International Journal of Modern Computation, Information, and Communication Technology
2023;6(1):25-30.
ISSN: 2581-5954

Investigation of Cyber Security Attacks and Security

A. KathijaNasreen[1*], N. Senthamilarasi[2], Monisha R[3]

[1]*Department of Computer Science and Engineering, RMK College of Engineering and Technology, Chennai, Tamil Nadu, India.*
[2]*Department of Information Technology, Panimalar Institute of Technology, Chennai, Tamil Nadu, India.*
[3]*Assistant Professor, Department of Management Studies, St. Joseph's College of Engineering, Chennai, Tamil Nadu, India.*

[*]*Corresponding author: kathijanasreencse@rmkcet.ac.in*

Abstract. Information security and cybersecurity are often used interchangeably; however, the latter recognizes the importance of humans as a target and an extra factor in the security process. However, including the ethical aspects of society in a discussion on cyber security has far-reaching implications. Several models and frameworks have been created to help with cyber security. The ideas of cybersecurity, including its infrastructure, workforce, and data pertaining to computerized personal information protection, are also introduced. In this article, look back at the history of efforts to counteract these dangers and discuss the strengths and weaknesses of these approaches. The paper also includes suggestions for more study.

Keywords: Cyber security, frameworks, workforces, threats, techniques

INTRODUCTION

Most today's economics, commercials, cultural, social, and governmental activity, and relationships between nations at all levels (individuals, NGOs, governments, and governmental institutions) take place in cyberspace. Cyber-attacks and the risk associated with wireless communications technology are a growing threat to businesses and governments throughout the globe. The modern worlds rely strongly on an electronic device, making cyber security a pressing concern. The goal of cyber assaults is to cause financial losses for targeted businesses [1]. Cyber-attacks might also serve military or political objectives. Computer viruses, information leaks, disruptions in the transfer of data, and other forms of attack are only some of the problems that might arise. To mitigate the effect of cyber assault, many businesses use numerous countermeasures. Cyber security is now based on constantly updated information systems data.

Researcher from all around the globe has offered many strategies for preventing or mitigating the effect of cyber assault. There are ways that are now in use and others that are still in the research stage. This research aims to analyze the obstacles, flaws, and strengths of the approach offered while also providing surveys and a complete analysis of the standard development provided in cyber security. There is much consideration given to several new forms of descendent assaults. Common security architectures are covered, along with their origins and first-generation cyber-security techniques. Cyber security, security risks, and issues, as well as new trends, are also discussed. Researchers in the fields of information technology and cyber security might perhaps benefit from the offered thorough review study [2].

In the last several years, data has been growing exponentially at an ever-increasing rate in volume and diversity. This has produced massive and complicated big data, posing difficulties in its storage, administration, analysis, and security. To streamline their big data operations, many companies are turning to cloud computing. However, many of these same companies aren't fully aware of the security and privacies challenges that cloud computing usage poses, and so they aren't taking the necessary precautions. As a result, greater investigation into these security concerns is needed to develop countermeasures for the cloud system setting. After examining papers released in 2019 and 2020, this article will conduct a cloud risk assessment case study at a Saudi Arabian company to compile a list of the most frequent cyber security risks in the cloud system environment and the most often employed mitigation measures [3].

Received: 13.03.2023 Revised: 24.04.2023 Accepted: 04.05.2023

Among the most potential network architectures for 6G is the spaces-airs-ground-seas integrated network (SAGSIN), which combines a satellite communications network with an aerials network, terrestrials' network, and marine communications network. SAGSIN presents numerous novel security issues because of its collaboration features of the multi-layers network, open communications environments, and time-varying topology; thus, several studies have been conducted on SAGSIN securities in recent years. As a result of this analysis, this paper provides comprehensive reviews of the state of SAGSIN security in terms of threat, attack methods, and defensive measures. To the best of knowledge, are the first to report the state-of-the-art in securities for SAGSIN since previous studies have only covered a subset of the integrated network, if any at all. Also, offer a few thoughts on cross-layers attack and securities countermeasures in SAGSINs, and highlight new issues and future research objectives in addition to analyzing previous studies on SAGSIN security [4].

Isolated customized systems are giving way to distributed systems that use general-purpose computer hosts, Internet of Things sensors, edge computing, wireless networks, and artificial intelligence to support critical infrastructure. While this shift enhances sensing and control capabilities and facilitates greater integration with business needs, it also makes these systems more vulnerable to assault by actors engaged in industrial espionage or sabotage. This study assesses the present status of cyber-security studies aimed at creating a country's water and waste-water treatment system safer for the public. Discuss the present state of cyber-securities for water systems, the challenge that used to be overcome, and the number of publications in this field [5].

