Crime and Cybersecurity as Advanced Persistent Threat: A Constant E-Commerce Challenges

Harshith Desamsetti

Senior Product Engineer (Java), ACA Group LLC, NY 10017, **USA**

E-mail for correspondence: harshithdesamsetti9@gmail.com

ABSTRACT

This study examines e-commerce technology and company cyber security threats. Technology for e-commerce is garnering academic and business attention. The business community and consumers can now do what was previously impossible. But it also created concerns, including cyber security. This study examines social engineering, denial of service, malware, and personal data assaults. Global firms spend a lot on cybersecurity, which grows each year. Because attackers constantly look for new vulnerabilities in persons, companies, and technology, it seems complicated to solve the obstacle. This study analyzes social engineering, DDoS, malware, and personal data threats. Using new technology for e-commerce and cybersecurity is a never-ending game of cat and mouse. Reliable technology, staff, customer training, and good corporate and government policies and regulations mitigate hazards.

Keywords: Cyber Attack, Cyber Security, E-Commerce, Cyber Theft, Social Engineering, Phishing

INTRODUCTION

The study of technical linkages between security and threat perspectives shows that computers have had a significant impact and will continue to do so. Cybersecurity has become a major issue since most individuals conduct their personal and professional lives online (Lal, 2015). Recognition of cybersecurity's future can help people maximize their assets and stay safe today and in the future. Cybersecurity involves preventing illegal access to networks, devices, and information and ensuring information security, confidentiality, morality, and ease of access. Everything depends on the Internet and computers. The cybersecurity industry changes frequently due to hackers' changing habits and new threats. Thus, predicting cybersecurity's future takes a lot of work. For instance, between 2018 and 2019, global ransomware attacks increased, forcing cybersecurity businesses to develop new technology to tackle them. Nobody knows how or where the next cybersecurity threat will come from, but experts know the general direction (Lal, 2016). Even though no one can predict the future, focusing on the cybersecurity forecasts below can help future-proof one's firm and internet activities.

TYPES OF CYBER-ATTACKS

There are as many kinds of cyberattacks as other malevolent goals that a cybercriminal would want to accomplish (Gcaza et al., 2017). To provide a brief overview, these are the most typical and widely recognized types of cyberattacks.

Malware: This is the most general term, and it can refer to a variety of different kinds of cyberattacks. Malicious software, such as viruses, Trojan horses, or worms, is typically the most common manifestation of this threat. The goal is to, among other things, cause harm to the targeted equipment, services, or networks, prevent them from operating as intended, install spyware, and take control of the situation.

Phishing: Phishing is one of the most common and damaging cybersecurity vulnerabilities. It also ranks towards the top in terms of frequency. The primary objective is to steal sensitive information (such as credentials or personal data) and exploit it for fraud after obtaining it illegally.

Ransomware: There have been instances where ransomware attacks have been successful against large organizations and even public agencies. This cyber-attack is widespread and hazardous because it prevents computer access and typically demands a ransom to regain access.

Dictionary attack: It is one of the stealthiest forms of cyberattack since it uses a computer program to try various possible password combinations to discover the victim's password. This makes it one of

the more covert forms of cyberattack. As a result, using passwords that are one-of-a-kind, consisting of a combination of upper and lower case letters, digits, and symbols, and being reasonably lengthy is always recommended.

Denial of service attack: It is a form of attack whose primary objective is to prevent users from accessing a particular website, service, or network. To accomplish this, it will send several requests at the same time until it is successful in crashing it.

Man-in-the-middle attack: It is an attack that, as its name suggests, aims to intercept the online traffic of a third party (whether it be a chat, surfing, uploading files, or anything else of the sort), all while the third party is entirely unaware that it is being spied on at any moment.

One of the most problematic sorts of cyberattacks is known as a SQL injection attack. This is one of the types of cyberattacks. The purpose of the SQL injection attack is to obtain sensitive data from the websites and databases of companies. It is possible to access sensitive data, such as the credit card numbers, physical addresses, and identity documents of users, amongst many other personal information.

Rootkit attack: This kind of cyberattack grants the attacker administrator privileges, allowing them to modify the systems they are attacking significantly.

