Cyber Security: Challenges, Threats and Protective Measures of an Organization

Haidar Ali[1], Mohammad Zonaid Bin Ferdous[2], Imran Hossain Showrov[1], Osman Goni[1], Mahbub Alam[1], and Abu Shameem[1]

(Corresponding author: Md. Haidar Ali)

Institute of Computer Science, Bangladesh Atomic Energy Commission, Bangladesh[1]

Email: haiderdiu@gmail.com

Department of ICT, ICT division, Bangladesh[2]

(Received Feb. 9, 2022; Revised and Accepted May 27, 2023; First Online Dec. 1, 2023)

Abstract

In today's computerized world, new risks emerge every day. Connecting to the Internet opens up the possibility of a hacker targeting every organization. Cybercrime can shatter any organization if it has no Cyber security. Because Cybercrime is becoming big business, it risks the cyberspace of organizations and governments globally. In addition, it can create Monetary and reputational risks if organizations don't have an appropriate cybersecurity plan. Every industry has its terminology, and the cyber world is no different. While built on technological foundations that we all know - computers, the internet, smartphones, and similar - as you delve deeper into the subject, you encounter acronyms and technical concepts that you may not be familiar with. And, if we're all to communicate on the subject of cybersecurity - across all sectors of government, business, industry, and academia - it can help to familiarize yourself with the terminology associated with this diverse and compelling subject.

Keywords: Artificial Intelligence; Cloud Computing; Cybersecurity

1 Introduction

Cybercrime is terminology for any illegal activity that uses a computer as its primary means of commission and theft. The U.S. Department of Justice hence expands the definition of cybercrime to include any illegal activity that uses a computer for the storage of evidence [1]. The growing list of cybercrimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying, unauthorized use of a network and terrorism, which have become as a major problem to people and nations [2]. In general, cybercrime is a crime committed using a computer and the internet to steal a person's identity, sell contraband, stalking victims, or disrupt operations with malicious software.

2 Cyber Security

We are presently living in a world where all the information is stored in a digital or cyber-form. Social networking sites provide a space where users feel safe as they interact with friends and family. This is a place where any person can be entrapped by hackers. Cyber-criminals would continue to target social media sites to steal personal data. Not only through social networking but also during business communications, bank transactions data can be compromised and be a digital threat.

According to the 2021 Data Breach Investigation Report of Verizon, the top action varieties in breaches are shown in Figure 1.

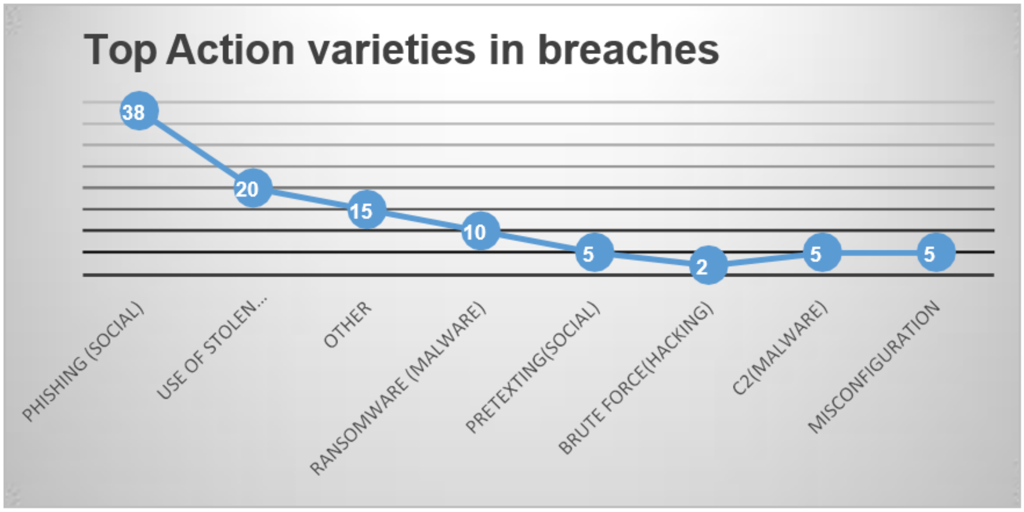

Figure 1: Top action varieties in breaches in 2021 (2021 Data Breach Investigation Report)

3 Patterns Changing in Cyber Security

Here mentioned below are some of the trends that are having a huge impact on cyber security.