LITERATURE SURVEY

The prevalence of cybercrime is increasing. Hackers, criminal organizations, and hostile nations pose financial risks to businesses throughout the globe. In recent years, cyber-attacks against small and medium-sized businesses (SMEs) have skyrocketed. Small and medium-sized enterprises (SMEs) often lack the knowledge and means to fully implement information security procedures. But the well-being of SMEs is essential to the public good: In Germany, for instance, small and medium-sized enterprises (SMEs) employ 38.8 percent of the workforce and produce 31.9 percent of the country's GDP [6]. Companies are encouraged to increase spending on information security by several rules and suggestions. However, knowledge gaps exist about the extent to which SMEs have adopted security measures, their perception of cybercrime risk, and their exposure to cyber-attacks. To fill this knowledge vacuum, conducted 5,000 CATI interviews with German small and medium-sized enterprise (SME) leaders. Discuss their encounters with cybercrime, how they handle information security, and how they evaluate risk [7].

Provide empirical findings on the extent to which small and medium-sized enterprise (SMEs) has adopted technological and organizational securities measures and a risk-aware mindset. Most businesses have implemented both fundamental security awareness and technology safeguards, as research shows. Find that small and medium-sized enterprises (SMEs) have varying rates of reporting cybercrime incidents depending on their sector, firm size, and level of security knowledge. Finish by offering suggestions for future researchers, businesses, and governments [8]. The spread of Covid-19 had a significant effect on how universities structured their course schedules. Since March 2020, there has been no other option for continuing the course but via distance learning. As a result of the Covid-19 epidemic, hitherto underutilized resources for online research have emerged as cloud computing, online learning platform, and video conference apps [9]. As a result, not only has the potential for DDoS/DoS assault, cross-site scripting, spoofing, unauthorized data accessing, infections with malicious applications, and thefts of personal data skyrocketed, but so has the potential for these threats. The findings of this study include not only suggestions for improving cyber security in e-learning environments but also categorizations of the types of assaults likely to do the most damage to the assets. System and patch management, access controls at the applications or resources levels, information classification, and the use of cryptographic protocol are all often cited best practices [10].

Some cities nowadays have adopted new technology and evolved into "smart cities." People's standard of living rises with the advent of new technology. However, each use of technology brings with it a set of fresh problems to solve. A smart city's security may be compromised by the careless actions of a single person or business. Cyber-securities concern (such as information leakages and harmful cyber-attack) in this sector impacts the behaviors of the smart city because of their dependence on information and communications technology [11]. As a result, cyber security must go in the same way smart city technologies are to react to the widespread enthusiasm for them. The focus of this research is to review the existing relevant literature on security in smart city technology and to discuss the explanation of cyber security. The current research endeavors to achieve this

goal by zeroing in on the four primary facets of smart cities: smart grids, smart buildings, smart transportation systems, and smart healthcare systems. Specific topics covered include a synopsis of two deep learning approaches, cyber-securities applications, and the relationship between technology and smart cities. Cyber securities and user privacies are also discussed, along with practical measures for ensuring their protection in smart cities [12].

Future developments in cyber-secure smart cities are outlined. Each security hole requires a unique set of solutions. This study's findings suggest that governments, technology manufacturers, and providers of IT security services will need to collaborate intensively to find solutions to these problems. To avoid financial, data, credit, and public-trust disasters that might result from a significant security incident, it is crucial to build adaptable systems with strong information protection capabilities [13]. With primary data and a quantitative study strategy in mind, the researcher set out to assess the efficacy of AI countermeasures against cyber security threats in the specific contexts of Iraq. The information was gathered from people currently employed in the IT sector by the researcher. The research included a total of 468 participants and included tests of hypothesis, discriminate validity, basic model analysis, and confirmatory component analysis. Except for the "expert system," which showed no significant relationship to AI or cyber security, all other factors were found to have statistically significant P-values. The primary challenges were related to distance, sample size, the number of variables considered, and accessibility [14-15].

