Digitalization & Sustainability Review

Vol 3, No 1 (2023)

Evolution of the Cyber Security Threat: An Overview of the Scale of Cyber Threat

Takudzwa Fadziso, *Institute of Lifelong Learning and Development Studies, Chinhoyi University of Technology, ZIMBABWE*

Upendar Rao Thaduri, *ACE Developer, iMINDS Technology Systems, Inc., Pittsburgh, PA 15243, USA*

Sreekanth Dekkati, *Assistant Vice President (System Administrator), MUFG Bank, Arizona, USA*

Venkata Koteswara Rao Ballamudi, *Sr. Software Engineer, HTC Global Services, USA*

Harshith Desamsetti, *Senior Software Engineer, Charter Communications, Stamford, Connecticut, USA*

Abstract

It is impossible to dismiss the importance of cybersecurity in today's digital world. Even a single breach in security can result in the exposure of the personal information of millions of individuals. Because of these breaches, the organizations suffer significant financial repercussions, and their customers lose trust. As a result, adequate cyber security is necessary to safeguard individuals and businesses from spammers and other cybercriminals. The term "cyber security" refers to the collection of technologies, procedures, and practices intended to protect networks, devices, programs, and data from being attacked, damaged, or accessed without authorization. Information technology security is another term that can be used interchangeably with cyber security. This study sheds light on some tactics, rapid measures, and forward-looking perspectives about cyber security and cyber danger.

Keywords: Cyber Security, Security Threat, Network Security, Cloud Security

INTRODUCTION

Cybersecurity is becoming more critical as the number of users, devices, and programs in the modern company grows, as does the amount of sensitive or confidential data. Rising numbers and skills of cyber attackers and attack methods exacerbate the problem. Cybersecurity protects internet-connected gear, software, and data from cyberattacks (Rademaker, 2016). Individuals and businesses use it to secure data centers & other digital systems. A good cybersecurity plan can protect an enterprise or user's systems and sensitive data from hostile attacks. Cybersecurity protects against attacks that disable or impair systems or devices (Štitilis et al., 2016).

Cybersecurity protects internet-connected devices and services from hackers, spammers, and cybercriminals. Companies employ it to prevent phishing, ransomware, identity theft, data

breaches, and financial losses (Pinkston, 2016). Today, technology is more critical than ever in daily life. From near-instant Internet connection to smart home automation and the Internet of Things, this movement offers many benefits.

With so much good coming from technology, it's hard to imagine hazards exist behind every device and platform. Despite society's optimistic view of technology, cyber security threats are real. Cybercrime is rising, exposing faults in gadgets and services we rely on. We must define cyber security, why it's essential, and how to learn about it. Cyber security protects computers, servers, mobile devices, electronic systems, networks, and data against hackers (Gheyas & Abdallah, 2016). Information technology security or electronic information security are other names.

Cyber security protects devices and services from hackers, spammers, and cybercriminals (Hashim et al., 2016). Some cyber security components aim to strike first, but most specialists focus on safeguarding all assets, from PCs and cellphones to networks and databases, from attacks. In the media, cyber security refers to protecting against all forms of cybercrime, from identity theft to international digital weaponry. Although relevant, these designations fail to represent the true nature of cyber security for persons without a computer science degree or digital sector experience. Cisco Systems, a tech company focusing on networking, cloud, and security, defines cybersecurity as protecting systems, networks, and programs from digital threats (Jaganathan et al., 2015). Cyberattacks frequently try to access, change, or delete sensitive data, extort user money, or disrupt company activities.

IMPORTANCE OF CYBER SECURITY

The government, the military, corporations, the financial sector, and medical organizations acquire, store, and process vast volumes of data on computers and other devices. This highlights the need for cyber security. A sizeable amount of such data may contain sensitive information, including intellectual property, personal information, financial data, or other forms of data for which unauthorized access to or exposure to the data could have potentially detrimental effects (Gutlapalli et al., 2019). While doing business, organizations send sensitive data across networks and to other devices. The field of study known as cyber security is dedicated to securing the information itself and the systems used to handle or store it (Khan, 2011). Companies and organizations, mainly those responsible for preserving information linked to national security, health records, or financial records, must take precautions to protect their sensitive business and people information as the volume and sophistication of cyberattacks continue to expand. Even as early as March 2013, the highest-ranking intelligence authorities in the country issued a warning that cyber-attacks and digital surveillance are the most significant threat to national security, surpassing even the threat posed by terrorism (Shukla et al., 2023).

