

# Evolution and technological competence of the cyber security - A comprehensive review

Rahul Kumar Sahu <sup>a</sup>, Raghavendra Prasad <sup>b\*</sup>

<sup>a, b</sup> Amity University Chhattisgarh

**\*Corresponding Author  
Raghavendra Prasad**

**Abstract:** Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber-attacks. Its objectives are to lower the danger of cyberattacks and safeguard against the unauthorised use of technology, networks, and systems (Sun et al., 2016). Cybersecurity refers to defending electronic systems, including vital information infrastructure, against misuse, attack, and sabotage as well as financial espionage. The term "cyber security" refers to preventing any type of illegal and malicious access. This review paper roll on machine learning IoT (Gulati et al., 2021). The cyber-world Cybersecurity is a set of different techniques, devices, and methods used to defend cyberspace against cyber-attacks and cyber threat most of the economic, commercial, cultural, social and governmental activities and interactions of countries, at all levels, new ideas and technics are including individuals, non-governmental organizations and government and governmental institutions, are carried out in cyberspace. The national strategy to secure cyberspace and various government policies have been discussed. (Srinivas et al., 2018). We then discuss the cyber security incident management rah and its various purposes.(Jenab & Moslehpour, 2016).We also discuss the standardization challenges in cyber security. We list and discuss the cyber-attacks and crimes, security requirements and measures(Reddy & Reddy, n.d.)

**Keywords :**Security, cyber-attacks, unauthorized access, phishing detection, cyber-crimes, threats and malware.

## 1 Introduction –

The techniques set to protect the cyber environment from cyber-crimes of the user is called Cyber security the devices, networks, application etc ,this environment uses the user (Khurana, 2017) in the branch of computer security the main Cyber security is related to internet and web application. (Reddy & Reddy, n.d.) objective is to project the device using various rules and to establish various measures against attack over the internet.(Khurana, 2017) To day cyberspace cyberworld in the world is rapid growth experiencing in today (Arora, 2016). Such an extraordinary growth in information- access gives opportunities to those with malicious intentions and unauthorized access It is the need of the hour(Kruse et al., 2017). In recent years and the present age ,the cyber security has gained a lot of attention in the research community. The cyber security makes protection of information systems and protect the data from cyber thief such as hardware, software and related infrastructure . (Ghelani, 2022) data on these systems and the services provided by these systems a layer protecting software, which can be done by illegal access by adversaries (intruders or attackers), and also can be caused by harm or misuse. Sometimes, intentionally a harm can be caused by an operator of the system. Therefore, either intentional or accidental harm can result in failing to obey the security procedures(Srinivas et al., 2018).

Cyber security is the techniques set to protect the cyber environment of the user. the devices, networks, application etc .This environment includes the user security to protect information and data from virus. (Khurana, 2017) Cyber security is the branch of computer security related to internet. The main security (Reddy & Reddy, n.d.)objective is to project the device using various rules and to establish various measures against attack over the internet.(Reeves et al., 2021) Even the latest technologies like cloud computing, mobile computing, E-commerce, net banking etc also needs high level of security for protect the system from unauthorized access .(Reddy & Reddy, n.d.). The number of security incidents rises and involved in protecting system. According to research, over 60% of businesses use technical information and data security countermeasures such as antivirus software, firewalls, anti-spyware software, virtual private networks (VPNs), vulnerability/patch management, and data encryption in transit, and intrusion detection systems (Ghelani, 2022).These reports also point out that organizations have been continuously subjected to targeted attacks to steal information. These same studies also show that security risk rises due to increased internal and external threats malware and viruses (Ghelani, 2022). The Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy. The fight against cyber-crime needs a high level security system comprehensive and a safer approach (Reddy & Reddy, n.d.). This paper will concentrate primarily on the fundamental nature of security in general and seek to illustrate, through examples that the purpose of cyber security assets is to protect an additional dimension that stretches beyond traditional information security boundaries, although this is not generally the case for information security where harm is often indirect(Taylor et al., 2019).