Threat Intelligence Today

Investigation, data collecting, and assault analysis are all components of threat intelligence, aiming to comprehend better why and how an attack was carried out. It provides professionals in the field of cyber security with a better understanding of why hostile actors target specific individuals or organizations. Cyber security specialists told Cyber Security Hub that, based on their threat intelligence analysis, they anticipate that essential employee/role targeting, malware, and ransomware will be the threat vectors that will have the most significant impact. These warnings about the potential for danger appear to be coming true: 81 percent of firms claimed that they faced cyber-attacks that directly targeted employees, and eight out of ten cyber security professionals said that ransomware is a "danger" and a "threat" to public safety. More than one billion malware programs are believed to be operating worldwide.

The market for threat intelligence is expected to expand from $4.97 billion in 2021 to $18.11 billion in 2030, according to research conducted by Cyber Security Hub, which revealed that 25 percent of cyber security experts believe threat intelligence will be the most crucial goal for cyber security investment.

According to Jojo Nufable, group IT infrastructure and cyber security head of Metro Pacific Health Solutions, a hospital operator based in the Philippines, threat intelligence is essential to ensuring businesses can withstand and recover from cyber-attacks.

"Threat intelligence encourages applying best practice, paving the way for cyber security teams to see threats and risks before they are realized," he continues. "This is the best course of action as it means that they can remediate before an attack is in full swing, allowing them to do so."

"Threat intelligence also helps to minimize false positive and high noise feeds of security events and information and streamlines threat response by having an adaptive and agile incident response management system," he adds. "False positives and high noise feeds of security events and information" refer to events and information that contain too much irrelevant information.

Companies can better respond to threats by focusing on threat intelligence. This is because they are proactive rather than reactive when dealing with risks. Because of this, they can prevent hostile actors from causing damage to their networks before it is too late.

Prevents Threat Intelligence Effectiveness

Cybersecurity professionals face many problems when gathering and using threat intelligence data. Cyber Security Hub found that 38% of cyber security professionals' most considerable non-threat-based difficulty was a lack of business-wide cyber security training/understanding, and 37% cited company culture integration. Threat intelligence from these challenges requires cyber security professionals to be especially careful when dealing with employees who may not understand how to prevent the most likely cyber assaults on their organizations. Verizon revealed that 74% of data breaches involve humans. Proper staff education prevents human error, privilege misuse, stolen credentials, and social engineering assaults.

Threat information may help firms implement the correct incident detection, response, and recovery strategy for their threat vector, according to cybersecurity expert Kim Crawley, author of Hacker Culture: A to Z.

Threat intelligence is most useful when a company can identify "x" as a network vulnerability, and threat modeling shows that attackers would conduct "y" to exploit it. Looking for intelligence on "x" being utilized for "y." We can obtain important and relevant threat intelligence that way, she says. Anthony Lim, Singapore University of Social Sciences fellow of cyber security and governance, says threat intelligence is needed to establish a tested incident response plan.

Lim said the probe report for Singapore's most significant data breach case showed this.

Anonymous state actors stole 1.5 million patient records from SingHealth, the country's largest healthcare group 2018. Between June 27 and July 4, 2018, hackers targeted

Prime Minister Lee Hsien Loong. The breach investigation found that the attackers designed and deployed proprietary malware to bypass SingHealth's cyber defenses. A 2016 internal audit found cyber security weaknesses that had yet to be fixed before the attack.

Lim said the study also determined that the company's incident response management was flawed, which may have avoided the attack.

SingHealth has an incident response plan. However, personnel needed to be made aware of how, when, and to whom to report a cyber security event. Lim explains that staff needed adequate cyber security awareness and training so they could not understand the severity of the attack or how to respond effectively to it. Though there was a framework to report cyber security incidents, employees needed to be sufficiently trained.

The Evolution of Threat Intelligence

Threat intelligence has progressed in tandem with the evolution of various threat vectors. Cyber security professionals have taken advantage of new technologies such as artificial intelligence (AI) and machine learning (ML), which have emerged due to the advancements made possible by the digital era, to prevent bad actors from obtaining access to their networks (Bodepudi et al., 2019).

In addition, professionals in the field of cyber security have shifted their approach to defending against threats from reactive to proactive. Instead of striving to lessen the impact of threats, professionals in the cybersecurity field focus on finding ways to eliminate them. One method they employ is to use threat intelligence to inform the development of proactive incident response plans (Lal & Ballamudi, 2017).

This section will investigate how threat intelligence is evolving due to the introduction of new technologies and mindsets. These include artificial intelligence and a shift from reactive to proactive threat detection and response techniques.

