applied sciences

MDPI

Article

An Effective Blockchain-Based Defense Model for Organizations against Vishing Attacks

Ahlam Fakieh and Aymen Akremi *

College of Computers and Information Systems, Umm Al-Qura University (UQU), Makkah 225400, Saudi Arabia
* Correspondence: amakremi@uqu.edu.sa

Abstract: Social engineering (SE) attacks (also called social hacking) refer to various methods used by cybercriminals to exploit the weak nature of human beings rather than the logical and physical security measures used by organizations. This research paper studies the various methods of SE used by criminals to exploit the psychological vulnerabilities of human beings. On this basis, the paper proposes a new defense categorization of SE attacks based on two security principles: dual control (i.e., more than one entity to complete the task) and split knowledge (i.e., dual controlling of the knowledge to complete the task). We describe how those measures could stop SE attacks and avoid human weaknesses. Then, we propose an original new SE defense model that implements the security principles using blockchain technology to both dual control the transactions and record them safely for organizations. The proposed model's first aim is to avoid the dependence on the cognitive or psychological status of the victim and enable more verification steps to be taken in a fast and flexible manner. The paper demonstrates the quick and easy adoption of the existing private blockchain platform to implement the proposed SE defense model.

Keywords: vishing social engineering attacks; organization defense model; security policies; blockchain; social engineering attack categorization

Citation: Fakieh, A.; Akremi, A. An Effective Blockchain-Based Defense Model for Organizations against Vishing Attacks. *Appl. Sci.* **2022**, *12*, 13020. https://doi.org/10.3390/app122413020

Received: 9 November 2022
Accepted: 16 December 2022
Published: 19 December 2022

1. Introduction

Social engineering (SE), otherwise referred to as social hacking, includes the various methods through which security is breached by exploiting the nature of human beings rather than attacking the established technologies and systems used by organizations [1,2]. Several SE tactics exist that cybercriminals use to attain their malicious and selfish interests that harm the victim. Those tactics include gaining illegal access to digital and physical resources, tapping the confidential and private information of the victim [3], installing malware and other harmful programs on the victim's system, and persuading the victim to initiate actions that will turn out to endanger their day-to-day organizational activities and even their social lives. The peak danger of SE attacks is the disclosure of privileged information after massive data breaches, which may lead to significant financial losses for the affected organization.

This paper focuses on vishing, which is a special type of phishing attack using phone calls against organizations. Vishing is a highly effective and focused type of SE attack that employs speech to entice victims into providing personal information. Vishing attacks are now very difficult to detect, especially when hackers use artificial intelligence (AI) to mimic speech patterns. A real example is when a caller who sounded just like the CEO of a UK energy supplier called the CEO in March 2019. The CEO transferred $243,000 to a "Hungarian supplier" since the conversation was so convincing, but the bank account belonged to a scammer [4]. Another attack, showing how creative cybercriminals have become in this SE ruse, is demonstrated by a recent data breach at the Ritz in London that turned into vishing assaults on hotel visitors. The Ritz assault's significance, among other high-profile incidents, shows that the phishing attack field has expanded as remote working has become more prevalent in corporate settings. The Ritz guests, who paid around

$3000 per night, fit a specific socioeconomic profile; as a result, the audio communications were carefully targeted and rehearsed. The attackers pretended to be from the Ritz and targeted corporate clients to obtain credit card information. Digital Trends claims that one victim fell for the hoax since the incoming phone number was faked to seem like the hotel's real number (https://www.forbes.com/sites/emilsayegh/2020/09/30/vishing-at-the-ritz-theres-a-new-type-of-cybercrime-in-town/?sh=386df16c700d, accessed on 5 November 2022). Due to the Ritz's lack of consumer education regarding what calls to anticipate about their patronage during regular business hours, the vishing assault was very successful. Additionally, working from home enhances SE assaults, meaning that company staff must identify acaller to evaluate whether he is a remote employee or a hacker impersonating an employee [5].

External factors may excite or provoke psychological traits in people, turning them into psychological flaws that could be the subject of an SE attack. We distinguish substantial influence overloading, reciprocity, deceptive relationships, responsibility and moral duty distribution, authority, integrity, consistency, and social verification that could influence the victim. Therefore, it is clear that human psychological conditions play a vital role in the success of SE attacks, even with security experts. We can never guarantee the separation between emotions and correct decisions.

This research seeks to respond to the question: How can businesses deal with people as a point of vulnerability that criminals might exploit through SE to further their illicit objectives? Enterprises must play a crucial part in making sure that this vulnerability is fixed and that SE assaults are drastically decreased. Creating a strong social media policy for the company's premises, and even while employees are off-site, is a realistic strategy that businesses adopt to reduce SE assaults [6]. However, such procedures and training will be ineffective if staff members do not follow them.

No defense framework or approach that effectively deals with human psychological characteristics exists, to the best of our knowledge. All of the existing defense approaches rely on security awareness and guidelines [7–11]. We distinguish the SEADM model [12], detailed in Section 2, that processes the psychological conditions and depends on the victim's decisions to stop communication with the attacker if the psychological conditions are deemed to be harmful. However, could we guarantee that the victim will follow the SEADM model?

This paper proposes a new effective SE defense model to overcome human weakness. The goal is to at least double the control of the transaction (i.e., from external sources) to ensure its integrity and avoid the possibility of the victim being deceived. We mainly implement the dual control and split knowledge principles [13] to mitigate SE attacks and avoid single failures through the use of blockchain networks. Split knowledge and dual control are used to avoid the possibility of one person being able to make the complete transaction or obtain full access to the information by themselves. Dual control focuses more on the transactions and task completion; however, the split knowledge condition essentially focuses on the data being split between two or more persons to prevent any person from having complete knowledge (i.e., dual controlling the information).

Blockchain is a mechanism for storing data in a way that makes system changes, hacking, and cheating hard or impossible. A blockchain is simply a network of computer systems that duplicates and distributes a digital record of transactions throughout the entire network. Each block on the chain comprises several transactions, and each participant's ledger receives a copy of each new transaction that takes place on the blockchain. Transactions on a blockchain are stored with an unchangeable cryptographic signature known as a hash. Distributed ledger technology (DLT) refers to a decentralized database that is governed by several users.

Our proposed method is the first that uses security principles for detection and mitigation of vishing attacks (i.e., a kind of SE attack achieved through phone calls). We first categorize the SE attacks according to the security principle required to stop them. Then, this paper proposes a new practical vishing attack defense model for organizations

that delineates the security principles to use to avoid attacks. The blockchain is a crucial solution used to ensure that decisions are taken transparently and collectively and that each transaction is trustworthy, backed up with a securely stored record [14]. It has a wide area of applications such as healthcare [15], agriculture [16], smart cities [17], etc. Blockchain is used mainly to enhance the dual control security principle by creating a new block only when all parties decide about a potential phone call and demonstrate the split knowledge principle since the victim does not have complete knowledge of any secret or sensitive information. The proposed model is for organizations and not for individuals. Thus, the word 'victim', in this paper, refers to the organization's employees targeted by the SE attacker. To summarize, the paper's contributions are:

1. The Categorization of SE attacks based on the security principles required to avoid them.
2. The proposition of a new framework that uses blockchain networks to dual control any potential transaction through its management flow and to enable split knowledge so that the victim does not have complete information and needs to request the remaining information from other parties within the blockchain network.
3. The easy adoption and practical implementation of the proposed model within organizations, using free open blockchain platforms.

The proposed framework has the following advantages:

- Avoiding the psychological status of the recipient of the vishing calls.
- Avoiding the recipient of the call having to act alone.
- Helping to make the right decision about received calls.
- Dual controlling critical phone calls.
- Using Blockchain to ensure that decisions are made collectively and transparently.
- Ensuring the accountability of any critical decision regarding phone call requests.

The remainder of this paper is divided as follows. Section 2 surveys the current works dealing with defense against SE attacks and discusses their limitations. In Section 3, we propose a new categorization of SE attacks based on the defensive measures to stop them. Section 4 presents a proposed new vishing defense model that uses Blockchain techniques to implement security principles. In Section 5, we demonstrate the easy adoption of the proposed framework using a hyperledger fabric and an open and free blockchain network. In Section 6, we discuss how well the suggested model performed. Finally, we conclude the paper in Section 7.