All systems must be designed to ensure security. It means that the main security objectives have to be satisfied and be protected Main security objectives are confidentiality, integrity, and availability (CIA triad). The exact identification of vulnerabilities and kinds of cyber-security threats in smart grid enables describing appropriate countermeasures and counter cyber-attack (Gunduz & Das, 2019). So, we present attack taxonomies according to CIA triad, and network layers. Also, we discuss how to enable secure smart grid communication system with highlight some of the latest solutions based on the IoT paradigm to phishing detection (Jain & Gupta, 2017). Then we summarize the existing state of the topic and future sights. Additionally, Researchers may have a more

understanding and the research trends of smart grid security system in the study (Gunduz & Das, 2019). Securing cyberspace is hard because the architecture of the internet was designed to promote connectivity, not security and we need to secure the information. Its founders focused on getting it to work and did not worry much about threats because the network was affiliated with America's military (Chongrui et al., 2018). As hackers turned up, layers of security, from antivirus programs to firewalls, were added to try to keep them at bay. Gartner, a research firm, reckons that last year organizations around the globe spent \$67 billion on information security (Jenab & Moslehpour, 2016).

### **Importance of standards in information security and cyber defence**

In information security the following important reasons are behind the development of standards, which play a crucial role in enhancing approaches to information security across various geographical regions and also the communities (Srinivas et al., 2018). Entitle various products or methods and technics which need to be compared significantly. Facilitate the systems integration and interoperability. Provide a means for users to evaluate new product (Sun et al., 2018). Improvement in the efficiency and effectiveness of key processes. cyber-attacks and cyber security Emerging trends and recent developments and improvements (Srinivas et al., 2018).

**Virus ,Threats of Cyber Security-** Malicious software a computer user can be forced sometimes to download a software onto a computer that is of malicious intent and threats ,Such software comes in many forms, such as viruses, Trojan horses, and worms .(Elmaghraby & Losavio, 2014),virus It is the type of malicious software that, when executed replicates itself by modifying other computer programs and software. Computer viruses causes economic damage and information loss due to system failure ,corrupting data, increasing maintenance cost etc(Khurana, 2017).

**Research Goal and Reconnaissance attack-** The purpose of this research is to existing studies their findings and summarize the efforts of research into blockchain applications for cyber security to make high level a protective layer. To assist in focusing the work, we developed three research questions, which are shown in(Taylor et al., 2019),an attack in which the perpetrator maps with targeted systems to scan any vulnerability in the machine to gather information and steal data. This is a kind of scenario similar to stealing for instance in the house which is vulnerable to break locks, doors, and windows that are not strong and are joined and gain unauthorized access. (Kaur & Ramkumar, 2021) . Attacks classification This section introduces multifarious types of attacks in different domains and is further categorized as shown in internet and many websites and web applications .(Kaur & Ramkumar, 2021) Securing cyberspace is hard because the architecture of the internet was designed to promote connectivity, not security. Its founders focused on getting it to work and did not worry much about threats because the network was affiliated with America's military for defence .(Qabajeh et al., 2018) As hackers turned up, layers of security, from antivirus programs to firewalls, were added to try to keep them at bay. Gartner, a research firm, reckons that last year organizations around the globe spent \$67 billion on information security and data security .(Jenab & Moslehpour, 2016)

