symmetry

MDPI

Article

Towards a Secure Signature Scheme Based on Multimodal Biometric Technology: Application for IOT Blockchain Network

Oday A. Hassen [1], Ansam A. Abdulhussein [2], Saad M. Darwish [3,*], Zulaiha Ali Othman [4], Sabrina Tiun [4] and Yasmin A. Lotfy [5]

[1] Ministry of Education, Wasit Education Directorate, Kut 52001, Iraq; odayali@uowasit.edu.iq
[2] Information Technology Center, Iraqi Commission for Computers and Informatics, Baghdad 10081, Iraq; P102907@siswa.ukm.edu.my
[3] Department of Information Technology, Institute of Graduate Studies and Research, Alexandria University, 163 Horreya Avenue, El–Shatby, Alexandria 21526, Egypt
[4] Centre of Artificial Intelligence, Faculty of Information Sciences and Technology, University Kebangsaan Malaysia (UKM), Bangi 43600, Malaysia; zao@ukm.edu.my (Z.A.O.); sabrinatiun@ukm.edu.my (S.T.)
[5] Department of Computers, Faculty of Engineering, Pharos University in Alexandria, Alexandria 21648, Egypt; yasmin.lotfy@pua.edu.eg
* Correspondence: saad.darwish@alexu.edu.eg; Tel.: +20-122-263-2369

Received: 13 September 2020; Accepted: 12 October 2020; Published: 15 October 2020

Abstract: Blockchain technology has been commonly used in the last years in numerous fields, such as transactions documenting and monitoring real assets (house, cash) or intangible assets (copyright, intellectual property). The internet of things (IoT) technology, on the other hand, has become the main driver of the fourth industrial revolution, and is currently utilized in diverse fields of industry. New approaches have been established through improving the authentication methods in the blockchain to address the constraints of scalability and protection in IoT operating environments of distributed blockchain technology by control of a private key. However, these authentication mechanisms do not consider security when applying IoT to the network, as the nature of IoT communication with numerous entities all the time in various locations increases security risks resulting in extreme asset damage. This posed many difficulties in finding harmony between security and scalability. To address this gap, the work suggested in this paper adapts multimodal biometrics to strengthen network security by extracting a private key with high entropy. Additionally, via a whitelist, the suggested scheme evaluates the security score for the IoT system with a blockchain smart contract to guarantee that highly secured applications authenticate easily and restrict compromised devices. Experimental results indicate that our system is existentially unforgeable to an efficient message attack, and therefore, decreases the expansion of infected devices to the network by up to 49 percent relative to traditional schemes.

Keywords: blockchain system; IoT; permissioned distributed ledger; bilinear pairing; fuzzy identity based signature; multimodal biometrics; feature fusion

1. Introduction

As life shifts rapidly online, one of the problems confronting internet users is making a transaction in an atmosphere where they cannot meet or trust each other. This eventually raises the demand for a cost-effective, safe data transmission setting. Blockchain is a peer-to-peer network that is cryptographically protected, irreversible, and modified only through peer agreement [1]. It is a successful application where peers can share values using transactions without the need for a central authority to safeguard consumer privacy and avoid identity fraud [2]. Transaction ownership is defined by digital keys, user identities, and digital signatures [3]. Digital signature authentication safeguards the blockchain transaction by ensuring the transaction author has a valid private key [4]. Unfortunately, in some sensitive fields where strict authentication is needed, this strategy does not guarantee that a transaction maker is an authorized person, as there is a possibility that an attacker may capture the secret and produce unauthorized transactions.

Early blockchain networks are being applied to Distributed Ledger Technology (DLT), which indicates that in a decentralized network without authorization, the users are exposed to each other, rather than private, and thus completely untrustworthy [5]. Thus, although participants are not willing to trust each other entirely, the network may be run on the basis of a governance model centered on the trust between participants, for instance, a legal arrangement or a conflict settlement system. This type of network needed participants to be known, high transaction efficiency, and low transaction confirmation duration, privacy, and transaction secrecy. Permissioned blockchain [6] work for a large variety of business uses, including accounting, finance, insurance, healthcare, human resources, supply chain, and even digital music.