The Implementation of AI and ML Technologies

The application of artificial intelligence (AI) in cyber security was estimated to be worth $10.5 billion in the year 2020, and its value is expected to rise to $46.3 billion by 2027. Additionally, AI is fundamentally altering the way threat intelligence functions. Cybersecurity teams can tackle typical problems with threat intelligence by utilizing artificial intelligence. These problems include a lack of time, competing priorities, and a lack of cyber security knowledge or competence. For instance, to handle "threat overload, laborious tools, and the talent gap," Google has implemented AI-powered threat intelligence (Ahmad et al., 2018).

Amanda Fennell, an expert in information technology and cybersecurity who is also an adjunct professor at the Tulane School of Professional Advancement points out that the field of threat intelligence has a wide variety of potential applications for artificial intelligence.

"There are optimization challenges that AI may be able to locate the information to answer, ranging from the most fundamental level of semiconductor design to programming interfaces. She points out that everyone is looking for products that can link as much information as possible and learn from it in real time to stop enemies from gaining momentum in the cyber arena (Chen et al., 2019).

Crawley reveals that, in her opinion, the future development of cyber risks will be driven by more advanced and publicly accessible artificial intelligence technology. For instance, cybercriminals are going to use the generative AI chatbot ChatGPT in a variety of different ways. However, she emphasizes that this does not imply that the technology should be banned; instead, the cybersecurity community will need to pay closer attention to how criminals utilize AI to stay one step ahead of them (Mandapuram, 2016).

Reactive to Proactive Threat Intelligence

The strategy for gathering threat intelligence has also undergone significant changes alongside the development of technology related to threat intelligence. Cyber security experts attempt to establish a cyber-resilient culture rather than developing a reactive incident response plan (Mandapuram et al., 2020). This strategy would have explained how to respond to cyber-attacks already occurring or still underway.

Irina Tsukerman, a geopolitical analyst and attorney specializing in national security issues in the United States, says, "The threat intelligence market is still ballooning." According to recent studies, the size of the worldwide threat intelligence market is projected to reach $16.1 billion by 2025. The reactive approach to the incident response that security teams currently use will be replaced with a proactive one as the function of security teams continues to expand (Desamsetti, 2016a). They will connect and communicate more at all levels, and it will be their responsibility to provide threat intelligence that detects risks and specifies corporate goals. In the future, threat intelligence will make it possible for security teams to predict and prevent threats at the earliest possible stage successfully, and it will also support proactive threat response.

Cyber resilience focuses on detection and reaction, whereas cyber risk management requires businesses to base their decisions regarding threat intelligence strategy on the organization as an individual entity. When companies do this, they can determine the danger vectors they are most likely to face and construct an incident response strategy based on this information.

Threat information is crucial to cyber security. Cyber security experts must investigate cyber threats to create a proactive incident response plan (Gutlapalli et al., 2019). Cyber security professionals have improved their threat intelligence tactics as hostile actors use AI and ML (Desamsetti, 2016b). Threat intelligence has become proactive as cyber threats increase in frequency and volume. This prevents and mitigates attacks. Organizational culture has also shifted, with non-cyber security staff realizing the threat cyber security poses to the firm. Even people outside the cyber security team are considering how dangers affect them and how to prevent cyber-attacks. Current threat research should inform threat intelligence tactics, and innovation should continue to allow enterprises to avoid and manage cyber security risks.

E-Commerce Domain

E-commerce is a rapidly increasing area that emerged from the convergence of technology and the Internet, where individuals conduct numerous business operations. E-commerce is online goods sales and purchases. It involves an internet money transfer for business completion. E-commerce employs digital technologies to develop and act on transactions between organizations or groups or between firms and customers. A survey shows over 12–24 million e-commerce websites exist worldwide (Fan & Yong, 2013).

In e-commerce, buying and selling are done online. Product selection, money transfer, and data exchange are primary e-commerce operations. Internet marketing, online administration, and automatic data collection are further tasks. E-commerce helps businesses expand their market scale and reduce operating expenses and restrictions (Dekkati & Thaduri, 2017). The evidence suggests it boosts the economy. Customers buy directly from online stores via mobile apps and websites in e-commerce. Chatbots, live chat, and voice assistants allow communication.

Alibaba, Amazon, and others are leading the shift from in-store to online buying. This trend is driving technological advances in online business procedures. E-commerce simplifies shopping and transforms businesses.