### **Literature review**

**History of Cyber Security Attacks-**(1980) Corporation (DEC) computer system that was used for developing their RSTS/E operating system for PDP-X series computers. He broke into the DEC Palo Alto Research Center and illegally duplicated their software and running system , a crime for which he was charged and convicted of in (1980-1988).(A *History of Cyber Security Attacks 1980*, 1980). (1999) The process of digitization in all aspects of human life, like healthcare, education, business, etc., has gradually led to the storage of all sorts of information and exploring new technics, the cybercrime rate also increases both in number and complexity.(Li et al., 2020). (2001) including sensitive data. Security, is the process of protecting the digitized information from theft or from physical damage while maintaining system and the confidentiality and availability of information and data but as technology is growing rapidly.(Li et al., 2020). (2009)-In this article, we argue that one reason for these findings is that employees become fatigued. For example, employees may find that the actions required to maintain cyber security to prevent cyber-crimes are overwhelming and tiresome and, as a result, they disengage from security-related behaviour.(Reeves et al., 2021). (Advantage of IoT) Internet of things is the revolution of the Internet and machine-to-machine (M2M) communication. IoT means connecting different devices via the Internet or IP-based solutions and control the system by using software. There will be 28.5 billion networked devices by 2022 .A device can be anything like fridge, sensor, air-conditioner, mobile phone .(Gunduz & Das, 2019). (2017) The internet usage rate was 48% globally, later it increased to 81% for developing countries. In 2017 The broad spectrum of the cyberspace embraces the internet, users, the system resources, The cyber-world Cybersecurity is a set of different techniques, devices, and methods used to defend cyberspace against cyber-attacks and cyber threats.(Shaukat et al., n.d.) . (At present age) most of the economic, commercial, cultural, social and governmental activities and interactions of countries, at all levels, new ideas and technics are including individuals, non-governmental organizations and government and governmental institutions, are carried out in cyberspace.(A *History of Cyber Security Attacks 1980*, 1980)

**Fundamental concepts-**Cyber-attacks fall into a broader context than what is traditionally called information and technical operations. Information technical operations integrated use of the main capabilities of electronic warfare, psychological, computer network, military trickery and security operations in coordination with special support and relevant abilities describes the anatomy of a cyber-attack. .(Kaur & Ramkumar, 2021). In 2004, the National Institute of Standards and Technology (NIST) published the document and files titled System Protection and security Profile - Industrial Control Systems which covers the risks and objective of SCADA and In 2005, a predecessor of the Centre for the Protection and providing security of National Infrastructure (CPNI) in the UK, published a good practice guide for firewall deployment in SCADA(Blyth et al., 2015). Cyber security is that the main a part of technologies practices and processes designed to shield network computers programs from attack damage or unauthorized

access. The word security implies cyber security. All the sectors like financial institutions ,business ,government corporations .So growing volume of cyber-attacks. (Chongrui et al., 2018)

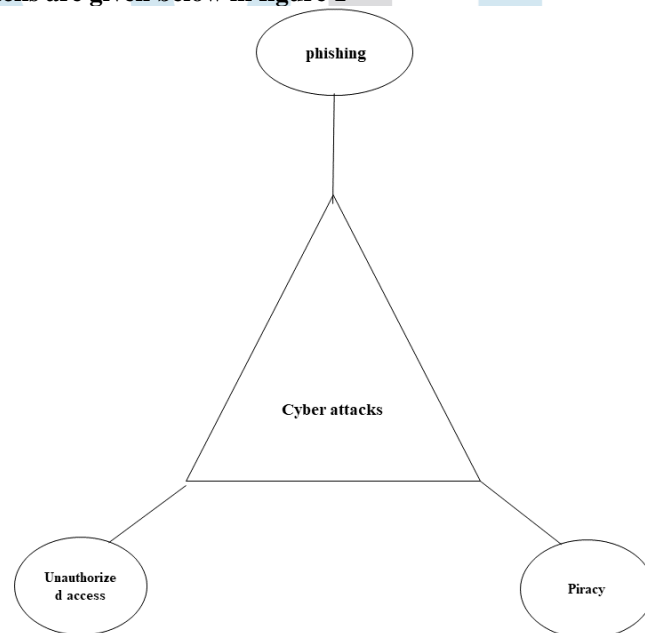
**Challenges of Trying to Keep a Step Ahead-**Considerations with Social Engineering Training and Awareness Programs for Security, The efficiency of organizational information systems in countering social engineering threats, malwares necessitates the combination of advanced technical measures along with managerial efforts to raise awareness of personnel and individual security to disable malicious attempts.(Aldawood & Skinner, 2019)

**Cyber-crimes, security requirements and measure-**In this section, we first discuss various cyber-attacks and crime. After that we also discuss the security major requirements and measures for cyber security(Srinivas et al., 2018). Passwords are “secret” words or phrases used by many sites and organizations to identify users prevent cyber-attacks security. Passwords are unfortunately a large security threat because they are vulnerable to being broken or guessed by a person or program hackers who done the cyber-attacks (Jenab & Moslehpour, 2016). There are also some security requirements and security operation in addition to the CIA triad to ensure cyber-security in smart grid applications. Many of these are interrelated. Therefore, to achieve a holistic cyber-security approach, the provision of aim and requirements should be ensured legally(Gunduz & Das, 2019).