2. Related Work

Existing research and models aiming to protect organization assets from SE attacks targeting the psychological status of the victim are scarce. We did not identify any model that dual controls potential transactions, and no approach that uses blockchain to implement security principles to deal with SE attacks.

An organization's employees can utilize the methodology suggested in papers [12,18] to find social assaults in engineering in a contact center setting. The model is a quick and effective technique to see if the requester is attempting to coerce an individual into providing details for which the requester does not have permission. The psychological and computer science viewpoints are the two basic approaches of SE. The psychological viewpoint is concerned with the individual's emotional condition and cognitive capacities. One of the cornerstones of information security is information sensitivity, addressed from a computer science perspective. Social engineers exploit a variety of psychological vulnerabilities and triggers, which have been identified. Strong effect, overloading, reciprocation, deception, diffusion of responsibility and moral duty, authority and integrity, and consistency are among them. Human characteristics, such as our limited ability to digest information, our use of heuristics (cognitive process or shortcuts designed to make judgments simple, which might lead to a major error), individual interests, and our susceptibility to emotional manipulation.

The authors of [12] propose an SE attack detection defense model (SEADM), which uses a decision tree composed of several manageable components to help in the decision making in possible SE attacks. The first and most crucial stage in this paradigm, and one that must be considered throughout the process, is for the person to be aware of and analyze their emotional state regularly. The subject should assess the emotions elicited by the requester, as exploitation of psychological vulnerabilities is designed to provoke specific emotional states in order to obtain information. People are more likely to be SE victims if they are in a state of negative emotions: the level of focus is low, impatience and frustration are strong, and an individual may offer information to a requester to get rid of them. It is crucial to note that assessing one's emotional conditions can be time-consuming, and some people cannot do so. As a result, an electronic questionnaire for automatic self-evaluation would be implemented, the correct completion of which would lead to the right decisions. The phone or email request should be passed to another person if the individual or the self-evaluation questionnaire indicates that the person is extremely emotional. Unfortunately, there is a chance that some people may use this as a means of assigning someone else their work responsibilities, which will just irritate everyone.

The risks of SE, such as obtaining privileged knowledge, can result in significant losses for the institution. SEADM was established as a non-deterministic flowchart that relies on extensive qualitative sub-procedures in order to serve as a model for identifying SE attempts in their initial stages. An enhanced version proposed by [19] concentrates on formalizing the SEADM's most recent iteration into an abstract deterministic finite-state automation. Their research effort intends to improve the extensibility of the SEADM and reduce the complexity of its implementation by rebuilding the operation to be cycle-free and predictable.

The I-E model, which is based on human vulnerability, was utilized to achieve socialization in the publication [20]. The vulnerabilities exploited by various SE techniques were examined, and several defensive approaches to fix human flaws were deduced based on this model. The report identifies pieces of malware that have been activated through SE routes, including psychological and technical ruses. Some persuasive psychological approaches include victim curiosity, empathy, excitement, fear, and greed. Human vulnerability is a strategic connection in both the attack and defense aspects of an SE assault, as we can see from the workflow of an SE attack. It is vital to avoid human vulnerability to thwart exploitation; social engineers depend on exploiting such vulnerabilities. The internal and external nature that evokes human vulnerabilities, called the I-E model based on the effects of human conditions and vulnerabilities, are the two basic levels for producing the features of a person's human psychological states. Features of human nature can be categorized into two broad groups from a psychological standpoint: positive and negative. According to the I-E-based paradigm, there are various defensive strategies to repair human vulnerabilities; these defense measures are divided into objective and subjective approaches, as discussed in [20].

Another tool proposed by [21] provides the attacked subject another chance to confirm his or her decision when clicking on new links from untrusted sources. However, their application still depends on the individual, who may be subjected to psychological disruption. Authors from Bournemouth University proposed a new SE attack defense framework named MINDSPACE [22]. The framework describes the victim's behavior regarding different SE attack types. However, they did not explicitly propose defensive mechanisms to deal with them. In paper [23], the authors survey the facts of SE attacks targeting the banking sector in New Zealand. They then propose a mitigation model by decomposing SE attacks in five steps and presenting recommendations to prevent the attack being successful at each stage. Their approach still requires the victim to strictly follow the guidelines and avoid exposure to a single-point failure.

3. Preventing Social Engineering Attacks Using Security Principle

In this effort, we propose implementing two security principles to deal with human weaknesses: split knowledge and dual control. To the best of our knowledge, no previous model or research has implemented those security principles to deal with SE attacks and the reliance on human decisions. This section categorizes different SE attacks according to the security principles that will stop them. In addition, this is the first categorization that links defense techniques with specific SE attacks, rather than simply categorizing attacks [11]. We aim to implement a solution using security principles that avoid dependence on the psychological status of the individual, even if he or she is well trained. Human decisions and actions are unpredictable during any psychological condition, and employees in certain circumstances will threaten any organization's policy. The idea is to minimize the privileges and need-to-know for employees to a minimum, so that no one could disclose complete knowledge or make a transaction without the endorsement of at least one other person. Thus, even if one person breaches security guidelines, the second will usually discover it and avoid disclosing information or making suspicious transactions. Of course, the use of those security principles is applicable only within organizations where information is classified according to its sensitivity and tasks are distributed over several employees.

The categorization process of SE attacks is based on the following factors:

- Split knowledge is a subset of the dual control principle but related only to the information. Dual control is more related to processes and mechanisms. The categorization is based on whether stopping the hacker from knowing the information or completing the hacking operation will avoid the attack or not. In other words, if the SE attack fails when the information is not completelty gathered, then the SE attack is classified within the split knowledge category. Equally, if the SE attack fails when the operation is not completed, then the SE attack is classified within the dual control category. Some of the SE attacks could be stopped by both split knowledge or dual control. In this case, we categorize them as dual control since it represents the big umbrella.
- We show in the Figure 1 only the SE attacks that use different contact/communication techniques with the victim. Therefore, attacks such as piggybacking and whaling are not depicted in Figure 1 but mentioned as similar attack types.

It should be noted that attacks, such as honeytraps, scareware, pharming, and watering hole assaults, which are categorized as spoofing attacks and employ spoofing techniques to deceive the target, are not taken into account, since those assaults are carried out without the victim having to be involved. For instance, eavesdropping, shoulder surfing, and dumpster diving assaults do not necessitate conversation with the victim. Instead, they include information acquisition by illegal listing, peering over someone's shoulder, or searching for treasure in someone else's garbage, respectively.

Figure 1 shows the proposed categorization of SE attacks and the security principle to stop them.

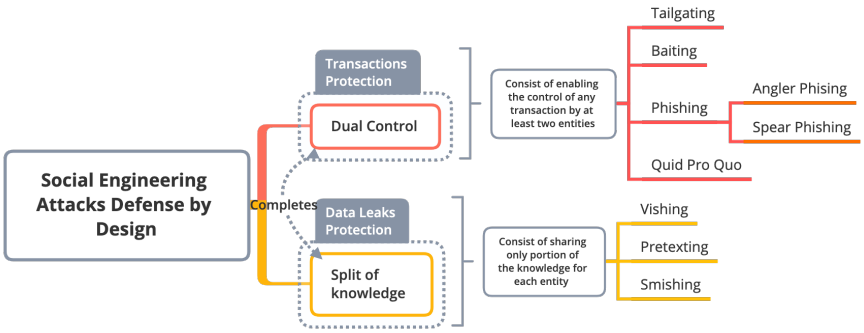

Figure 1. Categorization of SE attacks based on the security principles that prevent it. It describes how the security principle will avoid the associated SE attacks.

3.1. Defenses Based on Split Knowledge Principle

Split knowledge is a great security principle within organizations to avoid information disclosure by one person. It consists of dual controlling the knowledge (such as part of the password, cryptographic keys, etc.) to complete the task. In the USA, the cryptographic key responsible for launching nuclear bombs is divided among several persons, not only the president. Thus, the country is confident that such a critical decision will only be achieved after confirmation from the different parties. Split knowledge is achieved through precise definitions of privileges, good account management, and job rotation. This section will describe the different SE attacks that could be mitigated and stopped by implementing the split knowledge principle.