To define and retain a blockchain participant's proof of ownership of some digital properties, a blockchain is built on asymmetric cryptography [7,8] and a digital signature system; each consumer owns a pair of private keys and a public key. This scheme includes two phases: the signing and verification process. In the signing phase, a sender produces a transaction that contains the cryptographic signature of the sender (hash value extracted from the transaction, then encrypts it using its private key) and the public key of the recipient. In the verification phase, the digital signature of the sender is checked in the previous transaction by the public key of the sender and the hash by the same hash function as senders. If these two values are the same, the sender has already signed the contract, and the transaction will need to be legitimate, else the transaction is rejected [9]. This verification scheme is a key blockchain tool. In a traditional blockchain, users or membership servers handle private keys or store them at wallets to maintain security. Private keys, however, threaten leakage. The blockchain technology gets insecure. Figure 1 exemplifies a Blockchain transaction [10].

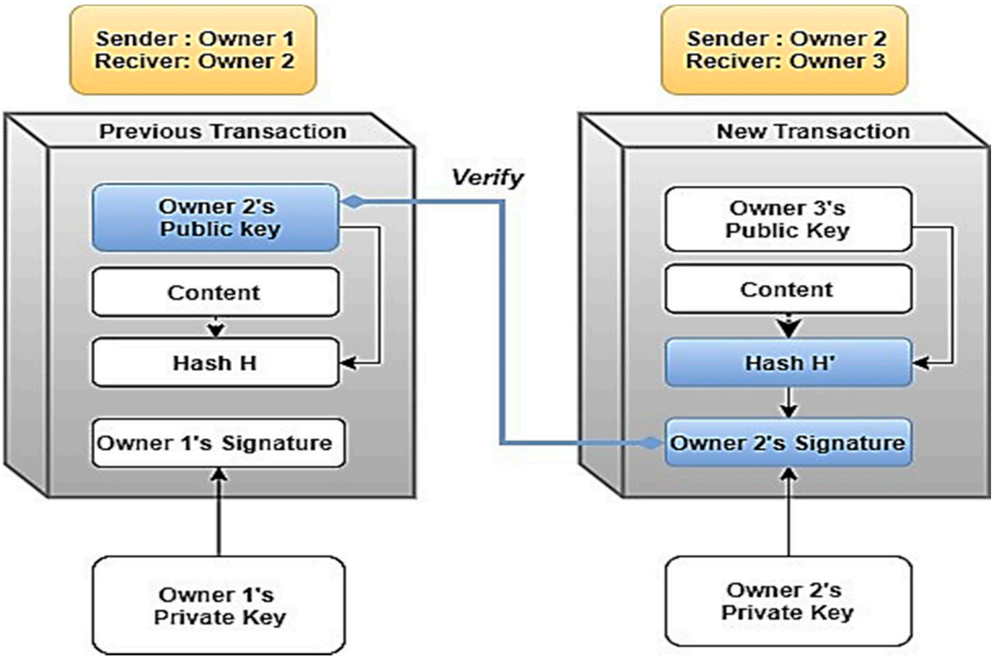

Figure 1. An example of blockchain transaction.

Several strategies were introduced in digital wallets [11] that attempt to force strict protection to handle key pairs to solve the above problems. Wallet software uses the cryptographic protocol to sign a private key transaction. The computer normally contains private keys. However, missing or revealing these private keys prevents a person from accessing funds [12,13]. Because possession of every resource in the blockchain network is checked with private key, the consumer needs to safely protect the private key. One of the interesting ways to solving this problem is to use biometric data [14], including using one's fingerprint, face, and iris as a private key. Since the biometrics of a consumer is part of the human body, it may provide a safer and accessible means of connecting the person with his private key; unlike passwords, it is not forgotten and much harder to hack than cards. Recently, the incorporation of a fuzzy private key in biometric authentication has gained much attention from researchers operating in this field to control vagueness in biometric details [15].