3.1 Artificial Intelligence

Perhaps the most effective weapon in a hacker's arsenal is spear phishing using personal information gathered about an intended target to send them an individually tailored message. An email seemingly written by a friend, or a link related to the target's hobbies, has a high chance of avoiding suspicion. This method is currently quite labour intensive, requiring the would-be hacker to manually conduct detailed research on each of their intended targets. However, an AI similar to chatbots could be used to automatically construct personalized messages for large numbers of people using data obtained from their browsing history, emails, and tweets [3].

3.2 Web Servers

Attacks on web applications to extract data or transmit malicious code are already a problem. Cyber-criminals distribute their malicious code via legitimate web servers they have compromised. However, data-stealing attacks, many of which receive public attention, are also a significant concern. We must now place a higher emphasis on the security of web servers and web applications. The ideal venue for these cyber offenders to steal data is through web servers. To avoid being a victim of these crimes, one should always use a safer browser, especially during critical transactions. Hence one must always use a safer browser, especially during important transactions in order not to fall prey to these crimes (Refer to Figure 2).

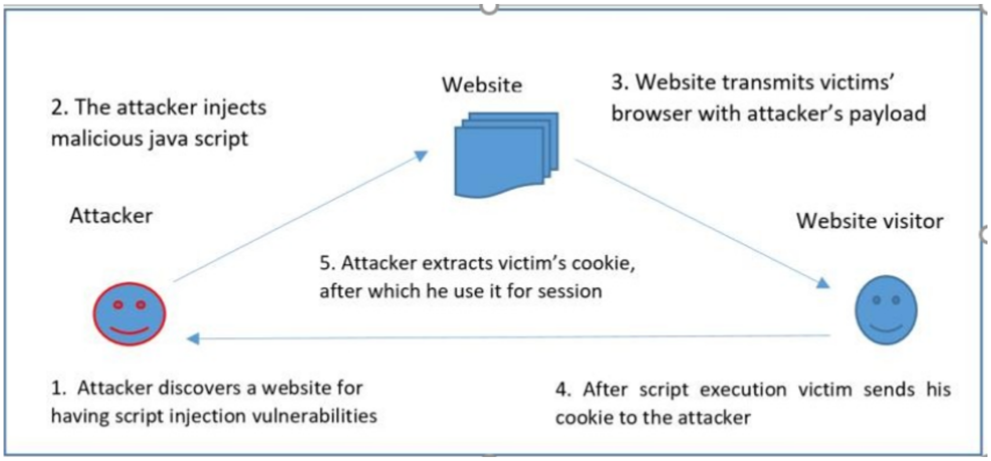
Website
2. The attacker injects malicious java script
3. Website transmits victims' browser with attacker's payload
Attacker
Website visitor
5. Attacker extracts victim's cookie, after which he use it for session
1. Attacker discovers a website for having script injection vulnerabilities
4. After script execution victim sends his cookie to the attacker

Figure 2: Scripting attack in website

3.3 Cloud Computing and Its Services

Cloud services are being steadily used by all small, medium, and large organizations these days. To put it another way, the world is slowly reaching the clouds. This latest tendency poses a big concern for cyber security because communications can circumvent established ports of inspection. As the number of apps available in the cloud grows, policy controls for web applications and cloud services will need to evolve to prevent the loss of essential information. Security issues persist, although cloud providers are developing their models. Although the cloud has tremendous benefits, it is vital to keep in mind that as the cloud evolves so do its security concerns (Refer to Figure 3).

69% of organizations point to data loss/leakage as their greatest cloud security concern and 44% of companies are concerned about their ability to perform incident response effectively in the cloud [5]. Data Privacy/Confidentiality, Accidental Exposure of Credentials are also potential threats in cloud computing.

3.4 APT's and Targeted Attacks

An advanced persistent threat (APT) is a stealthy threat actor, usually a nation-state or a state-sponsored group, that gains unauthorized access to a computer network and goes undiscovered for a long time [6]. In recent times, the term may also refer to non-state-sponsored groups conducting large-scale targeted intrusions for specific goals [7].