Networks, computers, other electronic devices, and software applications are all making significant contributions to the digitalization of human society. This has a positive impact on every facet of our life. Using computers and other digital devices, such as smartphones and tablets, is integral to the operations of all critical infrastructure, including healthcare, financial institutions, governments, and manufacturing (Reddyet al., 2020). The overwhelming majority of the devices

are linked to the internet. Threat actors currently have a more considerable incentive than ever before to find ways to breach those computer systems, whether for financial gain, extortion, political or social motives (also known as hacktivism), or simple vandalism.

Cyberattacks have been launched against essential infrastructure in every developed nation over the past two decades, and countless enterprises have suffered catastrophic losses. Every year, over 2,000 data breaches are confirmed worldwide, and the average cost of each breach is over $3.9 million (or $8.1 million in the United States). Since 2000, cybercriminals have stolen the personal information of nearly 3.5 billion people, equivalent to half of the planet's total population (Mandapuram, 2017a).

MANAGING CYBER SECURITY

Through its SafeOnline.org platform, the National Cyber Security Alliance advocates for a top-down approach to cyber security, in which corporate management takes the initiative to prioritize cyber security management across all business operations (Neghina & Scarlat, 2013). The NCSA recommends this strategy. The guidelines provided by the NCSA for conducting cyber risk assessments place a primary emphasis on three primary areas: identifying the "crown jewels" of your organization, which refers to the most valuable information that needs to be protected; identifying the threats and risks that face that information; and outlining the damage that our organization would incur should that data be lost or mistakenly exposed. Cyber risk assessments should consider regulations affecting how your firm collects, maintains, and secures data (Amin & Mandapuram, 2021). Some examples of such legislation include PCI-DSS, HIPAA, SOX, and FISMA. After analyzing the risks posed by cyberspace, you should devise and implement a strategy to reduce those risks, safeguard the "crown jewels" identified in the analysis, and effectively identify and respond to any security breaches that may occur. This plan must include not just the processes but also the technology that is necessary to construct an advanced cybersecurity program. As cyber security is an ever-evolving field, the industry's best practices must progress to keep up with the more sophisticated attacks by attackers (Li et al., 2013). The most effective protection method against cybercriminals attempting to access your firm's sensitive data is to combine strong cybersecurity measures with a workforce base that is both educated and aware of the importance of security (Mtsweni et al., 2016). Beginning on a small scale and concentrating on the information you deem to be the most sensitive will allow you to scale up your efforts as your cybersecurity program develops.

TYPES OF CYBER SECURITY

- Cybersecurity for critical infrastructure: Because SCADA (supervisory control and data acquisition) systems sometimes rely on older software, organizations responsible for critical infrastructure are frequently more susceptible to cyberattacks than other businesses. The NIS Regulations impose obligations on organizations that operate essential services in the United Kingdom's energy, transportation, health care, water, and digital infrastructure sectors and organizations that supply digital services (Mandapuram et al., 2020). The Regulations mandate that businesses put the necessary administrative and technological safeguards in place to mitigate the threats to their information security.

- Network security: Addressing vulnerabilities that influence our operating systems and network architecture, including servers & hosts, firewalls & wireless access points, and network protocols, is an integral part of network security.
- Cloud security refers to protecting sensitive information stored in the cloud, including applications, data, and physical infrastructure.
- Securing smart devices & networks that are connected to the Internet of Things (IoT) is part of what is meant by "Internet of Things" (IoT) security. IoT devices are things that connect to the internet without the need for human interaction. These devices include intelligent fire alarms, lighting, thermostats, and other home appliances.
- Application security entails resolving vulnerabilities resulting from unsafe development procedures in designing, coding, and publishing software or a website. Application security is also known as application protection.

EVOLUTION OF THE CYBER SECURITY THREAT

Even just a few years ago, cyber threats were not nearly as advanced as today. Because the landscape of cyber threats constantly shifts, enterprises require protection against hackers' current and future tools and strategies.

Gen V Assaults

The landscape of the threats posed by cyber security is constantly changing, and periodically, new generations of cyber threats emerge as a direct result of these improvements. Up until this point, we have seen five generations of cyber dangers and solutions aimed to protect against them. These include the following:

Gen I (Virus): Virus attacks against standalone computers in the late 1980s prompted the creation of the first antivirus systems.

Gen II (Network): When cyberattacks started coming in through the internet, a firewall was designed to detect and stop them.