The Internet of things (IoT) offers a more efficient experience by allowing multiple devices to connect and exchange information [16]. IoT devices gather and store different forms of information, including frequent personal and confidential details. However, intrusion and cyber-attacks targeting IoT devices increase every year and, like other low-power and low-performance IoT devices, find it impossible to extend protection methods implemented for conventional PCs to IoT devices, rendering them susceptible to cyber-attacks [17,18]. As IoT devices face such security challenges, it can quickly leak sensitive details, trigger financial damage, and even endanger human life. To solve this dilemma, Blockchain Technology and IoT Incorporation have attracted attention [19].

Motivated by the above-mentioned challenges, we aim in this paper to implement multimodal biometrics technology in the blockchain network for authentication which can safely and automatically broaden IoT products. By utilizing biometrics, the suggested model guarantees that not just the right key but also an authenticated user is in the transaction creator. We present a multi-modal biometric framework to minimize spoofing chance and compensate for shortcomings of biometric unimodal systems. It fuses two attributes and gets the most unique private entropy key. Furthermore, even though the consumer is authenticated to the network, our framework automatically calculates the IoT security score by utilizing the whitelist, and smart contract restricts the scalability of the infected devices while there is a low score and automatically changes the whitelist to improve the security score, which contributes to protect IoT devices being expanded to the network.

The proposed model relies on boosting the overall efficiency of (1) the image analysis used to enhance image properties, identifying edges and points where texture varies, (2) the feature level fusion used to offer quick matching speed with high precision by choosing several strong features, (3) the fuzzy coding based on identity, which is used to distinguish key pairs, (4) the fuzzy matching used in the transaction authorization process to match the digital signature, and (5) the whitelist used for measuring the IoT system protection score and restricting its low score software to maintain the security of the network.

The remainder of this article is structured as follows. Section 2 discusses several of the latest related works. Section 3 provides a detailed description of the proposed model. The results and discussions are given in Section 4. Finally, in Section 5, the conclusion is annotated.

2. Literature Review

The traditional protection of private blockchain keys is largely carried out in two forms, either by encrypting keys or designing wallets on hardware or software [20]. These are cumbersome, however, and confidentiality cannot be ensured, and all these wallets must synchronize the blockchain, while most existing mobile devices cannot store all blocks. In 2018, Dai et al. [21] suggested a lightweight wallet focused on Trustzone [22], a framework providing hardware-dependent isolation, which can create a stable and consistent code environment needing high protection. It is more compact than the hardware wallet and stronger than the software wallet.

The Internet of things has gained the most support from scholars in recent years [23]. For example, in 2016, the authors [24] create a shared blockchain-to-IoT framework for automated smart contract. This solution proposes a modular, stable, non-centralized authority network. The aim is not just to validate that the right computer produced a blockchain transaction, but also that a consumer can create a blockchain transaction for his purpose. However, verifying the user's purpose from automatically created blockchain transactions is difficult. In another work, in 2017, Balfanz [25] scanned biometric details such as fingerprints, irises, etc. in protected hardware and then triggered the private key. By integrating such security with blockchain, the author guaranteed a secure blockchain. However, it is important to hold a smartphone with registered biometric details and to enter biometric information from dedicated stable hardware.

Krishna in 2019 [26] presented a novel trust model, Vriksh: the Tree of Trust (VTT), tailored for use in IoT. This model aims to provide an embedded device-friendly entity authentication and limit the trust peripheries. With VTT, trust trees group the identities with equal access rights in the system using Merkle trees. The author prototyped the use of VTT with Transport Layer Security (TLS) on raw public keys to compare the energy and resource efficiency of VTT with Public Key Infrastructure (PKI) on an embedded platform. However, to establish VTT as an alternative to PKI, the verification of the revocation methods for VTT and independent security reviews are essential. The PKI certificate provides entity authentication for hyper ledger fabric.