APT (Advanced Persistent Threat) is a new type of cybercrime. For years, network security features like web filtering and intrusion prevention systems (IPS) have been critical in detecting such targeted attacks (mostly after the initial compromise). In order to detect attacks, network security must interact

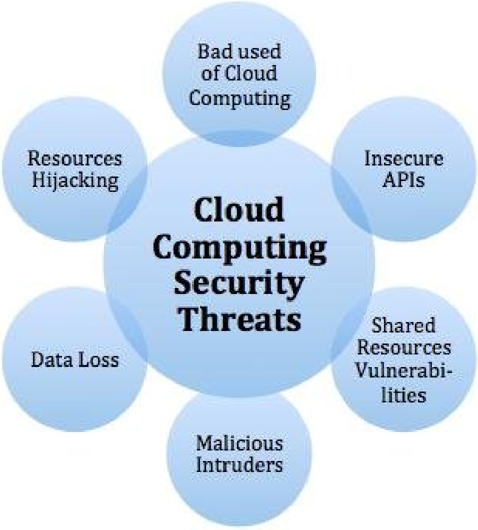
Cloud Computing Security Threats
Bad used of Cloud Computing
Insecure APIs
Shared Resources Vulnerabi-lities
Malicious Intruders
Data Loss
Resources Hijacking

Figure 3: Cloud Computing Security Threats [4]

with other security services as attackers become more daring and use more ambiguous approaches. As a result, we must improve our security techniques in order to prevent future threats.

3.5 Mobile Networks

In modern world, we are able to connect to anyone in any part of the world through mobile network. But for these mobile networks security is a very big concern. Like desktop computers, mobile devices have software and Internet access. Mobile malware (i.e. malicious applications) and malicious websites can accomplish the same objectives (stealing data, encrypting data, etc.) on mobile phones as on traditional computers.

Malicious apps may come in a variety of different forms. Sometimes users click the most common types of malicious mobile apps that are Trojans. Mobile ransom ware is a particular type of mobile malware, but the increased usage of mobile devices for business has made it a more common and damaging malware variant. Mobile ransomware encrypts files on a mobile device and then demands a ransom payment in exchange for the decryption key, which allows access to the encrypted data to be restored. Phishing is one of the most popular forms of cyber-attack. The majority of cyberattacks start with a phishing email that contains a dangerous link or a malware-infected attachment. Phishing attempts on mobile devices use a range of methods to send links and malware, including email, SMS messaging, social media platforms, and other apps. Man-in-the-Middle (MitM) attacks involve an attacker intercepting network communications to either eavesdrop on or modify the data being transmitted. While this type of attack can be carried out on a variety of platforms, mobile devices are particularly vulnerable to MitM attacks.

Unlike web traffic, which typically uses encrypted HTTPS for communication, SMS messages can be easily intercepted, and mobile apps may send potentially sensitive data through unencrypted HTTP [8].

3.6 IPv6

IPv6 is a new Internet protocol that will replace IPv4 (the previous version), which has served as the backbone of our networks and the Internet in general. It's not merely a matter of moving IPv4 features to IPv6. While IPv6 is a complete replacement for IPv4 in terms of increasing the number of available IP addresses, there are certain basic modifications to the protocol that must be considered in security policy. End-to-end encryption is possible with IPv6 (Why IPv6 Matters for Your Security). Despite the fact that this technology was retrofitted into IPv4, it is still an optional add-on that isn't widely used. Encryption and integrity-checking, which are common in today's VPNs, is a standard feature of IPv6, available for all connections and supported by all compatible devices and systems. As a result, widespread use of IPv6 will make man-in-the-middle assaults much more difficult. Hence it is always better to switch to IPv6 as soon as possible in order to reduce the risks regarding cybercrime.

3.7 Encryption of the Code

Encryption is the technique of encrypting communications (or information) in such a way that it cannot be read by eavesdroppers or hackers. An encryption technique converts a message or information into unreadable cipher text by encrypting it with an encryption algorithm. This is normally accomplished through the use of an encryption key, which determines the message's encoding method. At its most basic level, encryption safeguards data privacy and integrity. However, increasing encryption means more cyber security challenges. Encryption is also used to safeguard data in transit, such as data sent across networks (e.g., the Internet, e-commerce), mobile phones, wireless microphones, and wireless intercoms, among many other things. As a result, by encrypting the code, one may determine whether or not information has been leaked (Refer to Figure 4).

