Contents lists available at *Dergipark*

Journal of Scientific Reports-A

journal homepage: *https://dergipark.org.tr/tr/pub/jsr-a*

E-ISSN: 2687-6167 ***Number 61, June 2025***

REVIEW ARTICLE

Receive Date: 13.12.2024 *Accepted Date: 27.05.2025*

Types of cyber-attacks with using voice

Nursel Yalçın[a], Bilge Lale[b,*]

[a]*Gazi University, Gazi Faculty of Education, Department of Computer and Instructional Technologies Education, Ankara, Türkiye, ORCID: 0000-0002-0393-6408*

[b]*Gazi University, Department of Computer Forensics, Institute of Informatics, Ankara, Türkiye, ORCID: 0009-0005-1919-0929*

Abstract

Recently, attacks targeting individuals, organizations and even critical voice-activated systems have become widespread one after another. Basically, these are unauthorized access or control of a device using manipulated or synthesized voice commands to attack an identified vulnerability in voice technologies, usually supporting smart assistants and smart speakers. While such attacks are diversifying simultaneously with the regular implementation of voice technologies in daily life, the potential consequences of such attacks also increase their impact in cases where most users and organizations are not sufficiently aware. In this study, various voice-based cyber-attacks, such as voice phishing (vishing), voice command manipulation, attacks using ultrasonic sound waves, hard disk attacks via voice commands and acoustic eavesdropping attacks, their methods (e.g., synthesizing deceptive voice commands, using ultrasonic frequencies to bypass security systems, manipulating devices through inaudible commands, exploiting voice interfaces to access sensitive data on hard drives, capturing private conversations using sound waves) and possible effects are investigated and some legal situations related to these threats are also touched upon in the context of the current cyber security environment in Türkiye. This study aims to increase awareness by providing a comprehensive analysis of voice-based cyber-attacks and to better inform users and cybersecurity professionals about effective prevention and mitigation strategies. It serves as a comprehensive review of existing research in this field.

Keywords: Cybersecurity; cyber-attack; data breach; voice technologies; voice-based attacks

* Corresponding author. Tel.: +90-5395818598
E-mail address: bilge.lale@gazi.edu.tr

1. Introduction

Cyber-attacks are considered one of the huge threats of this digital era, as they pose a high risk to individuals' organizations and governments by destroying important information systems or networks, taking control of devices and illegally accessing personal data. There are various forms and methods of carrying out cyber-attacks, each of which differs depending on the attacker's goal and tools.

Cyber threats have grown considerably in recent years, boosted by the development of voice technologies. While voice assistants, smart speakers and all kinds of other devices that get turned on by the sound of one's voice started to be a feature in everyday life, so too they have increasingly turned out to be an attractive target for malicious actors. Most voice technology-based cyber-attacks rely on exploiting vulnerabilities of the systems using manipulated voice commands or phony voice recordings, which could be used to grant unauthorized access, data breach or system takeover.

While these emerging technologies are changing how humans interact with their devices, they come along with new risks of serious consequences in case manipulation to one's advantage ensues. Attacks on voice technology are among the most serious and fastest-growing attack vectors. Such risks are generally not well known and their potential impacts are worse in an environment where users are not well prepared for such an attack.

Most of the studies that have focused on voice-based cyber-attack vectors merely point to the fragmented treatment that this has received in the literature. Such kinds of studies focus on specific attack vectors; however, in this study some of them will be compiled into a comprehensive analysis of methodologies, objectives and results.

It also covers the legal frameworks of voice-based cyber-attacks within the context of cybersecurity and cybercrime legislation in Türkiye. Although challenges associated with voice technologies are relatively new, their legal counterparts have not yet been developed. This paper, therefore, will discuss recent developments regarding these types of attacks and will further propose how existing legal frameworks can be enhanced. Additionally, this study serves to set a basis of understanding changes in the technological and legal fronts concerning voice-based cyber-attacks and creates a demand for more stringent preventive measures in the face of constantly escalating cyber threats.

This study adopts a descriptive literature review methodology and aims to provide a structured and comprehensive overview of voice-based cyber-attack methods. The research was developed by examining up-to-date academic publications, technical reports and real case examples that reflect current attack techniques and defense mechanisms. Rather than generating new data, the goal is to synthesize existing knowledge in a thematically organized format. Literature was selected based on relevance, credibility and credibility. To ensure the comprehensiveness of the review, the search focused on publications between 2013 and 2024 sourced from academic databases including Scopus, ScienceDirect, IEEE Xplore and Web of Science. In addition, the most frequently discussed types of voice-based cyber-attacks identified in these sources were examined. These attack categories were selected based on their prevalence in the literature and their relevance to emerging cybersecurity challenges. While this method allows for broad contextualization of the topic, it also has limitations, such as the absence of empirical data and reliance on secondary sources, which may affect the granularity of the findings.

2. The concepts of voice and cyber-attacks

Voice is a form of physical energy and is produced by vibrations in a physical environment, the airway and atomic molecules. The vibrations produced originate from a sound source such as a musical instrument, a human voice or natural sound, causing the surrounding air molecules to move. These movements also propagate in the form of wave motions and are detected by the receiver's ear, allowing hearing to occur. The human voice is the sound generated by the vibration of the vocal cords while air from the lungs passes through the trachea. The frequency range for normal human voice, on average, ranges between 85-180 Hz for men and 165-255 Hz for women. This is the anatomic process by which speech can occur, whereby communication through speech, music and other sound signals is enabled. The frequency, amplitude and speed of sound waves determine the pitch, tone and intensity of the sound [1]. Voice plays

a critical role in the field of communication with applications ranging from music and speech to alarms and notifications commonly used in daily life. Recent developments in digital technologies have significantly affected various fields and have also affected audio technologies in many ways. Digital Signal Processing (DSP), for example, is one of them. DSP enables the conversion of audio signals into digital formats for processing and analysis. This field is widely used in audio engineering, music production, telecommunications technologies and numerous media applications [2]. Moreover, the increasing prevalence of voice-related technological advances has profound implications for cybersecurity. While voice data is widely used in devices, voice commands and voice assistants are increasingly vulnerable to threats related to the security of personal data [3].

Cyber-attacks are carried out through various methods that compromise the security of information systems. These attacks aim to disrupt the functionality of target systems, steal sensitive information, manipulate data or achieve financial gain [4]. Common types of cyber-attacks (Examples of some of these are also shown in Fig. 1.) include information theft, phishing, ransomware, malware and Distributed Denial of Service (DDoS) attacks.

Fig. 1. A diagram illustrating common types of cyber-attacks [5].

Information Theft refers to the unauthorized acquisition of personal data by an attacker. Cybercriminals often exploit vulnerabilities in target systems to steal this personal data, financial data or confidential corporate information [6].

Phishing attacks aim to trick users into giving their personal information to attackers through fake calls, emails or websites. Attackers use deceptive tactics called social engineering to steal sensitive information such as passwords or credit card information [7].

In ransomware attacks, attackers encrypt the files of target systems, deny access to the owner and attempt to charge users a fee. Such attacks can cause significant damage to both individuals and organizations [8].

There are many different types of malwares designed to harm computers or networks or steal information. These threats include viruses, trojans and worms.

DDoS attacks disrupt target systems, rendering them inoperable. These attacks are usually carried out over large-scale networks and can seriously reduce the availability of systems [9].

The convergence of voice technologies and cybersecurity has become increasingly significant in safeguarding information security and protecting personal data. Voice assistants and smart devices that collect and process vocal inputs to deliver various services introduce a range of security vulnerabilities. These devices and their associated voice commands can be exploited by malicious actors to access sensitive personal information. Of particular concern are the risks associated with the recording and processing of voice biometric data, which underscores the importance of

implementing comprehensive security measures for voice data within the broader context of cybersecurity. Biometric voice authentication systems are especially vulnerable and require heightened protection against cyber-attacks. Secure digital processing of voice data must be supported by robust cybersecurity protocols to maintain the integrity and confidentiality of these systems [10].

As a result of developing voice technologies and the proliferation of IoT (Internet of Things) devices, new types of attacks beyond traditional cyber-attacks are emerging.

The protection of voice data and the prevention of cyber-attacks in this area necessitate the strengthening of both technological and legal infrastructures. The connection between traditional cyber-attacks and voice-based attacks is important, especially in this period when voice technologies are developing, in terms of ensuring the security of the relevant systems. Because the basis of defense strategies is based on traditional cybersecurity methods.

3. Cyber-attacks utilizing voice

The rapid advancement of technology, especially in the field of voice technology, has led to the increased use of voice as a tool in cyber-attacks. Fig. 2 shows the stages of some of the attacks. Research conducted in various fields aims to clarify the effects of voice technologies on cybersecurity and to reveal the complexities and potential risks associated with voice-based attacks. Although there are many types, the most common voice-based cyber-attacks can be divided into two main types: voice phishing attacks (vishing) and system manipulations carried out through voice commands.

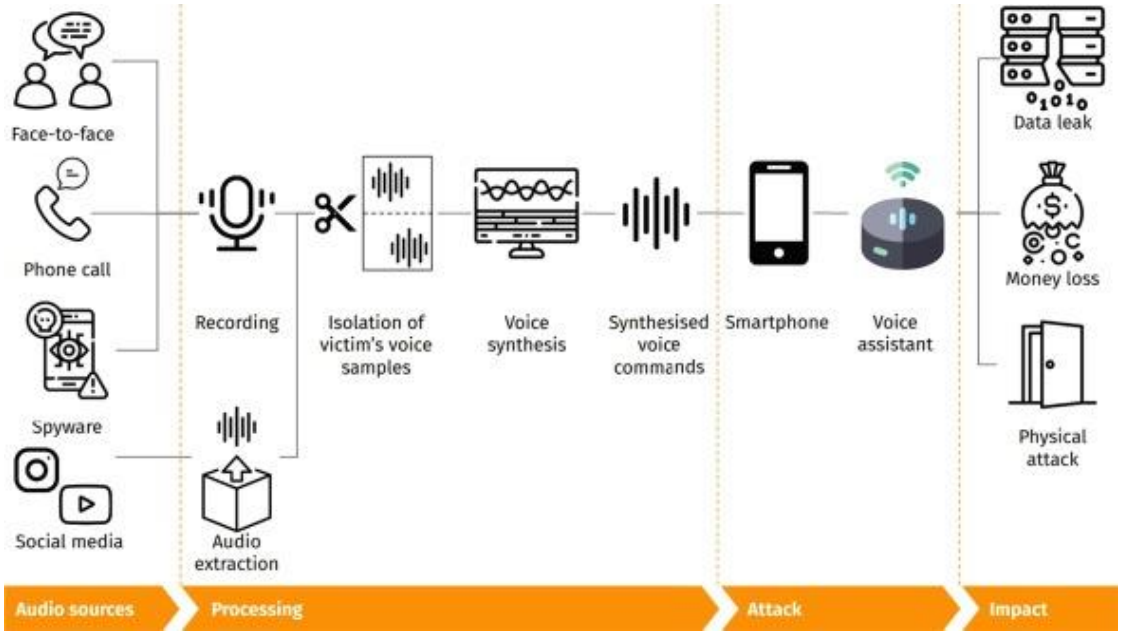

Fig. 2. An example of the stages involved in cyber-attacks executed using voice technology [11].

Voice phishing or vishing is the voice-driven counterpart of traditional phishing attacks, where attackers aim to steal users' personal data through phone calls or voice messages. Studies have revealed that during vishing attacks, perpetrators use social engineering techniques designed to establish an environment of trust with the target user, thus allowing personal data to be easily intercepted by unauthorized persons [3]. These types of attacks are extremely convincing and can often be designed specifically for specific individuals through software, taking advantage of

advances in voice analysis and speech synthesis technologies. For example, innovations in artificial intelligence and machine learning have significantly increased the possibility of deceiving target users by allowing attackers to produce almost one-to-one voice imitations through software [12].