Biswas in 2020 [27] utilized ring signature for the aim of enhancing the privacy of the decentralization identifiers. Ring signature schemes enable the generation of anonymous signatures where the real signer's identity is hidden in a set of possible signers; it could be used for anonymous membership authentication to keep the anonymity of the signer and can be publicly verifiable. Note that the size of any ring signature must grow linearly with the size of the ring since it must list the ring members; this is an inherent disadvantage of ring signatures as compared to group signatures that use predefined groups. In cases like know-your-customer and anti-money laundering, ring signature cannot be used, as the regulations must be followed, such as that participants must be identified/identifiable and networks need to be permissioned. Blockchain's fundamental principles are cryptographic and cryptographic technologies that include efficient, safe, decentralized solutions. Although several recent articles research the use-cases of blockchain in various industrial fields, such as IoT, few studies scrutinize the cryptographic principles used in blockchain. In [28], the authors studied and systematized all cryptographic principles already used in blockchain. They also included potential instantiations of these blockchain principles.

Since blockchain still considers modern technologies, actual implementations can still be made more effective and realistic. According to the above analysis, past research was mainly devoted to (1) creating various styles of wallets, either offline or online, utilizing private key storage and wallet backups, (2) creating modern singing and verification methods by encrypting a private key that also does not guarantee safe authentication, (3) not discussing the differing problem of issuing a transaction from a legitimate user and hacking a private key, and (4) not resolving the problem of expanding the infected device to the network. However, little attention has been paid to advise new optimal methods to merge blockchain and biometrics at the algorithm level to enhance IoT protection and accessibility in the blockchain-based framework.

Our work allows us to construct biometrics over the existing PKI by using a fuzzy identity-based signature. The suggested model uses multimodal biometrics to extract a secret key that varies the secret key every time the user scans his biometric traits. A fuzzy identity-based signature simplifies the key management procedures in case of a fuzzy biometric key in order to improve the privacy solutions in the blockchain network.

3. Methodology

This paper presents a new paradigm that integrates multimodal biometric and blockchain technologies in a single system focused on a fuzzy identity-based signature to ensure safe IoT application authentication and allow blockchain extension. The suggested model takes into account that each IoT system has security vulnerabilities and is vulnerable to installing infected applications, thus, the devices' security score is measured using the whitelist, which specifies the list of checked applications and then restricts things other than the list [29]. To derive a private key, we apply a modern multimodal biometrics-based feature level fusion of fingerprint and finger vein to obtain a biometric identity vector. In order for the creator of the transaction to send data through their IoT Device, they sign the piece of data with their own private biometric key to create a biometric digital signature, and send the transaction to the blockchain network, which includes the signature and copy of their public key, the content and their hash value, and the transaction with an unconfirmed state. To validate this, a specific strict authentication is implemented using the biometric public key from the previous transition, signature, and content hash. If the proof is true, the block is applied to the Blockchain's public ledger, and data are sent across the network; otherwise, the block is denied. The blockchain system's key diagram is seen in Figure 2.