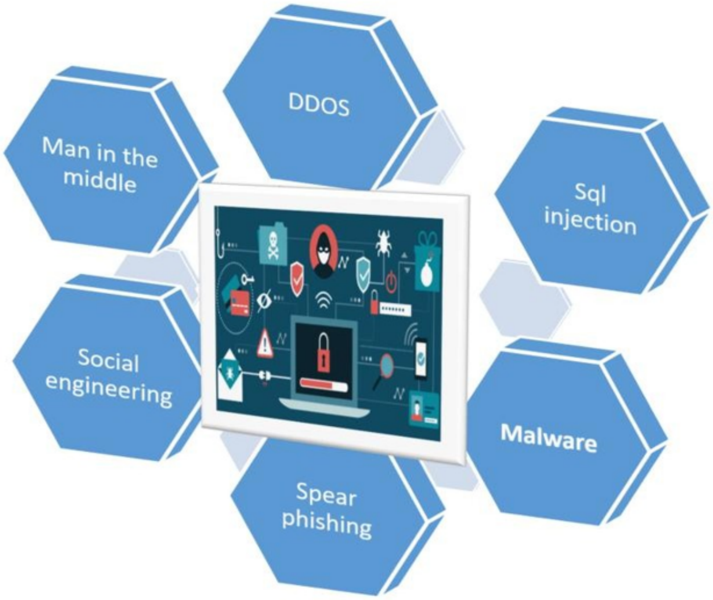

Figure 4: Cloud Computing Security Threats [6]

4 Role of Social Media in Cyber Security

As we become more social in an increasingly connected world, companies must find new ways to protect personal information. Social media has a significant impact on cyber security. It will play a significant part in personal cyber dangers. The use of social media by individuals is on the rise, as is the threat of an assault. Because most of them use social media or social networking sites on a daily basis, it has become a major platform for cyber criminals to hack private information and steal important data. Companies must ensure that they are equally as quick to recognize risks, respond in real time, and avoid any kind of breach in a world where we are quick to give over our personal information. Because these social media sites draw individuals readily, hackers utilize them as bait to obtain the information and data they seek.As a result, users must take necessary precautions, particularly while dealing with social media, to avoid losing their data. The ability of individuals to share information with a global audience is at the heart of the social media problem that businesses face. In addition to allowing anybody to share commercially sensitive information, social media also allows anyone to publish incorrect information, which can be just as destructive. Despite the fact that social media can be used for cybercrime, these businesses cannot afford to cease using it because it is a crucial part of their public relations strategy. Instead, they need solutions that will alert them to the hazard so that they can address it before it becomes a problem.

5 Protective Measures of Cyber Security

5.1 Anti-virus Software

Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. Antivirus software is a must and basic necessity for every system.

5.2 Access Control and Password Security

The concept of user name and password has been fundamental way of protecting our information. This may be one of the first measures regarding cyber security.

5.3 Authentication of Data

Before downloading, the documents we receive must always be validated, which means they must be checked to see whether they came from a trusted and credible source and if they have not been altered. Anti-virus software installed on the devices is frequently used to authenticate these papers. As a result, robust anti-virus software is also required to keep the devices safe from viruses.

5.4 Updating of Software

Ransomware attacks were a major attack vector of 2017 for both businesses and consumers [9]. Approximately 37% of global organizations said they were the victim of some form of ransomware attack in 2021, according to IDC's "2021 Ransomware Study" [10]. Ransom ware trends, statistics and facts in 2021. One of the most important cyber security measures for combating ransomware is patching obsolete software, both operating systems and applications. This helps to eliminate critical vulnerabilities that hackers use to get access to devices.

Automatic system updates for devices should be turned on. Web browser uses automatic security updates.

5.5 Malware Scanners

Viruses, worms, and Trojan horses are types of dangerous software that are frequently lumped together as malware. Those are computer programs that usually scans all the files and documents present in the system for malicious code or harmful viruses.

5.6 Firewalls

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the Internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting the malware.

Firewalls and other security protections are getting more porous as people use more devices such as tablets, phones, PCs, and other devices, all of which require additional security precautions in addition to those provided by the programs. We must always keep the security of these mobile networks in mind. Furthermore, because mobile networks are so vulnerable to cybercrime, extra caution must be exercised in the event of a security breach (Refer to Figure 5).

