WJCMS

Wasit Journal of Computer and Mathematics Science

Journal Homepage: https://wjcm.uowasit.edu.iq/index.php/WJCM

e-ISSN: 2788-5879 p-ISSN: 2788-5879

A Review on the Mechanism Mitigating and Eliminating Internet Crimes using Modern Technologies

Sahar Wahab khadim[1,*], Oday Ali Hassen[2] and Hussein k. Ibrahim[3]

[1]Ministry of Education, Karkh Second Directorate of Education, Iraq
[2]Ministry of Education, Wasit Education Directorate, Iraq
[3]Waist University, College of Computer Science and Information Technology. Iraq

*Corresponding Author: Sahar Wahab khadim

DOI: https://doi.org/10.31185/wjcm.48
Received: June 2022; Accepted: August 2022; Available online: September 2022

ABSTRACT: There is no doubting that contemporary technology creates new hazards, and these threats are many and significant, directly harming people's lives and threatening their stability. Because of the increased use of computers and Internet-connected cell-phones in recent years, the problem of cybercrime has expanded substantially. Unquestionably, this kind of crime is now a reality that jeopardizes people's reputations and lives, therefore we must be aware of it to prevent being a victim. The exponential growth in internet connectedness is closely tied to a rise in cyber-attack incidences, frequently with significant consequences. Malware is the weapon of choice for carrying out malicious intent in cyberspace, whether by exploiting pre-existing flaws or exploiting the unique properties of new technology. There is an urgent need in the cybersecurity area to develop more inventive and effective vi-rus defense techniques. To do this, we first give an overview of the most often exploited vulnerabilities in the current hardware, software, and network layers. This follows criticism of the most recent mitigation efforts and the reasons why they may or may not be helpful. Following that, we'll talk about new attack methods for cutting-edge technologies including social networking, cloud computing, mobile technology, as well as critical infrastructure. We conclude by sharing our speculative findings on poten-tial future research avenues.

Keywords: Cybercrimes, AL, Telecommunication infrastructure, HTTPS

CC BY

1. INTRODUCTION

A new type of crime known as cybercrime has started to emerge with the introduction of computers and the Internet into our societies and every aspect of our lives. As a result, there is a need to define these crimes, increase awareness of and follow up on this type of crime, and enact laws and legislation necessary to combat cybercrime due to the significant material and moral losses it causes. Every conduct that is punished by law or the failure to take legal action is considered a crime under man-made laws. Positive law establishes precise punishments for transgressions, therefore no action may be penalized unless the law expressly provides for it; otherwise, it is not regarded as a crime [1] Contrarily, crime is any destructive act a citizen does that has an adverse impact on other citizens. Therefore, a person committing a crime online is considered to have committed a cybercrime if they used illegal computers, mobile devices, telephone communication networks, information transmission networks, the Internet, or any other electronic data in general [2]. Due to the early Internet's small user base and restriction to a certain user group, notably academics and university professors, there was little worry about potential "crimes" that may be committed over the network. Because of this, the network's architecture and structure are not secure. [3]. However, as network use rose and more members of various societal categories joined the user list, crimes started to occur on the network. These crimes multiplied over time and took on a wide range of

forms. With the growth of the Internet, the diversification of its applications, and the rise in global user numbers. A lot of crimes may now be planned and committed via the Internet without being seen or caught by security personnel. Therefore, using computer networks, media, and the Internet to conduct or plot a crime is known as cybercrime. Many of the notions people are used to have changed as a result of technology since its birth, and these changes have ranged from harmful to beneficial. [4]. The difficulty of maintaining one's privacy due to the proliferation of many easy means, which people known as Internet hackers use, to break into the privacy of the individual, was perhaps the most significant of these negatives. At a time when technology, for example, has brought the distances between peoples closer by providing many means of communication and means of transportation that were not known before. These hackers engage in a variety of activities, and this diversity in their actions correlates to a further variability in the amount of damage they may do to an individual user depending on the activity they engage in [5]. Hackers often use the information they discover online to commit fraud on behalf of their victims by making purchases, selling items, applying for loans from banks, and other actions. Because there are so many methods to succeed on the Internet, identity theft has become simpler for hackers to do. For instance, this kind of stealing thrives in chat rooms where hackers create malware programs known as horses. The Horses Trojan may infiltrate a computer and spy on its user, gathering details like the passwords he uses, before returning the data to the hacker. The difficulties involving this sort of crime are many, with the most notable instances including copyright violations, publishing child pornography, efforts to coerce children into sexual exploitation, and unlawful commerce. Such crimes may endanger the security and financial integrity of the state (such as drug trafficking). Illegal [6]. Electronic espionage, of which the most notable examples were revealed by the leaks of the former contractor with the US National Security Agency Edward Snowden, who revealed many American plans to spy not only on individuals but on communications of other countries, and theft are examples of cybercrime that are not limited to individuals or groups but may extend to the level of countries. cross-border crimes involving money and other things [7].

Some of the goals of cybercrime may be summed up in a few points, the most significant of which are:

1. Being able to obtain unauthorized access to information, such as through stealing, gaining access to, deleting, or altering information to further one's agenda.t
2. aving the ability to access and shut down information servers across the Internet
3. Blackmailing people, institutions, banks, governments, and other parties by leveraging technology to get their sensitive information.
4. The unauthorized use of information technology for monetary, moral, or political gain, such as website hacking, destruction, credit card fraud, as well as bank account theft, and so on.

2. CYBER CRIMINAL

It is someone who is not like a typical criminal. This individual cannot be uninformed about contemporary information technology.

Studies that identify the offender, his character, and the seriousness of his conduct as a foundation for defending and calculating the sentencing range widely. In our instance, the issue is: Is there a special model for an information criminal? How can the penalty be evaluated and justified in the case of a computer and Internet criminal? Although there cannot be a precise model for the information criminal, these criminals share some characteristics, which are outlined as follows [8]:

1. **Specialized criminal:** He has outstanding technical abilities and utilizes them to access networks, crack passwords or ciphers, and navigate the network world in order to collect all the priceless data and information stored in computers and sent across networks..
2. **A criminal who returns to crime:** The trait of the information criminal is that he repeatedly gains illegal access to network systems using his knowledge of how computers operate, how to store data and information, and how to manipulate them.
3. **A professional criminal:** He is capable and technically skilled enough to exploit his hacking, theft, fraud, misuse of intellectual property rights, and other criminal activities as a means of making money..
4. **Smart criminal:** This criminal is capable of developing and altering security systems, making it impossible to find him and trace his illicit activities across networks or within computers.

An information criminal's key to finding vulnerabilities and breaking into dungeon programs is intelligence. The characteristics of the virtual world, which are nearly a consensus among many jurists, might be used to summarize the

commonalities among these offenders. Following are some areas where there is still contention on the ideas of information crime and new crimes in general [9]:

1. This group of offenders often ranges in age from 18 to 45.
2. nowledge, expertise, and outstanding technical prowess in the area of information systems The criminals that fall under this group are often well-educated have a specialization in computer crime and have the skills necessary to get beyond programming firms' fortifications and defenses.
3. Excessive self-confidence and the conviction that they can conduct crimes undetected
4. His thorough understanding of the crime scene and its equipment, as well as his avoidance of any unforeseen circumstances that would compromise his strategy and reveal his case.

There are many different types of perpetrators of information crime, including hackers, who are typically professional criminals who use their knowledge and skills in information technology to break into specific websites and steal sensitive data or sabotage and damage a specific system and cause losses with the intention of retaliation or extortion.

There are crackers, whether they are amateurs or experts, and these types of criminals often utilize their technical prowess to break into systems and gadgets in order to accomplish illicit objectives like collecting sensitive information or committing acts of sabotage. Code-cracking individuals, so-called "Malicious hackers," etc [10].

While an information criminal may use his crime to demonstrate his technical prowess and capacity to get into computers or to obtain specific monetary benefits, offenders in this category may also be motivated by a desire to damage others, such as an employee who is fired and seeks retribution. While an information criminal may use his crime to demonstrate his technical prowess and capacity to get into computers or to obtain specific monetary benefits, offenders in this category may also be motivated by a desire to damage others, such as an employee who is fired and seeks retribution [11].

In order for hackers to commit their electronic crimes, those tools must be available, most importantly:

- Internet access is seen as a crucial instrument for carrying out the crime.
- The availability of specialized software to duplicate the data that a user has saved on a computer.
- Espionage techniques, such as attaching cameras to phone lines.
- Barcodes are instruments for scanning and decoding digital coding.
- Printers.
- Mobile and digital devices.
- Trojan horses are examples of malware whose purpose is to trick the victim into running it and inflict extensive harm on the machine and its contents. Trojan horses are examples of malware whose purpose is to trick the victim into running it and inflict extensive harm on the machine and its contents.

Figure (1) shows the Cyber Criminal.

3. CURRENT SYSTEMS' VULNERABILITIES AND DEFENCE TACTICS

Accountability is added to perimeter defense and access control in order to spot or correct any wrongdoing, as seen in Figure (2). However, as malware develops and becomes more complicated, it has been shown that joint efforts of a perimeter protection approach are becoming less and less successful. Malware that is always growing tends to find ways through perimeter defenses entirely. At the hardware, software, and network layers—the three separate components of the modern information system—we go into great depth on the most prevalent attacks. Then, we go through the advantages and disadvantages of the most prevalent defensive strategies used in these tiers [12].

3.1 EXPLOITING EXISTING VULNERABILITIES

Once the virus is placed on the victim's PC, hackers may use a number of the system's vulnerabilities to further their illicit operations. We look at the hardware, software, and network system vulnerabilities that are currently being exploited the most. The discussion of current initiatives that have been suggested to lessen the harmful effects of exploitations comes next [13].