Another common type of voice-based cyber-attack, system manipulations via voice commands, refers to the unauthorized control of smart devices using voice commands. These attacks exploit vulnerabilities in the microphones or voice assistants of the target devices. Smart home systems and personal assistants are important targets of this attack technique and pose significant risks in this regard. Research has shown that vulnerabilities in these devices can be exploited by malware, thus compromising personal and financial data [13]. For example, an attacker can steal data stored on a targeted smartphone, such as passwords, financial data, photos, messages, phone numbers and contacts, by issuing malicious commands through the voice assistant of this targeted smartphone [14].

The main purposes of voice-based attacks usually include stealing personal data, obtaining financial information or completely disabling the target information systems. As a result of developments in voice recognition and speech synthesis technologies, it has become easier for malware to spread through voice commands or voice messages and affect users. In particular, the fact that smart devices can be remotely controlled for malicious purposes without the user's knowledge via voice commands creates significant security problems [15]. Research shows that voice commands are frequently used to install malware on smart devices or to exploit system vulnerabilities [16]. Thus, attackers can easily harm the target user and their device and obtain various amounts of financial benefit from the user.

4. Types of cyber-attacks with using voice

Cyber-attacks with using voice can be carried out by using people's voices or by exposing devices to sound waves. These types of attacks aim to capture personal data, financial information, corporate data, trade secrets and other sensitive information that can cause a lot of damage. Voice-based cyber-attacks can be divided into several types, including vishing, voice command manipulation, voice identity theft, voice messaging attacks and attacks using ultrasonic sound waves. Each type of attack is carried out using different techniques and methods. As a result, different damage is caused to the targeted users, devices and information systems.

4.1. Voice phishing (vishing)

Voice phishing (vishing) is a social engineering technique that attackers use to collect personal and financial information from people through phone calls. These attacks usually begin with attackers using trust-building strategies. These attackers usually present themselves to the person they are talking to as representatives of familiar and trusted institutions such as financial institutions, government agencies or technical support companies [3]. To do this, attackers can easily imitate the voice of a different person who does not belong to them but is trusted by the target person by using special software to deceive the target person.

In addition, vishing attacks are carried out in a systematic approach to identifying and targeting specific audiences. Attackers usually collect personal data using corporate databases, social media platforms and various websites and can create comprehensive profiles of their victims. They initiate phone calls aimed at creating panic or imposing a sense of urgency on the target person by bringing together many different personal information, Fig. 3 shows a simple example of this attack. For example, victims may receive alarming voice calls regarding the security of their bank accounts, and attackers may direct them to immediately transfer sensitive information or a certain amount of money to them [17].

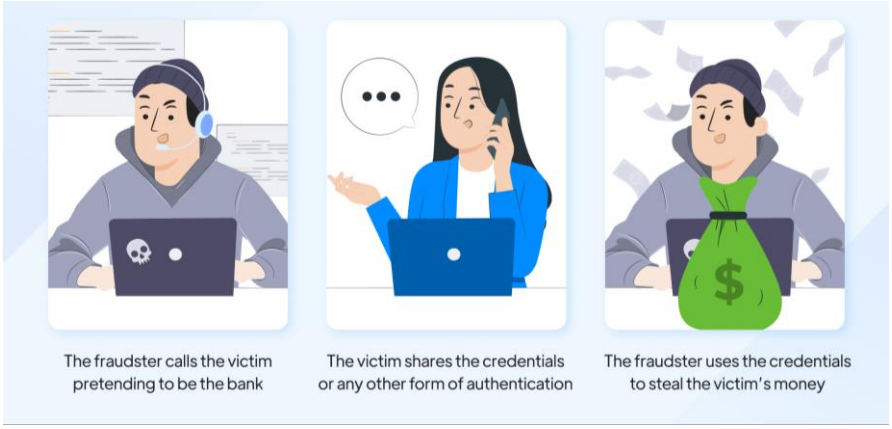

Fig. 3. The typical stages involved in a commonly executed vishing attack [18].

One of the most deceptive aspects with vishing concerns manipulation, in which the attacker distorts the perception of the authenticity of the call. By using an extremely simple voice-altering software, the attacker can make their voice sound like someone they can trust-a bank teller, family member or even coworker. This would sound incomparably more convincing for the targeted victim, who would be less likely to follow the request of an attacker. With the development of technology nowadays, voice synthesis or deepfake technology could enable hackers to imitate voices of people whom one really can trust; it also significantly blurs the line of which calls are legitimate and which ones are fake. Besides, during the call, an attacker may use a wide range of psychological manipulations and threats against the victims. They may also threaten the victim with consequences, such as the suspension of accounts or other legal actions, if financial information is not provided immediately. These types of threats may cost the victim losses in terms of finance and very fast, because one may be hoisted to a corner and made compulsorily to act accordingly upon the instructions given. Others may even claim that the victim has won some kind of reward and that the reward is to be given to the victim if a certain amount of money is given. They then use this to demand large amounts of money from them [12].

The effectiveness of vishing attacks and the variety of ways they are carried out are increasing with the use of rapidly developing technology, technological tools and methods in every field. For example, attackers can use the voice of a familiar or trusted person through software and in addition, they can display their phone numbers as caller ID. This deceptive practice can easily manipulate the target person, significantly reducing the likelihood that people will question the authenticity of the caller's identity. These techniques not only increase the probability of attackers' success, but also significantly weaken public trust in communication technologies.

As a result, vishing uses sophisticated social engineering techniques and psychological manipulation to target individuals. It is important for individuals to be aware of this type of attack and not to immediately establish trust. Financial institutions should also develop technological solutions to prevent vishing. Implementing robust security measures and conducting awareness campaigns to educate the public is an important step in reducing the risks associated with this sophisticated type of fraud and cyber-attack. Such preventive actions not only protect individuals, but also contribute to the broader goal of increasing societal safety and security.

4.2. Voice identity theft

Voice identity theft is a form of voice-based cyber-attacks in which attackers attempt to obtain victims' personal data through voice communication, a method involving phone calls, voice messages or even voice commands that

mimic the victim's or a trusted individual's voice. These attacks are carried out by creating the illusion that victims are interacting with a trusted person and by exploiting the victim's natural trust, which is often placed in public institutions. Attackers often impersonate financial entities, public officials or representatives of social media platforms to deceive individuals into disclosing sensitive personal information [19]. This manipulation, as in vishing attacks, effectively exploits the victim's psychological predisposition to trust familiar names, making it easier for attackers to reach their malicious targets.

Vishing is closely related to but distinct from voice identity theft - see a comparison in Fig. 4. While vishing is specifically carried out by tricking victims into giving personal information or tangible benefits via phone calls or voice messages, voice identity theft encompasses broader methods aimed solely at impersonating someone in order to extract personal data. These methods have also included the use of stolen personally identifiable information in fraud activities, such as opening new accounts or committing fraud via existing accounts, which is particularly vulnerable in voice communications and systems [20].

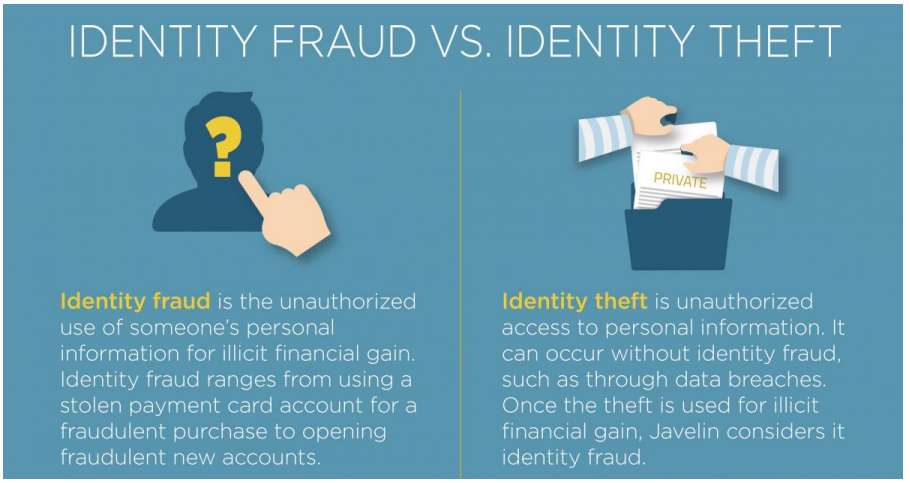

Fig. 4. A diagram illustrating the difference between identity fraud and identity theft [21].

As in vishing, voice identity theft attacks often involve the attacker pretending to be a familiar or trusted person. In this type of attack, the attacker can also abuse recorded voice samples or synthesized speech from a familiar or trusted person. This method becomes even more effective when attackers include specific details they have collected through previous research or social media, which can lead to financial data or even identity information falling into the hands of attackers [15]. Techniques such as requesting personal data under the pretext of "security verification" exploit the victim's instinct to protect their data, facilitating the attacker's goal of accessing critical information.

Despite vishing and voice identity theft sharing some superficial characteristics, such as the use of vocal communication as an attack vector, their core strategies, technological foundations and psychological mechanisms differ significantly. Table 1 summarizes their definitions, techniques, technological requirements, attack targets, real-world examples, and prevention strategies. This comparative analysis makes it easier to understand more fully how each attack works and what differentiates them from each other in reality.

Table 1. A general comparison of the characteristics of vishing and voice identity theft attacks.

Attack type	Vishing	Voice identity theft

Definition	A fraud method that uses social engineering techniques through phone calls or voice messages to trick victims into disclosing sensitive information.	The use of stolen voice samples to bypass identity verification systems or to commit fraud by impersonating the victim.
Purpose	To deceive the victim and obtain confidential data such as passwords, credit card details, and identity information.	To impersonate the victim by mimicking their voice in order to bypass biometric security systems or conduct fraudulent transactions.
Common techniques	• Impersonating a trusted figure (e.g., bank employee, police officer, government agent) • Creating a sense of urgency to force quick reactions • Using spoofed caller IDs	• Using AI-based voice cloning and deepfake technologies • Exploiting stored voice samples to deceive identity verification systems • Attacking biometric voice recognition mechanisms
Use of technology	Generally requires low technical skill, persuasive communication via phone is often sufficient.	Involves advanced technologies such as artificial intelligence, machine learning, and voice synthesis.
Target of the attack	Primarily focuses on human psychology and manipulating the victim emotionally.	Targets technological systems, especially biometric voice authentication mechanisms.
Prevention Methods	• Stay alert against suspicious calls • Verify the caller's identity before sharing personal data • Confirm that the phone number belongs to the real institution	• Implement multi-factor authentication in systems using voice biometrics • Avoid discussing sensitive topics in insecure environments • Use AI-based synthetic voice detection tools

As discussed in Section 4.1, plunderers create a sense of fear or urgency by applying psychological pressure to get their targets to take quick action. Thus, the victim suffers damage without realizing that the incident they are experiencing is an illusion. For example, attackers may claim that the victim's bank account will be blocked if action is not taken immediately and may force them to share personal data quickly without sufficient thought [22].

Raising awareness among individuals is of great importance in preventing voice identity theft. Victims should be careful about calls from unknown numbers and evaluate requests for personal information with suspicious approaches. Simple steps such as verifying the identity of the caller through official channels or not sharing personal data immediately can significantly reduce the risk of falling victim to these attacks. Financial institutions can also increase public awareness through user education programs and technological measures aimed at preventing fraud attempts, such as multi-factor authentication and caller verification systems.

In conclusion, voice identity theft attacks are an example of one of the risks posed by social engineering and psychological manipulation, which are widely used and pose a major threat in an increasingly digital environment.

The prevalence of both voice identity theft and related attacks and frauds are sophisticated tactics used by modern attackers, highlighting the need to be vigilant and take precautions to protect various personal and financial data.

4.3. Voice command manipulation

Manipulation of voice commands is a significant and current cybersecurity threat targeting smart homes, voice-activated virtual assistants and other voice-controlled technological systems. As the use of these systems in modern life becomes more widespread (from voice-activated personal assistants such as Amazon's Alexa, Google Assistant and Apple's Siri to voice-activated smart home systems), the potential for these systems to be exploited and exposed to security breaches also increases. These systems are based on voice recognition technology that can synthesize human speech according to the frequency, tone and amplitude of sound waves and generate various actions in response [3]. However, existing voice recognition technologies present some vulnerabilities. Attackers can also manipulate

these vulnerabilities in different ways to execute unauthorized voice commands, access private information or execute other malicious actions. Therefore, voice command manipulation is not only a significant security concern, but also a growing risk as multiple devices and user accounts are connected.