PROPOSED SYSTEM

Every business and organization should address the problems of cyber security inside its IT system. In a nutshell, the capacity to safeguard sensitive information and client records from the prying eye of rivals is the key to a thriving cyber security business or corporation. Company and their rival are cruel to their client and consumers. To successfully launch and grow, a firm or organization must first ensure this safety. Information, network, and data might be protected from both external and internal danger with the use of cyber-security techniques. Professionals in cyber security are tasked with keeping online infrastructure secure. Cyber security safeguards this data by limiting access to just those who need it. Understanding the many kinds of cyber security is crucial for staying safe online. Safety in a Network Computer network needs to be secured so that they are not disrupted by malicious software or hackers. Network security refers to the measures taken by businesses to protect their computer networks against malicious software, hacking attempts, and other forms of intrusion. The overall layout of the proposed system is seen in Figure 1.

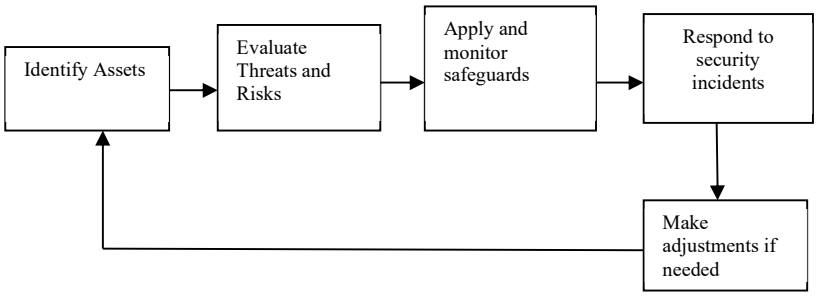

FIGURE 1. System architecture of the proposed system

Protection against outside interference with application development is achieved using hardware and software (such as anti-viruses and encryption software and a firewall). Data, whether digital or physical, must be protected against being seen, copied, modified, or deleted without permission. Data management and protection procedures constitute what is known as "operational security." For instance, procedures that dictate when and where data might be kept or exchanged and users' right to networking access. Information stored in the cloud (through the software) is safeguarded, and the threat of local assaults is mitigated thanks to constant monitoring. Training the User: Means human beings, a notoriously unpredictable variable in cyber security. A virus might inadvertently enter the system protection at any time. Every business needs comprehensive security strategies that include training employees to spot and delete malicious emails avoiding connecting to not known USB drives, and other important precautions. Any illegal action taken regarding computer hardware, software, or networks is considered a cybercrime.

There are two distinct categories of cybercrime: those that directly attack a computer network and those in which computers unwittingly facilitate criminal activity. Confidentiality, integrity, and availability are the cornerstones of every security system. These three tenets, known together as the CIA security triangle, have been the gold standard for system security from the very first computers. The idea of secrecy makes sure that only authorized individuals and entities have access to private data and procedures. Confidentiality in the military, for instance. According to the principle of integrities, only authorized personnel and resources should be able to make changes to or remove vital data and capabilities. The Integrity of a Database Is Compromised When. According to the SLA service level (Availability), system, function, and data should be made accessible on demand within predetermined limits. The finest cyber security practices go beyond the previously listed concepts. This weak protection may be easily broken by any skilled hacker. Cyber security challenges grow as an organization expands. The increasing overlap between the digital and physical spheres of information transmission presents another challenge for cyber security. The shortage of qualified workers is a major issue in cyber security.

Many individuals have a vague understanding of what constitutes "cyber security" at best. Cyberspace is a wide-ranging issue. This article provides overviews of the most general approaches to cyber security. A complete approach considers all these factors and more. The world's most important infrastructure is a hybrid of the cyber and physical worlds. The advantages of this magnificent building are many. However, exposing a system to the internet realm increases its susceptibility to breaches and other forms of cyber-attack. The potential effects of assaults on an organization's performance should be included in policy decisions. Several of the most promising up-and-coming hackers consider web application security to be an organization's greatest vulnerability. Excellent encryption is the foundation of secure applications. Each company has a unique strategy, which must be developed and executed by its leaders. This reduces the need for hacking and infiltrating data. The field of cyber security is growing more intricate. Companies must have a “security stance” toward understanding cyber security. Keeping ahead of cybercriminals always requires a high level of protection. Investments in cyber-security systems and services are growing because of an increase in security startups.