Due to significant development, enterprises improved their networks, operations, etc., to better serve suppliers and consumers. E-commerce technology gave businesses countless chances to locate and grab new markets and draw clients across borders, making yesterday's unattainable aim possible (Gutlapalli, 2017c). E-commerce has many benefits for companies and customers but requires sophisticated security.

E-commerce serves four markets. Business to Business, Business to Consumer, Consumer to Consumer, and Consumer to Business divisions sell products to businesses, consumers, and businesses.

E-commerce sales were 4.08 Trillion USD in 2019 and are predicted to reach 5.2 Trillion USD. The US e-commerce share was 468.2 billion USD in 2020.

According to trends and data, e-commerce is a rising business sector. It is typical of global internet and technology availability. Tourism is also using technology to change (Daniel, 2016). Ticket sales, hotel reservations, etc., may now be made online with the right technology. Global online travel agent sales are 432 billion USD, online travel booking platforms are 517 billion USD, and 65% of worldwide travel and tourism revenue comes from online sales.

E-commerce technologies and enterprises must be able to do business quickly and give customers the best experience (Reddy et al., 2020). As mentioned, buyers and sellers use technology to execute the transaction remotely after providing information. E-commerce has several challenges, but cyber security is the worst (Lal et al., 2018).

Cyber Security

Cyber security threats have plagued e-commerce from the start. Cyber security safeguards computer data, software, and hardware from disclosure, misdirection, damage, or theft. Electronic security is critical in e-commerce. Company firms spend on cyber defenses, but cybercriminals access company networks and data (Desamsetti & Mandapuram, 2017). Cybercriminals are using new methods to find weaknesses, changing cybersecurity challenges. Malicious actors are improving their abilities and using modern technology to target organizations. Most internet-connected companies, including healthcare, finance, transportation, government, and manufacturing, are constantly attacked. The number of users and technology dependence during the COVID-19 epidemic raised attacks by 600%. Cybercrime cost 3 trillion USD in 2015 and up to 6 trillion in 2020. Businesses will spend 10.5 billion USD by 2025, more than any country save the US and China. In the digital and technical age, businesses and organizations, especially e-commerce ones, need cybersecurity (Bamrara, 2015).

Knowing why cybersecurity breaches happen is crucial. Cybersecurity issues have three primary causes: The US and UK list humans as a significant source of CS. Eighty-six percent of security breaches are caused by humans, compared to 63% by technology. Another study found that human mistake causes 80% of cyberattacks (Scheau et al., 2016). Human technology interactions pose security concerns, and organizations struggle to prevent and manage behavioral-based information security vulnerabilities. Business firms invest in complex information technologies to gain a competitive edge and market share, which typically increases human errors (Dekkati et al., 2019). The weakest link in risk and security management is customers and workers. CS dangers increase daily, and organizations develop and use new technology to counter them (Gutlapalli, 2016a).

Along with inducing the latest technologies to counter risks, humans must be sufficiently trained and educated on their interactions with the organization's information systems to minimize behavioral risks. Cybersecurity issues entail human components, yet most firms have not invested in humans to address them (Thaduri et al., 2016). Customers may share their data erroneously, with the wrong person, or with an insecure information system, causing cybersecurity hazards (Gutlapalli, 2016b). Employees may need to be able to use technology appropriately, posing serious cybersecurity risks to the company and its customers (Deming et al., 2018). Lastly, the employee may use consumer and organizational data for personal advantage. E-commerce faces a significant threat from humans in all forms (Koehler et al., 2020).

Technology: In addition to humans, cyber risks can come from technology. Technology, hyper-connected systems, human blunders, and unprepared enterprises allow cybercriminals to exploit vulnerabilities. Phishing, social engineering, credential theft, and compromised or stolen devices accounted for 54, 27, and 31% of cyber threats in 2020. Other risks include spyware, ransomware, and trojans. According to a survey, 81% of breaches were caused by weak or stolen passwords, 62% by hacking, 51% by malware, and 43% by social engineering. Modern technology's hyper-connectivity and industry and commerce's dependence on these systems are significant cybersecurity challenges. It involves networked societies, technologies, and communication methods like email and instant messaging. E-business or e-commerce involves connecting an organization's massive information system to the outside world (Thaduri & Lal, 2020). Because of its connectedness, fraudsters can exploit it.