These attacks center on the voice recognition feature of smart devices, the working stages of this technique are illustrated in Fig. 5. The most common technique is voice spoofing, where attackers use pre-recorded voice samples and imitate a target's voice to give commands to a voice-activated smart device. In this technique, the attacker records the victim's voice and plays back the recorded audio to perform some action, such as opening doors or making unauthorized purchases [13].

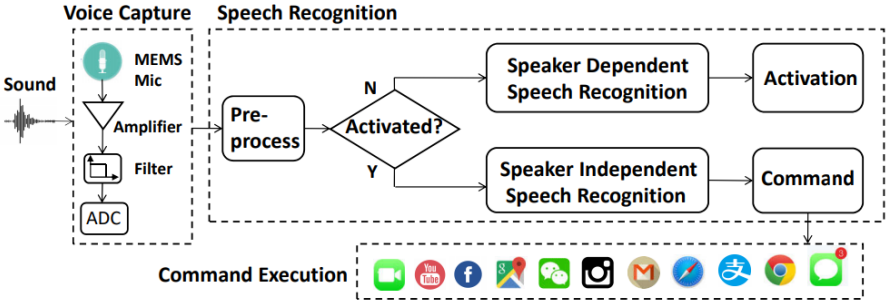

Fig. 5. Stages of a simple Voice Command Manipulation attack [23].

Although voice recognition systems are becoming increasingly sophisticated, they still fail to distinguish between a legitimate command and maliciously crafted speech, especially in basic speech recognition.

In addition to voice spoofing, acoustic attacks pose an advanced threat. These attacks use the physical properties of sound waves, especially frequencies that are outside the range of human hearing but can be detected by microphones in voice-activated devices. Attackers can use ultrasonic or subsonic sound waves, above 20 kHz and below 20 Hz, respectively, to send commands to the user's system without the user being aware of them. This technique can lead to serious risks that could allow an attacker to access personal data without the user knowing, open doors for smart homes or even control other smart devices in the home. Such attacks are carried out outside the detection capabilities of both users and devices, which makes this type of attack particularly dangerous.

Another danger is when malicious actors manipulate voice commands by interfering with the voice-to-text conversion process and modifying the voice and speech data before it is processed by the systems. In this case, attackers can intercept and modify a voice command while it is being transmitted, allowing a modified version of the command to be executed. This form of attack can lead to situations where, for example, a user intends to control their thermostat, but the attacker can instead execute a command to open a door or window or disable any security system.

Both technical and practical measures need to be taken to reduce these risks. From a technical perspective, the use of advanced biometric voice data is an important method for strengthening voice authentication systems. Voiceprint recognition is a more reliable method by analyzing not only the content of the speech but also the rhythm of the voice, speech patterns and speaker features such as phonetic details of the speaker [24]. However, biometric systems are not completely reliable and attackers are increasingly developing new techniques to imitate or defeat these systems and features. Therefore, combining voice recognition with multi-factor authentication (MFA), which requires users to verify their identity with a different form of authentication such as a PIN code or facial recognition, is a very important step in protecting systems against unauthorized access [25].

Other security measures depend on the regular updating of software and hardware so that all loopholes attacked by the attackers in the algorithms or software of voice recognition systems are patched. Users should update their devices because these manufacturers, such as Google, Apple and Amazon, provide regular updates for detecting these

vulnerabilities. Other potential risks can be mitigated by managing device and app permissions and settings with care regarding which applications should have access to voice data.

While voice-controlled and voice-guided technological gadgets increase, from voice assistants and smart homes to automotive systems, so does the potential danger regarding manipulation by voice command. For example, an attacker could use the voice control feature of a smart home system to disable security cameras or disable the alarm system. This would allow them to break into the security of a home using smart home technology based on the possible weaknesses in the voice recognition software. These kinds of security breaches demand further modification of hardware and software to ensure that these voice recognition systems are used correctly and securely. Educating people on how they can protect privacy and ensuring security in an ever-digitizing environment will also be necessary.

4.4. Voice messaging attacks

Voice Messaging Attacks are a serious cybersecurity threat where cybercriminals manipulate voicemail services to trick unsuspecting individuals into revealing sensitive personal information. Most attacks occur through fake voicemails that aim to extract confidential data such as account numbers, passwords and financial information. With the increasing use of automated voicemails by organizations for legitimate purposes, both in the field of analog telephone systems and modern messaging services such as WhatsApp and Facebook Messenger, the scope of voice messaging attacks has increased tremendously. For example, recently, cybercriminals utilized voicemails on Facebook Messenger to proliferate Trojans and other malware. In some instances, triggering the malware required merely hitting the button to play the voicemail. This has taken place all around the world as the attackers have gone so far as to target groups, sending multiple targets the fake messages. Clicking on the links may redirect users to attacker-controlled websites where the malware is hosted [26].

These attacks are also carried out based on psychological manipulation of the target. The language in such voicemails often contains emotional appeals that exploit cognitive judgments such as urgency or threat. Cognitive judgments are psychological shortcuts that people resort to when they act impulsively under stress or fear. Research has shown that many of these fear-based tactics, especially those that create a sense of urgency or personal threat, are highly effective in increasing stress levels and thus impairing decision-making abilities. A well-known feature of voice messasing attacks is the manipulation of tone and prosody. Attackers adopt a tone of voice that is similar to the tone, pace and formality of a professional organization that the target person trusts. These subtle vocal cues can positively enhance the perceived legitimacy of the message, thus making it harder to detect the scam. Using certain cultural words, pronunciations or excluding official language can further increase the credibility of the scam, especially if it targets certain demographic groups [22].

The primary protection against voice messaging attacks is again user education and awareness of the risks. First and foremost, people need to be somewhat sceptical when receiving unwanted voicemails, let alone those that demand urgent attention or even personal data. Users need training to recognize various manipulative cues, such as emotional language, unusual caller IDs or high-pressure tactics. The second step is for a person to verify the request for personal or financial information through independent contact with the organization, rather than responding directly to the message. This will help users be more resilient to voice messaging attacks and avoid falling victim to these increasingly common scams.

4.5. Deepfake technology and synthetic voice threats

Deepfake technology is one of the most complex and alarming threats in the contemporary digital world, supported by significant developments in artificial intelligence (AI) and machine learning techniques. The term "deepfake" is a combination of the words "deep learning" and "fake", which refers to the use of deep learning algorithms, especially generative adversarial networks (GANs), to create highly realistic and deceptive audio, video or other multimedia content. This includes not only altered visuals but also synthetic voices such as voice cloning, modification and

synthesis, all of which contribute to the increasing ability to impersonate individuals. Initially widely and popularly used in the entertainment field, deepfake technology has evolved over time, providing cybercriminals with new ways to impersonate people, manipulate media and personal data and conduct various fraudulent activities. Due to these threats, deepfake technology, particularly synthetic voice manipulation, has become a serious concern for cybersecurity experts, media organizations and individuals.

Attackers, scammers and malicious people are widely using deepfake technology to create realistic audio recordings or videos that mimic the voices and appearances of trusted people. This is basically done by following the steps in Fig. 6. Many new software tools are currently being developed for this purpose and through this software tools, the voice of each individual can be copied almost exactly and the content of their speech can be changed in seconds as the attackers want. These tools use AI and deep learning algorithms to convincingly mimic one's voice with high accuracy, allowing the changing of speech content in real time. For example, attackers can create a deepfake voice that mimics the voice of a CEO or senior manager in a company in seconds and use it to instruct employees to make unauthorized transactions or disclose important financial information. Using voice biometrics with AI-driven analysis, it becomes possible to identify and authenticate audio content, even detecting synthetic patterns in the voice. This helps in distinguishing between genuine and deepfake voices, ensuring security in communication systems.

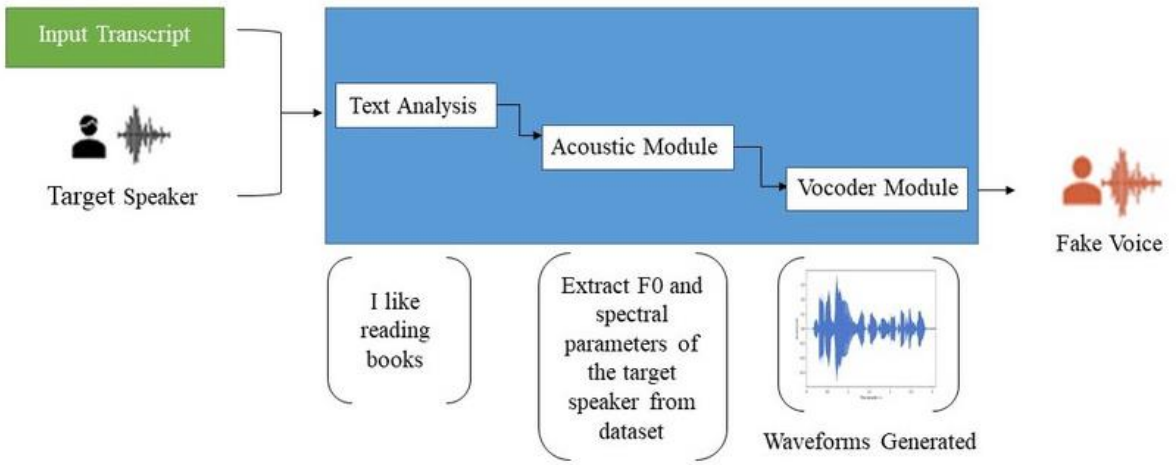

Fig. 6. A diagram showing how deepfake technology synthesizes a voice, segments of speech are analyzed and manipulated with sophisticated algorithms to fabricate a voice that sounds like the original speaker's tone and cadence [27].

In addition to individual financial fraud, deepfake technology also poses a significant threat to society. In high-risk scenarios such as elections, public health crises or international conflicts, deepfakes can be used to manipulate public opinion or destabilize social order. For example, deepfake videos or audio recordings of political leaders making false statements or behaving inappropriately can spread rapidly on social media, undermine trust in institutions and negatively impact public confidence. In 2024, cybercriminals targeted the global advertising giant WPP (World's Largest Advertising and Public Relations Group) by using a deepfake voice clone of CEO Mark Read. The fraudsters impersonated Read in a Microsoft Teams meeting, using a voice clone and YouTube footage to deceive employees into divulging sensitive information and money. While the attackers were not successful, the incident highlights the growing risk of deepfake technology in corporate environments, where it can be used to exploit trust and cause significant financial harm [28]. Such manipulations not only manipulate democratic processes, but also increase distrust in digital media and make it harder to distinguish truth from lies in the era of pervasive digital content.

The development of advanced detection mechanisms is increasingly important to mitigate the risks that deepfake technology may pose. Advanced deepfake detection methods rely on the effective use of machine learning and deep learning models. In particular, the MFCC-GNB XtractNet method, which combines MFCC (Mel-Frequency Cepstral Coefficients) and Gaussian Naive Bayes (GNB) models, has achieved a high accuracy rate in deepfake voice detection. This method extracts MFCC features from audio recordings, performs statistical analysis using the GNB model and then applies Non-Negative Matrix Factorization (NMF) to make the data more distinguishable. Studies have shown that this approach has achieved a remarkably high accuracy rate of 99.93%. With the advancement of deepfake technologies, the necessity of adopting such advanced detection mechanisms in the field of cybersecurity has become increasingly evident [29]. Today, researchers and cybersecurity experts focus on creating algorithms that can distinguish real and manipulated media. These detection methods often rely on subtle inconsistencies in content, such as unnatural eye blinking movements in the video or irregularities and distortions in tone and speech patterns. However, as deepfake creation techniques continue to evolve, detection tools must also evolve at the same pace. In addition to technological solutions, public awareness and education are critical components of a broader defense strategy. Media literacy campaigns aimed at helping individuals determine the reliability of deepfake content and creating scepticism about the authenticity of digital media can reduce the harm these attacks can cause.