RESULTS AND DISCUSSIONS

The participants were business majors at an urban-like suburban institution in the middle of the United States. Most of the students do not reside on campus and hold down at least part-time employment. On average, participants were 23.9 years old (with a standard deviation of 5.6), with 8.2 percent being sophomores, 73.2% being juniors, and 18.5 percent being seniors. There were little over 45% male participants and a little fewer than 61% female1. While Rhee and colleagues (2009) raised concerns about the generalizability of results from research with students standing in for actual managers, the current investigation does not use such a method. The purposes of this study are to investigate the connection between Internet security knowledge and more secure password practices. Everyone involved is a consumer. Participants were welcomed by the activity leader upon entering the computer lab and were then divided into two groups, one receiving more information than the other. Participants were instructed to visit a study-related website, where they would be prompted to register and choose a unique password. The study's primary pre-treatment dependent variable was this password, which was generated before any experimental modification took place. After checking in, users were shown a page prompting them to fill out their profile information. This included fields for entering their name and email address.

It was stressed to participants that they needed to remember their password and username so that they could log back in after two weeks and finish the research. Participants were given a presentation about the research once they connected to their computers, made a password, and filled out their profiles. This lecture either provided a broad overview of password and computer security (the low-information conditions) or a deep dive into the topic (the high-information condition). The effects of cyber security issues on incident responders are shown in Figure 2. Cyber assaults and data breaches occurred at the firms during the previous two years, as shown in Figure 3.

Within events, there was no randomization of treatments. Thus, everyone got the same thing. Participants in the low-information treatments entered the systems and were given a brief on the things they would complete when they returned two weeks later. They were told that their participation in the experiments was a small element of a bigger study comparing the results of standard job selection exams given using a computer to those given using paper and pencil. In addition, participants were provided with some background reading on passwords in general. They were instructed to use passwords that were at least eight characters long and had a combination of capital and lowercase letters, numerals, and punctuation marks (for example, SAial.04?). About an hour of each participant's time was needed in the low-information conditions.

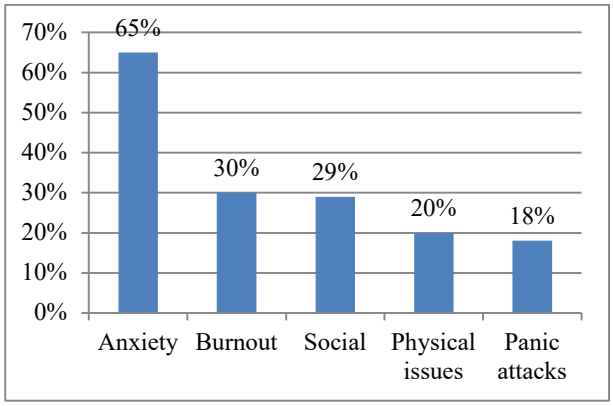

FIGURE 2. Impacts of cyber security incidents

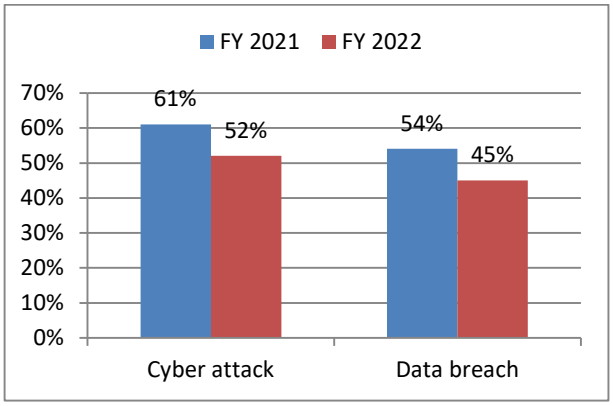

FIGURE 3. Cyber-attacks and Data breaches occurred in the organization.

Participants in this condition learned about the validity and utility of the employment-related measures (such as the NEO-FFI) they had previously completed (like how conscientiousness has been proven to predict work success). In the high-information treatment, users were given a briefing like what is discussed in the "Need for Information Security" portion of this page, after which they were given the same instructions for creating a strong password. Stories about criminal organizations' assaults on Internet banking were featured, as were screenshots and images of hackers' requests for money. They were never told the results of the tests they took. These individuals spent around an hour in the high-information condition. Two weeks transpired between Time 1 and Time 2 to offer solid proof of the impact of threats information on password resilience. After two weeks, everyone went back to the lab and logged back into the website. After a subject signed in, error messages informed them that their passwords had expired because of inactivity during the previous two weeks. To proceed, subjects were given the task of generating a new password, which served as the study's second crucial dependent variable.