Generation III (Applications): The widespread implementation of intrusion prevention systems (IPS) was a direct result of the widespread exploitation of vulnerabilities inside application software in Generation III (Applications).

Gen IV (Payload): As malware became more targeted and was able to circumvent signature-based defenses, anti-bot and sandboxing solutions became necessary to detect novel threats. Gen IV malware is referred to as "payload" malware.

Gen V (Mega): The most recent generation of cyber threats is known as Gen V (Mega), which employs large-scale, multi-vector attacks. Because of this, developing advanced threat protection solutions should be a top priority. Previous forms of cyber security have become either less effective over time or largely irrelevant as new generations of cyber threats emerge (Desamsetti & Mandapuram, 2017). Gen V cyber security solutions are required to protect against the present cyber threat landscape adequately.

Chain-attack supply

Many firms' security initiatives have centered on their apps and systems (Bodepudi et al., 2019). The corporate perimeter is hardened, and only authorized users and programs can access it to prevent cyber threat actors from breaching corporate networks. A spike in supply chain attacks has shown this approach's weaknesses and hackers' motivation and ability to exploit them. The SolarWinds, Microsoft Exchange Server, and Kaseya intrusions showed that trust ties with other companies could weaken company cyber security. A cyber threat actor can access all customer networks by exploiting one organization and abusing trust ties (Gutlapalli, 2017a). To prevent supply chain assaults, use zero trust security. Partnerships and vendor ties benefit the company, but third-party users and software should have limited access and be regulated.

Ransomware

Ransomware has been around for decades, but it has only become the dominating threat recently. WannaCry showed that ransomware assaults are profitable, sparking a boom in activities. Since then, ransomware has changed tremendously. Instead of encrypting files, ransomware now steals data to extort victims and clients in double and triple extortion assaults (Mandapuram et al., 2018). Some ransomware organizations threaten or use DDoS assaults to get victims to pay. Also helping ransomware expand is the ransomware as a Service (RaaS) concept, where developers give their virus to “affiliates” to distribute in exchange for a fee. Many cybercrime groups use RaaS to get advanced software, making sophisticated attacks more likely. Thus, ransomware protection is crucial to a company's cyber security.

Phishing

The most common and efficient way attackers get organizational access is through phishing assaults. Tricking a user into clicking a link or opening an attachment is more accessible than finding and exploiting an organization's defenses. In recent years, phishing assaults have become more sophisticated. The initial phishing scams were easy to spot, but modern ones are so convincing and clever that they can pass for legitimate emails. The current phishing threat requires more than employee cyber security awareness training (Mandapuram, 2017b). Cyber security systems must detect and stop phishing emails before they reach users' inboxes.

Malware

Malware evolution has characterized cyberattack generations. Cyber defenders and malware producers perform a constant cat-and-mouse game to defeat the latest defensive technology. Successful cyberattacks often inspire new ones (Chen et al., 2019). Modern malware is fast, stealthy, and intelligent. Legacy security technologies, such as signature-based detection, could be more effective, and security analysts often respond too late to a danger. No longer is detection "good enough" to prevent malware attacks. Gen V malware mitigation demands cyber security technologies that prevent attacks before they cause damage.

NEED FOR A CONSOLIDATED CYBER SECURITY ARCHITECTURE

Previously, businesses could get by with standalone security solutions tailored to target particular risks and use cases. Attacks by malicious software were less prevalent and less sophisticated, and the complexity of corporate infrastructures was reduced (Thaduri et al., 2016). In today's world, teams tasked with managing increasingly complex cybersecurity architectures frequently need help. This is due to several different variables, including the following:

- Sophisticated Attacks: Traditional computer security methods can no longer be used to identify sophisticated forms of online attack. It is vital to have greater visibility and conduct more in-depth investigations to identify campaigns run by advanced persistent threats (APTs) and other sophisticated cyber threat actors.
- Complicated Environments: The business network stretches across on-premises equipment and several cloud settings. Maintaining consistent security monitoring and policy enforcement across an organization's complete IT infrastructure makes it considerably more challenging.
- Heterogeneous Endpoints: Information technology is no longer limited to traditional desktop and laptop PCs. Because of developments in technology and the implementation of bring-your-own-device (BYOD) rules, it is now required for businesses to provide security measures for a wide variety of devices, some of which are not even owned by the organization.
- The response to the COVID-19 outbreak revealed that remote and hybrid work models were possible for many companies. This led to the rise of the phenomenon known as "the rise of remote work." Now more than ever, businesses require solutions that will enable them to safeguard their on-site personnel and remote workers successfully.
- It is impossible to scale up and be sustainable if one attempts to handle all of these problems using a variety of disconnected solutions. Companies can only correctly manage their cyber security risk if they consolidate and streamline their security infrastructures.