In conclusion, deepfake technology is a multifaceted threat that constantly concerns both individuals and institutions and requires significant attention. The increasing sophistication of deepfakes necessitates the continued development of detection tools and public education to increase awareness of this growing threat. For voice deepfakes, methods such as forensic audio analysis and deep learning models help detect inconsistencies, such as unnatural speech patterns or audio artifacts. Verification of content authenticity is also essential and can be achieved through metadata validation, digital signatures or watermarking. Deepfake technologies are fast evolving; challenges lie ahead while manipulations in non-native languages create even more difficulties. Future research will be toward perfecting methods for detection across languages and explorations beyond the realm of manipulations of facial expressions into the domains of changes in body language and group dynamics [30]. By implementing robust detection systems and increasing public awareness, the negative impacts of deepfakes can be mitigated. By implementing robust security measures and creating a more informed public, the negative effects of manipulations through increasingly widespread deceptive media can be reduced [31]. It is also vital to keep up the tempo of technological innovation along with creating public awareness regarding the developments associated with deepfake technology as a way to reduce possible risks and avoid giving malicious actors opportunities.

4.6. Attacks using ultrasonic sound waves

Attacks using ultrasonic sound waves are the most sophisticated, since these voice-based cyber-attacks take advantage of technological vulnerabilities, especially in voice-activated smart systems. These attack modes deploy high-frequency sound waves above the range of human hearing-usually above 20 kHz-and thus are imperceivable to human ears. It is called "DolphinAttack"; the idea is to manipulate the voice-detection mechanisms of voice-controlled devices, which include not only smartphones and smart speakers but also voice-activated virtual assistants, to let the attackers' issue unauthorized commands without the user knowing about it. This range beyond the hearing of the human ear enables such an attack to carry out its processes completely hidden from the targeted user, thus setting serious risks for both users and manufacturers of voice-activated technologies. The attackers get an advantage wherein they manipulate the devices with sounds that cannot be heard by humans and make calls, send text messages or basically conduct any financial transaction without detection. The execution framework of DolphinAttack consists of two major parts: generating ultrasonic sound waves and manipulating the voice recognition system of the target device, as shown in Fig. 7. It employs specialized hardware and software tools which produce inaudible ultrasonic signals to the human ear but are easily detected by the target device. Such high-frequency signals can be modulated to fall within the range of frequencies at which the device's microphone is most sensitive, thus allowing attackers to easily transmit commands to the system. For example, an attacker can use ultrasonic waves to command a smartphone to send money

to an unknown person or to transfer it into a virtual account operated by the attacker without the victim's knowledge [32].

Fig. 7. Stages of a cyber-attack using ultrasonic sound waves [33].

One of the major vulnerabilities through which an attack can be made by ultrasonic sound waves lies in the sensitivity of voice-controlled devices. While most voice-activated smart devices are designed to respond to voice commands across a wide frequency spectrum, their systems are often ill-equipped to make out the difference between legitimate commands and those carried by ultrasonic waves. This is where one finds a critical vulnerability that can be exploited by an attacker. To reduce these risks, manufacturers need to set up sophisticated security features in voice detection systems of voice-activated devices. This may include the development of algorithms specifically designed to detect ultrasonic sound waves and the given device an ability to distinguish between normal voice commands and probably malicious commands. It can be further extended in developing voice mechanisms like biometric voiceprints for enhancement of the security features of the devices against access by unauthorized users, improvements should also be made in other mechanisms like multi-factor authentication.

However, besides the technological advancements, there is an equal requirement for increasing the awareness of the users in mitigating the attacks resulting from the ultrasonic sound waves. Users must be aware of such vulnerabilities and potential risks pertaining to the use of voice-activated technologies. This helps the user in understanding specific signs when systems are compromised, for example, unexpected behavior of their devices or execution of unauthorized actions. In addition, a user is expected to ensure the software on their device is updated since most companies release patches and security updates whenever a new vulnerability is found.

The after-effects of such an attack, like those with ultrasonic sound waves, range from individual security breaches to corporate integrity, public safety and even national security. With more devices beginning to be put into use in critical infrastructures, smart home automation systems and security protocols, the prevalence and rate of success of DolphinAttack are also on a rise. Attackers will be able to manipulate voice-activated systems in corporate environments in such a way that they steal sensitive company data, perform unauthorized financial transactions or even disrupt business operations. Afterwards, financial losses, reputational damage and erosion of customer trust follow, with the long-term effects of threatening the sustainability of an organization. Moreover, voice recognition is already being applied to some public systems nowadays, such as public services or security infrastructures of national importance; therefore, they are susceptible to manipulation with the aim of creating serious damage.

Considering the growing sophistication in attacks using ultrasonic sound waves, all this calls for a multi-pronged cybersecurity approach. Emphasis should fall on adaptive detection mechanisms that would identify and neutralize such threats before they can cause much harm. It is also very important to generate public awareness among users

about the potential risks of such kinds of attacks. In this regard, users are called upon to come up with scepticism and vigilance each time they have to deal with voice-controlled gadgets. Manufacturing companies, on their part, should work with regulatory agencies and experts in cybersecurity to lay down standards that will ensure that, if followed by all in the industry, a proper level of ultrasonic-based cyber-attack detection and prevention can be instituted. It is at such a time when the rate of technological innovation equips the establishment of security protocols and mass education on emerging threats, such as DolphinAttack and others of this nature, that the information environment within the digital world is best protected.

In conclusion, ultrasonic sound wave cyber-attacks are an example of the growing, insidious threat that needs constant vigilance and innovation. With the capabilities of voice-controlled systems continuing to expand, both manufacturers and users must remain proactive in identifying and addressing vulnerabilities. Since voice-activated technologies will compose an immense part of future cybersecurity, development should be collaboratively carried out with robust methods of detection and enhancement of system security, thereby enlightening the public about the risks of such emerging threats. Technology keeps evolving and since what malicious actors have been up to also evolves with time, this means continuous research and development and above all, cooperation by all parties concerned.

4.7. NUIT (Near-ultrasound inaudible trojan)

The Near-Ultrasound Inaudible Trojan (NUIT) is another very sophisticated and upcoming form of cyber-attack whose target analysis is voice-activated technologies such as voice assistants, smart speakers and other IoT devices. This attack mechanism uses waves from the audio spectrum in the frequencies of 16 kHz to 20 kHz, which are inaudible to humans with an audibility of approximately 20 Hz to 20 kHz but can still be detected by the microphones of many modern devices as shown in Fig. 8. These are designed to be inaudible to the human ear. However, since smart devices are designed to listen to user commands, these ultrasonic sounds are in the range that voice assistants can detect, making them a potential target for malicious actors.

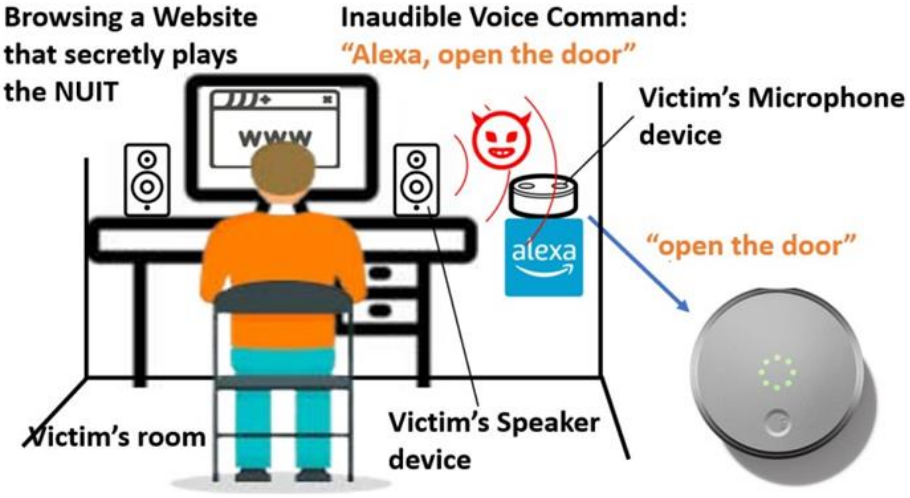

Fig. 8. A diagram illustrating how a NUIT attack is executed without the user's knowledge [14].

A classic example of how the operational mechanism of a NUIT attack can be carried out is the exploitation of ultrasonic signal coding. In this case, an attacker aims to insert complex instructions into the device using modulated sound waves. The sound waves are encoded with specific frequency patterns that can deceive speech recognition algorithms built into the device that mimic legitimate voice commands. For example, consider how researchers have successfully demonstrated how ultrasonic signals can be modulated into speech-like patterns that are recognized as commands after demodulation [33]. All these manipulations mostly occur without any trace of intrusion, because the attack exploits the device's existing microphone hardware as well as its normal listening capabilities.

This vulnerability arises because in many high-end voice-activated devices, from smartphones and smart televisions to smart assistants of all kinds, audio signals are processed without satisfactory distinction between audible and ultrasonic frequencies. When the malicious signal reaches the microphone, the speech recognition software does not recognize the frequency as an anomaly and thus the malicious action is successfully performed.

The consequences and impacts of these attacks by NUIT are enormous. One of the dangerous aspects of these attacks is that they are stealthy, leaving the victim completely unaware that their device has been compromised. There are several ways for a cybercriminal to gain control of a victim's device. For example, through this vulnerability, an attacker can remotely trigger certain unauthorized activities: opening smart locks, tampering with security cameras and performing financial transactions [34]. The attack can also be used to obtain sensitive personal information (passwords or credit card details) from voice-activated payment or communication platforms.

One of the most dangerous cases for NUIT could be focused attacks on people working in high-security environments: government facilities, prisons, research labs or corporate offices. Using a variety of voice-activated smart devices, attackers can bypass security protocols, for example and compromise sensitive information or even entire corporate networks. As IoT (Internet of things) devices proliferate, the scope of potential vulnerabilities related to ultrasonic attacks is growing, further increasing the risks to individuals and organizations.

Mitigating the risks posed by NUIT attacks requires initiatives from device manufacturers and users. In this context, the need to develop algorithms that can distinguish human voice commands from unusual ultrasonic signals stands out. Solutions range from dynamic filtering of the frequency to coding to discard certain frequency bands outside the audible range of the microphone, to developing voice recognition technologies that distinguish natural speech from artificial ultrasonic sound waves and somehow analyze the sound wave characteristics [33].

Moreover, voice-activated devices should be designed with much more serious security policies than in previous cases. This is possible by developing end-to-end encryption between voice assistants and back-end servers, anomaly detection systems and signalling that voice commands are unusual for such a user. Enabling these capabilities on devices ensures explicit consent of users before sensitive actions such as financial transactions and is an important measure to minimize the possibility of remote exploitation. This proactive security practice should be addressed at the end-user level. Permissions on devices should be reviewed from time to time and voice activation should be disabled when not in use. This can be done with Always Listening Mode for Voice Activated Payments and Transactions or Non-2FA Devices, preventing the possibility of unauthorized access. As a result, user education is extremely important in terms of ways to reduce exposure, as well as awareness of ultrasonic threats and recognition of potential vulnerabilities; this will greatly help to reduce vulnerabilities and prevent damage that may occur.

As voice-activated technologies become an increasingly important part of modern life, attacks like NUIT orchestrated by highly specialized attackers, are certain to become more sophisticated. Therefore, continuously evolving technical solutions and user education are highly recommended. The only way to reduce such risks in stealth attacks is to encourage manufacturers and consumers to develop good defenses against ultrasonic vulnerabilities. Sooner or later, more than just technological innovation will be required; a cultural shift will be required to create security awareness among users and smart devices to cope with the current emerging cybersecurity threats.

4.8. SurfingAttack

SurfingAttack technique is an advanced voice-based cyber-attack technique that uses the acoustic transmission properties of atomic structures of solid materials, especially focusing on the interaction of Micro-Electro-Mechanical Systems (MEMS) microphones in current and voice-controlled smart devices with high-frequency ultrasonic sound waves. This attack technique exploits the properties of MEMS microphones that are sensitive to sound frequencies, which are generally between 16 kHz and 100 kHz and are beyond the frequency range that humans can hear. These ultrasonic frequencies, which are not perceptible to the human ear, can be detected by MEMS microphones built into smart devices that are widely used by consumers, such as smartphones, smart speakers and other voice assistants. Attackers can manipulate these devices to establish covert communication, issue unauthorized commands or intercept sensitive data.