FIGURE 1. Cyber Criminal

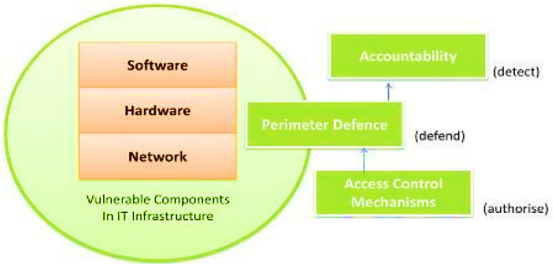

FIGURE 2. Weaknesses and Defense Strategies in Existing Systems

3.1.1. Hardware

The most powerful component that may influence a computer system is hardware. If the hardware is hacked, this level has the ability to allow attackers a great deal of freedom and capacity to undertake harmful security assaults. Many hardware-based assaults may avoid detection, in contrast to software-level attacks, which can often be caught by many security updates, intrusion detection systems, and antivirus scanners. Hardware-based assaults have been said to be on the increase, taking advantage of the absence of tools supporting hardware detection [14].

Hardware Trojans are the most heinous and prevalent device exploits out of all the numerous sorts of hardware abuse. Electronic components like Integrity Circuits (IC) in the hardware are modified maliciously and purposefully invisibly by hardware Trojans [15]. There are many degrees and kinds of adverse consequences caused by hardware Trojans. An error detection module could accept inputs that ought to be rejected as a result of a hardware Trojan. A Trojan may add additional buffers to the chip's interconnections, using more power as a result and rapidly depleting the battery. Denial-of-Service (DoS) Trojans are more dangerous since they stop a resource or function from operating. The target module may run out of limited resources, such as compute power, battery life, and bandwidth, due to a DoS Trojan. It might potentially physically damage, disable, or change the configuration of the device, for instance, by instructing the CPU to disregard an interrupt coming from a certain peripheral [16].

Since there is a greater risk that unlawfully manufactured hardware would include harmful backdoors or hardware Trojans, illegally copied hardware becomes a source of hardware-based exploitation. With a growing trend in IT firms attempting to reduce IT expenditures through outsourcing and obtaining doubtful gear from online marketplaces, the likelihood of producing unauthentic hardware has grown. According to Karri et al. [17], the current IT outsourcing paradigm has raised the possibility of receiving altered hardware components from unreliable manufacturing abroad. Similar to the previous point, it is also made clear that IT organizations often purchase dubious gear, Chipsets and routers, for example, can be purchased via auction sites as well as resellers. This device might then include harmful hardware-based Trojans. These acts raise the possibility that original design and specifications of internal states of the system will be divulged to unauthorized parties, which is troublesome for IT organizations operating on modified hardware with possible backdoor access.

When adversaries study physical information about a device, such as power usage, electromagnetic radiation, and data in and out of the CPU timing, they may learn about the internal states of a system. This is known as a side channel attack. These side channel attacks have the potential to expose sensitive data. A method has been described that looks at several

ways the secret key of a cryptographic algorithm might be revealed via the study of radio frequency [18].

Several methods have been put forward to resist hardware-level assaults. Tamper-resistant hardware has grown in importance as a result of its significance as a point of entry for system security in general. The Trusted Platform Module (TPM) offers secured storage, cryptographic primitives, and the ability to exchange tamper-resistant evidence with other distant servers. The definition of the term "Trusted Computing Base" (TCB), refers to the collection of all hardware and software pieces that are essential to the system's overall security. There must not be any faults or vulnerabilities present inside the TCB since this might compromise the system's security as a whole. To assure the security of TCB, Utilizing computer-assisted software audit as well as program verification, a thorough and precise review of its code base is performed. Hardware watermarking protects the host item against illicit counterfeiting by encoding and hiding ownership information in the description of a circuit. A purposeful method of hiding an electrical device's operation, hardware obfuscation modifies the description or structure of the device [19]. These techniques are designed to prevent adversaries from gaining access to the original design and replicating/counterfeiting critical bits of hardware, including such IC units. Certain defenses against side channel assaults include adding sounds to prevent physical information from being shown directly, filtering some physical information, and creating blindness, which aims to eliminate any link between the input data and side channel emission [20].

3.1.2. Software vulnerabilities

An error, defect, mistake, or problem in a computer program, such as an internal operating system, external I/O interface drivers, and applications, is referred to as a "software bug". Software flaws are exploited by cyberattacks to make systems act in ways that are contrary to their intended behavior. The bulk of current cyber assaults still originates from software vulnerabilities brought on by bugs and design defects in software [21].

Software-based exploitation happens when certain interface and software stack features are taken advantage of. The majority of frequently occurring software flaws originate from the exploitation of memory issues in software, user input validation, race situations, and user access rights [22]. Attackers commit memory safety breaches to change the contents of a memory location. The most excellent method is a buffer overrun. When software attempts to store more data in a buffer than it was designed to contain, a buffer overflow occurs. Since buffers are designed to hold a certain amount of data, excess data may overflow into neighbouring buffers and damage or replace the data that should have been stored there. It enables attackers to alter the code of active processes. The process of making sure that the input data complies with certain standards is known as input validation. Data corruption, such as that observed in SQL injection, may result from improper data validation. One of the most well-known methods for taking advantage of a software flaw on a website is SQL injection. To alter the content of the database or to have access to sensitive database information like credit card numbers and passwords, an attacker injects SQL instructions into the web form. The enemy takes advantage of a process fault where the output is unforeseen and vitally reliant on the timing of other occurrences. A defect known as the delay between check and use occurs when a system changes between a condition being checked and the use of the results of that check. It is also known as race situation error exploitation. Exploiting a defect by obtaining elevated access to resources that are typically secured from an application or user is known as privilege confusion. As a consequence, opponents with more access rights engage in unlawful activities like obtaining secret keys that are meant to be safeguarded [23].

Several initiatives have been started in the programming community with improving security as a primary objective [24]. In addition to addressing a common set of fundamental security issues, the main goal of these initiatives is to provide fresh perspectives to build a safe computing environment. Software engineers discover frequent programming mistakes that result in software vulnerabilities, In a code-based approach, design universal secure code, educate software developers, as well as improve the state of the art in safe coding. Techniques are created in a language-based secure coding approach to make sure that programs can be trusted not to flout crucial security regulations. The two methods that are most often utilized are analysis and transformation. Sort checking is a well-known type of analysis where the program finds any dangerous types of objects before the program is started. Another well-known type of program transformation is the inclusion on runtime checks, in which the program was instrumented in such a way that it is prohibited from conducting any policy-violating changes. [25]. Code obfuscation is the technique of creating source code or machine code that is challenging for humans to comprehend. Obfuscating code on purpose to hide its intent or logic is a common practice among programmers to avoid any chance of reverse engineering. A secure design and development cycle has also been put out in [26], and it offers a collection of design methodologies that make it possible to efficiently verify that a system component is free of any potential flaws from the design phase. Formal techniques provide the capacity to thoroughly study the design and pinpoint complex security issues, while not being simple ways. Techniques [27] and tools [28, 29] have been created to make it easier to verify mission-critical security attributes. These methods and technologies aid in converting more complex security goals into a set of atomic characteristics that can be checked.

3.1.3. Network infrastructure and protocol vulnerabilities

Early network protocols sometimes perform poorly in many of the circumstances in which they are used today since they were created to accommodate an altogether different environment than the one we have now on a much smaller scale. When both system administrators and users are unfamiliar with the networking architecture, weaknesses in network protocols are compounded. For instance, system administrators may fail to implement security filters or rules, choose an ineffective encryption strategy, or delay applying suggested fixes [30].

Exploiting the shortcomings of the widely used network protocols Internet Protocol (IP), Transmission Control Protocol (TCP), or Domain Name System (DNS) results in one of the most frequent network assaults. The IP is the network layer's primary protocol. It offers the data required for packet routing across network routers and computers. There was no method to verify the integrity and privacy of data being transferred in the original IP protocol. This made it possible for data that was being exchanged between two devices via an unidentified network to be intercepted or altered. To solve the issue, IPSec was created to provide IP traffic encryption [31]. For many years, IPSec has been one of the key technologies for building virtual private networks (VPNs), which provide secure communication channels across the Internet between distant computers and reliable networks (i.e., company intranet). TCP stands on top of IP to transfer packets in an orderly and reliable manner, including retransmitting missed packets. SSL was first created to offer end-to-end security between two computers that sit over the Transmission Control Protocol, as opposed to only layer-based security (TCP). Commonly, HTTP and SSL/TLS are combined to create HTTPS for secure Web sites. The mechanism that converts human-readable host names into 32-bit Internet protocol (IP) addresses is called a domain name server (DNS). When a user enters a URL, it effectively functions as an Internet directory book that instructs routers to send packets to a certain IP address. An attacker could be able to transmit malicious DNS messages to pretend to be an Internet server since DNS answers are not verified. The availability of DNS is a significant additional issue. The DNS service has been the subject of multiple Denial-of-Service (DoS) assaults since a successful assault on it would seriously impede Internet communication. [32].

By encrypting data so that only designated users with the right keys may decode it, cryptography is a crucial tool for protecting data that users transfer to one another. The most widely utilized method of data protection is cryptography. According to a 2007 Computer Security Institute report [33], 71% of businesses use encryption for their data in transit. Several initiatives are growing in order to better defend against the sophisticated attackers of today who take advantage of the weaknesses in the cryptographic algorithms that are now in use. The Advanced Hash Standard (ASH) will replace SHA-1 as of 2012, according to a recent announcement by the US National Institute of Standards and Technology (NIST) [34]. For applications that need high-speed encryption, identity-based encryption may be used instead of the sluggish 2048-bit RSA key length and the unrealistic participation of the trusted certifying authority.

The transmission of quantum states of light is used by two parties to concurrently produce shared, a secret cryptographic key material in quantum cryptography [35].