**Piracy and virus-** from figure 1 present world facing the one of the major problem of cyber-attack piracy. The illegal copying of books, video, tapes and stealing of information called piracy a virus is considered as an infectious program. It attaches itself to some other software (program) and reproduces itself when the software is executed and make error on program. Typically, virus spreads through sharing of infected software or files among different sources one to another devices, such as computers and smartphone(Srinivas et al., 2018).

**Cyber Security Techniques and Unauthorized access -** Cyber-attacks on cyberspace can grow by capitalizing on new techniques and new programs. Cybercriminals will most frequently change the current malware signatures to take advantage of new technical faults and errors. In other instances, they actually search for special features and technics of emerging technology to detect weaknesses in malware injection (Li et al., 2020). In this case from Figure 1 we know unauthorized access is a major problem of cyberattacks, someone can gain access to a program, server, website, service, or even other system using someone’s account or other modes and he/she has advantage to using files without access it is treated as an unauthorized access, For instance, if an adversary can keep guessing password or user identity for an account until he/she gains access, (Srinivas et al., 2018).

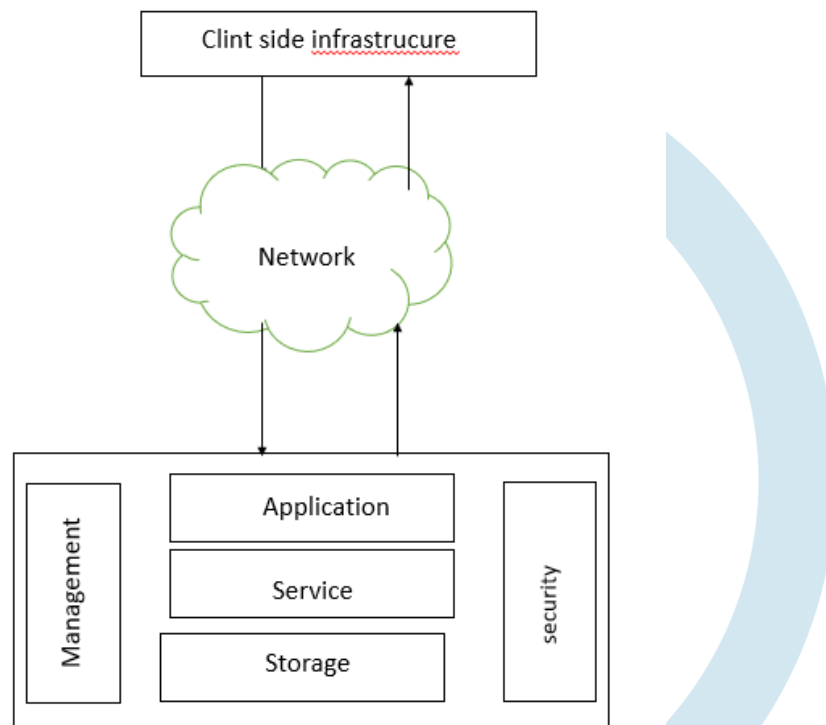
The major types of cyber-attacks are given below in figure 1 –



**Figure 1: popular major types of cyberattacks**

**Cybersecurity in IoT Architecture-** Since each layer of the IoT architecture has unique errors security issues and interacts with other layers, security measures should be considered for the entire architecture. A literature review of cybersecurity technologies through the lens of the Internet of Things architecture helps us have a systematic and integrative view of the IoT cybersecurity. Lee’s five-layer architecture of enterprise IoT and focuses on the layer-level cybersecurity issues and solutions (Lee, 2020). the latest security focused blockchain applications It is important to stress that this systematic literature review has focused on cyber security applications of blockchain and no other potential or existing applications to cyber-attacks, such as healthcare and logistics. The opportunities to improve security of the Internet of things are clearly abundant to focused things when consideration is given to the fact that almost half of all published cyber security blockchain application concerned IoT(Taylor et al., 2019).