We should note that an organization will classify data according to the sector it belongs to, as explained in Section 4.1. By Split knowledge, we mean that every person in the organization knows only the information he or she needs (need to know) according to the data classes defined by the organization, so the information is split between the different employees.

3.1.1. Smishing

Smishing is a mashup of the words SMS and phishing. Smishing is a type of cyber-attack in which the attacker deceives the victim into disclosing sensitive information or handing over money. The cybercriminals dupe the victim into thinking the message came from a well-known person or group. They frequently ask the victim to click on websites or contact a specific number to verify, update, or reactivate their account [24]. We distinguish another SE attack that uses instant messages named spimming. Spimmers typically employ bots to gather instant message IDs and send spam to victims. A bot is an application that performs automated activities over the network.

For cybercriminals, bank smishing is the most profitable sort of attack. Cybercriminals prey on the victim's fear of having their bank accounts compromised. They usually send the victim a text message purporting to be from the bank, warning them about a large financial transfer or a new payee being introduced. When the target responds and follows the instructions, the attackers collect sensitive information such as bank account login credentials and other personal information. The attacker can quickly access your bank account once they obtain your credentials. As a business owner, you must educate your personnel on how to recognize smishing and other sorts of attacks. The victim's psychological situation, on the other hand, puts training provisions in jeopardy.

When the split knowledge concept is employed, the victim will lack the necessary information to satisfy the attacker's objectives, rendering their attacks ineffective. Split knowledge will ensure that the victim does not possess the complete information to execute the transaction desired by the requester (possible hacker).

3.1.2. Vishing

Vishing is a unique assault that falls under the general umbrella of phishing and has the same objectives as phishing. Vishing uses fake phone numbers, voice-altering software, SMS messaging, and SE to deceive consumers into giving critical information that can be utilized for identity theft, financial gain, or account takeover. Voice is commonly used by vishing to mislead users.

Vishing, unlike phishing, is primarily a telephone-based assault that involves calls to a user's cell phone number. The first step would be for the visher to send a large number of text messages to possible victims from a vast list of phone numbers. The message may instruct users to dial the attacker's phone number. Another vishing technique involves sending a pre-recorded message to potential victims, which is then robo-dialed. To erase accents and develop confidence, it uses computer-generated audio communications. The voice message then leads the user to a human agent who either continues the fraud or asks them to visit an attacker-controlled website. The goal of vishers is to mislead the victims into thinking that they caller has authority by providing social proof [25].

Educating users helps organizations recognize vishing attacks, which they can then ignore or report. Individuals should never hand out personal information to someone who contacts them via text message or phone call. Those defenses all rely on an individual's accurate judgment; therefore, any error will result in losses for the organization. By applying split knowledge and dual control principles, the victim will not have complete sensitive information, and any suspicious call will be checked; therefore, the damages will be mitigated.

3.1.3. Pretexting

Pretexting is a SE method used to trick people into handing over information. A pretext is a made-up scenario concocted by threat actors to acquire a victim's personal information. Threat actors generally ask victims for specific information during pretexting assaults, claiming, for example, that it is required to authenticate the victim's identity. The threat actor steals this data and then uses it to launch secondary attacks or commit identity theft [26].

Pretexting assaults develop a false sense of trust with a targeted victim, whereas phishing attempts prefer to leverage urgency and fear to exploit victims. This means that threat actors need to fabricate a plausible explanation that does not lead victims to suspect illegal activity.

3.2. Defenses Based on Dual Control Principle

The dual control principle uses two or more separate entities (usually persons) to complete tasks. Thus, the responsibility of making a transaction is shared between the involved entities, which prevents a single person from accessing or using the materials individually.

This security principle will avoid the reliance just on one person's decision who may be subjected to a psychological situation. So, at least two persons, according to the organization's policy, will handle any transaction, which will reduce the possibility of human errors.

3.2.1. Quid Pro Quo

A quid pro quo attack is a low-level sort of SE-based hacking and a form of baiting. A cyberhacker offers the victim something in return rather than attempting to trick him or her out of curiosity or fear. It basically comes down to "a favor for a favor", which is what the Latin term implies. Attackers solicit information from the victim in exchange for anything. Given that humans adhere to the psychological reciprocity rule, the idea of exchange is essential. This implies that the victim feels obligated to repay someone for everything they offer or accomplish for him (https://blog.mailfence.com/quid-pro-quo-attacks/, accessed on 5 November 2022).

Quid pro quo assaults, like all other types of SE attacks, target an organization's human aspect. These attacks endanger your employees' online safety and jeopardize your entire company's cybersecurity [27].

Employees could be protected against SE attacks such as quid pro quo by implementing certain practices and rules. Security awareness training for all organization employees is required to spot prevalent SE approaches. However, it is still contingent on the victim's psychological condition and rigorous adherence to the training.

3.2.2. Tailgating

Tailgating is a straightforward physical SE technique that allows hackers to have access to password-protected physical assets. Tailgating is when you closely follow an authorized individual into a restricted location. When a typical employee swings a hefty door, a tailgating social engineer may seize it just as it closes, walking right into the targeted physical system. Organizations are particularly vulnerable to tailgating SE attacks if they have a large number of employees and a high rate of staff turnover. Another similar SE attack called piggybacking differs from tailgating in that piggybacking entails an authorized

person intentionally allowing a hacker to enter a restricted zone thinking he or she has a legitimate reason for being there.

To prevent tailgating attacks, businesses should ensure that the reception area is well-lit and that identification mechanisms are in place. Tailgating can also be controlled and thwarted with visitor badges and video surveillance. Employees should be cautious and follow security best practices in general. Dual entry control for the organization will provide extra defense lines and prevent tailgating.

3.2.3. Baiting

Baiting assaults, as the name describes, pique a victim's interest or avarice by making a false promise. In order to steal private information or infect systems with dangerous software, they manipulate individuals into falling into a trap. The most despised kind of baiting uses tangible material to spread malware [26]. For instance, attackers can set out the bait—malware-laced ash disks—in plain sight in places where potential victims are likely to encounter them (such as restrooms, elevators, or the parking lot of a targeted business). The lure has a realistic appearance and is tagged, for example, as the corporation's salary report.

Employing a dual control system, where at least two or more persons are in charge of a single process, will help defend organizations from cyber dangers.

3.2.4. Phishing

Phishing is a category of SE assault that is mainly used to gain sensitive information from users, such as login credentials and credit card information. It occurs when an attacker shows up masquerading as a trustworthy entity and convinces a victim to open an instant message, email, or text message. The recipient is duped into entering a malicious link, which can lead to a malware installation, the disclosure of sensitive data, and system freeze as part of a ransomware assault [28]. Whaling is a type of phishing attack when it targets a specific high-profile person and uses the same techniques as phishing.

Two-factor authentication (2FA) is the most effective approach for preventing phishing attacks when logging into sensitive applications since it offers an extra degree of verification. Users need two things to use 2FA: something they know, such as a password and username, and something they have, such as their smartphones. It would be best to use a 2FA approach to avoid psychological difficulties for more than one individual.

3.3. How Security Principles Prevents Social Engineering Attacks

Following the classification of SE attacks and showing how defenses can be based on the security principles that thwart them, in this part, we will discuss how such security principles may prevent SE attacks. Each SE attack is described in Table 1 along with the security concepts that may be used to mitigate it at the data and management levels.

3.3.1. Split Knowledge Effectiveness Analyis

The proposed model is designated for corporations and organizations in a working environment. It is not to protect individuals from SE attacks outside their job.

As we mentioned in Section 4.1, data within the organization are supposed to be classified according to the organization sector (governmental or private). So, the [recipient], who will be the first person in contact with a possible SE hacker, knows only public information. He or she does not have secret information to disclose. Smishing, for instance, uses SMS to contact the victim. If the victim (recipient) does not know the private information since the knowledge is split and classified, he or she will redirect the request through the blockchain network to another background verifier. Mostly, the second verifier will discover that the SMS is a kind of smishing and notify the recipient. The goal is to deal with the problem of single-point vulnerability presented by the recipient, but through split knowledge, the problem will be handled by more than one person who does not witness the psychological circumstances. Therefore, the secret information will not be disclosed since any transaction must be endorsed by several verifiers determined by the organization. Even, if one verifier

is tricked, the transaction will be accepted only if all the verifiers endorse it. In addition, it will not be a summative gathering of the information by the hacker since the transaction atomic can only be accepted after all defined organization peers endorse it.