Today's skilled attackers use a cutting-edge approach to mask malicious traffic payloads so that they resemble normal traffic payloads more closely. In addition, new analytical methods are needed to compute and depict the uncertainty associated with data sets due to the enormous amount of data flow over high-capacity networks. In order to capture the network traffic with improved visualization approaches, this problem has generated a new field of study [36], requiring the combined skill sets of network practitioners and the visualization community. Network specialists with in-depth subject knowledge of networking systems then assess the data's visual display.

4. EMERGING THREATS

Cyber assaults in cyberspace change with time, using fresh methods. Cybercriminals often alter the malware signatures already in use in order to take advantage of weaknesses in the newest technology. In other instances, they just investigate distinctive qualities of the new technology to discover security gaps to introduce malware. Cybercriminals employ modern Internet technologies, which have millions and billions of active users, to their advantage to swiftly and effectively reach out to a large number of victims. To illustrate the risks in these emerging technologies, we use four of them as illustrative examples: Social networking, cloud computing, smart phones, and essential infrastructure are all examples of critical infrastructure.

4.1 SOCIAL MEDIA

Social media platforms like Facebook and Twitter have grown rapidly in recent years. At the end of 2012, there were more than 450 million active user accounts on Twitter, but there were approximately 1 billion members on Facebook [37]. Most young generations now prefer using social networking sites as their primary form of communication. Each of these social networking platforms often offers facilities for users to post content such as images, stories, and links while also sharing personal information (such as name, address, gender, and preferences for music and movies).

Attackers are using the popularity of social media as a new platform for conducting sneaky assaults. More than 43,000 harmful files about social networking websites were included in the Kaspersky Lab collection by the end of 2008 [38]. An alarming increase in assaults on users of social networking networks has been documented in research released by IT security and data protection company Sophos. A little more than 60% of users of social networks have received spam, according to their survey [39]. Attackers have full access to user profiles, allowing them to discover corporate and business secrets. According to a Sophos poll, almost 60% of businesses worry that their staff is sharing too much information on social media, and 66% believe that social media use poses a danger to their businesses.

The most well-known malware attack that makes use of the expansion of social media sites is the Koobface worm [40], which spreads via social networking networks in 2009. The Koobface botnet uses its zombie arsenal to automatically create new social media profiles that are meant to befriend unsuspecting people and spam them with tempting links that lead to infection. Social engineering assault victims see how their social networking accounts are used to spread spam to the victims' friends, and how their computers are turned into zombies. The Koobface botnet was breached by Thomas and Nicol [40], who created a zombie emulator that was able to identify fake and compromised social network accounts that were used to spread malicious links to over 213,000 social networks users, resulting in over 157,000 hits. They found that the most well-known blacklisting services, which are currently provided by social network providers, are inefficient at filtering harmful viruses. While those who discovered that 81 percent of citizens to Koobface's spam occur during the first two days of the a link being posted, they claimed that all those blacklisting services just recognize 27 percent of threats as well as respond in an average of four days, leaving the majority of internet users vulnerable. Another common malware assault involves the deployment of a sizable number of phony or inactive Twitter or Facebook accounts. Cybercriminals' attempts to pass for reliable users are getting far more sophisticated. Then, the scammers persuade visitors to "like" or follow them on the social networking site and click on their status updates, which often direct users to harmful websites. Another research [41] shows that a lot of malware propagated when users clicked on articles related to "trending" subjects on Twitter has also explored how to use mock-up services on Facebook to propagate malware through understanding social network platforms.

Because of the centralized gathering of huge amounts of user data, the proximity of the gathered personal information, as well as the accessibility to current information that is continually tagged and shown, social networks have dramatically raised the stakes of privacy protection. [42]. Due to this, social networking sites are a desirable target for several businesses looking to collect vast quantities of user data, some for good and others for bad. The majority of the time, data extraction breaches consumers' expectations of privacy. It has been investigated how to safeguard users' private information stored by social networking service providers. Lucas et al [43] suggested a Facebook application for employing client-side JavaScript to encrypt and decode sensitive data. This design makes sure that no data ever reaches the service providers for social networks in an unencrypted form, preventing them from tracking and compiling the data that users transfer over the network. Issues about privacy awareness and solutions that might assist users in configuring their privacy settings more easily have also been suggested. For instance, a privacy wizard was suggested by Fang and LeFevre [44]. The wizard repeatedly requests that the user give certain friends privacy "labels," and then utilizes this information to build a classifier using a machine learning model that can then be used to automatically provide rights to the remainder of the user's friends. The design's inspiration came from the fact that actual users conceptualize their privacy choices for which friends should be allowed to see which information based on an implicit set of guidelines they establish and often use in most friend settings.

4.2 CLOUD COMPUTING

Customers who store their data in DropBox and iCloud, manage their email using Gmail and Live mail, and keep track of their life using services like Evernote and Mint.com are drawn to the benefits of shifting data and apps to the cloud. Undoubtedly, one of the most important technological advancements in recent years is cloud computing [45]. The sheer concept of utilizing computers in a way that is comparable to using a utility is altering the world of IT services and has enormous potential. Customers are driven to the cloud by its promises of agility, lower capital expenditures, and improved IT resources, whether they are major corporations or small companies. IT organizations are moving away from building their own IT infrastructure and toward using the cloud's compute services for their information technology requirements [46].

Unlike conventional methods, cloud computing has certain qualities that set it apart. On-demand self-service, ubiquitous network access, location-independent resource pooling, quick elasticity, and measurable service are the five main features of cloud computing, all of which are focused on utilizing clouds smoothly and transparently [47]. When resources are pooled together to serve several customers rather than being allocated to one user, this capability is referred to as resource polling. These consumers are given and given away resources as necessary, whether those resources are at the application, host, or network levels. On-demand self-service refers to a situation in which customers may automatically

allocate themselves more resources, such as storage or processing capacity, without human involvement. Similar to autonomic computing, which enables a computer system to manage itself. Along with resource self-provisioning, the capacity of cloud computing to find and release resources as quickly as required—a characteristic known as "elasticity"—defines the technology. As a result, users may scale up the resources they require whenever there are strong loads or consumption spikes, and when they are done, they can scale down by returning the resources to the pool [47]. The ability to provide the cloud as a utility where customers pay on a consumption basis, much as it is done to pay for utilities like electricity, gas, and water, is made possible by measured service, also known as pay as you go.

Another integration paradigm that uses different resources and distributes different resources to clients at different tiers of the system is cloud computing. The hardware layer (including data centers), the infrastructure layer, the platform layer, and the application layer are the four main layers that make up the architecture of a cloud computing system [48].

- **The hardware layer**: The physical resources of the cloud, such as actual servers, routers, switches, and power and cooling systems, are managed by this layer. In actuality, data centers are often where the hardware layer is put into use. Thousands of servers are often housed in data centers, where they are arranged in racks and linked by switches, routers, or other fabrics. Hardware setup, fault tolerance, traffic management, and resource management for power and cooling are typical problems at the hardware layer.

- **The infrastructure layer:** The virtualization layer is another name for this layer. By leveraging virtualization technologies like Xen, Kernel-based Virtual Machine, and VMware to split the physical resources, the infrastructure layer generates a pool of storage and computational resources. The infrastructure layer is crucial to cloud computing since virtualization technologies are the only ones that can provide several vital capabilities, such as dynamic resource assignment..

- **The platform layer:** Operating systems and application frameworks make up the p**latform** layer, which is built on top of the infrastructure layer. The platform layer's goal is to lessen the difficulty of delivering programs directly into VM containers. For instance, Google App Engine works at the platform layer to allow API implementation for storage, databases, and business logic of ordinary web apps.

- **The application layer:** The real cloud apps are found at the application layer, which is at the top of the structure. The automatic-scaling functionality may be used by cloud applications, as opposed to conventional ones, to improve performance, availability, and operational costs.

In actuality, clouds provide three types of services: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) [49]. Depending on the underlying delivery and deployment patterns, applications operating on or being created for cloud computing platforms present a variety of security and privacy problems. IaaS allows users to construct and operate applications on a set of virtualized infrastructure elements, such as storage and virtual machines (VMs), provided by the cloud provider. The virtual machine and the virtual operating system will ultimately house the program. Programming environments may now access and use more application-building elements thanks to PaaS. Such programming environments have a clear effect on the architecture of the application, imposing limitations on what services the application may ask the OS for. The cloud service providers allow and provide application software as on-demand services via SaaS, to finish.

Cloud providers may more effectively control resource use thanks to a technology called multi-tenancy, which divides a virtualized, shared infrastructure among several clients. For instance, Amazon utilizes hypervisors at the hardware level, but Salesforce.com uses query rewriters at the database level to isolate the data of various tenants. In this context, virtualization is a key enabling technology that makes resources and infrastructure accessible to customers as separate virtual machines (VMs). There is current research in the areas of strong isolation, mediated sharing, and secure communication across VMs. One possible fix has been proposed [50]: using a flexible access control system that controls the management and sharing capabilities of VMs inside a cloud host. Important concerns involve safely composing them and guaranteeing that the information managed by these written services is effectively safeguarded since consumers purchase and employ software components from various vendors [51]. For instance, a PaaS environment could restrict access to clearly specified file system components, necessitating the use of a fine-grained authorization service. The outsourcing model of the cloud, in which cloud providers control and manage users' data and services, forces clients to have a high level of trust in their provider's technical competence [52]. As a result, trust management and policy integration are active areas of research in cloud computing. The interconnections between various service domains in cloud computing systems are also intense, dynamic, and driven by service needs. Thus, a framework for developing trust has been suggested to enable the effective capture of a general set of factors necessary for creating trust and handling changing needs for interaction and sharing [53]. Another prominent field of study to solve issues like semantic heterogeneity, safe interoperability, and management of

policy evolution is cloud policy integration [54]. Additionally, client behavior might change quickly, which has an impact on established trust standards. This implies the necessity for an integrated, trust-based, secure interoperation framework that aids in the creation, maintenance, and negotiation of trust to promote policy integration adaptively [55].