Non-preparedness: Cybersecurity hazards also stem from unpreparedness. Many companies need to prepare for cyberattacks. They need advanced protocols and tools to prevent cyberattacks or respond poorly (Liu et al., 2017). Attackers capitalize on their unpreparedness.

Statistics show that only 21.3 Billion USD was spent on cybersecurity in 2020, compared to 5.1 Billion USD in 2017, 5.9 Billion USD in 2018, 8.3 Billion USD in 2019, and 8.9 Billion USD in 2020. Cybersecurity investment peaked at 7.7 billion USD in the fourth quarter of 2020.

Cybersecurity investment is rising annually, especially in 2020. From Figure 6, cybersecurity funding increased suddenly in the last quarter of 2020 from 3.8 Billion USD in the first quarter, 5.3 Billion USD in the second, 4.8 Billion USD in the third, and 7.8 Billion USD in the fourth. To conclude, cybersecurity is worsening as actors gain experience and more sophisticated attack methods. This exacerbated data leaks and jeopardized the e-commerce company.

Social Engineering

Social engineering is cybercriminals' most prevalent fraud. Any activity that influences someone to choose an unfavorable action. It involves psychologically manipulating clients to execute tasks, provide confidential information, etc (Gutlapalli, 2017b). It may be a one-step or multi-step trick, but the goal is to obtain conditional details or access the system (Anderson, 2008). The "forget password" option is the simplest form of social engineering, which leads users to a malicious link and gives attackers access to their accounts or systems (Balzacq & Cavelty, 2016).

Additionally, the original user cannot access the invoice. Top executives or students may be targeted using social engineering. Social engineering attacks can target anyone. Social engineering accounts for 98% of cyberattacks, demonstrating its seriousness. The most frequent malevolent social engineering methods are:

Phishing: When an attacker sends a fake email from a trusted source and requests information. Through this procedure, the criminal collects and uses personal data. About 70% of firms worldwide were victims of phishing websites in 2020, 75 times more than malware. It caused $1.8 billion in business losses in 2020 (Conteh & Schmick, 2016).

Vishing: An attacker calls to try or urge an action. Data collection is done to gain information a company or someone can use to compromise. Only in 2020 did vishing attacks, 27% of response-based threats, increase by 554%. These facts show it will rise. The attacker impersonates another person or firm and socializes to access a firm, system, etc. Personalization increased 131% between 2020 and 202, costing targeted firms 1.8 billion USD.

Smishing: When an attacker sends phone messages to influence a victim's immediate behavior, such as visiting a malicious website or downloading anything. Only 328% more smishing frauds were recorded in 2020.

When customers join e-commerce websites or pages, attackers socialize and collect the data after building confidence, then utilize it for personal use (Gutlapalli, 2017a). Any victim may be targeted regardless of experience, education, or status.

Attack on Consumer Personal Data

Personal data targeting is another primary e-commerce concern (Shang, 2013). As the world becomes more digital, the amount of company and customer data shared, stored, and saved on systems and online constantly grows. Data and network use are also rising. This increases the danger of cybercrime to steal confidential data and lowers consumer and corporate confidence. The company may learn and store a lot about customers through e-commerce because they must submit their private information (Ballamudi et al., 2021). Home address, phone number, bank card number, birthdate, etc. The online retailer or organization may also compare our buying history to our details.

Personal data threats fall into two categories:

- Online stores and organizations can utilize client data without consent.
- External cyber attackers can take data from the online firm.

About 15 billion data records were hacked in 2019. It means that e-commerce's biggest challenge is data breaches. Customers and e-commerce enterprises must comprehend data dangers and breach costs. The information age is here, and information is the most valuable thing. Organizations plan strategies, products, and investments using the data (Thodupunori & Gutlapalli, 2018). Sharing information with someone or an organization requires a lot of trust and a purpose. The company must protect client data from unauthorized usage to preserve confidence and use it strategically (Mandapuram & Hosen, 2018). Assume attackers steal customer data. If so, it will damage customer trust and prevent the company from competing strategically.

DDoS Attacks

In this cyberattack, the criminal disrupts the service or system, making it unavailable to users. The most typical denial of service attack is a deluge of requests to overload the system and prohibit genuine submissions. Multiple sources cause most traffic flooding, making it hard to halt. DDoS attacks include several authorities sending demands to take down a website. In e-commerce, they swamp online stores with traffic, preventing buyers from buying. This turns off the internet firm for hours or days. If the attack occurs during peak season, it is more severe and bothersome and may cause a lot of customer and money loss (Ramkumar et al., 2015).