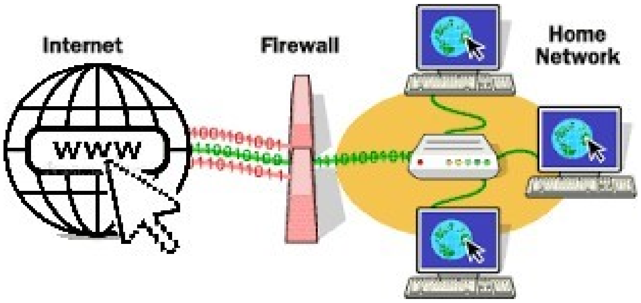

Figure 5: Firewall

5.6.1 What Does a Firewall Do?

A firewall is a device that separates a trusted network from an untrusted network like a gatekeeper [11]. It monitors attempts to gain access to your operating system and blocks unwanted traffic or unrecognized sources. Between your computer and another network, such as the internet, a firewall acts as a barrier or filter. A firewall can be compared to a traffic controller. It manages network traffic to help safeguard your network and information. This involves blocking unsolicited incoming network traffic and authenticating access by scanning network traffic for unwanted content such as hackers and viruses. Operating system and security software usually come with a pre-installed firewall. It's a good idea to make sure those features are turned on. Also, security settings should be configured to run updates automatically.

5.6.2 How Does a Firewall Work?

A firewalled system analyzes network traffic based on rules to begin with. Only those inbound connections that have been set to accept are accepted by a firewall. It accomplishes this by allowing or disallowing specific data packets-the units of communication that one send over digital networks-based on pre-determined security criteria. Through the firewall, only trustworthy sources or IP addresses are allowed in. IP addresses are significant because they identify a computer or source, much like a postal address does.

5.6.3 Types of Firewalls

Firewalls are available in both software and hardware. Each format has a distinct yet critical function. A hardware firewall is a physical device that sits between the user's network and the gateway, similar to a broadband router. A software firewall is an internal program that works with port numbers and applications on a user's computer.

Cloud-based firewalls, often known as Firewall as a Service, are also available (FaaS). One advantage of cloud-based firewalls is that they can scale with the business and, like hardware firewalls, are effective at perimeter protection.

Depending on the scale of our network and the level of security we require, there are various distinct types of firewalls based on their structure and functioning.

Packet-filtering firewalls: A packet-filtering firewall is a network traffic management tool that can restrict network traffic based on the IP protocol, IP address, and port number. This is the most basic type of firewall, and it's designed for smaller networks [12].

But caution should be taken. While packet-filtering firewalls have their advantages, they also have their drawbacks. A packet-filtering firewall does not block web-based assaults because all web traffic is allowed. As a result, extra security to discern between benign and dangerous online traffic should also be taken.

Proxy service firewalls: The proxy service firewall is a system that can help protect your network security by filtering messages at the application layer. It essentially serves as a gateway or middle man between user's internal network and outside servers on the web. Also known as a gateway firewall, it is more secure in its use of stateful and deep packet inspection technology to analyze incoming traffic [12].

Stateful multi-layer inspection (SMLI) firewalls: The stateful multi-layer inspection (SMLI) firewall employs a complex packet-filtering technique that evaluates all seven layers of the OSI architecture [13]. Each packet is inspected and compared to known friendly packet states. SMLI firewalls check the full packet, including the data, whereas screening router firewalls simply examine the packet header.

However, it is still unable to differentiate between good and harmful online traffic, necessitating the use of extra software.

Unified threat management (UTM) firewalls: Unified threat management (UTM) is an approach to information security in which multiple security functions are provided by a single hardware or software installation. In contrast to the previous way of having point solutions for each security function, this approach is more flexible [14]. Instead of managing multiple products from different vendors, UTM simplifies information-security management by providing a single management and reporting point for the security administrator.

Next-generation firewalls (NGFW): Next-generation firewalls are more sophisticated than packet-filtering and stateful inspection firewalls. A next generation firewall (NGFW) is, as Gartner defines it, a —deep-packet inspection firewall that moves beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall [15].

They have higher security levels, going beyond standard packet filtering to examine a packet in its entirety. This entails not only inspecting the packet header, but also the contents and source of the packet. More sophisticated and emerging security threats, such as advanced malware, can be blocked by NGFW.

Virtual firewalls: A virtual firewall is an appliance that can be utilized in both private and public cloud-based systems. This firewall evaluates and manages internet traffic across both physical and virtual networks.