4.3 SMARTPHONES

Smartphones have evolved into more advanced computers and communication tools that people can easily carry with them throughout the day thanks to advancements in wireless technology. They are an appealing method for planning and organizing people's professional and personal lives because of the combination of rising computational power, personalization, and mobility. According to [56], there is an immediate need for proactive mobile security solutions given the vast number of mobile phone users around the globe. Over 4.5 billion people are predicted to use mobile phones daily, and by 2013, 2 billion smartphones are anticipated to be in use.

More and more sensitive data is being saved on cellphones beyond just basic SMS texting. These technologies are fundamentally altering how information systems are organized inside businesses, which has led to the creation of new hazards. Access must be restricted as cellphones gather an ever-increasing quantity of private data in order to safeguard user privacy and corporate intellectual property.

Due to the exponential rise of mobile technology, cybercriminals now have an appealing target. Due to their integrated nature and unique operating environment, security challenges in mobile are distinct from the usual security issues in PC and corporate computing. The following elements specific to mobile computing were mentioned by Mulliner [57].

- **Mobility:** The most significant feature of mobile phones is this. Compared to fixed gadgets, mobile devices have a higher potential of being physically damaged, stolen, or lost since mobile users may take them anywhere.
- **Strong Personalization:** Mobile devices are typically used by a single user and are not shared.
- **Strong Connectivity:** In order to share data with other devices, mobile phones often connect to them through wireless networks (or wireless Internet).
- **Technology Convergence:** Today's mobile phones provide a wide range of useful capabilities, such as gaming, video and data sharing, and web surfing.
- **Limited Resources and Reduced Capabilities:** Mobile devices have four main drawbacks in comparison to stationary computers: a) short battery life; b) low computational power; c) tiny display screens, and d) tiny input buttons. Building mobile security systems is difficult because of these constraints.

Several distinct attack types aim to profit from the rise of mobile computing. Attacks on communications stem from shortcomings in the planning and administration of the mobile communication infrastructure. The attacker could attempt to bypass the mobile network's encryption. The A5/1 and A5/2 algorithms, the latter of which is believed to be weaker, are the two variations of the GSM (Global System for Mobile Communication) network now in use. It has been shown that the encryption can be broken in around 6 hours when the technique was made public [57]. To get information, an attacker may attempt to eavesdrop on Wi-Fi conversations (e.g. username, password). Smartphones are not immune to these assaults; nevertheless, they are particularly susceptible to them since Wi-Fi is sometimes their sole connection to the Internet. The study of Bluetooth security vulnerabilities on mobile devices has shown a variety of difficulties. Cabir, for instance, is a worm that spreads through Bluetooth [58]. The worm uses Bluetooth in discoverable mode to look for neighboring phones before sending itself to the target handset. The user has to install the software and accept the incoming file. The worm infects the system after it has been installed. Network traffic exchanged by phones may be watched, such as surveillance on network routing points or watching the usage of network mobile protocols, to avoid threats connected to communication.

The vulnerabilities in mobile software, especially when mobile web browsers are exploited, may be used to launch other types of attacks. Mobile web browsers, like traditional online browsers, provide additional features such as widgets and plug-ins that help hackers spread malware. Web browser flaws[121] brought on by a stack-based buffer overflow in a library that the web browser used were the foundation of the whole jailbreaking procedure for iPhones. A vulnerability in the Android web browser that might be exploited by utilizing a weaker library was discovered in October 2008 [59].

Malicious attackers that wish to spread malware mostly target mobile devices [60]. The Center for Emerging Cybersecurity Threats at Georgia Tech [61] and Symantec's Danger Reports [62] have both published studies in the past few years that have increased public awareness of the threat posed by malware specifically made to target mobile devices like Apple iPhones and Google Android-based phones. To stop malware from spreading, mobile carriers provide a centralized public marketplace with an approval process before hosting the application. Any software that is regarded as questionable

is eliminated with the help of the central marketplace before being downloaded by users. For instance, Apple employs a screening process before any apps are made accessible through the App Store to ensure that all comply with Apple's rules. Apple gives its approval by employing encryption keys to sign the application's code. The App Store is the only place where iPhone users may get apps. Android has a public marketplace where applications may be discovered, much like Apple. However, unlike Apple, the Android application may be self-signed. Android uses crowdsourcing to get app user evaluations. Based on user concerns, applications may be removed from the device and the market. Another tactic employed by mobile businesses to protect their mobile platforms is the idea of sandboxing. By compartmentalizing distinct processes to stop them from interacting and damaging one another, sandboxing greatly minimizes the potential of malicious code being injected and prevents currently running processes from engaging in destructive behavior. While Apple iOS focuses on limiting access to its API for programs from the Apple Store, Android uses its sandboxing on an underlying legacy Linux kernel.

4.4 CRITICAL INFRASTRUCTURE

The health of the economy and the reliability and security of the key infrastructure systems that support contemporary society is of utmost significance to both. A nation's vital infrastructure is mostly supported by its cyber systems, which implies that a serious security event on one of these systems might have a big influence on the dependability and security of the physical systems that depend on it. The most current data, which is supported by official publications [63], shows that physical and cyber assaults on vital infrastructure systems like electric grids are becoming more frequent and sophisticated. Critical infrastructure cybersecurity aims to keep the weaknesses of these systems and buildings to [64]:

- **Terrorism** – Those responsible for the purposeful targeting of crucial infrastructure do so for political purposes. The Taj hotel and the Mumbai Central Station were targeted intentionally in the November 2008 Mumbai assault.
- **Sabotage** – Ex-employees, political opponents of governments, environmental organizations fighting for the environment, and so on. For instance, protesters recently took control of Bangkok's international airport.
- **Information warfare** – Private individuals hacking for personal gain or nations launching assaults to collect data and harm a nation's infrastructure For instance, during the dispute between Estonia and Russia over the transfer of a complex burial market and war graves, a wave of cyberattacks deluged the websites of Estonian entities, including the parliament, banks, ministries, newspapers, and broadcasters.
- **Natural disaster** – hurricanes or other natural disasters that cause essential infrastructures, such as water and electricity systems, and oil pipelines, to be damaged

The intricacy of these infrastructures' interconnections, which may result in a variety of issues, makes critical infrastructure protection more difficult to solve than ICT protection [65]. Consider the electrical grid, which transports electricity from geo-graphically separated production locations to various voltage level stations (from higher to lower voltage) before it reaches our homes. Supervisory control and data acquisition (SCADA) systems, which are remotely linked to supervision centers and the corporate networks (intranets) of the businesses controlling the infrastructures, are often used to manage both the production and distribution locations. To make it easier to communicate with power regulators and end users, for instance, the intranets are connected to the Internet. These connections provide outside attackers with a route. SCADA systems may be accessed remote-ly by operators for maintenance tasks, and sometimes equipment providers maintain modem connections to the systems. In order to suggest ways to defend the nation's vital infrastructure, it is necessary to consider the presence of proprietary solutions and the usage of outdated versions that are rife with security flaws.

Researchers are continually working to understand the characteristics of critical infrastructure systems since research into critical systems is still in its early stages. Understanding the criticality of a system, the interdependencies across systems and infrastructures, and detecting and quantifying the effects of assaults on the critical systems are all included in this. Due to the close reliance of these systems and the millions of users on them in their daily lives, the essential infrastructure must continue to run smoothly. Heartbeats, challenge-response, built-in monitoring of vital operations, and detection of process abnormalities as self-diagnostic procedures that may capture any indications of non-operative processes have been suggested. The creation of self-healing systems to pursue automated and coordinated assault response and recovery is another pertinent area of focus [66].

4.5 OTHER EMERGING AREAS OF CONCERN

Due to the growing usage of embedded systems and sensors in many aspects of our life, these issues have drawn more atten-tion from both business and academics in recent years. As an example, embedded tiny gadgets that are installed

in automo-biles, household appliances, mobile phones, and audio/video equipment becoming a bigger part of our life every day. Similar to this, sensors are being used in more extensive research and commercial applications in the military, sciences, and business, such as the observation of biological ecosystems, farming, and industrial operations. Due to their distinct embedded structure and operating environment, security concerns in these sectors vary from the usual security issues in PC and corporate computing [67]. As a result, embedded systems and sensors often have to employ smaller CPUs, which have less storage for security over-head, such as holding a large cryptographic key. As a result, in the area of embedded systems, the majority of corporate securi-ty solutions are ineffective. Due to their compact size, embedded systems and sensors have limited amounts of energy, memory, processing power, and bandwidth for communications. Their physical trust border is exceedingly flimsy. For instance, they may be put in homes and businesses, placed outdoors, or carried by people in their hands or pockets, allowing for a variety of physical assaults. They often do not employ an operating system's protection, instead using a close relationship between hardware and software. Different sets of security flaws have been produced by the embedded nature of embedded systems and sensors [68]. For instance, embedded systems are susceptible to assaults that deplete their battery power because of their restricted battery capacity [69]. Embedded systems are vulnerable to assaults that need physical access to the system because of how close they are to a prospective attacker. This makes it possible for attackers to conduct attacks that entail studying how a physical system is being used, such as power analysis attacks or system bus spying attacks. Systems that are embedded must function in a realistic context. The operational environment of embedded systems is largely exposed, making them susceptible to assaults that cause the device to overheat (or cause other environmental damage). An embedded system that has been sto-len is reprogrammed by attackers for future abuse. In this discipline, there is a lot of interest in the standard security measures to prevent unwanted access via user authentication, methods to maintain data integrity using cryptographies, and network defensive mechanisms. Though fairly uncommon, approaches like masking, window methods, and fake instruction insertion in the code/algorithm have been suggested [70] to avoid assaults carried out by analyzing or modifying the physical system. Since network connectivity through wired or wireless access is becoming more widespread for embedded systems to improve remote control data collection and update, the vulnerabilities that exploit such network connectivity, such as virus spread and wire tapping, have grown to be another source of growing concern in the industry.