The main goal is to block internet firms and stores from delivering services. Its form relies on the attackers' plan and the e-commerce store's nature. DDoS assaults fall into three categories:

- Volume-based: Attackers flood a server or website with traffic to turn it off.
- Network layer: Attackers target network infrastructures with numerous data packets.
- Application layer: Attackers overwhelm applications with malicious queries, making them unavailable to actual clients.

One of the most significant cybersecurity risks in e-commerce is when thieves render a source or resource unavailable to customers (Mandapuram et al., 2018). Service availability is critical to user attraction. If a service is available and better than competitors, customers will automatically choose it. Thus, if a service is unavailable or of poor quality, customers will choose a better one. Losses occur both times. Therefore, e-commerce companies must offer more excellent service than competitors. DDoS assaults must be detected and responded to quickly (Guynes et al., 2011).

Software Malware

Cybercriminals inject malware into target websites. The goal is to steal passwords, account details, and money or prevent the system owner from utilizing it. This usually deceives users and redirects them to another site. Worldwide malware attacks commit crimes on the victim's system (Mandapuram, 2017a). It could be ransomware, device control, or spyware. Servers, computers, and networks are targeted by malware. The system is breached, and private data is obtained after unauthorized access. Worms, viruses, trojans, ransomware, horses, spyware, rogue software, scareware, adware, etc. are malware. Because each threat has its defense approach—antivirus, firewalls, algorithms, etc.—it is challenging to address all hazards with the same technique. It plagues e-commerce. Since malware attacks are rising annually, e-commerce is at risk. In 2017, there were 670,000,000 malware types, nearly double in 2016.

Modern technology benefits businesses but also introduces malware. As technology advances and its applications expand, incidents and risks rise annually. E-commerce companies need technology that can detect and block harmful software (Mandapuram, 2017b). Again, it can target the company and its consumers, who must be aware and employ secure technology and service.

Conclusion

E-commerce is appealing to modern businesses, but cyber security threats threaten it. Despite corporations investing much to address the issue, it can be challenging. Cyberattacks target personal and organizational data. Technology offers new methods to operate business and many benefits, but cyber security risks will always exist. Investing in e-commerce security is crucial for competitive advantage and business success. No one can afford to lose clients' trust due to data exposure. Organizational and customer mishaps require strict monitoring measures. For instance, solid passwords and careful clicking and downloading. Taking precautions and investing in secure e-commerce technology is essential. No matter how much the employees and consumers are trained and skilled to do e-commerce, how much the e-commerce firm implements and focuses on cyber security protocols and policies, and how advanced technology is used for e-commerce business activities, cyber security threats will always be there to hurt the business at some point.

References

Ahmad, B., Wang, J., Ali, Z. A. (2018). Role of Machine Learning and Data Mining in Internet Security: Standing State with Future Directions. *Journal of*

Computer Networks and Communications, 2018. https://doi.org/10.1155/2018/6383145

Ballamudi, V. K. R., Lal, K., Desamsetti, H., & Dekkati, S. (2021). Getting Started Modern Web Development with Next.js: An Indispensable React Framework. *Digitalization & Sustainability Review*, *1*(1), 1–11. https://upright.pub/index.php/dsr/article/view/83

Balzacq, T., & Cavelty, M. D. (2016). A theory of actor-network for cyber-security. *European Journal of International Security*, *Cambridge*, *1*(2), 176-198. https://doi.org/10.1017/eis.2016.8

Bamrara, A. (2015). Evaluating Database Security and Cyber Attacks: A Relational Approach. *Journal of Internet Banking and Commerce*, *20*(2), 1-17. https://www.proquest.com/docview/1799378132/DDC4CD9969A244CBPQ/29

Bodepudi, A., Reddy, M., Gutlapalli, S. S., & Mandapuram, M. (2019). Voice Recognition Systems in the Cloud Networks: Has It Reached Its Full Potential?. *Asian Journal of Applied Science and Engineering*, *8*(1), 51–60. https://doi.org/10.18034/ajase.v8i1.12

Chen, S., Thaduri, U. R., & Ballamudi, V. K. R. (2019). Front-End Development in React: An Overview. *Engineering International*, *7*(2), 117–126. https://doi.org/10.18034/ei.v7i2.662

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities, and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6*(23), 31-38. https://doi.org/10.19101/IJACR.2016.623006