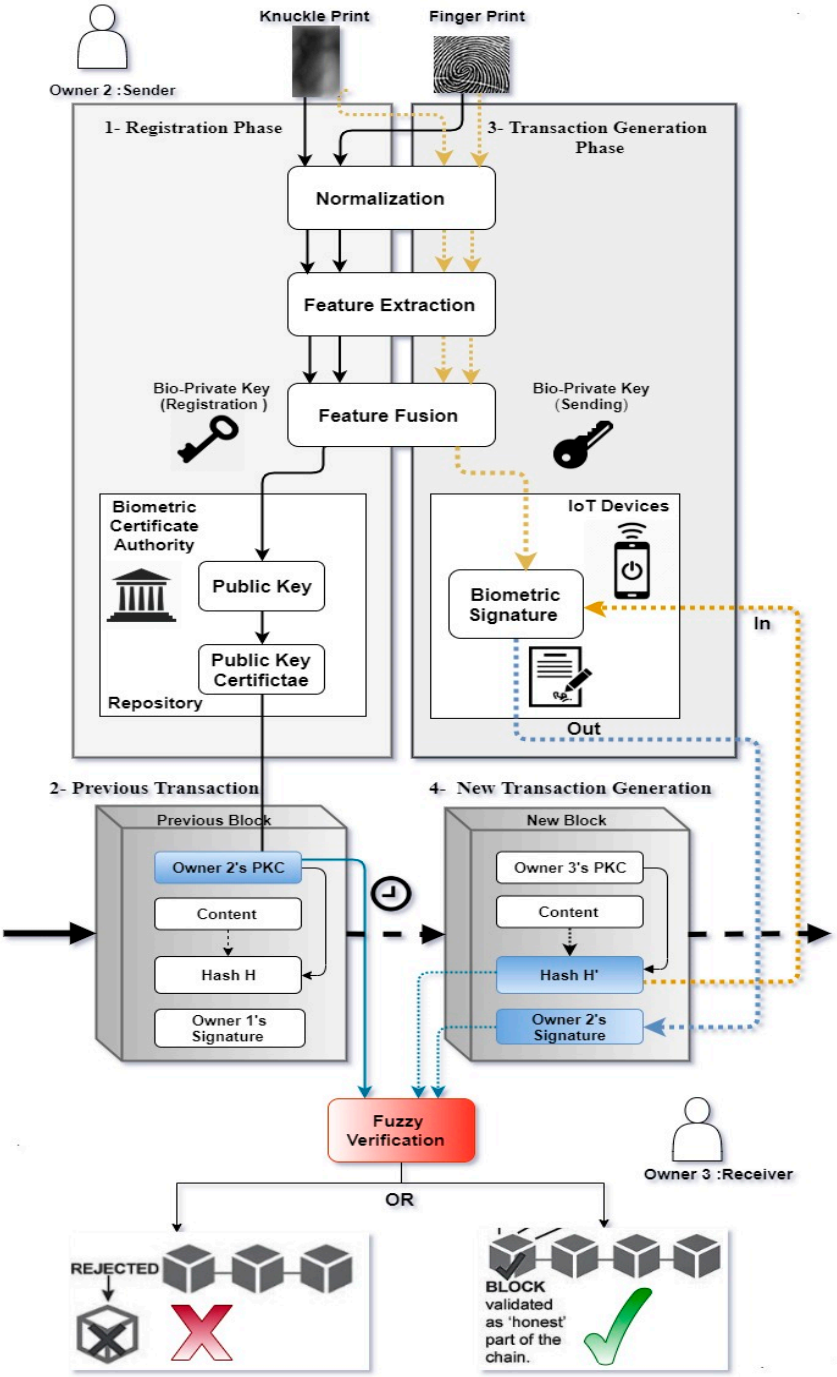

Figure 2. Block diagram of the proposed scheme.

Despite the benefits of biometric identification, biometric details are significantly challenging to replicate and noisy, since two biometric scans of the same characteristics are seldom equivalent. Therefore, standard protocols cannot guarantee consistency, even when parties are utilizing mutual biometric secrets. We use a fuzzy identity-based signature to solve this issue to sign and validate the blockchain framework. This paper is a substantial extension of our conference paper [30]. Compared with this small version, further details of the suggested method are presented, and a more extensive performance evaluation is conducted. We also give a more comprehensive literature review to introduce the background of the offered method and make the paper more self-contained. Therefore, this version of the paper provides a more comprehensive and systematic report of the previous work.