Attackers specifically use directed ultrasonic signals to interact with voice-controlled smart devices without requiring direct access to the device or its physical microphone. By exploiting the nonlinear nature of MEMS microphones (according to which the microphone's response to sound waves becomes more complex as the frequency increases), attackers send ultrasonic signals that are then demodulated by the device's speech recognition system and interpreted as a legitimate command [35]. This covert manipulation allows the attacker to issue commands to the device without the user's knowledge, such as unlocking the device, initiating transactions or accessing private data.

The SurfingAttack technique is based on the interaction between ultrasonic waves and the nonlinear properties of MEMS microphones. MEMS microphones are commonly found in mobile phones, voice assistants and other smart devices. These microphones easily convert high-frequency acoustic signals into electrical signals, which are then processed by the firmware as if they were legitimate voice commands. The problem is that MEMS microphones lack proper filtering mechanisms for ultrasonic signals; therefore, guided ultrasonic waves can manipulate them quite easily [36].

A modulated ultrasonic signal can be equipped with digital information such as commands or data that are inaudible to the victim and interpreted by the device. This signal can be transmitted over short distances - for example, from a hidden speaker or smartphone - and can be reflected by the transmission of atomic particles from surrounding surfaces such as walls, windows or furniture and as a result, it can be detected by the microphone connected to the voice assistant. It can then be transmitted to the device as a valid command by the microphone where it is detected. Thus, the attacker can remotely operate the device to perform many actions or obtain sensitive information from the device. In most scenarios, such attacks are also possible at extremely long ranges, assuming a suitable condition for ultrasonic wave propagation.

Another important factor that makes SurfingAttack dangerous is that it may work covertly, considering the acoustic properties of materials which usually reflect or absorb high-frequency sound waves. For instance, in a normal household environment, walls and furniture would serve as reflectors for ultrasonic signals, extending the attack range. This further benefits from the low energy required to transmit these ultrasonic signals, together with increased sensitivity in MEMS microphones; this therefore allows attacks that are power-efficient and difficult to detect.

Given the various threats mentioned, voice-activated smart device manufacturers should invest in advanced filtering technologies that distinguish legitimate voice commands from malicious ultrasonic signals. Various mitigation strategies can be developed, including:

- Ultrasonic Signal Detection: Improved signal processing algorithms allow devices to identify and eliminate non-human speech pattern ultrasonic signals. For example, active noise cancellation systems or DSPs can distinguish between high-frequency ultrasonic waves and standard voice commands.
- Frequency Range Limitation: One of the best measures in this regard is to limit the frequency range of the microphone so that it does not pick up ultrasonic frequencies. This can be done through hardware-based filters or software-based algorithms that simply ignore frequencies above 20 kHz and render ultrasonic commands ineffective.

- Two-Factor Authentication (2FA): For any high-risk activity, such as financial transactions or account changes, the integration of multi-factor authentication will reduce successful exploitation. Even if an attacker manages to issue a command via SurfingAttack, requiring secondary verification in the form of a PIN or biometric authentication can prevent unauthorized actions.
- Mic Sensitivity Controls: Devices would also be developed to support variable microphone sensitivity based on contextual information. For example, reducing the sensitivity of a microphone when a device is not active to listen for commands can prevent unnecessary ultrasonic waves from being detected.

Furthermore, users should be informed about the risks associated with acoustic attacks and why their voice-controlled devices need to be secured. Regularly updating device software, disabling voice assistants in public places and avoiding potentially sensitive voice commands in untrusted environments significantly reduce the potential for exploitation.

While the adoption of voice-activated devices increases, the technique of SurfingAttack points to an intrinsic vulnerability that requires both technological innovation and awareness. In other words, manufacturers can take long strides toward limiting the possibility of such exploits by dealing with the intrinsic security weaknesses in MEMS microphones and adopting effective strategies for detecting and mitigating such attacks. Similarly, user education and vigilance form the basis of safe and secure usage of voice-activated devices in daily life. In this manner, therefore, in a rapidly changing voice-activated technology environment, advanced security measures together with public awareness and smart device design are an integral component of protection against these and other emerging threats.

4.8.1. Piezoelectric transducers' role in SurfingAttack

One of the key components that makes attacks like SurfingAttack so effective is the use of piezoelectric transducers. These devices can convert mechanical stress (e.g. mechanical waves) into electrical stress and vice versa. Some materials, such as quartz, exhibit piezoelectricity; that is, an electrical charge is generated by mechanical perturbation and vice versa, the application of an electric charge causes mechanical oscillations. This is why these piezoelectric transducers are so effective in generating and controlling ultrasonic waves for covert communication.

In the context of SurfingAttack, piezoelectric transducers can emit high-frequency ultrasonic signals that are quite effective for manipulating MEMS microphones in voice-activated devices. Added to this are the advantages of compactness, low power consumption and high sound emission accuracy; these are exactly what SurfingAttack needs to be effective. This makes them an ideal tool for an attacker who wants to transmit high-frequency acoustic signals undetected over long distances from the target device. Ultrasonic transmitters using piezoelectric materials can be placed to interact with voice-activated devices either directly by transmission or by reflection from surrounding surfaces, thus increasing the range and effectiveness of the attack, as a diagram of how an attack is carried out is shown in Fig. 9.

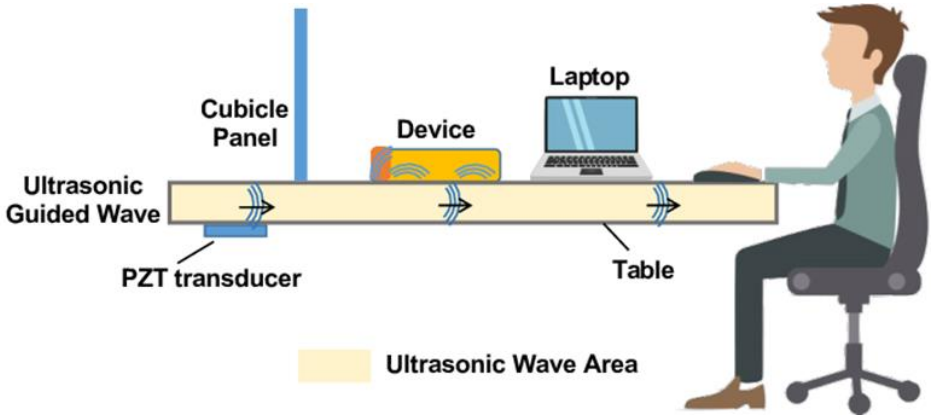

Fig. 9. A diagram illustrating how a simple SurfingAttack is carried out using a piezoelectric transducer [37].

Another important feature of piezoelectric materials is that they operate over a wide frequency range, giving an attacker tremendous opportunities to fine-tune ultrasonic signals to exploit specific vulnerabilities in voice-activated devices. For example, attackers can increase the probability of a successful exploit by emitting frequencies that correspond to the resonant frequency of materials or device components. The sensitivity and directionality provided to piezoelectric transducers make them effective in directing ultrasonic signals exactly where they need to go and do not spread into the environment [36]. In the case of an attacker, they can use the piezoelectric transducer to generate highly directed high-frequency waves ultrasonically and manipulate voice-activated devices in stealthy and difficult-to-detect ways.

With further developments in piezoelectric technology in terms of efficiency, size and power consumption, such devices are expected to be more widely used in cyber-attacks on acoustic interfaces in smart environments. Therefore, with the increasing awareness of the risks arising from such vulnerabilities, it is necessary to go a step further in countermeasures such as advanced measures such as filtering ultrasonic signals.

4.9. Hard disk attacks

Recent research has revealed a surprising and important new avenue for voice-based cyber-attacks: ultrasonic sound waves aimed at hard disk drives. Researchers at the University of Michigan and Zhejiang University have shown that high-frequency sound waves, far beyond human audible ranges, can severely damage the firmware of hard disk drives (HDDs) and instantly disable a device beyond repair [38]. These ultrasonic attacks exploit mechanical weaknesses in HDD components, particularly the highly sensitive disk platters and read/write heads, to perform sabotage. This interference by these waves results in data corruption, system crashes and sometimes irreversible hardware damage. This poses a new critical problem in cybersecurity, where an attacker can use sound as a powerful tool to manipulate hardware.

The mechanism of hard disk attacks using ultrasonic sound waves is to exploit the interaction between high-frequency sound waves and sensitive physical components inside the HDD. Therefore, when an ultrasonic signal is directed at a hard disk, it causes interference in the vibration movements that occur between the moving parts inside the device. Specifically, it targets the micro-mechanical components: the spindle motor, the read/write head and the disk platters. These components are critical to the accuracy of reading or writing data stored on magnetic platters. The delicate balance and accuracy involved here can be altered when exposed to ultrasonic sound waves, leading to incorrect data being read, written or lost.

In most such attacks, an action revolves around the generation of ultrasonic frequencies in the range of 16 kHz to 100 kHz - beyond the audibility of the human ear. The frequencies can penetrate the devices either through the air or through direct contact with surfaces. Once the attack begins, the sound waves can cause misalignment of the read/write heads or even induce micro-vibrations that physically damage the storage plates. In some cases, the vibrations are enough to cause the reading heads to come into contact with the platters, which may result in data loss or permanent hardware damage [38].

The effects of such attacks are extensive. An ultrasonic attack on the HDD can completely crash the entire system and therefore you cannot start the operating system or recover critical data. In such an environment where hard drives are used to store sensitive corporate or personal data, such attacks have disastrous consequences, ranging from irreversible data loss to compromise of confidential information.

The problem with ultrasonic sound wave attacks on HDDs is that they are undetectable when they tamper with the hardware. Often, the effects of an attack will not seem harmful at first; the system may slow down erratically, produce some errors or crashes and it will not be considered that these are due to malicious activity. This is the main reason why such an attack is almost impossible for a user or even an IT administrator to detect from the very beginning. In this case, critical data may become unrecoverable once the damage becomes apparent due to the lack of proper backups.

Additionally, ultrasonic attacks do not require local physical proximity; they can also be carried out remotely by directing ultrasonic waves at an HDD through acoustic reflections from the air or nearby surfaces. This makes such attacks stealthy and difficult to detect, especially if the system in question is in a secure and controlled environment such as a data center or office space. The use of piezoelectric actuators allows attackers to generate precise, high-frequency ultrasonic waves that target vulnerable components of the hard drive, which can make the attack more effective.

Another serious consequence of this attack would be data loss. Since modern HDDs store large amounts of critical data such as financial records, personal information and intellectual property, the loss of this data can be catastrophic for both individuals and organizations. Worse still, if these attacks occur against corporate storage systems or servers, the impact can easily range from simple individual data loss to corporate paralysis, financial loss and even reputational damage. Ultrasonic attacks are becoming an increasingly greater risk due to the continued reliance of companies on Hard Disk Drives and other such storage media for sensitive data.

The fact that technology is still improving means that the ultrasonic attacks, post-attack complications and the need to increase actions by individual users and organizations to protect the integrity of devices and hardware will also increase. Following are a few key measures which can reduce the effectiveness of such an attack and the damage caused: Periodic backup of sensitive information with remote servers or the cloud remains one of the most reliable security measures that could be employed against data loss by ultrasonic attacks.

The other security features that could be implemented are mainly when noise filtering and vibration dampening is highly advanced on a device containing critical data. Some of the hardware filtering techniques include the installation of high-frequency sound wave barriers or installation of software that may run in the device to detect any abnormal vibration or sound.

Firmware and security software need to be regularly updated to protect devices from newly discovered vulnerabilities that may also target the physical layer of the hardware. Software updates could enhance the capabilities of the firmware in terms of processing such external inputs and protecting it from ultrasonic manipulations.