Daniel, O. (2016). The Internet of Things**.** *Journal of Democracy*, *27*(3), 176-178. https://doi.org/10.1353/jod.2016.0042

Dekkati, S., & Thaduri, U. R. (2017). Innovative Method for the Prediction of Software Defects Based on Class Imbalance Datasets. *Technology & Management Review*, *2*, 1–5. https://upright.pub/index.php/tmr/article/view/78

Dekkati, S., Lal, K., & Desamsetti, H. (2019). React Native for Android: Cross-Platform Mobile Application Development. *Global Disclosure of Economics and Business*, *8*(2), 153-164. https://doi.org/10.18034/gdeb.v8i2.696

Deming, C., Dekkati, S., & Desamsetti, H. (2018). Exploratory Data Analysis and Visualization for Business Analytics. *Asian Journal of Applied Science and Engineering*, *7*(1), 93–100. https://doi.org/10.18034/ajase.v7i1.53

Desamsetti, H. (2016a). A Fused Homomorphic Encryption Technique to Increase Secure Data Storage in Cloud Based Systems. *The International Journal of Science & Technoledge*, *4*(10), 151-155.

Desamsetti, H. (2016b). Issues with the Cloud Computing Technology. *International Research Journal of Engineering and Technology (IRJET)*, *3*(5), 321-323.

Desamsetti, H., & Mandapuram, M. (2017). A Review of Meta-Model Designed for the Model-Based Testing Technique. *Engineering International*, *5*(2), 107–110. https://doi.org/10.18034/ei.v5i2.661

Fan, J., Yong, F. (2013). Research of Existing Security Problems in E-Commerce Sites and Defense Technology. *Applied Mechanics and Materials, 380-384,* (2519). https://doi.org/10.4028/www.scientific.net/AMM.380-384.2519

Gcaza, N., Solms, R. V., Grobler, M. M., Vuuren, J. J.V. (2017). A general morphological analysis: delineating a cyber-security culture. *Information and Computer Security*, *25*(3), 259-278. https://doi.org/10.1108/ICS-12-2015-0046

Gutlapalli, S. S. (2016a). An Examination of Nanotechnology's Role as an Integral Part of Electronics. *ABC Research Alert*, *4*(3), 21–27. https://doi.org/10.18034/ra.v4i3.651

Gutlapalli, S. S. (2016b). Commercial Applications of Blockchain and Distributed Ledger Technology. *Engineering International*, *4*(2), 89–94. https://doi.org/10.18034/ei.v4i2.653

Gutlapalli, S. S. (2017a). Analysis of Multimodal Data Using Deep Learning and Machine Learning. *Asian Journal of Humanity, Art and Literature*, *4*(2), 171–176. https://doi.org/10.18034/ajhal.v4i2.658

Gutlapalli, S. S. (2017b). The Role of Deep Learning in the Fourth Industrial Revolution: A Digital Transformation Approach. *Asian Accounting and Auditing Advancement*, *8*(1), 52–56. Retrieved from https://4ajournal.com/article/view/77

Gutlapalli, S. S. (2017c). An Early Cautionary Scan of the Security Risks of the Internet of Things. *Asian Journal of Applied Science and Engineering*, *6*, 163–168. Retrieved from https://ajase.net/article/view/14

Gutlapalli, S. S., Mandapuram, M., Reddy, M., & Bodepudi, A. (2019). Evaluation of Hospital Information Systems (HIS) in terms of their Suitability for Tasks. *Malaysian Journal of Medical and Biological Research*, *6*(2), 143–150. https://mjmbr.my/index.php/mjmbr/article/view/661

Guynes, C. S., Wu, Y. A., John, W. (2011). E-Commerce/Network Security Considerations.

International Journal of Management and Information Systems, 15(2), 1-7.