3.1. Signature Scheme Using Fuzzy Identity

A Fuzzy Identity Based Signature (FIBS) [31–34] is used to produce and validate IoT blockchain transactions. An FIBS uses fuzzy data as a cryptographic key, such as a fingerprint, iris, finger vein, etc., unlike conventional digital signature schemes, which require fixed data as a key, since the individual here can produce a different key each time they want to make a transaction. An FIBS lets a person with identity w create a signature that can be checked with identity w' only if w and w' are within a certain range. By adding biometrics to a blockchain scheme, the protection can be enhanced through the strict checking of the transaction's author. The fuzzy signature scheme for identification consists of the following four steps:

- Setup (n, d): The setup algorithm takes a security parameter n and an error tolerance parameter d as input. It generates the master key (MK) and public parameters (PP) (Public Key).
- Extract (PP, MK, w): The private key generation algorithm takes the master key MK and the user biometric fused vector w as input. It outputs a private key associated with w, denoted by K_w.
- Sign (PP, K_w, M): The signing algorithm takes the public parameters PP, a private key K_w, and a message M as input. It outputs the signature σ.
- Verify (PP, w', M, σ): The verification algorithm takes the public parameters PP, a user biometric fused vector w' such that $|w' \cap w| \geq d$, the message M and the corresponding signature σ as input. It returns a bit b, where b = 1 means that the signature is valid; otherwise, the signature is not valid.

In order for user to create and send a transaction to another user in our scheme, they have to go through four phases: biometric key extraction, Registration, Transaction generation, and the Verification phases. Algorithm 1 illustrates the pseudo code of our proposed model.

Algorithm 1 Pseudo Code of our Proposed Scheme

```
1-Biometric Key Extraction Phase
    Pre-Processing
    Feature Extraction
    Feature Level Fusion
Return $w$
2-Registration Phase
    Algorithm Setup ($n$,$d$)
Return PP
    Algorithm Extract (PP, MK, $w$)
Return $K_w$
3-Transaction Generation Phase
    Algorithm Sign (PP, $K_w$, H)
Return σ
4-Verification Phase
    Algorithm Verify (PP, $w'$, H, σ)
Return True or False
```

In terms of internally protecting the IoT device from being compromised due to malicious application installed through inattention of the consumer or hackers, the suggested model calculates the security score dependent on checking a whitelist stored in an agent inserted in a protected region of the system. The whitelist includes all IoT-installed applications. Figure 3 shows the system configuration for evaluating the security score for the IoT device, which is described in the following steps [29]:

Step 1: IoT device manufacturers compose whitelist software that is installed on IoT devices.

Step 2: Device manufacturers build a smart contract comprising manufacturers' whitelist and the agent's initial agent hash value (IAHV) that is embedded in an IoT device. The Whitelist Smart Contract (WSC) records this value in the blockchain.

Step 3: The IoT device access the WSC recorded in the blockchain and verifies if the IAHV of the agent matches the Device Agent Hash Value (DAHV) of the current whitelist installed on the device.

Step 4: In the case of successful verification, the device is not infected nor hacked and the security score is set to be high and vice versa.

Step 5: A Scoring Smart Contract (SSC) is created, which involves the security status of the IoT device, which is evaluated by the agent and the device-unique identifier, and is recorded in the blockchain.

Step 6: The SSC of the device can be inquired when the device is connected to other devices. Based on the recording in the blockchain, the IoT device can be extended safely and quickly when connected to other devices. The WSC collects and records in the blockchain the whitelist of each IoT system and the IAHV from the producer. If the WSC tests by matching the IAHV with the device's current hash, it may give a warning message to the IoT and the vendor if they do not fit. The whitelist recorded in the blockchain is then forwarded to the IoT device, and the Agent uses the transmitted details and sends the list of the checked and unverified apps to the SSC [35]. Figure 4 illustrates the concept of WSC.