This is the imminent danger to hard disks: an attack with the use of ultrasonic sound waves, which opens an entirely new dimension of cybersecurity vulnerabilities. With the rise of connectivity and sensitivity to environmental factors, there is an ever-increasing need for advanced detection systems against ultrasonic attacks on critical hardware components such as HDDs. While these systems are designed to protect many critical hardware, the vulnerability of HDDs due to their delicate mechanical components and wide usage for data storage makes their protection particularly important. Hence, this development of such detection systems is not only crucial for protecting HDDs but also for developing better security practices and awareness among users and organizations. Fully implemented data protection

policies consisting of regular backups, updated security software measures and physical security measures will go long towards making our digital assets much more difficult to breach for such advanced threats emanating from ultrasonic sound wave exploits.

Additionally, a general comparison of the types of cyber-attacks carried out with ultrasonic sound waves can be seen in Table 2 below.

Table 2. A general comparison of the types of cyber-attacks carried out with ultrasonic sound waves.

Attack type	Method	Target	Key feature	Primary challenge
DolphinAttack	Ultrasonic sound waves manipulate voice recognition systems	Voice-activated systems (e.g., smartphones, smart homes)	Uses inaudible ultrasonic signals to bypass audio filters	Difficult to detect due to inaudible frequency
NUIT	Electromagnetic pulses interfere with electronics	Voice-activated systems	Manipulates electromagnetic signals to issue commands	Requires specialized hardware for detection
SurfingAttack	Exploits MEMS microphones with high-frequency ultrasonic waves	Voice-activated smart devices (e.g., smartphones, smart speakers)	Uses ultrasonic waves to covertly issue commands via MEMS microphones without direct device access	Difficult to detect due to high-frequency sound, works over long distances and reflections from surfaces
HDD attacks	Ultrasonic sound waves damage mechanical components	Hard disk drives (HDDs)	Uses high-frequency sound to damage HDD's physical parts	Detection difficulty due to inaudible frequencies

4.10. Acoustic eavesdropping attacks

Acoustic eavesdropping attacks are a new and emerging type of voice-based cyber-attack in which attackers use sound to covertly collect sensitive information in specific environments. Aside from traditional eavesdropping methods that rely on physical access to devices or networks, acoustic eavesdropping attacks exploit vulnerabilities in the microphones and voice detection systems found in modern technology. The danger of such an attack has increased exponentially with the proliferation of smart devices and voice-activated technologies, making voice assistants, smartphones, laptops and other internet-connected devices extremely vulnerable targets. Designed to listen for specific commands by default, such devices can become unwitting aids in capturing a wide range of information, from passwords and personal information to financial data and sensitive conversations. The more people rely on these technologies in their daily lives, the more likely acoustic surveillance is to occur, but since most eavesdropping tools are already built into microphones that are commonly used, they are increasingly difficult to detect.

Different approaches can be used for acoustic eavesdropping, each relying on a different interpretation of sound selection and processing. The most common techniques are related to the compromise of smart devices by malware. Once the device is infected, it grants an attacker access to the microphone and remotely captures audio directly from an environment. These compromised devices are then used to record private conversations, monitor phone calls or even listen to keystrokes. These types of attacks are quite successful when used in conjunction with social engineering techniques. For example, some attackers may use social engineering tactics, tricking users into installing malicious apps or clicking on phishing links that give the attacker access to control of the device's microphone. When the device

is not actively being used, an attacker can simply use the built-in microphone to listen in on conversations around them or obtain sensitive information without the user's knowledge.

A much more sophisticated approach involves manipulating specific frequencies of sound waves. For example, the DolphinAttack attack mentioned above uses ultrasonic sounds to communicate with voice assistants or smart devices to issue voice commands or record audio without the victim being detected [39].

Another technique, such as Keylogger, will use acoustic reflections from physical surfaces. In this context, attackers will want to place microphones or voice recorders in certain strategic locations and then analyze the sound reflected off walls, tables or other objects in the vicinity. These reflected sound waves can leak keystroke patterns, thus

allowing an attacker to extract text input from typing sounds. Research has shown that keystroke extraction can be quite accurate when background noise levels are low, even when small differences in the sound produced between different keys can be analyzed to reconstruct typed text. This technique requires proper placement of the recording devices and involves extensive processing, but it represents a critical vulnerability for environments where sensitive information is written or discussed near any digital recording device.

Acoustic eavesdropping on individuals and organizations imposes potential hazards that need to be avoided by implementing prevention strategies that are layered in nature. Devices and communication must be secured in a multitude of ways. First, as simple as it may sound, perform constant reviews and modifications of the settings of devices, particularly the settings that regard the microphones. As well as controlling the sharing of the devices, turning off the unnecessary microphone functions of devices that are not used to participate in any conversation is a wise move that helps the situation from acoustic monitoring. Furthermore, checking the application that have the permission to microphones and only allow the trusted ones can prevent the resources from being a trap to a microphone via a virus.

Another one of the most significant steps to take is the implementation of the means of communications that are not easy to break. Take the case of the telephone call of voice-based devices for example, it is often the case of encrypted services, especially end-to-end encrypted messaging services that are used, which means that only the sender and the receiver are the parties who are able to listen to the content, even though the information is with a third party, who is in possession of the audio recording of the conversation. These methods make it impossible for third parties to hear the conversations even if a bug is placed in the microphone to send the signal outside the users. Besides, a peaceful place for face-to-face meetings or proper noise control techniques are sure factors that may significantly decrease the odds of unwanted acoustic interception of communications. Non-voice surroundings are also noise-free rooms or sound suppression techniques that are used to protect the larger coverage of the sound eavesdropping. Fig. 10 below shows simple examples of various types of Acoustic Eavesdropping Attacks.

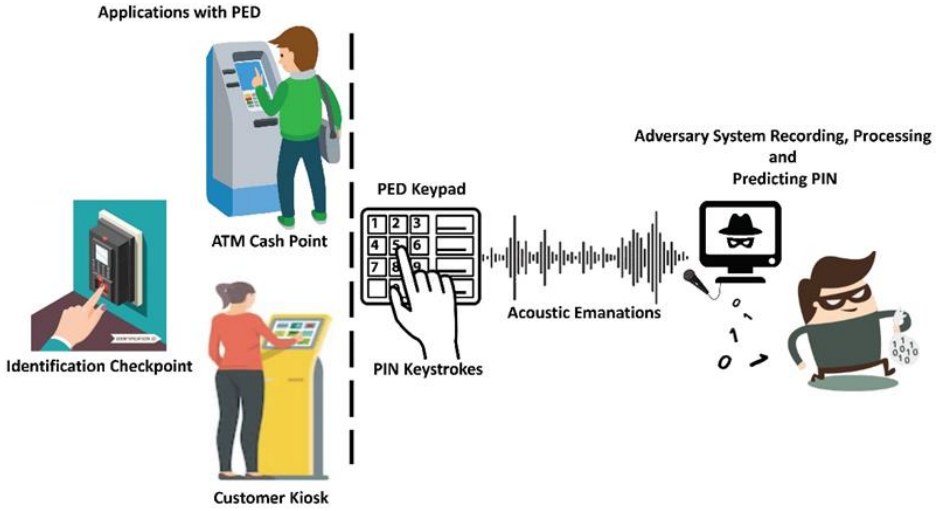

Fig. 10. Simple examples of various types of Acoustic Eavesdropping Attacks [40].

Acoustic devices as data manipulators can be something not so typical therefore, it is the responsibility of security personnel dealing with information and physical countermeasures to be aware of the associated risks. So far as practitioners are concerned, a proper mechanism such as a jamming device would in most occurrences be the one helpful in the affirmation of the acoustic threats. Suggestions on the measures taken to secure the audio such as the user's audio safety guidelines and thus the informed audio threat surveillance, help will set an organization in a good stand for a smart action taking company. In simple words, it means, that the various institutes, firms and businesses are required to implement efficient means, systems and strategies that will ensure customer Personally Identifiable Information (PII) and other confidential information is safe and made especially through data transmission within the organizations and outside.

While smart devices and voice-enabled technologies become increasingly integrated into our lives, the risk of eavesdropping attacks will also continue to increase. In such attacks, attackers take advantage of the microphones and voice detection system of these devices to intercept sensitive data, monitor conversations or even capture keystrokes without being detectable. It complicates the problem because it is sophisticated and kept secret, making it hard to identify the attack and defend oneself against it. However, it's possible to reduce a person's or organization's vulnerability to eavesdropping by means of control measures. This may be achieved through periodic review permissions for devices, utilization of encrypted communication devices and protection of the environment from within which one shares confidential information. The deep understanding of risks associated with cyber-attacks is critical to trying to maintain privacy and keep sensitive information from easy access as this field of cyber security continues to evolve.

4.11. Audio-delivered malware

Audio delivered malware is a new and highly advanced type of cyber-attack where malware is transmitted from one device to another via sound waves. Given the pervasive nature of sound in contemporary life, this method stands out as a new and sophisticated line in the evolution of cyber threats targeting the physical and digital interfaces of voice-activated systems, microphones and other audio input devices. The whole concept of voice-delivered malware aims to encode malicious payloads into sound and make them invisible to traditional security set up for network traffic and file-based threats [41]. Since malware signals in such attacks are usually placed using sophisticated obfuscation

techniques such as cryptography and steganography, the transmission of the malicious code becomes extremely stealthy, allowing attackers to carry out attacks without raising any obvious alarms.

The attack usually consists of two steps: first, the vocal transmission of the malware and then the activation of the malware upon reception. First, the attacker broadcasts sound waves at high frequencies, between 16 kHz and 100 kHz, which are inaudible to humans [42]. Therefore, the malware can be transmitted without alerting the user because the sound is not actually audible to humans. Certain modulation techniques will encode the malware into these sound waves, where the frequencies or patterns are used to encode the data in the audio signal. The problem with this type of concealment scheme is that the malicious code is guaranteed to be hidden in a file that looks and sounds like any normal audio file, which could include a song, a voice note or even an advertisement.

Later in the attack chain, after the sound waves are emitted, the target device receives the sound and decodes the malicious code embedded in it. The decoding process can be done through native audio processing systems on the device or other voice recognition technologies that can interpret these high-frequency audio signals as harmless sounds or instructions. Sometimes, malware can instantly and automatically execute commands encoded in the sound waves, such as downloading and installing them, changing system settings or opening backdoors for further attacks. The attack is complex because, in this case, the malware distribution tools, specifically voice-based tools and the entire chain of its activation are outside the scope of traditional security measures, which are very prone to looking at aspects of network traffic and file system scans. As a result, even the most careful security systems cannot detect this attack, since its structures are transmitted through information flow channels designed to bypass traditional detection mechanisms.

The implications of audio-delivered malware are broad. Since the use of voice-activated devices-such as smartphones, smart speakers and virtual assistants-is increasingly pervasive, so is the potential for such an attack. These devices are often equipped with always-on microphones, which listen continuously for commands, therefore making them ideal targets for attackers who want to inject code via sound. Apart from the infection of devices owned by individuals, audio-delivered malware has the potential for organizational network compromise: this depends on communication means such as Voice Over Internet Protocol (VoIP) or video conferencing applications or various remote collaboration platforms that are dependent on audio signals. An attack against such a system might result in information disclosure, disruption of services or the exploitation of network access for further malicious activity.

In fact, audio as a medium of transmission has brought cybersecurity professionals a whole new set of challenges. Other than traditional malware, most of which can be screened via scanning for files or network signatures, audio-delivered malware operates at a totally different dimension of attack surface. Due to the nature of audio encoding and signal modulation techniques, detecting malicious payloads requires further expertise and specific tools. For example, most of the audio-delivered attacks use steganographic methods so that the payload remains well hidden, invisible even within seemingly benign audio files. This in turn challenges traditional security frameworks, which might not be designed to inspect audio signals in real time.

Because of the increased threat of audio-delivered malware, proactive users and organizations go the extra mile to enhance their security posture. The most efficient way to ward off the attacks is a full turnout of patches in devices and software, updating them to their latest security updates. Quite obviously, frequent updates patch vulnerabilities in the device audio processing system or software before the attackers get a chance. Besides the updates, strong endpoint security solutions, like antivirus programs and firewalls, help in the detection of unusual or suspicious activity in malware execution. While these are not infallible, they nevertheless form a first line of defense against many common attack vectors.