Politically motivated hacking for sabotage and espionage is referred to as cyberwarfare. The term "cyber warfare" refers to "activities by a nation-state to breach another nation's systems or networks for the intent of inflicting harm or disruption," ac-cording to the book Cyber Ware [71]. The majority of cyber warfare worries are centered on invasions of national security and disruption of vital national infrastructure [72]. The former instance involves international espionage, in which unauthorized individuals unlawfully access or modify secret material that might compromise national security. The latter instance is con-cerned with any possible disturbance to the nation's vital infrastructure, including the transportation and electrical grids. The Department of Homeland Security carried out a mock drill in 2008 under the codename "Cyber Storm." The exercise was de-signed to evaluate the country's protection against cyber espionage. The Cyber Storm exercise revealed the weaknesses and inadequacies in the country's cyber defenses. Researchers have now suggested many additional goals for the country's cyber security strategy [73]. It has been suggested [74] to identify the Internet-enabled systems that are essential to a country's cyber security as well as any interdependencies between the systems. There have been many suggested methods for securing the vital infrastructures of the country, including threat mitigation and response, vulnerability assessment and rectification, and threat mitigation.

5. PREVENT CYBERCRIME

5.1 PREVENT EXPLOITING EXISTING VULNERABILITIES

The conventional method has chosen packaged security protection strategies that shield everything within from outside threats, even though several distinct techniques and ideas exist to address vulnerabilities in the hardware, software, and network layers. To protect their network from any possible outside incursion, the vast majority of businesses use a perimeter de-fense security strategy [75]. This strategy emphasizes "layered defense" or "defense in depth" tactics in which crucial internal IT assets, such as servers or mission-critical data, are guarded by fortifications and walls.

Technology such as firewalls and intrusion detection systems are common perimeter defenses (IDS). The most popular tech-nique for safeguarding internal assets has been the firewall. Its main goal is to manage the incoming and outgoing network traffic by inspecting the data packets and deciding whether to let them through or not by a predefined set of rules. A firewall may be positioned at many network infrastructure layers. Network layer firewalls, sometimes referred to as packet filters, func-tion at a very low level of the network layer and prohibit packets from passing through the firewall unless they comply with the specified rule set (i.e., settings) provided by network administrators. The network layer firewalls cannot filter unwanted traffic, such as malware payload, that uses valid IP addresses and ports, despite the fact

that many newer firewalls are more intelligent. Application layer firewalls function by observing and perhaps blocking input, output, or system service calls that do not adhere to the network layer firewall's specified rules. By responding to the input packets (such as connection requests) as an applica-tion while blocking other packets, a proxy server may function as a firewall. Proxy servers and application layer firewalls both increase the difficulty of breaking into an internal system. However, attackers nowadays have developed more sophisticated attack techniques to send malicious packets to a target network due to their improved skill and sophistication. For instance, hackers might take control of a system that is accessible to the whole public and utilize it for their ends. In order to disguise the sender's identity or impersonate another computer system, the intrusive party produces packets with a faked IP address using the intercepted proxy.

Any suspicious or unusual behavior occurring across the network is filtered by the intrusion detection systems [19], [47]. These detection systems are useful in that they try to identify the first phases of an attack (such as an attacker exploring a computer or network for certain vulnerabilities) and may subsequently help shield a machine from the later phases of the as-sault. Additionally, these systems look for telltale signals of questionable behavior or patterns, whether they come from a user, an application, or malicious code, which firewalls or other security tools may overlook or ignore. To detect malicious network payloads, there are several detect system variations available. These discoveries are either anomaly-based or signature-based. When an attack packet crosses the network gateway threshold using signature-based detection, the detection system may iden-tify the attack packet based on its well-known fingerprint or signature. The detection mechanism in anomaly-based does not already know what bad packets are. The detection system analyzes the pattern to identify what typical traffic looks like, often in real-time and reports anomalous traffic behaviors based on the pattern analysis. As the prevalence and skill of malware writers have increased in recent years, the signature-based detection technique has been deemed inefficient [16], [17]. Pattern recognition techniques, which are often used in the signature-based approach, are said to make it very hard to keep up with malware signatures that are constantly developing. A current field of study is the proposal of enhanced anomaly-based detec-tions [75]. By watching traffic for a long time and developing a model of the underlying process, the system in this way learns by doing (self-learning) what is usual. As the malware's signature changes, the process adapts on its own (evolves).

To create stronger defenses against unwanted traffic originating from outside sources, it is necessary to take a more broad approach to understand network attack patterns rather than concentrating on solving individual problems with firewalls and IDS. Network forensics is the study of eavesdropping on Ethernet, TCP/IP, or the Internet to monitor and analyze network data, including web browser, email, newsgroup, synchronous chat, and peer-to-peer communication. The evidence is utilized in court cases or to analyze patterns of network traffic attacks. In order to identify the computer that sent the email and identify the sender, eMailTrackerPro [15] examines the email header. Tools like SmartWhoIs [16], which look up all the information that is available about an IP address, hostname, or domain, including country, state or province, city, name of the network provider, administrator, and technical support contact information, are useful for investigating web browser traffic. Users may examine website URLs that are saved in the history files with the help of a Web Historian [17]. The Index.dat analyzer [8] is a forensic program used to look into index.dat files and evaluate the cache, cookies, and browser history. While AirPcap [10] is the packet capture utility for IEEE 802.11b/g Wireless LAN interfaces, WinPcap [9] collects packets received at the network interface of a device running the Windows Operating System. Honeypots are employed in research to acquire data on the intentions and strategies of cybercriminals. A honeypot is a trap that is put up to catch anyone trying to access resources without authoriza-tion [52]. Any data collected by honeypots are used to study the dangers that companies face and discover better ways to defend against them. Multiple honeypots may often be hosted on a single physical system using virtualization methods. There-fore, there is a prospect for a speedier recovery at a lower cost even if the honeypot is compromised. For monitoring a bigger and more diversified network, a large honeypot is utilized, such as a honeynet that joins two or more honeypots on a network. Commonly used as a component of bigger network intrusion detection systems. A centrally located collection of honeypots and analytical equipment is known as a honey farm [54].

Access control techniques have been developed to allow an authority to restrict access to just certain resources since it is im-possible to provide universal access to resources. The entities that may conduct actions inside the system are referred to as "subjects" in access control, while the entities that represent resources to which access may need to be regulated are referred to as "objects" in access control. A person is given access to an item under the capability-based access control if they possess a reference or capability. For instance, if a person enters a valid userID and password, they may read their bank statement. Through the transmission of such a capacity through a secure channel, access is granted to a different party. For instance, a certificate may be generated and given to the user for verification purposes. In a method based on access control lists, a sub-ject's access to an object is contingent upon whether its identity is included on a list connected to the object. For instance, Alice would be permitted to examine patient information if she was included among the physicians. The list may be edited to indi-cate access. For instance, Alice won't be able to access the patient's information once she leaves the hospital since she is no longer listed among the physicians. Role-based access control, mandatory access control, and discretionary access control are the three approaches that are most often used (RBAC). In DAC, the

owner controls who has access to what items and what rights they are granted. In the MAC approach, the operating system limits how subjects (such as processes or threads) can ac-cess or interact with objects (such as files, directories, TCP/UDP ports, or shared memory segments), either by a rule that speci-fies specific conditions or by a mathematical structure that specifies greatest lower-bound and least upper-bound values. RBAC is a more recent substitute strategy for MAC and DAC that limits system access to authorized users only. The majority of businesses utilize it, and the majority of IT suppliers provide RBAC in one or more of their products.

Access control techniques have been developed to allow an authority to restrict access to just certain resources since it is im-possible to provide universal access to resources. The entities that may conduct actions inside the system are referred to as "subjects" in access control, while the entities that represent resources to which access may need to be regulated are referred to as "objects" in access control. A person is given access to an item under the capability-based access control if they possess a reference or capability. For instance, if a person enters a valid userID and password, they may read their bank statement. Through the transmission of such a capacity through a secure channel, access is granted to a different party. For instance, a certificate may be generated and given to the user for verification purposes. In a method based on access control lists, a sub-ject's access to an object is contingent upon whether its identity is included on a list connected to the object. For instance, Alice would be permitted to examine patient information if she was included among the physicians. The list may be edited to indi-cate access. For instance, Alice won't be able to access the patient's information once she leaves the hospital since she is no longer listed among the physicians. Role-based access control, mandatory access control, and discretionary access control are the three approaches that are most often used (RBAC). In DAC, the owner controls who has access to what items and what rights they are granted. In the MAC approach, the operating system limits how subjects (such as processes or threads) can ac-cess or interact with objects (such as files, directories, TCP/UDP ports, or shared memory segments), either by a rule that speci-fies specific conditions or by a mathematical structure that specifies greatest lower-bound and least upper-bound values. RBAC is a more recent substitute strategy for MAC and DAC that limits system access to authorized users only. The majority of businesses utilize it, and the majority of IT suppliers provide RBAC in one or more of their products.

The fundamental functions, including accountability, authorization, and authentication, are offered by traditional access control systems. The process of confirming that a person is connected to an item is known as authentication and authoriza-tion. To identify a person and determine if that subject has the proper authority to access an item, traditional authentication and authorization systems employ three main elements. Your knowledge, such as a password or personal identification number, serves as the first factor (PIN). This presupposes that the only person who knows the PIN or password required to access the account is the account owner. The second component is something you own, such as a security token or smart card. This pre-supposes that the only person with the requisite smart card or token to unlock the account is the account owner. The third component is something about you, like your voice, fingerprints, or iris features. The layered method, also known as strong authentication, which response to the presentation of two or more authentication elements, is the current trend in authentica-tion [55]. There are several designs for small authentication tokens that have been presented. These tokens have a crypto-graphic key stored on them in tamper-proof storage. Utilizing the widespread availability of modern computers with USB ports, USB-based tokens have also been suggested [56], [13] either as a simple means of storing an X.509 certificate or often as a means of executing the challenge/response protocol. A variety of authentication procedures aimed at mobile users have been developed [56], [57], and [58] to capitalize on the population of mobile users, which is constantly expanding. Only a few uses of biometric technology have been implemented. There is growing interest in using biometric authentication technologies in the network environment, and certain PCs and workstations have gotten more sophisticated with audio-visual interfaces [59], [60], [62].

