though people feel pretty informed, a lot of them still ignore basic online safety. Just knowing what to do doesn't mean they actually do it. Why is that? Two reasons pop up again and again: threats keep changing, and sometimes people just aren't paying close attention. There's a real gap here between knowing the risks and actually being careful.

When people use security tools only sometimes, weak spots show up. If they skip important login steps, they leave the door open. That's when attacks sneak in and go after personal files. Cloud systems get even more vulnerable when people let their guard down. Basically, any time defences get sloppy or uneven, hackers have an easier time getting through.

V. CYBER SECURITY FRAMEWORKS AND DEFENCE MECHANISMS

Fighting back starts with building real defences—layers that block, spot, and react fast. Security works best when different tools team up but don't get tangled, so if one falls, the rest stand strong.

- Not long ago, digital "fences" relied on firewalls, alarms, or shields to stop threats we already knew about. Things have changed. Now, smarter systems watch how data moves, learning what looks normal so they can flag anything strange right away. Attacks nobody's seen before? These new guards catch them early just because something feels off.

- Even if someone grabs your data, encryption keeps it unreadable unless they have the right key. Most stored files use AES—it's pretty much the gold standard. When info travels online, SSL or TLS steps in to keep it safe on the move. Without these, private stuff spills out way too easily. Keeping data both correct and out of strangers' hands depends on tools like these.

- *Good Hackers*

yes, the ones on your side—test for weak spots by thinking like real attackers. When defenders act like bad guys, they spot problems faster. Testing regularly keeps security sharp, and rules like GDPR demand it. ISO 27001? You can't get certified without showing you run these stress tests. Basically, let the good guys break things first so the bad ones can't.

VI. CHALLENGES IN CYBER SECURITY

Even with all the fancy tools out there, new problems keep piling up.

Hackers don't wait. Every day, they dream up new tricks, and security teams always seem a step behind. Attacks move faster than the fixes. Most days, it feels like you're chasing shadows.

There's also just not enough talent. The ISC2 Report in 2024 counted over three million open cybersecurity jobs worldwide. That leaves companies scrambling, and with fewer skilled workers, defences get weaker.

Then there's privacy. When companies collect info to keep systems safe, people start wondering if their rights are at risk. Keeping things secure clashes with the privacy people expect—and the law protects.

The rise of internet-connected gadgets only makes things messier. Every new device is another door for hackers, and a lot of them are built on the cheap, with weak security. These holes pop up in places you wouldn't expect.

And if you try to chase hackers across borders? Good luck. Many countries haven't sorted out solid cyber laws. With gaps in the rules, criminals slip away, and trying to hold them accountable turns into a bureaucratic nightmare.

VII. FINDINGS AND ANALYSIS

Cybersecurity isn't just code and firewalls—it's just as much about people and rules. Sure, things like blockchain and AI open new doors, but someone needs to set the rules and make sure they're used responsibly. Strangely enough, the biggest weakness often isn't the tech—it's whether users actually get the risks. Even the best defences fail if someone hands over the keys by mistake. Teams that train staff often and keep a close watch on activity stay safer than those who just wait for trouble to show up.

VIII. CONCLUSION AND RECOMMENDATIONS

➢ *Change Never Really Lets Up in Cyber Safety*

As threats get sneakier, we need smarter defences. That's where automation jumps in, data drives our decisions, and ongoing training covers the gaps. Still, people know the risks but sometimes act carelessly anyway. Just knowing the facts doesn't fix sloppy habits. Instead of just dumping info on people, systems need to help shape how they behave—bake good choices right into the design. Because, honestly, awareness fades fast if it doesn't turn into action.

➢ *Recommendations*

Let's start by ditching the old idea of fixed network boundaries. Trust nothing by default—check who's asking for data every single time, whether they're inside or outside. Don't just let them through because they're "one of us." Flip those old assumptions. Security should follow the person, not just sit behind a firewall.

Make cyber awareness part of daily life, not just a once-a-year box to tick. When people practice spotting scams all the time, it starts to come naturally. Imagine staff thinking twice before clicking something sketchy because they've seen that trick in a drill. Realistic simulations sharpen instincts across the board. Training sticks when it feels real, not forced. Everyone benefits—interns, execs, the whole team—when this is ongoing.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb739

We catch threats faster when smart tools work together. Machines spot things people miss and act in real time. It's like reflexes kicking in before you even think.

When new risks pop up, the rules have to keep up. Tech moves fast, so our laws can't just sit still. Old policies won't catch modern threats. That's why we need to update them—otherwise, gaps open up where we should be protected.

Solving these problems means schools and businesses need to team up. When labs and companies work together, new ideas pop up faster. Sharing tools and training closes the skill gap. The tough problems get solved more often when people swap insights. We make more progress together than on our own.

- *Here's Another Thing to Dig Into:*

Why do people still gamble online even when they know it's risky? Emotions and social pressure play a role—figuring out how might show patterns we're missing. And keep an eye on quantum computers. They could break today's codes sooner than we think. Plus, working across countries matters more than ever, especially when tracking digital evidence. When different nations put the pieces together, it changes how cases play out. Every angle brings something real to the table, not just theory.

REFERENCES

[1]. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.
[2]. Cisco. (2023). *Annual Cybersecurity Report*. Cisco Systems.
[3]. ENISA. (2024). *Threat Landscape Report*. European Union Agency for Cybersecurity.
[4]. ISC2. (2024). *Global Cybersecurity Workforce Study*.
[5]. NIST. (2021). *Cybersecurity Framework*. U.S. Department of Commerce.
[6]. Schneier, B. (2018). *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World*. Norton.
[7]. Stallings, W. (2019). *Cryptography and Network Security: Principles and Practice*. Pearson.
[8]. Symantec. (2022). *Internet Security Threat Report*. Retrieved from www.symantec.com.
[9]. Xu, Y., & Li, T. (2021). Artificial Intelligence in Cybersecurity. *IEEE Access*, 9, 45132–45147.