Further, the user should be cautious when accessing audio from untrusted sources. Since malicious payloads in most of the recent malware attacks delivered through audio appear to the target as normal audio files, users must remain sceptical of opening unsolicited files or interacting with unfamiliar links that contain audio. Clearly, file integrity checks could be employed or specialized software designed to scan and analyze audio files for any hidden threats. It is also very important that organizations make employees aware of the risks posed by voice-based malware, especially in those contexts where the employees use voice-activated devices or systems to share sensitive information.

Another effective measure is disabling the microphone on devices while it is not in active use. Most microphones are always on-even when not in use from a range of devices from smartphones and laptops to IoT devices. An attacker would have to first exploit this as an entry point. Disabling microphone access for applications or services that do not need it may reduce the risk of voice-based threats. Highly sensitive settings may also consider anti-eavesdropping technologies or the adoption of secure channels of communication that make it nearly impossible for unauthorized people to get any kind of audio.

Considering the increasing sophistication of cyber-attacks, voice-transmitted malware is a particularly insidious threat as it can exploit widespread audio systems in modern devices. This introduces new complexity to the use of sound waves as a vehicle for malware delivery in security frameworks that are unable to control such innovations. With the increasing use of technology via voice-activated functions and voice-activated communication devices, awareness and defense mechanisms have become key. Keeping software up to date, being suspicious of the inclusion of audio files and using specialized security utilities go a long way in ensuring that users and organizations reduce their vulnerability to voice-transmitted malware and other evolving acoustic threats.

5. Legal frameworks and digital evidence in voice-based cyber-attacks under Turkish legislation

In order to solve the increasing incidents of cyber-attacks in the global society, various legal frameworks have been created to ensure the rights and security of people in online communities. The systems aim not only to prevent the occurrence of cybercrimes but also to mitigate the effects of damage caused to people. In Türkiye, legislative efforts have been made to redefine existing legal instruments to accommodate new forms of cyber threats, including voice technology. While voice assistants, smart home devices and voice-controlled devices become more and more prevalent in daily life, the demand for a legal explanation in this context has increased even more.

Although crime, penalty and security measures are rightly defined in the earliest concepts of Turkish criminal law, the law itself no longer always considers the unique nature of voice-based cyber-attacks. For this purpose, Turkish law rigorously adheres to "no crime without a law." In accordance with Article 2 of the Turkish Penal Code (Law No. 5237), no individual can be penalized for an act unless it has been explicitly delineated as a criminal offense [43]. This principle sets a structural limit in prosecuting actions under emerging technologies, particularly when the subject acts, such as ultrasonic attacks or voice-controlled interference, are not specifically addressed by current texts of law.

The usual objectives of cyber-attacks are to disrupt information systems, data theft or manipulation and financial fraud. These acts are provided for in Articles 243 to 245 of the Turkish Penal Code. Article 243 criminalizes illegal access into information systems and comes with penalties of one-year imprisonment. Article 244 widens the scope further by criminalizing destruction, alteration or hindering of system operation. Article 245 also criminalizes misuse of bank and credit card information with a view to attending to the monetary aspect of cybercrimes [44].

While these statutes represent a solid legal basis for the fight against traditional cybercrimes, they do not go far enough to be adequate to govern more advanced varieties of attack, e.g., the utilization of inaudible acoustic signals or the covert operation of voice-commanded machines. The legality of these emerging methods is, therefore, primarily an issue of judicial interpretation of terminology like "unauthorized access" and "information system." Consequently, existing law must be extended interpretatively or modified by statute to adequately encompass such emerging threats.

At the global level, there are a few conventions and treaties that provide a collaborative platform to combat cybercrime. The most prominent among them is the Budapest Convention, signed by the Council of Europe in 2001, which provides a comprehensive blueprint for transborder legal convergence on matters of cybersecurity. The treaty promotes the exchange of common legal standards and cooperation internationally in investigation and prosecution. Türkiye is a party to the convention and has pledged itself to the harmonization of its domestic law with its provisions, although controversy about its actual implementation exists among Turkish jurists [45].

Another relevant regulation as far as voice-based attacks are concerned is Law No. 6698 on Protection of Personal Data (according to its abbreviation in Turkish: KVKK). This act forms a full legal framework of processing, storage and safeguarding personal data. It imposes severe administrative sanctions in the event of non-compliance. Even

though protection of personal data is crucial to prevention of cyber-attacks, current provisions under KVKK do not include interception of voice data or voice-controlled system vulnerabilities, thereby showing a legislative gap.

In order to provide effective legal protection against advanced and dynamic cyber threats, continuous legislative adaptation and international cooperation covering voice technologies are required. Although Turkish legislation has a detailed framework to tackle cybercrime, the growing sophistication of attacks necessitates more targeted fine-tuning. Specifically, the incorporation of precise legal definitions of voice attacks in the Penal Code and related legislation would enhance the legal framework to effectively prosecute such offenses. With evolving cyber-attacks riding with advances in technology, law needs to be agile enough to sustain both human rights and cybersecurity in an ever-changing environment.

6. Detection and prevention of voice-based cyber-attacks

Detecting and preventing voice-based cyber-attacks is a major concern in today's complex, interconnected digital environment. The rapid adoption and use of voice-activated devices and technologies is increasing the risks associated with voice-based cyberthreats. Detection and prevention mechanisms will be crucial in reducing the losses that such attacks can cause, as they can sometimes lead to unauthorized access, data theft and manipulation of voice-controlled systems. Fig. 11 shows a flowchart illustrating the strategic stages of cybersecurity measures in general.

Fig. 11. A flowchart illustrating the strategic stages of cybersecurity measures in general. / Source: IWM Cybersec. (n.d.). Information security audit. Retrieved November 11, 2024, from https://iwmcybersec.com/information-security-audit/ [46].

These voice-based attacks are currently detected using machine learning algorithms, a central strategy. These sophisticated algorithms are tuned using large datasets of voice recordings to learn what normal voice patterns are and to recognize anomalies that may indicate malicious activity. Machine learning models that can analyze voice input in real time can detect subtle changes in frequency, tone or speech patterns that may indicate an attack. In this context, ML can be applied to the issue of voice command systems: detecting deviations in speech, abnormal intonations or unusual sentence structures that may indicate the presence of unauthorized commands or even maliciously crafted voices. These algorithms will increasingly learn and adapt to better build the ability of devices to compare legitimate

user inputs with any suspicious sounds. If the system predicts an attack, it will alert you for quick action that can reduce the risk of exploitation.

Along with machine learning, audio analysis is extremely important when it comes to identifying any voice-based threat. This analysis software uses advanced techniques such as frequency analysis and time domain analysis to examine the characteristics of sound waves in any environment. Therefore, frequency analysis can allow systems to measure the frequency capture range for certain commands based on known profiles. For example, if a voice command system is designed to be sensitive to a certain frequency range, sounds outside this range can indicate that the device is being manipulated using high-frequency sound waves that are inaudible to the human ear but detectable by the system. In contrast, time domain analysis focuses on the timing and rhythm of audio signals and can therefore identify unusual patterns, such as those produced by ultrasonic signals used in attacks like NUIT or SurfingAttack [38]. These analyses detect irregularities in the sound environment and enable the establishment of proactive defense mechanisms.

Most devices or even all, have pre-configured voice assistants and therefore there are only a few prevention techniques and methods that can be taken as precautions to reduce the possibility of such an attack. It is a good tool to combat cyber threats. Users need to be educated about the various techniques that attackers use in this attack. Users should be more careful and observant than before when communicating with a voice-activated device, as there is potential for some kind of risk. For example, making people aware of the risk of sensitive personal information being leaked by word of mouth, which can be used against a person if discovered by an attacker, is a good example [47]. Awareness of voice command security, for example, keeping microphones muted when not in use, can reduce the likelihood of devices being exploited. The second approach is to ensure that voice-activated systems strengthen their authentication mechanisms. Today's voice recognition systems verify them through spoken inputs or comparison of stored voiceprints/unique biometric features to ensure that only authorized individuals can access the system or perform certain sensitive operations. This means that when combined with other forms of biometric authentication such as passwords or fingerprints, the use of MFA in voice recognition can exponentially increase the overall security level of voice-based systems. This will also be important to help stop unauthorized access and minimize the scope of various attacks that may be directed at voice-activated devices.

Regular software updates, along with the installation of security patches, protect systems from newly identified vulnerabilities. Since attackers are always finding new ways to carry out cyber-attacks, it is critical that device manufacturers regularly update their various security measures and patch known vulnerabilities in voice recognition software. This ensures that devices are equipped with the latest defense mechanisms against emerging voice-based threats.

Because each of these threats requires a multi-layered defense strategy, including the latest technology, end-user training and corporate security controls, caution will be required by users and manufacturers amid the explosion of voice-activated technologies and increasing sophistication for cyber-attacks. All these combined—machine learning algorithms, advanced voice analytics, strong authentication methods, ongoing security updates and user awareness—can greatly reduce the likelihood of cyberthreats via voice.

7. Conclusion

While modern technology provides many comforts, voice-based cyber-attacks pose serious threats to security. This study examines various types of cyber-attacks using voice and discusses the methods and possible consequences of such attacks. From vishing, acoustic eavesdropping attacks, voice-delivered malware and special attack types such as NUIT and DolphinAttack, many types of attacks pose a real threat to cybersecurity and can violate people's privacy and security. The proliferation of these attacks is related to the increase in voice command systems and smart devices used by users. Nevertheless, the widespread lack of awareness of the vulnerability of voice command systems allows malicious individuals to carry out their activities to access personal information. Since voice-controlled devices are on the rise, more attention should be paid to manipulation using sound waves.

Voice-based cyber-attacks are a complex problem for users and organizations in general. The real attack exploits the inherent vulnerabilities in the same technologies that enable voice recognition and acoustic sensors to function. This type of attack is difficult to detect because most attacks use inaudible audio frequencies or transmit audio from hidden sources, which requires the creation of advanced detection techniques and prevention measures. Since cybercriminals are not standing still and new technologies continue to emerge every day, the security of voice-activated systems must also keep pace. Machine learning models, frequency analysis tools and voice filtering techniques are some of the most promising solutions to detect and mitigate these attacks so that immediate action can be taken in the event of suspicious activity.

Moreover, preventive measures cannot be limited to technological defenses. The complexities involved in voice-based attacks make extensive user education on their use important. Nevertheless, many people are still in the dark about the potential risks associated with this new generation of voice-activated devices and therefore can easily fall victim to attacks such as vishing, acoustic eavesdropping or malware-carrying audio files. This is because a lack of preparation paves the way for some form of interaction with digital assistants; such interaction is considered harmless but serves hidden villains. This means that manufacturing companies and software developers must take responsibility for embedding strong security measures in their products, including secure authentication mechanisms, periodic software updates and advanced encryption protocols for voice data.

Finally, voice-based cyber-attacks are detailed and multifaceted in their approach; they pose serious threats to users' security. It is time to inform users about the security protocols of voice command systems and to educate them about cybersecurity issues. Although the studies in literature generally focus on specific attack types, in this current study, the most common types of voice-based cyber-attacks were selected and each attack type was examined separately; a systematic study was prepared on the subject rather than a scattered structure. The issues require further research and study in-depth in order to create more robust security systems; hence, more literature is required in this aspect and the users of technology should be informed on the subject. In addition, device manufacturers need to produce systems that are resilient to such attacks and conduct training programs to increase users' awareness. In the future, more effective protection mechanisms and security measures, especially regarding voice-based cyber-attacks, will play an important role in ensuring cybersecurity at both individual and societal levels. In this context, research needs to be further supported to prevent and detect voice-based cyber-attacks with the aim of creating a single secure digital environment. Therefore, the increasing tendency for reliance on voice-activated devices and the ever-increasing level of cyber threats make the multi-layered security approach supported by technological innovation in a careful user a key factor in ensuring the security of digital systems.

Acknowledgements

This research was conducted independently without any external funding or financial support. Authors declare no conflicts of interest related to this work.

References

[1] T. D. Rossing, F. R. Moore, and P. A. Wheeler, *The Science of Sound*, 3rd ed. SF, USA: Addison Wesley, 2002.

[2] B. Mulgrew, P. Grant, and J. Thompson, *Digital Signal Processing: Concepts and Applications. London,* 1st ed. U.K.: Palgrave HE UK, 1999.