ACHIEVING COMPREHENSIVE CYBERSECURITY WITH CHECK POINT

Consolidated and created from technologies designed to function together, a contemporary cybersecurity infrastructure is intended to thwart cyberattacks. To accomplish this, our company must partner with a security provider with prior expertise in guarding an organization's assets against cyber threats (Patrick, 2004). Check Point can provide solutions for an organization's complete range of security requirements, including the following:

- Security for Computer Networks: Check Point Quantum
- Security for the Internet of Things provided by Check Point Quantum IoT Protect
- For security in the cloud, check out Check Point CloudGuard
- Application Security Provided by Check Point CloudGuard AppSec
- Check Point Harmony Endpoint, a security solution for endpoints
- Check Point Harmony Mobile is the Solution for Mobile Security.

TOP CYBERSECURITY CHALLENGES

Hackers, data loss, privacy concerns, changing cybersecurity techniques, and risk management all pose ongoing challenges to the security of computer networks (Dekkati et al., 2022). It is not anticipated that there will be a reduction in the number of cyberattacks shortly. In addition, there are now more access points for attacks, such as with the introduction of the Internet of Things (IoT), and the attack surface is rising, which makes it even more critical to secure networks and devices (Thodupunori & Gutlapalli, 2018). The constantly changing threats, the onslaught of data, the lack of cybersecurity awareness training, the personnel shortage and skills gap, and the hazards posed by third parties and supply chains are all significant concerns that must be handled consistently.

The ever-changing dangers

The ever-changing character of potential security breaches is one of the aspects of cybersecurity that presents the most significant challenge. New attack vectors become available as new technologies exist and existing technologies are exploited in novel or unconventional ways (Ballamudi et al., 2022). It can be challenging to keep up with the rapid changes and advancements in assaults and the need to update practices to protect against these changes and improvements. Concerns include ensuring that all branches of cybersecurity are kept up to date to provide adequate defense against any potential weaknesses. This can be incredibly challenging for smaller firms with insufficient organizational people or resources.

A flood of data

In addition, businesses can collect a large quantity of potential data about individuals who utilize one or more of their services. As more data is collected, there is a greater possibility that a cybercriminal will attempt to acquire personally identifiable information (PII). This raises a new set of concerns. An organization that, for instance, saves personally identifiable information on the cloud may be vulnerable to ransomware attacks (Bodepudi et al., 2021). A cloud security breach can be avoided if organizations take the necessary precautions.

Training for heightened awareness of cybersecurity

Education of end users is another component that should be included in cybersecurity programs. It is possible for employees, using their personal laptops or mobile devices, to inadvertently bring vulnerabilities and hazards into the workplace (Gutlapalli, 2017b). In the same vein, kids might engage in risky behavior, such as opening links or attachments from phishing emails and clicking on them. Employees will be better able to do their bit in protecting their organization from potential cyberattacks if they receive regular training on security awareness.

Shortage of available workers and a knowledge gap

A lack of appropriately trained employees is another obstacle that cybersecurity must overcome. As businesses continue to amass and use more significant quantities of data, there will be an

increased demand for cybersecurity personnel who can investigate, administer, and respond to events (Mandapuram & Hosen, 2018). (ISC) projected a 3.4 million worker gap between the number of essential cybersecurity positions and the number of security experts.

Attacks on the supply chain and dangers posed by third parties

Suppose the partners, suppliers, and third-party vendors that access an organization's network do not behave securely. In that case, the organization's most significant efforts to preserve security are for naught, even if those organizations do everything they can to do so. Attacks on supply chains that are software- and hardware-based are becoming increasingly difficult to combat on the front of information security (Deming et al., 2018). Organizations must handle the risk posed by third parties in the supply chain and decrease the problems associated with software delivery, for instance, by utilizing software bills of materials.

HOW IS AUTOMATION USED IN CYBERSECURITY?