**Cloud computing architectural framework & habituation of actions and to advice** – In this section, the basic cloud computing architectural framework is presented, shown to understand the security issues, first it is important to understand the basic concept and framework of cloud computing major requirements. The NIST defines three service delivery models, five essential characteristics, and four deployment models, that is widely accepted (Singh & Chatterjee, 2017). Employees form cyber security habits through their daily interactions for work with cyber security-related tasks. Cybersecurity-related stimuli can include notifications instructions to employees receive such as an SSL warning on a website, and reminders and key points for cyber security from Other sources (e.g., educational stimuli presented as important part of cyber security training, or warnings of data breaches in the media) (Reeves et al., 2021).



**Figure 2: cloud computing architecture**

**Machine learning based cyber security**-Exploring Security Data set security datasets typically represent a collection of information records consisting of several security features and related facts that can be used for the purpose of building security system a data-driven cybersecurity intrusion detection model (Intrusion & Model, 2020). thus it is important to understand the nature of raw cybersecurity data and the patterns and terminology of security incidents in order to detect malicious behaviour or anomalies In this work (Intrusion & Model, 2020).

**Cyber threats and Phishing attack**- Machine learning techniques and operations are playing a vital role in fighting against cybersecurity threats, malwares and attacks such as intrusion detection system, malware detection phishing detection, spam detection, and fraud detection, virus detection to prevent cyber-attacks name A few. We will focus on malware detection, intrusion detection system, and spam classification for this review (Shaukat et al., n.d.). Victim's Age: performed a role-play demographics and phishing susceptibility. Targeted victims: They found that participants' age linearly predicts their susceptibility to phishing. Older one was less likely to fall prey for phishing, while younger users particularly between the age of 18–25 consistently more vulnerable to phishing attack (Mughaid et al., 2022).

**Cyber security phishing detection system & Case study analysis** - In general, anti-phishing approaches exist to prevent phishing attacks and crimes. In this study, we explore several existing anti-phishing related works and new technics, visual similarities and web browser plug-in toolbars for phishing attack detection systems focusing on feature-based, content based or heuristic and blacklist-based approaches (Barraclough et al., 2021). The system specifications used for this project is Intel core i5 with 8GB RAM and 5GB free hard disk space. we can use Google cloud service to implement the project. It was performed on GNU/Linux (can also be performed on Windows /Mac OS). Project is written in Python using its libraries in Jupyter Notebook. Alternatively,

**Cybersecurity and Health Care**-Cyber-attacks in the industry and consumer and customer sectors have been widely echoed in the past and recent cyber-attacks in the healthcare sector are of concern. Recently, for example, the attacks on health systems make error and the potential vulnerabilities that have come to light for some types of critical medical sources, (Giansanti, 2021). Cybersecurity should be a key part of patient care culture as convenient and insecure processes must be replaced with more secure many health department facing challenges substantive approaches. This means not simply being seen to be secure. Cyber-insurance

is a rapidly growing business with estimated global sales of \$7.5 billion by 2020.(Coventry & Branley, 2018). Only recently, however, has the problem begun to be given due attention. In the current healthcare sector, the criticality relating to the extraordinary diffusion of innovative technologies (e.g., artificial pancreas, pacemakers) connected to the network in the healthcare sector (over 300,000 classes of Medical Devices)(Giansanti, 2021)<sup>1</sup>

**Cyber security in robotics and Robot application domains-** Cyber security in robotics is big challenge for us because protect automatic devices from cyber-attacks. Robotic systems have aided various technological developments during the previous decade. During the 1990s, robotic and network technologies were combined to expand the range of functional values of the robots, e.g. Electric vehicle .(Sayeed et al., 2022)Robots have been deployed in different domains and employed in different fields, including civilian and military ones, which are summarized. The various robotic usages in different fields of operations for many tasks and purposes such as photography, product delivery, agriculture, wildlife monitoring, policing, search and rescue, emergency response and science.(Hassan et al., 2022)

**Wireless automatic system-** We are directly connected to the Internet via communication protocols such as Wi-Fi (802.11), Hotspots, Bluetooth and numerous other communication protocols. These networks consist of devices known as “Things” which can be constrained by hardware shortcomings that reduce their security effectiveness in protecting protocols. Objects in the higher powered computers like Transmission Control Protocol (TCP).(Mcdaid et al., 2021).