Similarly, split knowledge will protect corporations against all SE attacks classified on its category.

Table 1. Security principles ability to stop SE attacks.

SE Attacks	Security Principles	How to	
		Data Level	Management Level
Smishing Vishing Pretexting	Split knowledege	Sort information into categories according to its sensitivity and the sector it belongs to. The original recipient of external emails, SMS, or phone calls will only know information that is available to the public. Split knowledge is therefore information classification rather than data slicing.	Information classification will be governed by organizational policies. Each person will only be allowed to know the information necessary to perform his or her job, and those who have direct contact with the outside world will only be allowed to know information that the company deems appropriate to transmit or is generally known.
Quid Pro Quo Tailgating Baiting Phishing	Dual Control	The information required to complete a task is divided between at least two persons. So, if the attackers deceive one victim it will be harder to trick the second also.	The management system should allow double verification of any transaction.

3.3.2. Dual Control Effectiveness Analysis

Dual control is an implementation of a defense-in-depth strategy. It involves more protection mechanisms to complete any transaction. Dual control requires at least two persons to handle any transaction so that if one person is tricked, the second will discover it. For instance, quid pro quo, tailgating, baiting, and phishing attack success depends on bypassing one direct person. It does not require information disclosure but mostly incites the victim to do something. Dual control will stop those attacks since every transaction will be verified twice.

Similarly, dual control will protect corporations against all SE attacks classified in its category.

4. A Social Engineering Attack Defense Model for Organizations Performed via Merging Security Principles and Blockchain

Figure 2 represents the proposed new SE defense model that implements dual control and split knowledge security principles using private blockchain technology. Figure 2 shows the different ingredients and connections between the different entities of the proposed SE attack defense model. It consists of separating the control between involved parties and documenting agreed processes in a decentralized way to improve accountability and transparency. Thus, any potential request for non-public information or unusual transactions by phone call will be dual controlled and collectively processed. The issues of the psychological status of the phone recipient will be avoided, and the attacker will find it harder to collect information about each background verifier of the transaction.

The proposed model uses blockchain technology to implement and manage dual control requirements. Blocks are created only when all participating parties positively endorse the transaction. In that event, a new block is issued containing the different transaction details. The blockchain will also enable the recording of all transactions in

a non-repudiation manner, which is very important for accountability requirements. We use private blockchain since all parties are within the same organization. Private blockchain does not face scalability and time-relentless issues since it does not require proof of work as in a public blockchain.

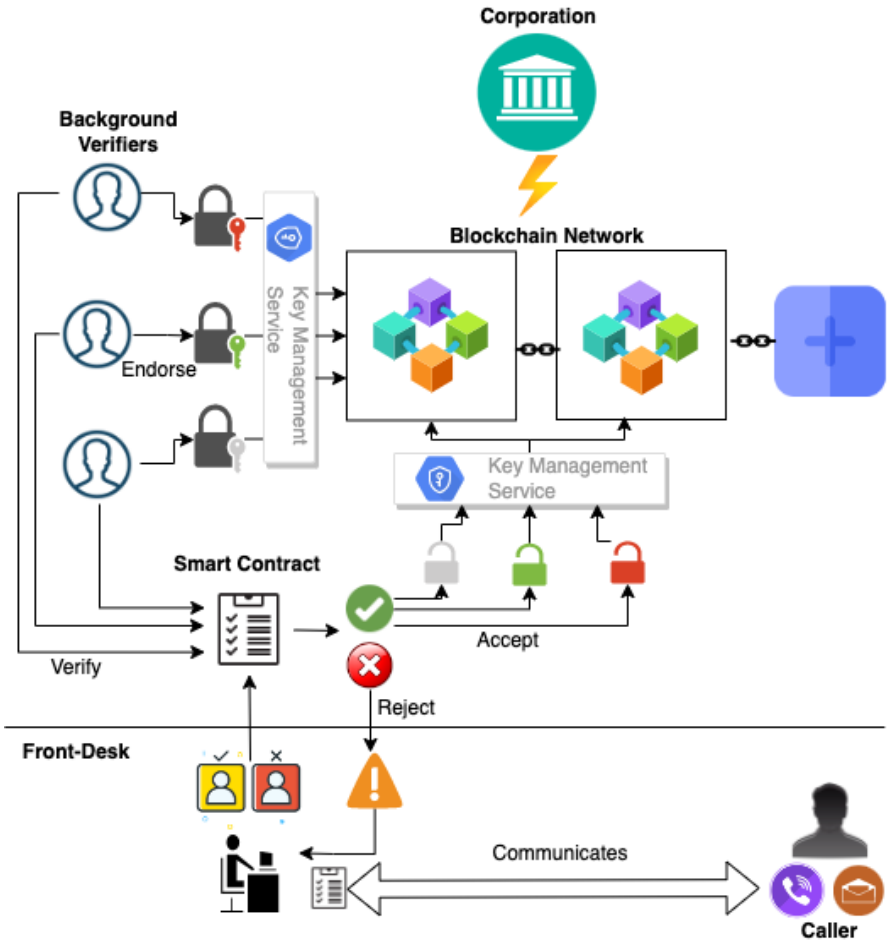

Figure 2. A blockchain-based defense model against vishing attacks.

4.1. System Requirements

The proposed model is supposed to run in a well-established organization that applies standard-based information security guidelines. More specifically, the proposed framework requires that the organization already practice the following security routines:

- The organization's data are supposed to be classified according to the sector (governmental or commercial) [29]. The data are classified by the data owner, maintained by the data custodian, and confirmed by the security manager. The classifications for the data sensitivity used in government and military applications are top secret, secret, confidential, sensitive but unclassified, and unclassified [29]. However, the classification of the data sensitivity used in the commercial sector is sensitive, confidential, private, proprietary, and public [29]. So, the organization splits the knowledge according to this classification between the recipient and the background verifiers. Mostly, the recipient will have the least sensitive data that does not cause any harmful consequences if disclosed.
- The organization possesses an internal private network to communicate. Obviously, almost all organizations implement private networks to enhance their performance.
- The organization has a precise procedure to verify a caller's identity, such as the information that the caller must provide to accomplish his or her request.

Integrating the proposed defense model within the organization is straightforward if it just practices the security standards.

4.2. Model Components

The proposed model encompasses several units:

- Recipient (front-desk): is a representative who answers all incoming calls from outside the company. Their role is to provide information about the caller's requests if they know the answer. The recipient knows public information. If they do not possess the knowledge, they will ask the information from other employees. The recipient does not know anything considered secret about the organization's data and is not permitted to make any transactions.
- Social engineer (caller): is an external caller wishing to obtain sensitive information or make illegal transactions, such as changing bank account-associated phone numbers.
- Background verifications: are performed by any number of individuals to ensure that the transaction complies with the organization's security regulations. They receive any requests for information or certain transactions made by the recipient. If they suspect the query, they reject it and notify the recipient about a possible SE attack. If all background verifiers confirm the transaction's validity, the transaction is registered and saved in a blockchain. Then, the recipient can deliver the information or transfer the caller to the requested service.
- Blockchain: is the data structure that enables decentralized registration of transactions requested through phone calls. The main goal of using blockchain is to create a new block when all involved parties agree to a transaction: no one can individually decide without others knowing about it. No transaction will be made before creating the new block that records the transaction endorsed by the involved parties. The blockchain manages the endorsement process and resolves the synchronization issues. It implements dual control security principles.
- Blockchain owner: is any organization interested in installing a secure mechanism to avoid social attacks by phone, especially within the banking sector. The blockchain owner is responsible for implementing the various policies, such as assigning permissions to allowed agents that check for a potential SE attack. Those checkers could have the same or different sensitive data according to the organization's policies.
- Key management system: generates access keys used to access the private blockchain. In addition, the keys are used to create the new blocks. A new block will only be formed when it is endorsed by all the parties involved, using their keys during the verification process. The key management system is generally incorporated within the blockchain platforms. In this way, the organization can implement a blockchain network and access management systems from scratch or reuse and adapt existing platforms, such as the hyperledger fabric blockchain network.