Automation has developed into a crucial component in defending businesses from the increasing quantity and level of complexity of cyberattacks (Urciuoli et al., 2013). Artificial intelligence and machine learning can assist in improving cybersecurity in three primary categories if they are used in settings with vast volumes of data streams:

- Detection of potential dangers. Platforms powered by AI can do data analysis, identify previously discovered threats, and forecast the appearance of new hazards.
- A response to the threat. AI platforms also produce and automatically implement various sorts of security protection.
- Enhancement of the human race. Those who work in security are frequently inundated with repetitive notifications and tasks. AI has the potential to alleviate alert fatigue by automatically triaging low-risk warnings, automating extensive data analysis, and other repetitive duties, freeing up human workers to concentrate on more complex responsibilities.
- Additional advantages of implementing automation in cybersecurity include the categorization of attacks and malware, as well as the classification of traffic and compliance analysis.

CYBERSECURITY MYTHS

We know that the number of cyberattacks is expected to continue to rise. In the modern technological era, individuals and organizations alike are required to take precautions against a wide variety of potential dangers (Dekkati & Thaduri, 2017). Unfortunately, several misunderstandings regarding cybersecurity continue to discourage too many people from taking the steps necessary to protect sensitive personal information (Dinicu, 2014). The following are some frequent misconceptions about computer security that everyone should know.

- Relying entirely on passwords to safeguard one's data is not prudent; you can protect yourself by using passwords, but you shouldn't. Even if solid passwords are necessary, thieves may still discover a way to circumvent them. As a result, it is essential to put stringent cybersecurity measures in place to have a multilayered defense.

- Deleting the file from the computer: When you delete it from the computer, it goes to the Recycle Bin, & when you empty the Recycle Bin, the Recycle Bin is cleared out. Even after the data has been deleted, it is still on the hard drive, for example, in the folder designated for temporary files.
- Encryption solutions are not worth the investment: Some companies still believe that encryption software is an unnecessary expense for their company. It is a common misunderstanding that encryption will protect against data leaks. When it comes to protecting against cybercriminals and attacks by ransomware, encryption is a vital tool.
- Large companies are the only ones targeted by cybercriminals; small and medium-sized enterprises are not a concern for them (Desamsetti, 2016). It is a common misconception that only large corporations lack adequate security and are only targeted by cybercriminals. 61% of all small and medium firms reported having had at least one cyber assault during the year, as stated in the report on investigations into data breaches for 2021. Because these businesses employ less rigorous security procedures. As a result, it is essential to protect businesses from cybercrimes.

BUILDING A CYBER SECURITY STRATEGY

Senior management should support and share a cyber security strategy with the entire firm. Build your security plan using this process:

- Inventory computing assets, identifying apps, data, and potential harm in case of attack or compromise. List assets to safeguard.
- Identify threats and risks—assess industry-specific threats, prioritize relevant ones for your firm, and assess significant system vulnerability to attacks. For instance, a website operator should check its web applications for vulnerabilities like code injection and harmful bots.
- Identify the most significant risks based on system protection, compliance, and common threats. What systems are most valuable to the firm and potentially attacked? Target these threats first in your cybersecurity program.
- Assess security maturity and tooling—Does your company have a cybersecurity program? Are security services provided in-house or by vendors? Map existing cybersecurity measures. Consider physical facility security (a security guard, locked server rooms), security systems like firewalls & antivirus, and application and service security, including cloud services.
- Establish a cybersecurity team by utilizing existing staff, hiring new people, and consulting as needed. Improve your security by building a team that can execute a cybersecurity plan.
- Establish a cybersecurity timeline and goals, identifying immediate quick wins for essential system protection. What long-term cybersecurity precautions take time but are important? Create a 1-2-year long-term strategy with quarterly milestones for the security team.

CONCLUSION

Cybersecurity protects computer systems, back-end systems, & end-user applications, as well as the users of those systems and the data that those systems contain. This is similar to the goal of physical security, which is to safeguard people and physical property against criminal activity or accidental harm. Cyber security aims to prevent unauthorized users—criminals, malicious insiders, or others—from gaining access to, damaging, interrupting, or otherwise changing

information technology systems and applications. Our lives in this age of the internet are becoming increasingly reliant on activities such as banking, buying, and socializing that can be done online. The cloud, as well as our computers, are used to store photographs and other personal information. The likelihood of being a victim of cybercrime increases in tandem with the amount of our lives that are moved online. The practice of defending computer systems and networks against intrusion or attack by unauthorized users is referred to as cybersecurity. Individuals, organizations, and governments must invest in cybersecurity to safeguard their data and assets from thieves. Cybersecurity is of the utmost significance in a world increasingly dependent on the internet.