[3] B. Naqvi, K. Perova, A. Farooq, I. Makhdoom, S. Oyedeji and J. Porras, "Mitigation strategies against phishing attacks: A systematic literature review," *Comput. & Security*, vol. 132, p. 103387, 2023, doi: 10.1016/j.cose.2023.103387.

[4] W. Stallings, *Network Security Essentials: Applications and Standards*, 6th ed. Upper Saddle River, NJ, USA: Pearson, 2016.

[5] A. Saxena. "What is cybersecurity and why is it important?" Sprinto.com. https://sprinto.com/blog/importance-of-cyber-security/ (accessed Nov. 11, 2024).

[6] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems.* Hoboken, NJ, USA: Wiley, 2021.

[7] M. E. Whitman and H. J. Mattord, *Management of Information Security*, 6th ed. Boston, MA, USA: Cengage Learning, 2018.

[8] V Malik, A. Khanna, N. Sharma, and S. Nalluri, (2024). Trends in Ransomware Attacks: Analysis and Future Predictions. *International Journal of Global Innovations and Solutions (IJGIS).* doi:10.21428/e90189c8.f2996624.

[9] J. Mirkovic and P. Reiher, (2004). "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Computer Communication Review,* vol. 34, no.2, pp. 39-53. doi:10.1145/997150.997156.

[10] P. Cheng and U. Roedig, "Personal voice assistant security and privacy-A survey," *IEEE J. Emerg. Sel. Top. Circuits Syst.,* vol. 10, no. 4, pp. 476–507, Apr. 2022, doi: 10.1109/JPROC.2022.3153167. https://doi.org/10.1109/JPROC.2022.3153167.

[11] D. Bilika, N. Michopoulou, E. Alepis, and C. Patsakis, "Hello me, meet the real me: Voice synthesis attacks on voice assistants," *Computers & Security,* vol. 137, p. 103617, 2024, doi: 10.1016/j.cose.2023.103617.

[12] A. G. Desetty, V. D. Jangampet, and S. R. Pulyala, "Phishing attacks: Evolving techniques, emerging trends, and countermeasure strategies," International Journal for Innovative Engineering and Management Research, vol. 9, no. 12, pp. 985–991, 2020. [Online]. Available: https://www.researchgate.net/profile/Vinay-Dutt/publication/376645699_Phishing_Attacks_Evolving_Techniques_Emerging_Trends_and_Countermeasure_Strategies/links/673eb65d440ad82b18a086fb/Phishing-Attacks-Evolving-Techniques-Emerging-Trends-and-Countermeasure-Strategies.pdf

[13] A. Ansari and M. Nazir. "Risk assessment of security vulnerabilities in smart home using CAPEC and defensive goals." *Advances in Data and Information Science*, vol 318, p. 705–722, 2022, doi:10.1007/978-981-16-5689-7_63.

[14] F. McKee and D. Noever, "Acoustic cybersecurity: Exploiting voice-activated systems," *Cryptography and Security*, vol. 2023, p. 2312.00039, 2023, doi:10.48550/arXiv.2312.00039.

[15] S. Hussain, P. Neekhara, S. Dubnov, J. McAuley and F. Koushanfar, "WaveGuard: Understanding and mitigating audio adversarial examples," in *Usenix Security 2021,* 2021, pp. 1–10, doi:10.48550/arXiv.2103.03344.

[16] D. Buil-Gil, S. Kemp, S. Kuenzel, L. Coventry, S. Zakhary, D. Tilley and J. Nicholson, "The digital harms of smart home devices: A systematic literature review," *Comput. in Hum. Behav.,* vol. 145, p. 107770, 2023, doi: 10.1016/j.chb.2023.107770.

[17] F. Toapanta, B. Rivadeneira, C. Tipantuña, and D. Guamán, "AI-Driven vishing attacks: A practical approach," *Engineering Proceedings,* vol. 77, no. 1, p. 15, 2024, doi: 10.3390/engproc2024077015.

[18] C. Dinu. "What is vishing? Unmasking voice phishing scams and techniques." TextMagic.com. https://www.textmagic.com/blog/what-is-vishing/ (accessed Nov. 11, 2024).

[19] N. Bhatnagar and M. Pry, "Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study," *Information Systems Education Journal,* vol. 18, no. 1, pp. 48–58, 2020. [Online]. Available: https://files.eric.ed.gov/fulltext/EJ1246231.pdf

[20] C. S. Kayser, S. Back, and M. M. Toro-Alvarez, "Identity theft: The importance of prosecuting on behalf of victims," *Laws,* vol. 13, no. 6, pp. 68, 2024, doi: 10.3390/laws13060068.

[21] K. Marchini. "2018 Identity fraud: Fraud enters a new era of complexity." JavelinStrategy.com. https://www.javelinstrategy.com/research/2018-identity-fraud-fraud-enters-new-era-complexity (accessed Nov. 11, 2024).

[22] M.A. Siddiqi, W. Pak and M.A. Siddiqi, "A study on the psychology of social engineering-based cyberattacks and existing countermeasures," *Appl. Sci.,* vol. 12, p. 6042, 2022, doi: 10.3390/app12126042.

[23] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang and W. Xu, "DolphinAttack: Inaudible voice commands," in *ACM SIGSAC Conf. on Computer and Communications Security (CCS '17),* 2017, pp. 103–117, doi: 10.1145/3133956.3134052.

[24] H. Shah, M.Z. Rashid, M.F. Abdollah, M.N. Kamarudin, C.K. Lin and Z. Kamis, "Biometric voice recognition in security system," *Indian J. Sci. Technol.,* vol. 7, no. 1, pp. 104–112, Jan. 2014, doi: 10.17485/ijst/2014/v7i1.9.

[25] A. Hamed and N. Abdelbaki, "Acoustic attacks in iot era: Risks and mitigations," in *Proc. of the 2020 5th Int. Conf. on Cloud Computing and Internet of Things (CCIOT '20),* Okinawa, Japan, 2020, pp. 13–19, doi: 10.1145/3429523.3429530.

[26] European Parliamentary Research Service, "Data subjects, digital surveillance, AI and the future of work," in *Panel for the Future of Science and Technology,* Dec. 2020. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656305/EPRS_STU(2020)656305_EN.pdf

[27] A. Dixit, N. Kaur, and S. Kingra, "Review of audio deepfake detection techniques: Issues and prospects," *Expert Systems,* vol. 40, e13322, 2023, doi: 10.1111/exsy.13322.

[28] N. Robins-Early. "CEO of WPP Targeted by Deepfake Scam." TheGuardian.com. https://www.theguardian.com/technology/article/2024/may/10/ceo-wpp-deepfake-scam (accessed Jan. 9, 2025).

[29] M. U. Tanveer, K. Munir, M. Amjad, A. U. Rehman and A. Bermak, "Unmasking the fake: Machine learning approach for deepfake voice detection," in *IEEE Access*, vol. 12, pp. 197442-197453, Apr. 2024, doi: 10.1109/ACCESS.2024.3521026.

[30] Z. Cai, A. Dhall, S. Ghosh, M. Hayat, D. Kollias, K. Stefanov and U. Tariq, "1M-Deepfakes detection challenge," in *Proc. 32nd ACM Int. Conf. Multimedia (MM '24),* 2024, pp. 11355–11359, doi: 10.1145/3664647.3689145.

[31] J. R. Reeder and T. Hall, "Cybersecurity's Pearl Harbor moment: Lessons learned from the colonial pipeline ransomware attack," *The Cyber Defense Review,* vol. 6, no. 3, pp. 15–40, 2021. [Online]. Available: https://www.jstor.org/stable/48631153.

[32] S. S. Wang, "Integrated framework for information security investment and cyber insurance," *Pacific-Basin Finance Journal,* vol. 57, pp. 101173, 2019, doi: 10.1016/j.pacfin.2019.101173.

[33] Q. Xia, Q. Chen and S. Xu, "Near-ultrasound inaudible trojan (nuit): Exploiting your speaker to attack your microphone," in *Proc. 32nd USENIX Security Symp. (USENIX Security 23),* Anaheim, CA, 2023, pp. 4589–4606. [Online]. Available: https://www.usenix.org/conference/usenixsecurity23/presentation/xia.

[34] C. Yan, X. Ji, K. Wang, Q. Jiang, Z. Jin and W. Xu, "A survey on voice assistant security: Attacks and countermeasures," *ACM Comput. Surv.,* vol. 55, no. 4, Art. no. 84, Apr. 2023, pp. 1–36, doi: 10.1145/3527153.

[35] J. S. Lloyd, C. G. Ludwikowski, C. Malik and C. Shen, "Mitigating inaudible ultrasound attacks on voice assistants with acoustic metamaterials," *IEEE Access,* vol. 11, pp. 36464-36470, 2023, doi: 10.1109/ACCESS.2023.3266722.

[36] F. Hall, L. Maglaras, T. Aivaliotis, L. Xagoraris and I. Kantzavelou, "Smart homes: Security challenges and privacy concerns," in *Proc. 2020 arXiv Preprint,* Oct. 2020. [Online]. Available: https://arxiv.org/abs/2010.15394.

[37] Q. Yan, K. Liu, Q. Zhou, H. Guo and N. Zhang, "SurfingAttack: Interactive hidden attack on voice assistants using ultrasonic guided waves," in *Proc. Network and Distributed System Security Symposium (NDSS),* 2020. doi: 10.14722/ndss.2020.24068.

[38] C. Bolton, S. Rampazzi, C. Li, A. Kwong, W. Xu and K. Fu, "Blue note: How intentional acoustic interference damages availability and integrity in hard disk drives and operating systems," in *2018 IEEE Symposium on Security and Privacy (SP),* San Francisco, CA, USA, 2018, pp. 1048-1062, doi: 10.1109/SP.2018.00050.

[39] A. Kwong, W. Xu and K. Fu, "Hard drive of hearing: Disks that eavesdrop with a synthesized microphone," in *2019 IEEE Symposium on Security and Privacy (SP),* San Francisco, CA, USA, 2019, pp. 905-919, doi: 10.1109/SP.2019.00008.

[40] S. Panda, Y. Liu, G. P. Hancke and U. M. Qureshi, "Behavioral acoustic emanations: Attack and verification of PIN entry using keypress sounds," *Sensors,* vol. 20, no. 11, pp. 3015, Nov. 2020, doi: 10.3390/s20113015.

[41] X. Xu, Y. Liang, X. Zhang, Y. Wang, Y. Lin, B. Adebisi, H. Gacanin and G. Gui, "Self-evolving malware detection for cyber security using network traffic and incremental learning," in *Conference: 2022 9th International Conference on Dependable Systems and Their Applications (DSA),* 2022, pp. 454–463, doi: 10.1109/DSA56465.2022.00066.

[42] H. Ahmetoglu and R. Das, "A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges and future research directions," *Internet of Things,* vol. 20, p. 100615, 2022, doi: 10.1016/j.iot.2022.100615.

[43] B. Akbulut, "The principle of legality in the law of misdemeanors and violation the measures taken due to Covid-19," *Journal of Penal Law and Criminology,* vol. 9, no. 1, pp. 197–253, 2021. doi: 10.26650/JPLC2020-837085.

[44] R. Erbaş, "Organized crime-related legislation in the Turkish criminal law," *Ceza Hukuku ve Kriminoloji Dergisi,* vol. 3, no. 1, pp. 275–311, Jun. 2015. [Online]. Available: https://dergipark.org.tr/tr/download/article-file/14682.

[45] Council of Europe. "Convention on Cybercrime." rm.coe.int. https://rm.coe.int/prems-105223-gbr-2023-convention-cybercrimininalite-a5-web-4-/1680ae7118 (accessed October 10, 2024).

[46] IWM Cybersec. "Information Security Audit." IWMCybersec.com. https://iwmcybersec.com/information-security-audit/ (accessed October 10, 2024).

[47] Z. Wang, L. Sun and H. Zhu, "Defining social engineering in cybersecurity," *IEEE Access,* vol. 8, pp. 85094–85115, Aug. 2020, doi: 10.1109/ACCESS.2020.2992807.