4.3. Framework Design Description

4.3.1. Control Flow Description

This section describes a scenario of the different interactions that could occur during the execution of the model within an organization. We choose, as a demonstration example, the Banking sector where the hacker aims to exploit the over-helpfulness of help desk employees. The SE attacker wants to switch Eric's account-associated phone number to one of his phone numbers. If he succeeds, the attacker might use Eric's account to complete numerous transactions. The scenario is inspired from ECCouncil's *Certified Ethical Hacker Study Guide* [30], more specifically from the vishing attacks section. Following, we describe the control flow without deploying the proposed model and then after applying it.

Control Flow Description before Applying the Proposed Model

Social engineering attempts regularly target help desks. Since the staff employees are instructed to be helpful, they frequently divulge private information, including passwords

and network details, without first confirming the caller's identity. To be successful, the attacker has to know the identities of the workers and specifics about the person he is posing as. When calling a company's help desk, an attacker can pose as a senior figure to obtain access to confidential information. In this example, a person contacts the help desk of a bank corporation and claims to have changed his phone number, requesting to change the current bank account associated number to another new phone number. He continues by saying that his employer could fire him if he misses the transfer of an important advertising fee within the next thirty minutes. The help desk staff member immediately changes the bank account associated phone number out of sympathy and unintentionally allows the attacker access to the compromised bank account.

In this scenario, the hacker achieved his goal by exploiting the over-helpfulness of the recipient (help desk employee). There is no control to verify the correctness of the recipient's action.

Control Flow Description after Applying the Proposed Model

It starts when the organization recipient receives an external call from an unknown person. The caller requests to change his or her account-associated phone number since the telecommunication provider has changed. The recipient will provide the caller with any public information. However, when asking for confidential information or modifying data, such as passwords or phone numbers in the case of a banking organization, the recipient will ask for more identity details already specified by the organization. Once receiving the caller's required identity parameters, the recipient will send a request through the blockchain network to modify or perform some tasks. Requests are transformed into smart contracts via a dedicated front-desk application and sent to one, two, or more transaction verifiers according to the organization's policies. The verifier could be a cybersecurity agent, a bank agent, a data custodian, or any permitted entity by the organization. They verify the request and can endorse (accept) or reject the transaction.

In case of transaction acceptance by the verifiers, the requested information is returned to the recipient. In case of SE attack suspicion, the recipient is alerted of possible SE attacks demanding more details or ordering him or her to end the call and block the caller number.

4.3.2. Multiaccess Control Management

Each blockchain interacting entity's access management and privileges are achieved through the identity verification and validation process and via the access control list enforced by following detailed policies.

Identity Verification and Membership Validation of Different Actors

Once the recipient sends a request for further data or task completion, it is first handled by other persons specified according to the organization's policy. They will use their digital identities in the form of cryptographic digital certificates according to X.509 standards generated by the organization's certification authority to endorse or reject the recipient's request. Only permitted persons could join the endorsement process according to the request type and content.

The implementation of this scenario is achieved through the use of private blockchain technology. It consists, as shown in Figure 3, of generating digital identities that contain the digital signature generated through the public and private keys of the person verified and issued by the certification authority. Any suspicious or invalid identities are stored in a revocation list to accelerate the verification process and detect fraudulent identities. According to the organization's policy, these valid digital certificates are stored on a membership service provider (MSP). The MSP's role is to verify if the person who has the specific digital certificate is allowed to participate in the transaction validation. The organization determines and sets the eligibility of each endorser (person) through policies. The MSP also has a role in turning newly defined entities into recognized entities in the blockchain

network. In this way, the MSP enables any newly defined organization entity to participate in the private blockchain network.

Once all involved parties agree on the transaction and endorse it, a new block is created and added to the main organization's blockchain ledger. Otherwise, the transaction is rejected. Thus, access management is achieved by generating digital entities via the certificate authorities (CA) and validating the person's eligibility to join the transaction verification process through the MSP.

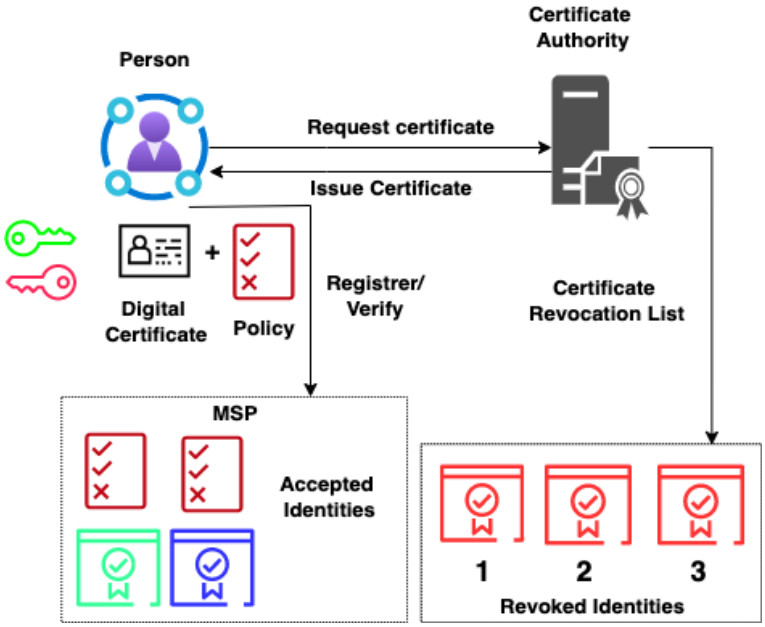

Figure 3. Identity certifications issuing and membership service provider verification.

Access Control List Enforcement through Policies

Access to the blockchain is determined by the policies defined during the establishment of the blockchain network. The policies identify how to add a new entity or remove it. These policies also describe the characteristics of entities and their privileges to access the blockchain. The organization could change the policies according to their needs even after blockchain creation since we adopted a permissioned blockchain technology. Details and samples of access control list policies are in the implementation and results section.

5. Implementation and Results

This section demonstrates the feasibility of the proposed approach through the easy transformation of the proposed model into a working environment based on blockchain technology. As we mentioned, we will use a private blockchain requiring authentication of every involved party through the access management service. More specifically, we will use the hyperledger fabric technology (https://www.hyperledger.org/use/fabric, accessed on 10 September 2022), which fits our design needs, to implement the proposed model.

5.1. Adoption of Hyperledger Fabric Blockchain Technology

Many organizations provide different implementations of blockchain networks, such as ethereum. Our proposed model could be implemented from scratch or using existing blockchain frameworks. Since our model consists of a permissioned blockchain network within an organization, we choose hyperledger fabric implementation. Our choice is motivated by the following arguments:

- Hyperledger fabric is a permissioned blockchain network.
- Hyperledger framework is not dedicated to cryptocurrency but for any transaction requiring trust recording and management of different involved entities securely and transparently.

- Hyperledger framework is an open software that can be freely modified and improved to fit the application domain.
- Hyperledger's fabric enables enforcement of the organization's policies during the creation of the blockchain network, management of different entities, and endorsement rules.
- Hyperledger fabric uses smart contracts to interact with the blockchain network, which is very flexible and enables wide interaction options.

Therefore, our model could be easily and quickly adopted and implemented within any organization using hyperledger's fabric-free and open software, which is very important to minimize the time and cost of using the proposed model. The following sections will provide samples of the main hyperledger fabric components and their adoption to implement the proposed SE defense model.

5.1.1. Blockchain and Policy Creation

The creation of the hyperledger fabric blockchain starts by defining the organization channel configuration contained in the configuration block. The channel configurations are formulated in the configtx.yaml file. The channel enables the interaction between the different peers (employees in our case) and defines the organization that governs the network to organize the various transactions. The agreed organization to control the blockchain network will contain an orderer entity that receives smart contracts and distributes them to blockchain network peers. The network governor can be changed after the network creation. We have only one bank organization and many employees interacting with the blockchain in our model. Therefore, the network governor will be the ban,k and it will manage the permitted employees through the orderer. Through the channel, the recipient, who receives the client's calls in our case, will communicate with the different peers.