### Discussion-

Discussion Although several review paper efforts have been directed towards cybersecurity information and types of cyber security, discussed in Background “Cybersecurity data science”, and “Machine learning tasks in cybersecurity” sections in different directions, this paper presents a comprehensive view of cybersecurity data science. For this, we have conducted a literature review to understand cybersecurity data, various defence strategies and preventing unauthorized access strategies including intrusion detection, malware detection, virus detection techniques, different types of machine learning techniques and many types of IoT detection system in cybersecurity tasks. Based on our discussion on existing work, several review issues related to security datasets, data quality problems, policy rule generation, learning methods, data protection, feature engineering, security alert generation, recency analysis etc. we are identified that require further review attention in the domain of Cybersecurity data science. To scope of cybersecurity data science is broad. Several data-driven tasks such as intrusion detection and prevention unauthorized access, control management, security policy generation, anomaly detection, spam fraud detection and prevention, various types of malware attack detection and defence strategies, etc. can be considered as the scope of cybersecurity data science. Although in this paper, we discuss cybersecurity data science focusing on examining raw security data to data-driven decision making for intelligent security solutions, it could also be related to big data analytics in terms of data processing and decision making, several advanced data analysis techniques such as AI, data mining, machine learning could play an important role in processing big data by converting big problems to small problems.

### Some discussion question answer ?

**How to measure secure server?** Secure servers use the Secure Sockets Layer (SSL) protocol for data encryption and decryption to protect data from unauthorized interception.

Here are four simple ways to secure server: -

**Step 1:** Make sure you have a secure password for your root and administrator users,

**Step 2:** The next thing you need to do is make new users on your system. These will be the users you use to manage the system,

**Step 3:** Remove remote access from the default root/administrator accounts,

**Step 4:** The next step is to configure your firewall rules for remote access

**Cyber security phishing detection system?**In general, anti-phishing approaches exist to prevent phishing attacks and crimes. In this study, we explore several existing anti-phishing related works and new technics, visual similarities and web browser plug-in toolbars for phishing attack detection systems focusing on feature-based, content based or heuristic and blacklist-based approaches.

**Risk, Vulnerability & Threat in a network?** Threat someone with the potential to harm a system or an organization vulnerability, Weakness in a system that can be exploited by a potential hacker risk: Potential for loss or damage when threat exploits a vulnerability.

**What is Robotic Cybersecurity?** Cyber security in robotics is big challenge for us because protect automatic devices from cyber-attacks, robotic systems have aided various technological developments during the previous decade. During the 1990s, robotic and network technologies were combined to expand the range of functional values of the robots, e.g. Electric vehicle

### Future Work

Cyberspace security faces a lot of challenges and opportunities. In the future we have new ideas and technics and some new topics should be paid more attention. First, human-factor security is an interdisciplinary topic, intrusion-tolerant cryptography is an

important issue for new networks, such as 5G/6G. Third, the applications of cyberspace security (Wu et al., 2018). Currently, most of the web applications and android applications adopt the registration of the user name and the password, E-mail, or the phone number and one-time password system so that it concludes difficult to confirm the identity and easy to steal and abuse the identity. but it also discloses the real identity information for many applications(Zou et al., 2012). In recent days, the demand for cyber security and protection against various types of cyber-attacks and crimes has been ever increasing day by day .The main reason is the popularity of Internet-of-Things (IoT), the tremendous growth of computer networks and speed of internet , and the huge number of relevant applications that are used by individuals or groups for the purpose of either personal or commercial use(Intrusion & Model, 2020). In 2018, 35% of Chief Cyber Security Officers reported employee security education and training as the highest priority to ensure cyber security to prevent stealing information, outweighing infrastructure upgrades, breach defence and network defence (Financial Services Information Sharing and Analysis Canter 2018). To facilitate this, organizations have invested in security education, training, and awareness (SETA) programs for their employees(Reeves et al., 2021).