6. PREVENT EMERGING THREATS

The malware detected in the new technologies we outlined above has several similar features.

A. Increased Attack through Web Browser – Web browsers are often used to provide the services offered by new technologies. Undoubtedly one of the most widely used programs is the web browser, which gives users access to a variety of functions and connects them to the outside world. Thus, web browsers are a tool that millions of people who use computers now use more and more often. Web browsers have a multitude of security flaws, just like any other piece of software [70], [71]. These flaws are used by the attackers to get access to the victim's computer, steal their data, delete their files, and attack other computers using the victim's compromised machine. A study by Osterman Research [3] found that 11 million malware types had been found by 2008, and 90% of this malware was downloaded secretly from well-known and often trusted websites.

Scripting languages like JavaScript or VBScript as well as extensions, which are sometimes referred to as "plug-ins" or "add-ons," are some of the popular assaults that take advantage of browser security. Extensions are reusable software parts that may be inserted into a browser to provide new features or alter the way users interact with a website. Anyone who

has some knowledge and training in software development may create an extension, which many unwary consumers can download for free. These extensions often include software flaws, which dramatically expand the attack surface available to attackers. The addition of several features and interactivity to a web page is made possible by the ability to execute scripting languages like JavaScript or VBScript. Attackers, however, have the capacity to misuse this feature. Cross-site Scripting is a well-known flaw in scripting languages that may be exploited (XSS). Attackers may insert harmful scripts onto web pages using XSS. Harmful code is run to carry out malicious actions on a user's machine when unwary customers access the web pages.

To guarantee that the online page is only accessible by authorized users, the most frequent protection method against web browser vulnerabilities takes the shape of stronger user authentication. Another widely used method [69] for finding any dan-gerous scripts included in web pages is content filtering. To strengthen browser security, certain browsers or browser extensions may be set up to deactivate client-side scripting on a per-domain basis. The Internet naturally offers anonymity. To take ad-vantage of this aspect of the Internet, there are now a substantial number of online assaults. A requirement has been increased [61] that both users and the server must authenticate themselves to users in order for both sides to be certain of the other's iden-tity. To meet this need, the method is known as "mutual authentication" has grown in favor. Password authenticated key ex-change (PAKE), Dynamic Security Skins (DSS), and the remote attestation method suggested by Trusted Computing Group (TCG) are some of the mutual attestation mechanisms currently being explored [70].

B. Platform Switch – The battleground for cybercrime is shifting from desktops to other platforms, such as mobile phones, tablets, and VoIP. Malware designed specifically for mobile platforms is increasing as a result of the increased use of mobile devices worldwide and their increased ability to provide numerous internet services. In 2012, there were 17 times as many dis-tinct malware detections for Android as there were in 2011, according to research [1]. Similar security trend studies [16], [17], and [11] express similar worries about the propagation of malware on ubiquitous computing systems. For instance, a mobile version of the wildly popular banking Trojan Zeus is already being developed [11]. Cybercriminals also use SMS phishing, of-ten known as "smishing," to target mobile devices. VoIP technology is become more dependable and offers higher-quality calls. Presently, leading manufacturers include VoIP in their integrated multimedia experiences that are available in programs like Skype, MSN, Facebook, etc. Internet telephony is increasingly being targeted by cybercriminals since it handles more and more data. Attacks on VoIP infrastructure, in particular, are increasing. Voice is vulnerable to abuse when it is digitized, encoded, compressed into packets, and sent across IP networks. It is a fear that VoIP may attract cyber criminals who will use it for voice fraud, data theft, and other crimes. Vishing (also known as telephone-based phishing) tactics, which are becoming more and more common, are supported by VoIP systems.

C. Social Engineering Scams - According to industry analysts [71], and [76], major social networking sites like Facebook and Twitter are increasingly being utilized as a delivery system to trick unwary users into installing or spreading malware. When using social engineering to distribute malware, attackers have almost no creative constraints. An adversary may, for instance, use a social network to befriend a gullible user and then trick them into knowingly running malicious malware on the victim's computer. This happens often under pretenses. The malicious party requests that a user install a certain "codec" in order to play the movie or click an image file attached to a spam email, but these actions end up installing malware. Social networking sites also play a bigger role in cybercriminals' efforts to find money mules to help with their money laundering activities throughout the world. Spammers are using users' faith in their social networking connections to lure in new victims in addition to forging social networking communications to get targeted to click on links in emails.

Bots (short for "robots") are malware programs that are secretly placed on a user's computer and enable an unauthorized us-er to remotely manipulate the compromised computer for a range of destructive reasons. There are more organized attacks employing botnets. Botnets are collections of computers that have been infected with malicious software and placed under the command of an enemy. Because they provide a distributed platform for significant unlawful operations in the cyber space, such as distributed denial of service assaults (DDoS), botnets are emerging among the many types of malware as the most severe danger to cybersecurity [15], [16], and [17]. The negative effects would be catastrophic if bots were to proliferate across developing technologies with hundreds of millions or perhaps billions of registered users.

Earlier bots communicated with an enemy operating a Command and Control (C&C) server from a distance via covert channels on the conventional Internet Relay Chat (IRC) protocol. This method of communication is quite simple to identify in plaintext. Bot masters have evolved their approaches and methods to escape detection as knowledge of botnets has grown. The most popular techniques include rootkits, domain flux, encrypted traffic, and Internet protocol [77]. Alternative protocols like HTTP or HTTPS are used by more recent bots. The most used network protocol, HTTP, makes it difficult to filter out bot activity, making it helpful for bot masters. Additionally, using HTTPS encrypts the orders, making it difficult to identify or keep track of the communication between an opponent and a botnet. Another technique used by many botnets to evade discovery is domain flux. The botmaster creates a list of domain names and often switches the point of contact. This makes it difficult to disable or stop the C&C server, even when their locations are discovered at a certain

moment but afterward shift as a result of the domain flux approach. Rootkits are another tool used by bot masters to mask a system's vulnerability. Rootkits, like webroot [4], evade detection by antivirus software by using a variety of tactics, such as altering boot records, which force the rootkit to start before the antivirus program when the machine boots up.

The signature-based defensive systems provide a built-in defense against botnets. It has also been suggested to use Internet-scale virtual testbeds and containment technologies in addition to catching the virus by comprehending its signature [15]. Inter-net-scale emulators are designed to capture botnets using a vast network of honeypots that entice any malware for further investigation. This makes it possible to observe the activity of botnets and develop new defenses against them. For the testbeds, it has been recommended to employ a hybrid of honeynet and virtualization approaches [74]. In these methods, malware is interacted with in order to capture a copy of it for later examination. A virtualized network environment is set up on unused address space. The containment technology's research hypothesis acknowledges that bots and other viruses are a natural com-ponent of the computer environment. Instead of attempting to protect the whole system, it promotes the concept of securing only a portion of it, enabling trustworthy transactions to occur from a potentially unsafe system. In order to catch botnets em-ploying a tiny portion of a trusted compartment in an untrusted computing environment, industry research is expanding virtual machines to Trusted Platform Module (TPM) and hypervisor technologies in hardware and software [15].

D. Insider Threats – Protecting important resources from external threats has been the main focus of earlier research on cyber security. But according to studies [16, [17], a significant portion of security and privacy breaches are caused by insider assaults. Because insiders may have access to many sensitive resources and high-privileged system accounts, protecting against insider threats is difficult. When the authentication is exploited by an insider, similar types of exploitation are mentioned in [63], [64].

Research on insider threats has placed a strong emphasis on monitoring in order to identify any unique access patterns used by insiders. There have been several visualization tools that suggested tracking rights requested and granted about each person and each item [63], [64]. Insider abuse and alleged abnormalities are often found using multidisciplinary detection systems. Using data mining approaches [52], behavior-based detection to uncover insider threats [15], and an integrated model that combines prediction and detection techniques are some of the new detection strategies that are being developed in this field. To safeguard systems against excessive privileges granted by system insiders, new breeds of access control techniques have been tried. The division of privileges and multi-level access control are two recent innovations in access control that are particularly effective against insider threats. Various anti-tampering systems have been examined depending on whether insiders have unauthorized physical access or logical access [63]. [63] explores the security that maintains the integrity of many levels at hardware, software, and data with finer-grained controls. By looking through system log files, audit trails have also been uti-lized to identify users who have used the system [15]. However, several ways to establish audit trails that are unalterable (for example, once-writable) and non-bypassable are recommended due to the possibility that insiders may have high power over most system files, including logs.

7. FUTURE OF CYBERCRIME AND TECHNOLOGICAL DEVELOPMENTS

Estonia may think about comprehensive anti-cybercrime capacity development, pursue legal, regulatory, and organizational agility, and invest in technology experience, skills, and research to prepare for and lessen the effect of future technologies on cybercrime.

ICT (information and communication technology) and digital systems are now indispensable in all spheres of economic activity in Europe and beyond. Today, many enterprises and the smooth operation of society depend on having access to the inter-net and an unhindered flow of information.

Therefore, purposeful or unintentional cybersecurity events have the potential to significantly disrupt both economic and social activity as well as important services. Cybercrime is a huge and expanding danger to digital systems, as well as to the safe operation of digital institutions and economies.