After entering their new password, participants took three surveys through the system. These evaluations were designed to conceal the true nature of the research. Initially, participants filled out the NEO-FFI personality tests created by Costa and McCrae, which evaluated traits including extraversion, agreeableness, openness to new experiences, and emotional stability. Second, participants filled out the computer attitudes scales created by Loyd and Gressard to gauge their level of computer literacy and confidence. At the end of the study, participants filled out a demographics survey. Students were asked about their graduation year, genders, races, ages, place of birth (if not the US), and native languages (if not English) on the survey. Subjects then signed off the computers and conducted a timed papers-and-pencils intelligence exam, the Wonderlic Personnel exam, after completing the online measurements. Students were unable to articulate the study's rationale in post-experiment debriefs.

CONCLUSIONS

The bulk of research has focused on email security, firewalls, and vulnerabilities. However, there haven't been many investigations on password safety. While there are certain best practices for protecting the password, there is no verified methodology in place to safeguard the system itself. To guarantee that passwords are secure, additional research is required in terms of techniques and models from this angle. In the modern day, cyberspace and associated technologies represent a significant source of energy. Cyberspace's characteristics—including its low barriers to entry, anonymities, vulnerability, and asymmetries—have given rise to the phenomenon of power dissipations, meaning that if governments have so far divided the games of power among themselves, then it should be another actor, including private company, organized terrorists and criminal group, and individual. It's obvious that this won't compromise governmental efforts to ensure citizens' safety.

REFERENCES

[1]. Y. Li, and Q. Liu, 2021, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports*," **7**, pp. 8176-8186.

[2]. R. Al Nafea, and M. A. Almaiah, 2021, "Cyber security threats in cloud: Literature review," *International conference on information technology*," pp. 779-786.

[3]. H. Guo, J. Li, J. Liu, N. Tian, and N. Kato, 2021, "A survey on space-air-ground-sea integrated network security in 6G," *IEEE Communications Surveys and Tutorials*, **24(1)**, pp. 53-87.

[4]. B. Gunes, G. Kayisoglu, and P. Bolat, 2021, "Cyber security risk assessment for seaports: A case study of a container port," *Computers and Security*, **103**, pp. 1-6.

[5]. N. Huaman, B. von Skarczinski, C. Stransky, D. Wermke, Y. Acar, A. Dreißigacker, and S. Fahl, 2021, "A {Large-Scale} Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises," *In 30th USENIX Security Symposium*. pp. 1-7.

[6]. L.A. Alexei, and A. Alexei, 2021, "Cyber security threat analysis in higher education institutions as a result of distance learning," *International Journal of Scientific and Technology Research*," **31(3)**, pp. 128-133.

[7]. C. Ma, 2021, "Smart city and cyber-security; technologies used, leading challenges and future recommendations," *Energy Reports*," **7**, pp. 7999-8012.

[8]. B. Alhayani, H. J. Mohammed, I.Z. Chaloob, and J.S. Ahmed, 2021, "Effectiveness of artificial intelligence techniques against cybersecurity risks apply of the IT industry," *Materials Today: Proceedings*, pp. 1-7.

[9]. W. Ahmad, A. Rasool, A.R. Javed, T. Baker, and Z. Jalil, 2021, "Cyber security in IoT-based cloud computing: A comprehensive survey," *Electronics*, **11(1)**, pp. 1-8.

[10]. H.S. Lallie, L.A. Shepherd, J.R. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens, 2021, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Computers & security*, **105**, pp. 1-5.

[11]. K. Khando, S. Gao, SM. Islam, and A. Salman, 2021, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," *Computers & security*, **106(2021)**, pp. 1-22.

[12]. X. Sun, FR. Yu, and P. Zhang, 2021, "A survey on cyber-security of connected and autonomous vehicles (CAVs)," *IEEE Transactions on Intelligent Transportation Systems*, **23(7)**, pp. 6240-6259.

[13]. T.R. Reshmi, 2021, "Information security breaches due to ransomware attacks-a systematic literature review," *International Journal of Information Management Data Insights*, **1(2)**, pp. 1-6.

[14]. N. Jan, A. Nasir, M.S. Alhilal, S.U. Khan, D. Pamucar, and A. Alothaim, 2021, "Investigation of cyber-security and cyber-crimes in oil and gas sectors using the innovative structures of complex intuitionistic fuzzy relations," *Entropy*," **23(09)**, pp. 1-8.

[15]. R. Kumar, S. Sharma, C. Vachhani, and N. Yadav, 2022, "What changed in the cyber-security after COVID-19?" *Computers and Security*, **120**, pp. 1-9.