6 Cyber Ethics

The code of the internet is known as cyber ethics. When we follow these cyber ethics, there's a strong chance we'll be able to use the internet properly and safely. Here are a few examples:

1) Bulling on the Internet, calling people names, sending embarrassing pictures of them is offensive crime in many countries. So it should be avoided.

2) Do not use other people's passwords to access their accounts.

3) Never try to corrupt other people's computers by sending malware to them.

4) Sharing personal information in internet is not a good idea.

5) Always follow copyrighted information and only download games or media if they are allowed. The preceding are some cyber ethics to observe when utilizing the internet.

6) Accessibility, censorship, and filtering raise a slew of ethical dilemmas, each with its own branch of cyber ethics. Many questions have arisen, challenging our notion of privacy, security, and our social engagement. Throughout history, systems have been built for the purposes of protection and security. Today's applications take the shape of software that filters domains and material so that they can't be easily accessed or obtained without a lot of effort, or on a personal or business level using free or content-control software [16]. Censorship and filtering on the internet are used to limit or prevent material from being published or accessed. Offline censorship and filtering raise legal difficulties similar to online censorship and filtering.

7 Conclusion

Computer security is a huge topic that is growing increasingly relevant as the world becomes increasingly interconnected, with networks being used to conduct critical transactions. With the evolution of new

technologies, every year cybercrime and the protection of information continue to split along distinct routes. Organizations are being challenged not just by how they safeguard their infrastructure, but also by how they require new platforms and intelligence to do so, as a result of the latest and disruptive technology, as well as new cyber tools and threats that emerge. Although no system is invincible to cybercrime, we should do everything we can to reduce it in order to ensure a safe and secure future in cyberspace.

References

[1] K. Brush, M. Cobb, "Cybercrime," Mar. 16, 2024. (https://www.techtarget.com/searchsecurity/definition/cybercrime)

[2] G. N. Reddy, G. J. Reddy, "A study of cyber security challenges and its emerging trends on latest technologies," *arXiv preprint*, arXiv: 1402.1842, 2014.

[3] M. Brundage, *et al.*, "The malicious use of artificial intelligence: Forecasting, prevention, and mitigation," *arXiv preprint*, arXiv: 1802.07228, 2018.

[4] H. Laarabi, R. Sacile, A. Boulmakoul, "Road dangerous goods transport: Open architecture, performance, and scalability of a real-time GPS data collection," Jan. 22, 2022. https://www.researchgate.net/figure/Fig-Cloud-Computing-Security-Threats_fig12_233781365)

[5] Check Point, "Top 15 Cloud Security Issues, Threats and Concerns," Mar. 16, 2024. (https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/)

[6] Wikipedia, "Advanced/ persistent/ threat," Mar. 16, 2024. (https://en.wikipedia.org/wiki/Advanced_persistent_threat)

[7] S. Maloney, "What is an Advanced Persistent Threat (APT)?," Mar. 16, 2024. (https://www.cybereason.com/blog/advanced-persistent-threat-apt)

[8] Check Point, "Top 6 Mobile Security Threats and How to Prevent Them," Mar. 16, 2024. (https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-mobile-security/top-6-mobile-security-threats-and-how-to-prevent-them/)

[9] Sophos, "Cybersecurity Best Practices Toolkit," Mar. 16, 2024. (https://www.sophos.com/en-us/security-news-trends/security-trends/why-switch-to-ipv6.aspx)

[10] Cipher, , "Enhance Your Cybersecurity Visibility and Protection," Mar. 16, 2024. (https://www.cipher.com/)

[11] R. Oppliger, "Internet security: firewalls and beyond," *Communications of the ACM*, vol. 40, no. 5, pp. 92–102, 1997.

[12] C. Stouffer, "What is a firewall? Firewalls explained and why you need one," July 12, 2023. (https://us.norton.com/internetsecurity-emerging-threats-what-is-firewall.html)

[13] IBM, "Stateful multi-layer inspection (SMLI) firewalls," Mar. 16, 2024. (https://www.ibm.com/docs/en/db2/11.1?topic=support-stateful-multi-layer-inspection-smli-firewalls)

[14] Wikipedia, "Unified/ threat/ management," Mar. 16, 2024. (https://en.wikipedia.org/wiki/Unified_threat_management)

[15] Digital Guardian, "What is a Next Generation Firewall? Learn about the differences between NGFW and traditional firewalls," Mar. 16, 2024. (https://www.digitalguardian.com/blog/what-next-generation-firewall-learn-about-differences-between-ngfw-and-traditional-firewalls)

[16] A. Chanda, C. Westphal and D. Raychaudhuri, "Content based traffic engineering in software defined information centric networks," in *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS'13)*, Turin, Italy, pp. 357-362, 2013.