In response to a request from the government of Estonia, the European Commission's Structural Reform Support Service (DG REFORM) hired RAND Europe to perform an examination of emerging technologies and identify those that could influence cybercrime.

The study examined the potential implications of technology progress on cybercrime and proposed potential strategies for avoiding future technologies from being misused by criminals by using horizon scanning, desk research, expert interviews, and serious gaming.

Seven new and emerging technological clusters were highlighted by researchers as having the potential to significantly affect cybercrime during the next ten years:

1. Artificial Intelligence/Machine Learning

AI and machine learning can boost attack autom tion, speed, frequency, and efficiency while also enabling the possibility of targeted assaults that are specifically aimed at certain groups. They could also speed up cyber detection, protection, and recovery systems from a cybersecurity standpoint [70].

2. Autonomous Devices and Systems

Autonomous systems might be used to carry out covert crimes and create new ways for criminals to operate or launch massive, automated strikes. They may also make forensic investigations more difficult to conduct and make it more difficult to pinpoint the origin of crimes brought on by autonomous gadgets [71].

3. Computing and Data Storage Technologies

Criminals may take advantage of the advancement and expanding usage of computer and data storage technology to access and spread illegal recordings and data [72].

4. Telecommunication Infrastructure

Technological advancements may be exploited to increase the speed, capacity, and anonymity of criminal activity or to steal sensitive and private data. To create widespread disruption, telecommunications infrastructure might potentially be attacked[73.

5. Internet of Things (IoT)

IoT devices' growing amounts of acquired data may be susceptible to theft, corruption, destruction, extortion, or sale. IoT devices are also anticipated to widen the breadth of cybercrime-related assaults and present new vulnerabilities in intricate IT settings and systems [74].

6. Privacy-Enhancing Technologies (PETs)

It may become more difficult to identify, monitor, and investigate criminal conduct as a result of PETs being used maliciously by individuals to carry out illegal acts covertly and anonymously. Additionally, bad actors may attack PETs in an effort to get access to private or secret data [71] [74].

7. Blockchain and Distributed Ledger Technologies (DLTs)

Transactions might be manipulated for malevolent reasons, such as blocking them from being processed, since they are digitalized and processed by DLTs. DLTs may also be used to store objectionable or disruptive material that is hard to get rid of. [78]

There were more technological clusters found, but they weren't included in the primary study. This was because experts and stakeholders believed they were either substantially less important to cybercrime or only likely to materialize on a significant scale after the study's completion.

8. CONCLUSION

The growth of civilization and the spread of technology have made life easier in countless ways, but they have also exposed us to numerous risks and harms related to computers and the Internet, prompting governments and societies to focus on the need to raise awareness of these crimes by explaining and analyzing them to the public and demonstrating the means and methods of prevention.

The two areas of information systems that were the focus of this study were potential risks in the future of telecommunications and information technologies as well as analyzing weaknesses in current technologies. Emerging technologies, such as social media, cloud computing, smartphone technology, and critical infrastructure, have seen an increase in threats that often exploit their particular qualities. We discussed each developing technology's properties as well as the

numerous virus distribution meth-ods used by these new technologies. The typical set of broad attack patterns that may be discovered in new technologies is then discussed. For instance, since the majority of these developing technologies provide services online, some of the frequent as-saults increasingly take advantage of browser security by using malware cloaked in extensions or flaws in scripting languages to access private information. In order to avoid being discovered, adversaries are also shifting their battleground from desktop to other platforms including mobile phones, tablet PCs, and VoIP. With the increase of mobile users and the complexity of mobile apps over the last several years, malware, particularly mobile malware, has increased significantly. Social engineering scams are becoming more prevalent. The use of well-known social networking sites like Facebook, Twitter, and others as delivery channels to trick unwary users into installing or spreading malware has increased. There have been reports of more coordinated botnet-based assaults. There is an increasing concern to stop botnets since the effect of such harm is far greater than that of individual assaults. A growing percentage of cyberattacks are being targeted against certain systems, such as command and control systems, utilizing inside information and individuals, according to recent figures.

We also provided examples of prospective paths for further study. As more and more individuals connect to the Internet, it has been recommended that security measures should be designed to match to the confidence levels of all users, including both experts and non-experts in computer systems. Many security experts have underlined that protecting user privacy is a crucial area for future study since the quantity of personal data being shared online has grown significantly in recent years. Some evi-dence suggests that the capacity of today's modern technology saturates and does not scale well any longer using traditional incremental approaches, so more creative approaches to see "a bigger picture" or think "outside the box" have been proposed rather than trying to fix a specific problem on existing Internet and computing systems incrementally. Future research efforts should focus on the advancements of trustworthy systems and the next generation of safe Internet. Future focus has also been drawn to the development of traceback and identity management methods that may be used to locate enemies on a global scale.

FUNDING

None

ACKNOWLEDGEMENT

None

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

[1] R. Karri, J. Rajendran, K. Rosenfeld, and M. Tehranipoor, "Trustworthy hardware,"dentifying and classifying hardware Trojans," *Comput-er*, vol. 43, no. 10, pp. 39–46, 2001.
[2] N. Potlapally, "Hardware security in practice: Challenges and opportunities," *2011 IEEE International Symposium on Hardware-Oriented Security and Trust*, pp. 93–98, 2011.
[3] A. R. Sadeghi, "Trusted computing-special aspects and challenges," in *International Conference on Current Trends in Theory and Prac-tice of Computer Science*, pp. 98–117, Springer, 2008.
[4] H. Mouratidis and M. Kang, "Secure by Design: Developing Secure Software Systems from the Ground Up"," *International Journal of Se-cure Software Engineering (IJSSE)*, vol. 2, no. 3, pp. 23–41, 2011.
[5] T. Hoare, J. Misra, G. T. Leavens, and Shankar, "The verified software initiative: A manifesto," *Theories of Programming: The Life and Works of Tony Hoare*, pp. 2021–2021.
[6] K. R. M. Leino and Dafny, "An automatic program verifier for functional correctness," in *International conference on logic for programming artificial intelligence and reasoning*, pp. 348–370, Springer, 2010.
[7] R. Gennaro, J. Katz, H. Krawczyk, and T. Rabin, "Secure network coding over the integers," in *International Workshop on Public Key Cryptography*, pp. 142–160, Springer, 2010.
[8] D. Boneh and D. M. Freeman, "Homomorphic signatures for polynomial functions," in *annual international conference on the theory and applications of cryptographic techniques*, pp. 149–168, Springer, 2011.
[9] M. Fujita, Y. Matsunaga, and T. Kakuda, "On variable ordering of binary decision diagrams for the application of multi-level logic synthe-sis," *Proceedings of the European Conference on Design Automation*, pp. 50–54, 1991.
[10] C. B. Nielsen, P. G. Larsen, J. Fitzgerald, J. Woodcock, and J. Peleska, "Systems of systems engineering: basic concepts, model-based techniques, and research directions"," *ACM Computing Surveys (CSUR)*, vol. 48, no. 2, pp. 1–41, 2015.
[11] J. Hatcliff, G. T. Leavens, K. R. M. Leino, P. Müller, and M. Parkinson, "Behavioral interface specification languages," *ACM Compu-ting Surveys (CSUR)*, vol. 44, no. 3, pp. 1–58, 2012.
[12] X. Cheng, C. Chen, W. Zhang, and Y. Yang, "5G-Enabled cooperative intelligent vehicular (5GenCIV) framework: when Benz meets Mar-coni"," *IEEE Intelligent Systems*, vol. 32, no. 3, pp. 53–59, 2017.