5.1.2. Peers Definitions

Peers in the hyperledger fabric represent the fundamental entity of transaction endorsement, validation, or rejection. Peers represent the entities that receive and process the client's smart contracts. The network gateway service is responsible for managing the distribution of the smart contracts between all peers and its retransmission to the client for final endorsement. After that, the orderer is responsible for the new block addition to every peer ledger. The orderer is responsible for updating the blockchain ledger between all peers. No probabilistic approach is used within the fabric network, since any block validated by the peer is guaranteed to be final. This is explained by the fact that all participating peers are within a private network.

In our case, the peers are the background persons (e.g., those who dual-control the transactions) who verify the recipient's request. Here, the recipient is the peer who initiates the interaction. Through a well-defined application, the recipient will create the smart contracts that contain the transaction details (i.e., the information provided by the caller) and then send the smart contract (request) to the verification process. The organization specifies the number and type of peers required to endorse the transaction. In this way, the system keeps its flexibility to deal with missing peers or endorsements, such as ruling that at least two peers must approve the transaction, instead of four, if they have privileges and the data equivalent to those with the missing peers. Thus, the processing time will be faster and avoid delay in a case when one or more peers do not respond quickly.

Listing 1 shows an example of the bank channel configuration that defines the access list of permitted peers and their privileges. The peer's identities are verified through the MSP already detailed in the multi-access control management section. After adding their digital signature, the peer endorses a proposal response to a smart contract by using their private key to sign the entire payload. This endorsement serves as proof that this organization's peer generated that response. Therefore, the organization will ensure the non-repudiation of actions made by its employees.

Listing 1. Sample of policies enforcing ACLs within the Bank organization.

```
&BankOrg
#DefaultOrg defines organizations involved in the blockchain network
Name: BankOrgMSP
# ID to load the MSP definition
ID: BankOrgMSP
MSPDir: ../organizations/peerOrganizations/BankOrg.bank.com/msp
#Policies defines the set of policies at this level of the config tree
#For organization policies, their canonical path is usually
#/Channel/<Application|Orderer>/<OrgName>/<PolicyName>
Policies:
Readers:
Type: Signature
Rule: ''AND('BankOrgMSP.admin','BankOrgMSP.peer','BankOrgMSP.employee')''
Writers:
Type: Signature
Rule: ''AND('BankOrgMSP.admin', 'BankOrgMSP.employee')''
Admins:
Type: Signature
Rule: ''OR('BankOrgMSP.admin')''
Endorsement:
Type: Signature
Rule: ''AND('BankOrgMSP.peer')''
```

5.1.3. Consensus Configuration

We adopt Raft (http://thesecretlivesofdata.com/raft/, accessed on 5 September 2022) implementation which is a crash-fault-tolerant (CFT) ordering service. Raft uses a "leader and follower" structure. Decisions are made by the leader, and followers obediently execute them. The peer who stands in for the leader regularly switches. Every follower gets a chance to run for the position of leader in the upcoming round. As Raft works, the leader could be any peer defined by the organization and elected as leader once they receive the majority of votes from the other peer nodes. Since the organization adopts data classification and split knowledge among their employees, the consensus will be validated once all peers endorse the transaction. In case of missing peers, the service orderer will consider the remaining peers on the condition they have equivalent data and privileges to those of the missing peers. Otherwise, the transaction is held pending connection with the missing peers. We have only endorser peers, since the blockchain network is implemented within only one organization. Thus, there is no need for anchor peers, which are required to communicate with other organizations.

5.1.4. Smart Contract Definition

The smart contract is a program that defines the structure and possible actions already agreed to by the organization before deploying the blockchain network. The smart contract contains the data that must exist or is optional. It also defines the interaction rules between the different peers. The execution of a smart contract starts a new transaction that, when it is endorsed by the required peers, will be added to the ledger of each peer. Figure 4 presents an example of a smart contract structure that contains the details of the recipient's request and the possible actions that the peer could determine.

It also specifies the peers required to endorse the transaction. The smart contract may re-use several APIs to create, modify, or delete an object from the peer ledger. The main blockchain remains, and after the transaction is finished, all peers' ledgers synchronize with the main blockchain.

In Figure 4, we use four methods to verify the caller's identity and update the required information or reject it. A 'get' method often denotes a request to obtain details regarding an object's current status. In this example, the get query asks for the caller's identity credentials. The recipient provides the different identity parameters according to the information provided by the caller. The 'verify' method returns the peers' decisions about the validity of the query and the information integrity that identifies the caller. An 'update'

method creates a new object containing an updated version of an existing one in the ledger world state. A 'reject' method represents the rejection of the transaction since the required endorsements are not satisfied.

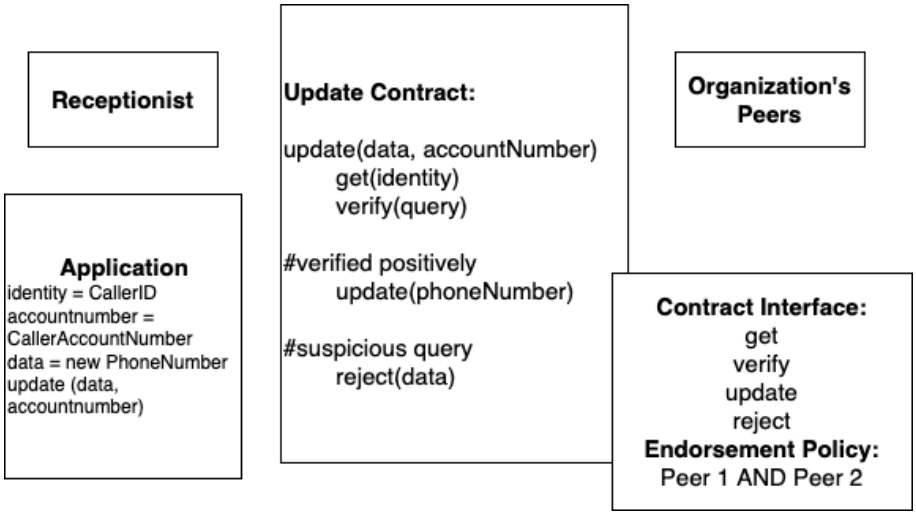

Figure 4. Smart contract structures, methods, and endorsement policies.

Listing 2 shows an example written in JavaScript of a smart contract filled by the recipient requesting an update of the client's bank account phone number. The orderer serves as a collector of endorsements from the peers. The blockchain network will create a new block only if the different involved peers endorse the transaction.

Since smart contracts are the only piece of code that communicates with the blockchain network, it is necessary to exercise security software testing techniques [31,32] to ensure that they are bug-free before deploying them.

Listing 2. Sample of smart contract for requesting bank phone number update.

```
async UpdatePhoneNumber(clientID, ClientAccountNumber, newPhoneNumber,
changeReason, requestType) {
        const query = {
                clientID: 18,
                ClientAccountNumber: Bank001122,
                newphoneNumber: 5483790102,
                changeReason: "I change my old phone number",
                requestType: "phoneCall
        };
 return ctx.stub.putState(clientID, Buffer.from(JSON.stringify(query)));
}
```

5.2. Application Interface to Interact with the Organization Blockchain

As a prototype of the application interface that the recipient uses to submit queries, we implemented a web-based user interface that enables interaction with other organization members. Figure 5 shows a prototype of the request submission form. Mainly, it contains the fields to identify the caller as provided by the caller and a description of the caller's request. Each request sent by the recipient is converted into a smart contract. Smart contracts are the only means to interact with the blockchain. Other blockchain members must either accept the addition of the smart contract to the blockchain or reject it to disable the transaction. In our implementation of the SE defense model, the smart contract will contain the request details, such as the caller identifiers and the request description.