REFERENCES

Amin, R., & Mandapuram, M. (2021). CMS - Intelligent Machine Translation with Adaptation and AI. *ABC Journal of Advanced Research*, *10*(2), 199-206. https://doi.org/10.18034/abcjar.v10i2.693

Ballamudi, V. K. R., Desamsetti, H., & Mandapuram, M. (2022). Influence of Digitization on Human Resources (HR) Services and Processes. *ABC Research Alert*, *10*(3), 32–36. https://doi.org/10.18034/ra.v10i3.653

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

Bodepudi, A., Reddy, M., Gutlapalli, S. S., & Mandapuram, M. (2021). Algorithm Policy for the Authentication of Indirect Fingerprints Used in Cloud Computing. *American Journal of Trade and Policy*, *8*(3), 231–238. https://doi.org/10.18034/ajtp.v8i3.651

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

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., Gutlapalli, S. S., Thaduri, U. R., & Ballamudi, V. K. R. (2022). AI and Machine Learning for Remote Suspicious Action Detection and Recognition. *ABC Journal of Advanced Research*, *11*(2), 97-102. https://doi.org/10.18034/abcjar.v11i2.694

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. (2016). 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

Dinicu, A. (2014). Cyber threats to national security. Specific features and actors involved. *Scientific Bulletin - Nicolae Balcescu Land Forces Academy; Sibiu,* 19(2), 109-113.

Gheyas, I. A., & Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. *Big Data Anal, 1*. https://doi.org/10.1186/s41044-016-0006-0

Gutlapalli, S. S. (2017a). 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. (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., 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://doi.org/10.18034/mjmbr.v6i2.661

Hashim, M. S., Masrek, M. N., & Yunos, Z. (2016). Elements in the Cyber Security Framework for Protecting the Critical Information Infrastructure against Cyber Threats. *International Information Institute (Tokyo). Information; Koganei,* 19(7B), 2989-2994.

Jaganathan, V., Cherurveettil, P., Sivashanmugam, P. M. (2015). Using a Prediction Model to Manage Cyber Security Threats. *The Scientific World Journal, 2015*, Article ID 703713. https://doi.org/10.1155/2015/703713

Khan, F. U. (2011). States rather than criminals pose a greater threat to global cyber security: a critical analysis. *Strategic Studies; Islamabad,* XXXI(3).

Li, Z. W., Cheng, L., Zhang, H. L., & Tong, W. M. (2013). Communication and Cyber Security Analysis of Advanced Metering Infrastructure of Smart Grid. *Applied Mechanics and Materials 325–326*, 637–642. https://doi.org/10.4028/www.scientific.net/amm.325-326.637

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

Mtsweni, J, Mutemwa, M, Mkhonto, N. (2016). Development of a Cyber-Threat Intelligence-Sharing Model from Big Data Sources. *Yorktown Journal of Information Warfare, 15*(3), 56-68.

Neghina, D., Scarlat, E. (2013). Managing Information Technology Security in the Context of Cyber Crime Trends. *International Journal of Computers Communications & Control, 8*(1), 97-104. https://doi.org/10.15837/ijccc.2013.1.173

Patrick, R. B. (2004). IT security resource to foster cyber threat disclosure. *Network World Canada; Downsview***,** 14(5).

Pinkston, D. A. (2016). Inter-Korean Rivalry in the Cyber Domain: The North Korean Cyber Threat in the *Sŏn'gun* Era. *Georgetown Journal of International Affairs, 17*(3), 60-76. https://doi.org/10.1353/gia.2016.0037

Rademaker, M**.** (2016). Assessing Cyber Security 2015. *Information & Security; Sofia***,** 34(2), 93-104. https://doi.org/10.11610/isij.3407

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

Shukla, G. P., Chaudhary, P., Ghosh, P., Mandapuram, M., Gutlapalli, S. S., Lourens, M. (2023). Human resource management: a conceptual framework for comprehending the Internet of Things (IoT) and Machine Learning. *Official Journal of the Patent Office (IN)*, Issue No. 26/2023 (30/06/2023). Patent number 202321036845 A.

Štitilis, D., Pakutinskas, P., Malinauskaitė, I. (2016). Preconditions of sustainable ecosystem: cyber security policy and strategies. *Entrepreneurship and Sustainability Issues, 4*(2), 174-182. https://doi.org/10.9770/jesi.2016.4.2(5)

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.

Urciuoli, L., Männistö, T., Hintsa, J., Khan, T. (2013). Supply Chain Cyber Security - Potential Threats. *Information & Security; Sofia*, 29(1), 51-68.