[13] V. M. Igure and R. D. Williams, "Taxonomies of attacks and vulnerabilities in computer systems," *IEEE Communications Surveys & Tu-torials*, vol. 10, no. 1, pp. 6–19, 2008.
[14] V. M. Igure and R. D. Williams, "Taxonomies of attacks and vulnerabilities in computer systems," *IEEE Communications Surveys & Tu-torials*, vol. 10, no. 1, pp. 6–19, 2008.
[15] M. Fujita, Y. Matsunaga, and T. Kakuda, "On variable ordering of binary decision diagrams for the application of multi-level logic synthe-sis," *Proceedings of the European Conference on Design Automatio*, pp. 50–54, 1991.
[16] E. Luiijf *Next Generation Information-Based Infrastructures: New Dependencies and Threats" , In Critical Information Infrastructure Protection and Resilience in the ICT Sector*, pp. 304–317, 2013.
[17] C. Haley, R. Laney, J. Moffett, and B. Nuseibeh, "Security requirements engineering: A framework for representation and analysis," *IEEE Transactions on Software Engineering*, vol. 34, no. 1, pp. 133–153, 2008.
[18] X. Cheng, C. Chen, W. Zhang, and Y. Yang, "5G-Enabled cooperative intelligent vehicular (5GenCIV) framework: when Benz meets Mar-coni"," *IEEE Intelligent Systems*, vol. 32, no. 3, pp. 53–59, 2017.
[19] L. Lamport, "Time, clocks, and the ordering of events in a distributed system," *Concurrency: the Works of Leslie Lamport*, pp. 179–196, 2019.
[20] M. Howard, D. Leblanc, and Viega, "24 deadly sins of software security: Programming flaws and how to fix them", McGraw-Hill Ed-ucation," 2010.
[21] M. E. Whitman and H. J. Mattord, "Principles of information security", Cengage learning," 2021.
[22] F. T. Sheldon and C. Vishik, "Moving toward trustworthy systems," *R&D Essentials"*, vol. 43, no. 9, pp. 31–40, 2010.
[23] A. M. Al-Khouri, ""eGovernment strategies the case of the United Arab Emirates (UAE)"," *European Journal of ePractice*, vol. 17, pp. 126–150, 2012.
[24] K. Tsipenyuk, B. Chess, and G. Mcgraw, "Seven pernicious kingdoms: A taxonomy of software security errors," *IEEE Security & Pri-vacy*, vol. 3, no. 6, pp. 81–84, 2005.
[25] M. Gegick, P. Rotella, and T. Xie, "Identifying security bug reports via text mining: An industrial case study," *2010 7th IEEE Working Conference on Mining Software*, 2010.
[26] A. Almulhem and I. Traore, "Experience with engineering a network forensics system," 2005.
[27] E. Ancillotti, R. Bruno, and M. Conti, "The role of communication systems in smart grids: Architectures, technical solutions and research challenges"," *Computer Communications*, vol. 36, pp. 1665–1697, 2013.
[28] G. Deepa and P. S. Thilagam *Securing web applications from injection and logic vulnerabilities: Approaches and challenges", Infor-mation and Software Technology*, vol. 74, pp. 160–180, 2016.
[29] A. Mairh, D. Barik, K. Verma, and D. Jena, "Honeypot in network security: a survey," *Proceedings of the 2011 international confer-ence on communication, computing & security*, pp. 600–605, 2011.
[30] B. J. Nikkel *A portable network forensic evidence collector", digital investigation*, vol. 3, pp. 127–135, 2006.
[31] F. Fischer, F. Mansmann, D. A. Keim, S. Pietzko, and M. Waldvogel, "Large-scale network monitoring for visual analysis of attacks," in *International Workshop on Visualization for Computer Security*, pp. 111–118, Springer, 2008.
[32] H. K. Lu and A. Ali, "Communication security between a computer and a hardware token," *Third International Conference on Systems*, pp. 220–225, 2008.
[33] H. K. Lu, A. M. Ali, S. Durand, and L. Castillo, "A new secure communication framework for smart cards," *6th IEEE Consumer Communications and Networking Conference*, pp. 1–5, 2009.
[34] F. Aloul, S. Zahidi, and W. El-Hajj, "Two factor authentication using mobile phones," *2009 IEEE/ACS international conference on computer systems and applications*, pp. 641–644, 2009.
[35] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge computing security: State of the art and challenges," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1608–1631, 2019.
[36] A. Dmitrienko, C. Liebchen, C. Rossow, and A. R. Sadeghi, "On the (in) security of mobile two-factor authentication," in *International Conference on Financial Cryptography and Data Security*, pp. 365–383, Springer, 2014.
[37] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge computing security: State of the art and challenges," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1608–1631, 2019.
[38] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," *Cryp-tography*, vol. 2, pp. 1–1, 2018.
[39] J. Bringer and H. Chabanne, "An authentication protocol with encrypted biometric data," in *International Conference on Cryptology in Af-rica*, pp. 109–124, Springer, 2008.
[40] J. Hunker and C. W. Probst, "Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques," *J. Wirel. Mob. Net-works Ubiquitous Comput, Dependable Appl*, vol. 2, no. 1, pp. 4–27, 2011.
[41] P. Guarda and N. Zannone, "Towards the development of privacy-aware systems," *Information and Software Technology*, vol. 51, pp. 337–350, 2009.
[42] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey," *Security in distributed, grid, mobile, and pervasive computing*, pp. 367–409, 2007.
[43] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey", Security in distributed, grid, and per-vasive computing," 2006. 208-222.
[44] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 3, pp. 6–28, 2008.
[45] S. Abraham and I. Chengalur-Smith, "An overview of social engineering malware: Trends, tactics, and implications"," *Technology in Socie-ty*, vol. 32, no. 3, pp. 183–196, 2010.
[46] F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack examples, templates and scenarios," *Computers & Security*, vol. 59, pp. 186–209, 2016.
[47] F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack examples, templates and scenarios," *Computers & Security*, vol. 59, pp. 186–209, 2016.
[48] M. Ozsoy, C. Donovick, I. Gorelik, N. Abu-Ghazaleh, and D. Ponomarev, "Malware-aware processors: A framework for efficient online malware detection," *2015 IEEE 21st International Symposium on High Performance Computer Architecture (HPCA)*, pp. 651–661, 2015.
[49] H, K. Ibrahim, O, and A. Hassen, "Preventive Approach against HULK Attacks in Network Environment," *International Journal of Computing and Business Research (IJCBR)*, vol. 7, no. 3, pp. 1–11, 2020.
[50] Y. Sharma, B. Javadi, W. Si, and D. Sun, "Reliability and energy efficiency in cloud computing systems: Survey and taxonomy"," *Journal of*

Network and Computer Applications, vol. 74, pp. 66–85, 2016.
[51] A. Vance, B. B. Anderson, C. B. Kirwan, and D. Eargle, "Using measures of risk perception to predict information security behavior: In-sights from electroencephalography (EEG)"," *Journal of the Association for Information Systems*, vol. 15, no. 10, 2014.
[52] M. Junger, L. Montoya, and F. J. Overink, "Priming and warnings are not effective to prevent social engineering attacks"," *Computers in human behavior*, vol. 66, pp. 75–87, 2017.
[53] H. Aldawood and G. Skinner, "Reviewing cyber security social engineering training and awareness programs-Pitfalls and ongoing is-sues"," *Future Internet*, vol. 11, no. 3, pp. 73–73, 2019.
[54] F. Mouton, L. Leenen, M. M. Malan, and H. S. Venter, "Towards an ontological model defining the social engineering domain," in *IFIP International Conference on Human Choice and Computers*, pp. 266–279, Springer, 2014.
[55] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pp. 71–80, 2005.
[56] N. B. Ellison, C. Steinfield, and C. Lampe, "The benefits of Facebook "friends:" Social capital and college students' use of online social network sites"," *Journal of computer-mediated communication*, vol. 12, no. 4, pp. 1143–1168, 2007.
[57] J. V. Dijck, "The culture of connectivity: A critical history of social media," 2013. Oxford University Press.
[58] D. M. Boyd and N. B. Ellison, "Social network sites: Definition, history, and scholarship"," *Journal of computer-mediated Communica-tion*, vol. 13, no. 1, pp. 210–230, 2007.
[59] W. Luo, J. Liu, J. Liu, and C. Fan, "An analysis of security in social networks," *Eighth IEEE International Conference on De-pendable*, pp. 648–651, 2009.
[60] S. Rathore, P. K. Sharma, V. Loia, Y. S. Jeong, and J. H. Park *Social network security: Issues, challenges, threats, and solutions, In-formation sciences*, vol. 421, pp. 43–69, 2017.
[61] S. Abu-Nimeh, T. Chen, and O. Alzubi, "Malicious and spam posts in online social networks," *Computer*, vol. 44, no. 9, pp. 23–28, 2011.
[62] R. Ajami, N. Ramadan, N. Mohamed, and J. Jaroodi, "Security challenges and approaches in online social networks: A sur-vey"," *IJCSNS*, vol. 11, no. 8, pp. 1–1, 2011.
[63] J. S. Li, L. C. Chen, J. V. Monaco, P. Singh, and C. C. Tappert, "A comparison of classifiers and features for authorship authentication of social networking messages," *Concurrency and Computation: Practice and Experience*, vol. 29, no. 14, pp. 3918–3918, 2017.
[64] K. Thomas and D. M. Nicol, "The Koobface botnet and the rise of social malware," *2010 5th International Conference on Malicious and Unwanted Software*, pp. 63–70, 2010.
[65] W. Luo, J. Liu, J. Liu, and C. Fan, "An analysis of security in social networks," *Eighth IEEE International Conference on De-pendable*, pp. 648–651, 2009.
[66] D. Rupprecht, K. Kohls, T. Holz, and C. Pöpper, "Breaking LTE on layer two," *2019 IEEE Symposium on Security and Privacy (SP)*, pp. 1121–1136, 2019.
[67] A. Dabrowski, G. Petzl, and E. R. Weippl, "The messenger shoots back: Network operator based IMSI catcher detection," in *International Symposium on Research in Attacks, Intrusions, and Defenses*, pp. 279–302, Springer, 2016.
[68] A. Dabrowski, G. Petzl, and E. R. Weippl, "The messenger shoots back: Network operator based IMSI catcher detection," in *International Symposium on Research in Attacks, Intrusions, and Defenses*, pp. 279–302, Springer, 2016.
[69] M. Jurecek, J. Bucek, and R. Lórencz, "Side-Channel Attack on the A5/1 Stream Cipher, 633-638," 2019. IEEE.
[70] C. R. Mulliner, *Security of smart phones" , (Doctoral dissertation*. 2006.
[71] S. Töyssy and M. Helenius, "About malicious software in smartphones"," *Journal in Computer Virology*, vol. 2, no. 2, pp. 109–119, 2006.
[72] E. Ancillotti, R. Bruno, and M. Conti, "The role of communication systems in smart grids: Architectures, technical solutions and research challenges"," *Computer Communications*, vol. 36, pp. 1665–1697, 2013.
[73] E. Ancillotti, R. Bruno, and M. Conti, "The role of the RPL routing protocol for smart grid communications," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 75–83, 2013.
[74] S. Paul, J. Pan, and R. Jain, "Architectures for the future networks and the next generation Internet: A survey"," *Computer Communica-tions*, vol. 34, no. 1, pp. 2–42, 2011.
[75] J. Pan, S. Paul, and R. Jain, "A survey of the research on future internet architectures," *IEEE Communications Magazine*, vol. 49, no. 7, pp. 26–36, 2011.
[76] O and A. Hassen, "Big Data Based Machine Learning and Predictive Analytics using Apache Mahout and Storm"," *International Refereed Jour-nal of Reviews and Research*, vol. 5, 2017.
[77] N, A. Abu, and Z. Abidin, "Human Identification System: A Review"," *International Journal of Computing and Business Research (IJCBR)*, vol. 9, pp. 1–26, 2019.
[78] M. B. Khorsheed, "The Application of Fractal Transform and Entropy for Improving Fault Tolerance and Load Balancing in Grid Computing Environments," *Entropy*, vol. 22, pp. 1410–1410, 2020.