Koehler, S., Desamsetti, H., Ballamudi, V. K. R., & Dekkati, S. (2020). Real World Applications of Cloud Computing: Architecture, Reasons for Using, and Challenges. *Asia Pacific Journal of Energy and Environment*, *7*(2), 93-102. https://doi.org/10.18034/apjee.v7i2.698

Lal, K. (2015). How Does Cloud Infrastructure Work?. *Asia Pacific Journal of Energy and Environment*, *2*(2), 61-64. https://doi.org/10.18034/apjee.v2i2.697

Lal, K. (2016). Impact of Multi-Cloud Infrastructure on Business Organizations to Use Cloud Platforms to Fulfill Their Cloud Needs. *American Journal of Trade and Policy*, *3*(3), 121–126. https://doi.org/10.18034/ajtp.v3i3.663

Lal, K., & Ballamudi, V. K. R. (2017). Unlock Data's Full Potential with Segment: A Cloud Data Integration Approach. *Technology &Amp; Management Review*, *2*, 6–12. https://upright.pub/index.php/tmr/article/view/80

Lal, K., Ballamudi, V. K. R., & Thaduri, U. R. (2018). Exploiting the Potential of Artificial Intelligence in Decision Support Systems. *ABC Journal of Advanced Research*, *7*(2), 131-138. https://doi.org/10.18034/abcjar.v7i2.695

Liu, X., Zhao, M., Li, S., Zhang, F., Wade, T. (2017). A Security Framework for the Internet of Things in the Future Internet Architecture. *Future Internet, 9*(3), 27. https://doi.org/10.3390/fi9030027

Mandapuram, M. (2016). Applications of Blockchain and Distributed Ledger Technology (DLT) in Commercial Settings. *Asian Accounting and Auditing Advancement, 7*(1), 50–57. Retrieved from https://4ajournal.com/article/view/76

Mandapuram, M. (2017a). Application of Artificial Intelligence in Contemporary Business: An Analysis for Content Management System Optimization. *Asian Business Review*, *7*(3), 117–122. https://doi.org/10.18034/abr.v7i3.650

Mandapuram, M. (2017b). Security Risk Analysis of the Internet of Things: An Early Cautionary Scan. *ABC Research Alert*, *5*(3), 49–55. https://doi.org/10.18034/ra.v5i3.650

Mandapuram, M., & Hosen, M. F. (2018). The Object-Oriented Database Management System versus the Relational Database Management System: A Comparison. *Global Disclosure of Economics and Business*, *7*(2), 89–96. https://doi.org/10.18034/gdeb.v7i2.657

Mandapuram, M., Gutlapalli, S. S., Bodepudi, A., & Reddy, M. (2018). Investigating the Prospects of Generative Artificial Intelligence. *Asian Journal of Humanity, Art and Literature*, *5*(2), 167–174. https://doi.org/10.18034/ajhal.v5i2.659

Mandapuram, M., Gutlapalli, S. S., Reddy, M., Bodepudi, A. (2020). Application of Artificial Intelligence (AI) Technologies to Accelerate Market Segmentation. *Global Disclosure of Economics and Business 9*(2), 141–150. https://doi.org/10.18034/gdeb.v9i2.662

Ramkumar, R., Rahul, R., & Gowtham, S. (2015). Anomaly Based Approach for Defending Denial of Service Attack in Web Traffic. *Compusoft, 4*(4), 1657-1664.

Reddy, M., Bodepudi, A., Mandapuram, M., & Gutlapalli, S. S. (2020). Face Detection and Recognition Techniques through the Cloud Network: An Exploratory Study. *ABC Journal of Advanced Research*, *9*(2), 103–114. https://doi.org/10.18034/abcjar.v9i2.660

Scheau, M. C., Arsene, A. L., Gerald, D. (2016). Phishing and E-Commerce: An Information Security Management Problem. *Journal of Defense Resources Management, 7*(1), 129-140.

Shang, Q. Y. (2013). Discussion on the Computer Security Technology and E-Commerce Transaction Security. *Applied Mechanics and Materials, 427-429*, (2724). https://doi.org/10.4028/www.scientific.net/AMM.427-429.2724

Thaduri, U. R., & Lal, K. (2020). Making a Dynamic Website: A Simple JavaScript Guide. *Technology & Management Review*, *5*, 15–27. https://upright.pub/index.php/tmr/article/view/81

Thaduri, U. R., Ballamudi, V. K. R., Dekkati, S., & Mandapuram, M. (2016). Making the Cloud Adoption Decisions: Gaining Advantages from Taking an Integrated Approach. *International Journal of Reciprocal Symmetry and Theoretical Physics*, *3*, 11–16. https://upright.pub/index.php/ijrstp/article/view/77

Thodupunori, S. R., & Gutlapalli, S. S. (2018). Overview of LeOra Software: A Statistical Tool for Decision Makers. *Technology & Management Review, 3*(1), 7–11.

--0--

Archive Link: https://abc.us.org/ojs/index.php/ajtp/issue/archive