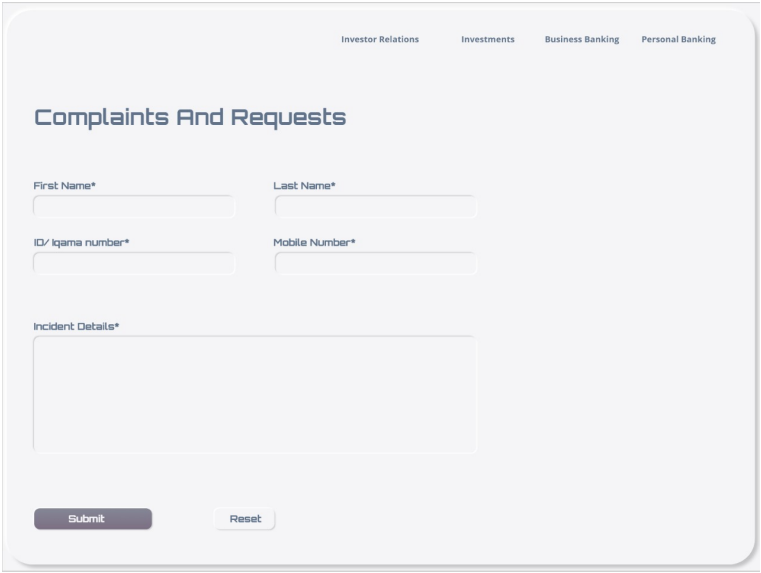

Figure 5. A prototype of the recipient web-based application to submit caller requests and therefore interact with the blockchain network.

6. Discussion

Throughout this paper, we described a new SE attack defense model that avoids the psychological issues exploited by the SE attacker [26]. In Table 2, we depicted the proposed model's advantages compared to the existing models dealing with SE attacks, which are very scarce. In addition, the table describes features of the model enabling the implementation of security principles.

Table 2. Proposed model features and ability to implement security principles: comparison with other models.

Features Features	Psychological Status	Dual Control	Split Knowledge	Transactions Storage	Single Point of Failure	Easy to Adopt
SEADM	✓				✓	
SEADM II	✓				✓	
I-E model	✓				✓	
MindSpace	✓				✓	
Our Model	✓	✓	✓	✓		✓

6.1. Ability of the Model to Deal with Employee's Psychological Status

The models listed in Table 2 all aim to solve the dependence on individual psychological status when subjected to SE. Except for ours, their success depends on the person's strict compliance with the instructions of the model; however, the model never enforces compliance, so the victim could ignore the regulations and therefore be defeated by the attacker.

Existing models such as SEADM rely on the person's strict compliance with the model's instructions; however, the model never compels the person. Consequently, the victim could ignore the regulations and therefore accede to the requests of the attacker. The SEADM and similar models require humans with robotic hearts and minds to effectively deal with SE attackers experienced in exploiting the psychological susceptibility of the victim. However, an individual's actions depend on their culture, environment, and things that are important to them; if these are correctly exploited, the victim will not follow the organization's regulations.

Only our proposed model, which involves background checks, can double-check a transaction before it takes place since one of the model's purposes is to avoid a single point of vulnerability. By enforcing security principles, we are confident that the attacker

will not succeed in his objective by just bypassing the person called; the attacker must also get beyond the background checks conducted by other persons, about whom the attacker knows nothing. The control and monitoring of the attacker's attempt to trick the recipient are enabled via the blockchain model's component. The model, via the blockchain data's flow, will treat the request from the recipient who received the suspicious call first by translating it into a smart contract. Then, the orderer will deliver the transaction to all required peers (verifiers). The transaction is accepted if all peers endorse it; otherwise, it is rejected. This is how the model implements dual control and benefits from the blockchain management mechanisms. We are aware that SE relies on the attacker carefully collecting information on the victim to craft successful deception. Since the background verifier(s) are unknown to the attacker, they cannot be psychologically deceived.

6.2. Ability to Enforce Security Principles (Dual Control and Split Knowledge)

To the best of our knowledge, no approach deals with the psychological depression of the victim regarding vishing attacks by enforcing the organization's policies. Our proposed model enforces the organization's rules by implementing two security principles: split knowledge and dual control. The main idea is to subject suspected SE attacks to double or greater verification. The enforcement of security policies is enabled through blockchain deployment. It manages dual control through separation of the request (smart contract) sent by the client (recipient) and the required verification by peers (background verifiers) to endorse (accept) or reject it. Consequently, split knowledge is enforced, since the information known by the recipient is not sensitive based on the organization's data sensitivity classification, as explained in Section 4.1.

The blockchain has the power to coordinate between the different parties without negatively impacting the business process. Moreover, blockchain technology will not delay the response to the request, since we adopt a private blockchain network, which does not require proof of work to create a new block. In addition, the proposed approach will not cause any business disruption by requiring more entities to verify customers' requests since the organization can determine the minimum number of endorsers needed to create a new block according to the sensitivity of the transaction and the business requirements.

The ability to avoid a single point of failure is a consequence of security principles enforcement since any potential transaction is dually verified.

6.3. Ability to Keep Track of Completed Transactions

In our proposed model, accepted transactions are securely recorded using blockchain technology, maintaining their integrity, validity, and transparency. Additionally, since no block will be deleted or changed, blockchain technology ensures that past transactions can be easily tracked. Relational databases cannot match the immutability and transparency of the blockchain. Therefore, once the block data are published to the blockchain, no one will be able to refute them, ensuring the non-repudiation feature needed in such a potential investigation [33].

The other existing studies do not provide tracking features for employees' actions to hold accountable those violating the company regulations.

6.4. Ability to Integrate and Adopt the Model Easily within the Organization

We demonstrated the easy implementation and deployment of blockchain technology within any organization using an already implemented open-source blockchain network; specifically, we selected the hyperledger fabric private blockchain network. This paper is the only study among the research referred to, such as SEADM [12] and its enhanced version SEADM II [18], that provides technical guidance for implementing the suggested model within organizations.

7. Conclusions

This paper proposed a new model for defense against SE attacks, which uses blockchain technology to enforce security principles. Our model specifically addresses vishing assaults, which are currently very successful, especially when using social networks to acquire information.

We also categorized the SE attacks based on the security principles that could avoid them; essentially, all SE attacks can be mitigated using the principles of dual control and split knowledge.

We demonstrated our proposed model's easy adoption and materialization within any organization using open-source private blockchain networks. The main philosophy of the proposed approach is to avoid a single point of failure and increase the in-depth defense principle regarding SE attacks. Our proposed model is the first, to the best of our knowledge, to require vishing attacks to be checked at least twice by different entities using blockchain technology.

Blockchain technology is a key component of the proposed solution since it provides flexible and trustful flow management of different transactions within the organization. Flow management is required to enable security principles (i.e., dual control and split knowledge), while trusted recording is essential to ensure transparency, non-repudiation, and accountability. Usually, during the hiring of an employee, the organization requires him or her to sign a non-disclosure agreement in which the employee is informed about the confidential data and sharing rules. The organization must have a mechanism to track any agreement breach while ensuring non-repudiation and transparency between employees. Blockchain technology enables non-repudiation and accountability of every employee action through its immutability (i.e., permanent and unaltered), distribution (i.e., all network participants have a copy of the ledger for complete transparency), and security (i.e., ledger secured with cryptographic techniques) characteristics. Blockchain technology outperforms traditional databases in terms of security since every block is encrypted and extremely hard to compromise. It also provides management process inclusion to coordinate amongst the many network partners. As a result, integrating the blockchain into an organization's network is easier, quicker, and less expensive.

We aim to include forensics requirements during the block creation to ensure the admissibility of the records. The use of ontological data representation will automate the search for valuable evidence quickly [34,35]. In addition, we aim to create new metrics that compute the effectiveness of our proposed approach regarding SE attacks using metric elicitation methodologies [36].

Author Contributions: Conceptualization, A.F. and A.A.; data curation, A.F. and A.A.; formal analysis, A.F. and A.A.; funding acquisition, A.A.; investigation, A.A.; methodology, A.A.; project administration, A.A.; resources, A.F. and A.A.; software, A.F.; supervision, A.A.; validation, A.F. and A.A.; visualization, A.A.; writing—original draft, A.F. and A.A.; writing—review and editing, A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Deanship of Scientific Research at Umm Al-Qura University, grant number 22UQU4361220DSR01.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code: 22UQU4361220DSR01.

Conflicts of Interest: The authors declare no conflict of interest.

Sample Availability: Samples of the compounds are available from the authors.