### Conclusion:

In this present age every day internet speed and numbers of new software are increasing and many server junction and stations are need to a protective layer from unauthorized access from cyber thief's and hackers to protect information and data from malware and threats Various methods exist to detect phishing websites and web applications but phishing attacks persist. In this study, we presented a methodology cyber security based. web content-based and heuristic -based approaches with features, using multiple ML and IoT classifiers for detecting phishing attacks more accurately. The main contribution in this study includes a combined methodology that is protecting data and information from malware and threats websites content-based and -based features approaches. We identified many categories of cyber security attacks and crimes and describe the brief history of cyber security extract comprehensive features that can be used to improve phishing detection accuracy. We experimentally demonstrate that the proposed method can detect phishing attacks more accurately and protect online users in real-time. We evaluated the proposed method based on.

### References

- 1 *A History of Cyber Security Attacks 1980*. (1980).
- 2 Aldawood, H., & Skinner, G. (2019). *Reviewing Cyber Security Social Engineering Training and Awareness Programs — Pitfalls and Ongoing Issues*. <https://doi.org/10.3390/fi11030073>
- 3 Barraclough, P. A., Fehringer, G., & Woodward, J. (2021). Intelligent cyber-phishing detection for online. *Computers & Security*, *104*, 102123. <https://doi.org/10.1016/j.cose.2020.102123>
- 4 Blyth, A., Eden, P., & Stoddart, K. (2015). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*. <https://doi.org/10.1016/j.cose.2015.09.009>
- 5 Chongrui, L., Zhiqiang, W., Cong, W., Das, R., & Sandhane, R. (2018). *A Review on Cybersecurity Threats and Statistical Models*. <https://doi.org/10.1088/1757-899X/396/1/012029>
- 6 Coventry, L., & Branley, D. (2018). Maturitas Cybersecurity in healthcare : A narrative review of trends , threats and ways forward. *Maturitas*, *113*(March), 48–52. <https://doi.org/10.1016/j.maturitas.2018.04.008>
- 7 Elmaghaby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities : Safety , security and privacy. *JOURNAL OF ADVANCED RESEARCH*. <https://doi.org/10.1016/j.jare.2014.02.006>
- 8 Ghelani, D. (2022). *Cyber Security , Cyber Threats , Implications and Future Perspectives : A Review*. 8345(X). <https://doi.org/10.11648/j.XXXX.2022XXXX.XX>
- 9 Giansanti, D. (2021). *Cybersecurity and the Digital-Health : The Challenge of This Millennium*. 0–3.
- 10 Gunduz, M. Z., & Das, R. (2019). Cyber-security on smart grid : Threats and potential solutions. *Computer Networks*, 107094. <https://doi.org/10.1016/j.comnet.2019.107094>
- 11 Hassan, J. A. Y., Ola, N. N., & Chehab, A. (2022). Robotics cyber security : vulnerabilities , attacks , countermeasures , and recommendations. *International Journal of Information Security*, *21*(1), 115–158. <https://doi.org/10.1007/s10207-021-00545-8>
- 12 Intrusion, S., & Model, D. (2020). *SS symmetry IntruDTree : A Machine Learning Based Cyber*. May 2017, 1–15. <https://doi.org/10.3390/sym12050754>
- 13 Jain, A. K., & Gupta, B. B. (2017). *Phishing Detection : Analysis of Visual Similarity Based Approaches*. 2017(i).
- 14 Jenab, K., & Moslehpour, S. (2016). *Cyber Security Management : A Review* © Society for Business and Management Dynamics © Society for Business and Management Dynamics. 5(11), 16–39.
- 15 Kaur, J., & Ramkumar, K. R. (2021). The recent trends in cyber security : A review. *Journal of King Saud University - Computer and Information Sciences*, xxx. <https://doi.org/10.1016/j.jksuci.2021.01.018>
- 16 Khurana, S. (2017). *Securityn Cyber A Review Paper o*. 5(23), 1–2.
- 17 Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). *Cybersecurity in healthcare : A systematic review of modern threats and trends*. 25, 1–10. <https://doi.org/10.3233/THC-161263>
- 18 Lee, I. (2020). *Internet of Things ( IoT ) Cybersecurity : Literature Review and IoT Cyber Risk Management*.
- 19 Li, J., He, P., Wu, Y., Xiang, D., Gao, J., Yadi, W., & Yuxin, B. (2020). *Cyber Security Challenges and its Emerging Trends on Latest Technologies*. 0–7. <https://doi.org/10.1088/1757-899X/981/2/022062>
- 20 Mcdaid, A., Furey, E., & Curran, K. (2021). *Wireless Interference Analysis for Home IoT Security Vulnerability Detection*. 10. <https://doi.org/10.4018/ijwnbt.2021070104>