Biography

Md. Haidar Ali was born in Kishorgonj, Bangladesh, on 25th January, 1985. He received the B.Sc. Degree in Computer Science and Engineering from the Daffodil International University, Bangladesh in 2010, and in 2012, he received the M.Sc. degree in Computer Science and Engineering from Daffodil International University. He worked at Padma Multipurpose Bridge Project, Bridge Division under Ministry of Road Transport & Bridges, Bangladesh from 14 October 2014 to 05 November, 2016 as a Assistant Programmer. From 15 November 2016 to still now, He is being a scientific officer of Computer Science Division in Bangladesh Atomic Energy Commission. He is a Life Time Member of Bangladesh

Computer Society and Also Life Time Member of IEB. His research interest includes Network and Cyber security, communication Engineering.

Mohammad Zonaid Bin Ferdous was born in Brahmanbaria, Bangladesh, on 16th October, 1986. He received the B.Sc. Degree in Computer Science and Engineering from the Daffodil International University, Bangladesh in 2010, and in 2012, he received the M.Sc. degree in Computer Science and Engineering from Daffodil International University. He is working in Department of ICT, ICT division as Programmer. He is a Life Time Member of Bangladesh Computer Society. His research interest includes Wireless Network, Communication Engineering, cyber security and artificial intelligence.

Md. Imran Hossain Showrov is currently working as a researcher at the Institute of Computer Science at Bangladesh Atomic Energy Commission. His research interest lies in but not limited to data mining, information retrieval etc. He has completed his undergraduate from Shahjalal University of Science & Technology and graduated from South Asian University.

Osman Goni was born at Chandpur, Bangladesh, on 25th September, 1982. He has completed his Diploma-in-Computer Engineering and obtained 3rd place from Bangladesh Technical Education Board (BTEB) and B.Sc. in Computer Science & Engineering from the department of Computer Science and Engineering World University of Bangladesh (WUB) and M.Sc. in Computer Science & Engineering from the department of Computer Science and Engineering Jagannath University (JnU) in Bangladesh. Currently, he is working as a Senior Engineer (Senior Engineer, Computer Science and Engineering) in Bangladesh Atomic Energy Commission. He is the member of Institution of Diploma Engineers, Bangladesh (IDEB) and the associate member The Institution of Engineers, Bangladesh (IEB) and the associate member Bangladesh Computer Society (BCS). His research interest includes Computer Hardware and Networking, artificial intelligence (AI) and Robotics, Cyber Security, E-Commerce etc.

Md. Mahbub Alam was born in a rural area called Dhamrai of Dhaka in 1991. He has completed his B.Sc and M.Sc from the Department of Computer Science and Engineering, Jahangirnagar University, Savar, Dhaka, Bangladesh. He worked as a lecturer in Gono University at the department of CSE from January 2015 to February 2016. He worked as an Assistant Engineer in WALTON Group at the Computer R&D section from February 2016 to November 2017. Currently, he is working as a Scientific Officer at the Institute of Computer Science in Bangladesh Atomic Energy Commission. His research interests include big data analysis, artificial intelligence, pattern recognition and expert system, computer vision, system that can provide distinct service through internet protocol and any system that can be beneficiary for common people. He is also interested in entrepreneurship.

Md. Abu Shameem was born in Bhairab, Kishoregonj, Bangladesh in 1969. He has completed Bachelor of Science in electronics & telecommunications engineering from the department of electronics & telecommunications engineering Prime University, Dhaka and Master of Science in telecommunications engineering from the department of electronics & communications engineering East West University, Dhaka. He worked as a senior instructor in department of youth development from January 1994 to December 1995. Currently, he is working as a Principal Engineer & divisional head of Computer System & Networking Division at the Institute of Computer Science in Bangladesh Atomic Energy Commission. His research interest includes communication engineering, networking & security system, server administration and instrumentation & control system etc.