Abbreviations

The following abbreviations are used in this manuscript:

SE	Social Enginneering
SEADM	Social Engineering Attacks Defense Model
CFT	Crash Fault-Tolerant
MSP	Membership Service Provider
CA	Certificate Authority

References

1. Heartfield, R.; Loukas, G. Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. *Comput. Secur.* **2018**, *76*, 101–127. [CrossRef]
2. Krombholz, K.; Hobel, H.; Huber, M.; Weippl, E. Advanced social engineering attacks. *J. Inf. Secur. Appl.* **2015**, *22*, 113–122. [CrossRef]
3. Akremi, A.; Rouached, M. A comprehensive and holistic knowledge model for cloud privacy protection. *J. Supercomput.* **2021**, *77*, 7956–7988. [CrossRef]
4. Schick, N. *Deep Fakes and the Infocalypse: What You Urgently Need to Know*; Hachette UK: Paris, France, 2020.
5. Georgiadou, A.; Mouzakitis, S.; Askounis, D. Working from home during COVID-19 crisis: A cyber security culture assessment survey. *Secur. J.* **2022**, *35*, 486–505. [CrossRef]
6. Breda, F.; Barbosa, H.; Morais, T. Social engineering and cyber security. In Proceedings of the International Technology, Education and Development Conference, Valencia, Spain, 6–8 March 2017; Volume 3, pp. 106–108.
7. Aldawood, H.; Skinner, G. Contemporary cyber security social engineering solutions, measures, policies, tools and applications: A critical appraisal. *Int. J. Secur. (IJS)* **2019**, *10*, 1.
8. Saleem, J.; Hammoudeh, M. Defense Methods Against Social Engineering Attacks. In *Computer and Network Security Essentials*; Daimi, K., Ed.; Springer International Publishing: Cham, Switzerland, 2018; pp. 603–618.
9. Alharthi, D.; Regan, A. A literature survey and analysis on social engineering defense mechanisms and infosec policies. *Int. J. Netw. Secur. Its Appl. (IJNSA)* **2021**, *13*. [CrossRef]
10. Bhusal, C.S. Systematic Review on Social Engineering: Hacking by Manipulating Humans. *J. Inf. Secur.* **2021**, *12*, 104–114. [CrossRef]
11. Salahdine, F.; Kaabouch, N. Social engineering attacks: A survey. *Future Internet* **2019**, *11*, 89. [CrossRef]
12. Bezuidenhout, M.; Mouton, F.; Venter, H.S. Social engineering attack detection model: Seadm. In Proceedings of the 2010 Information Security for South Africa, Johannesburg, South Africa, 2–4 August 2010; pp. 1–8.
13. Tipton, H.F.; Krause, M. *Information Security Management Handbook*; CRC Press: Boca Raton, FL, USA, 2007.
14. Ahmad, A.; Saad, M.; Al Ghamdi, M.; Nyang, D.; Mohaisen, D. BlockTrail: A Service for Secure and Transparent Blockchain-Driven Audit Trails. *IEEE Syst. J.* **2021**, *16*, 1367–1378. [CrossRef]
15. Mani, V.; Manickam, P.; Alotaibi, Y.; Alghamdi, S.; Khalaf, O.I. Hyperledger healthchain: Patient-centric IPFS-based storage of health records. *Electronics* **2021**, *10*, 3003. [CrossRef]
16. Shahid, A.; Almogren, A.; Javaid, N.; Al-Zahrani, F.A.; Zuair, M.; Alam, M. Blockchain-based agri-food supply chain: A complete solution. *IEEE Access* **2020**, *8*, 69230–69243. [CrossRef]
17. Al-Qarafi, A.; Alrowais, F.; Alotaibi, S.; Nemri, N.; Al-Wesabi, F.N.; Al Duhayyim, M.; Marzouk, R.; Othman, M.; Al-Shabi, M. Optimal Machine Learning Based Privacy Preserving Blockchain Assisted Internet of Things with Smart Cities Environment. *Appl. Sci.* **2022**, *12*, 5893. [CrossRef]
18. Mouton, F.; Leenen, L.; Venter, H. Social engineering attack detection model: Seadmv2. In Proceedings of the 2015 International Conference on Cyberworlds (CW), Visby, Sweden, 7–9 October 2015; pp. 216–223.
19. Mouton, F.; Nottingham, A.; Leenen, L.; Venter, H. Finite state machine for the social engineering attack detection model: SEADM. *SAIEE Afr. Res. J.* **2018**, *109*, 133–148. [CrossRef]
20. Fan, W.; Lwakatare, K.; Rong, R. Social engineering: IE based model of human weakness for attack and defense investigations. *Int. J. Comput. Netw. Inf. Secur.* **2017**, *9*, 1–11. [CrossRef]
21. Astakhova, L.; Medvedev, I. An Information Tool for Increasing the Resistance of Employees of an Organization to Social Engineering Attacks. *Sci. Tech. Inf. Process.* **2021**, *48*, 15–20. [CrossRef]
22. Kalio, S. Phishing Attack: Raising Awareness and Protection Techniques. 2022. Available online: https://psyarxiv.com/uxeth/ (accessed on 5 November 2022).
23. Airehrour, D.; Vasudevan Nair, N.; Madanian, S. Social engineering attacks and countermeasures in the new zealand banking system: Advancing a user-reflective mitigation model. *Information* **2018**, *9*, 110. [CrossRef]
24. Yeboah-Boateng, E.O.; Amanor, P.M. Phishing, SMiShing & Vishing: An assessment of threats against mobile devices. *J. Emerg. Trends Comput. Inf. Sci.* **2014**, *5*, 297–307.
25. Jones, K.S.; Armstrong, M.E.; Tornblad, M.K.; Namin, A.S. How social engineers use persuasion principles during vishing attacks. *Inf. Comput. Secur.* **2020**, *29*, 314–331. [CrossRef]

26. Ghafir, I.; Saleem, J.; Hammoudeh, M.; Faour, H.; Prenosil, V.; Jaf, S.; Jabbar, S.; Baker, T. Security threats to critical infrastructure: The human factor. *J. Supercomput.* **2018**, *74*, 4986–5002. [CrossRef]
27. Conteh, N.Y. The dynamics of social engineering and cybercrime in the digital age. In *Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention*; IGI Global: Hershey, Pennsylvania 2021; pp. 144–149.
28. Balaanand, M.; Karthikeyan, N.; Karthik, S.; Varatharajan, R.; Manogaran, G.; Sivaparthipan, C. An enhanced graph-based semi-supervised learning algorithm to detect fake users on Twitter. *J. Supercomput.* **2019**, *75*, 6085–6105. [CrossRef]
29. Chapple, M.; Stewart, J.M.; Gibson, D. *(ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide*; Wiley Online Library: New York, NY, USA, 2021.
30. Shimonski, R. *CEH v9: Certified Ethical Hacker Version 9 Study Guide*; John Wiley & Sons: Hoboken, NJ, USA, 2016.
31. Akremi, A. Software Security Static Analysis False Alerts Handling Approaches. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 702–711. [CrossRef]
32. Agrawal, A.; Seh, A.H.; Baz, A.; Alhakami, H.; Alhakami, W.; Baz, M.; Kumar, R.; Khan, R.A. Software security estimation using the hybrid fuzzy ANP-TOPSIS approach: Design tactics perspective. *Symmetry* **2020**, *12*, 598. [CrossRef]
33. Akremi, A.; Sallay, H.; Rouached, M.; Bouaziz, R. Applying digital forensics to service oriented architecture. *Int. J. Web Serv. Res. (IJWSR)* **2020**, *17*, 17–42. [CrossRef]
34. Akremi, A. A forensic-driven data model for automatic vehicles events analysis. *PeerJ Comput. Sci.* **2022**, *8*, e841. [CrossRef]
35. Akremi, A.; Sriti, M.F.; Sallay, H.; Rouached, M. Ontology-Based Smart Sound Digital Forensics Analysis for Web Services. *Int. J. Web Serv. Res. (IJWSR)* **2019**, *16*, 70–92. [CrossRef]
36. Akremi, A. An adaptative and compliant forensics admissibility metrics generation methodology. In Proceedings of the 23rd International Conference on Information Integration and Web Intelligence, Linz, Austria, 29 November–1 December 2021; pp. 495–503.