- 21 Mughaid, A., Alzu, S., Hnaif, A., Taamneh, S., Alnajjar, A., & Elsoud, E. A. (2022). An intelligent cyber security phishing detection system using deep learning techniques. *Cluster Computing*, 25(6), 3819–3828. <https://doi.org/10.1007/s10586-022-03604-4>
- 22 Qabajeh, I., Thabtah, F., & Chiclana, F. (2018). A recent review of conventional vs . automated cybersecurity anti-phishing techniques. *Computer Science Review*, 29, 44–55. <https://doi.org/10.1016/j.cosrev.2018.05.003>
- 23 Reddy, G. N., & Reddy, G. J. U. (n.d.). *A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGNING TRENDS ON LATEST TECHNOLOGIES*.
- 24 Reeves, A., Delfabbro, P., & Calic, D. (2021). *Encouraging Employee Engagement With Cybersecurity : How to Tackle Cyber Fatigue*. <https://doi.org/10.1177/21582440211000049>
- 25 Sayeed, A., Verma, C., Kumar, N., & Koul, N. (2022). *Approaches and Challenges in Internet of Robotic Things*. 1–30.
- 26 Shaukat, K., Luo, S., Varadharajan, V., & Hameed, I. A. (n.d.). *Performance Comparison and Current Challenges of Using Machine Learning Techniques in Cybersecurity*.
- 27 Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, 79, 88–115. <https://doi.org/10.1016/j.jnca.2016.11.027>
- 28 Srinivas, J., Das, A. K., & Kumar, N. (2018). Government Regulations in Cyber Security : Framework , Standards and Recommendations. *Future Generation Computer Systems*. <https://doi.org/10.1016/j.future.2018.09.063>
- 29 Sun, C., Hahn, A., & Liu, C. (2018). *Electrical Power and Energy Systems Cyber security of a power grid : State-of-the-art*. 99(November 2017), 45–56. <https://doi.org/10.1016/j.ijepes.2017.12.020>
- 30 Sun, C., Liu, C., & Xie, J. (2016). *Cyber-Physical System Security of a Power Grid* : <https://doi.org/10.3390/electronics5030040>
- 31 Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, R. (2019). AC A Systematic Literature Review of. *Digital Communications and Networks*. <https://doi.org/10.1016/j.dcan.2019.01.005>
- 32 Wu, J., Li, J., & Ji, X. (2018). *Security for cyberspace : challenges and opportunities*. 19(12), 1459–1461.
- 33 Zou, X., Chen, B., & Jin, B. (2012). *Procedia Engineering Cloud-Based Identity Attribute Service with Privacy Protection in Cyberspace*. 086. <https://doi.org/10.1016/j.proeng.2012.01.105>

A large, light blue watermark logo is centered on the page. It features a stylized lightbulb shape with a circular base and a vertical stem. The letters 'IJRTI' are prominently displayed in white, bold, sans-serif font across the middle of the lightbulb's body. The background of the logo is a light blue circle with a white outline.

IJRTI