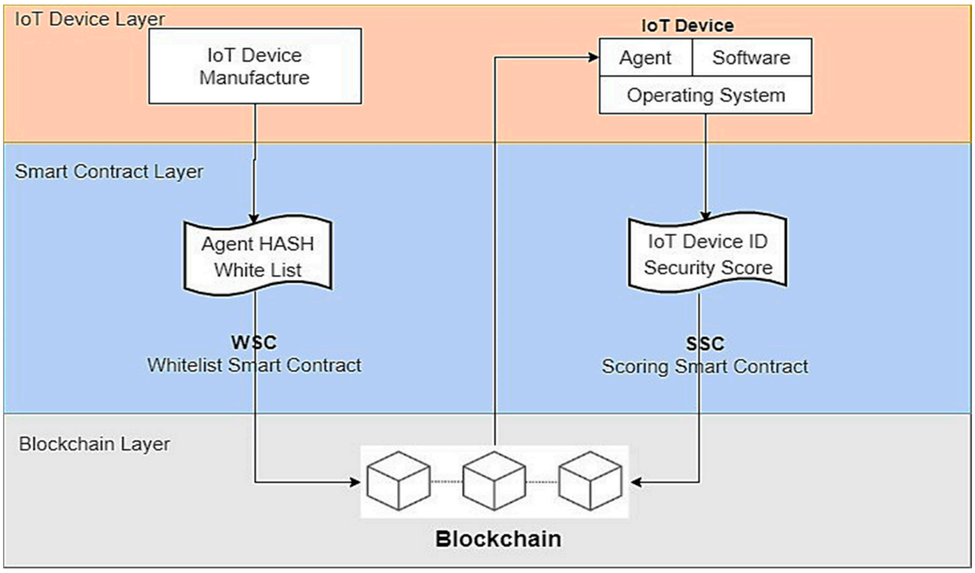

Figure 3. Security Score Evaluation for the internet of things (IoT) Device.

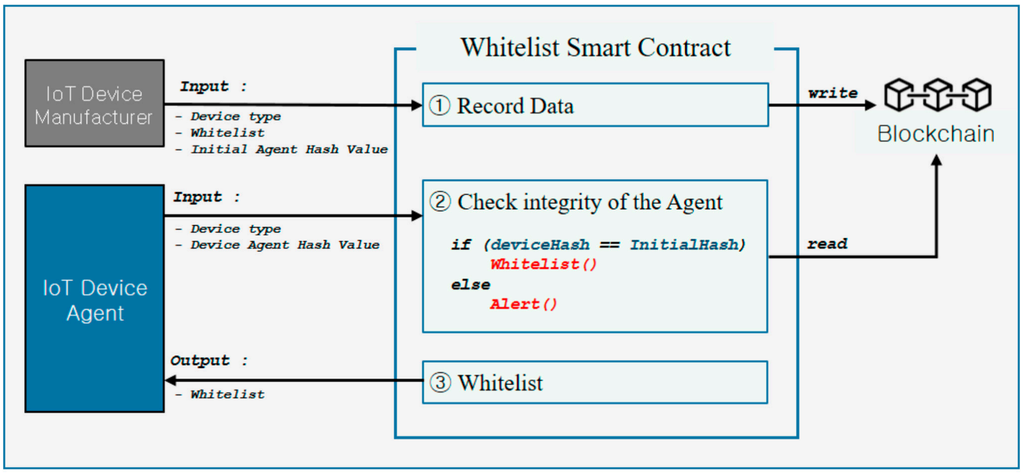

Figure 4. Whitelist Smart Contract [35].

3.2. Biometric Key Extraction Phase

This process aims to produce biometric data w by extracting specific features from both the fingerprint and finger vein. The proposed model implements image-enhancing strategies to increase contrast, brightness, and noise removal. Regions of interest (ROIs) are derived for both biometric images. Based on a unified Gabor filters frame, a fingerprint vector and a finger vein vector are created. Then, the two vectors are decreased in dimensionality by implementing Principle Component Analysis (PCA) to construct the private key. The reasons for the combination of fingerprint and finger vein characteristics are that (1) the finger vein and fingerprint are two characteristics borne by one finger and both have completely accurate biometric properties [36], (2) ridge texture specifics dominate all biometric images, and (3) fingerprints and finger veins are complementary in universality, precision, and protection. Figure 5 displays the biometric key extraction graphical diagram. The method of generating the private key is as follows:

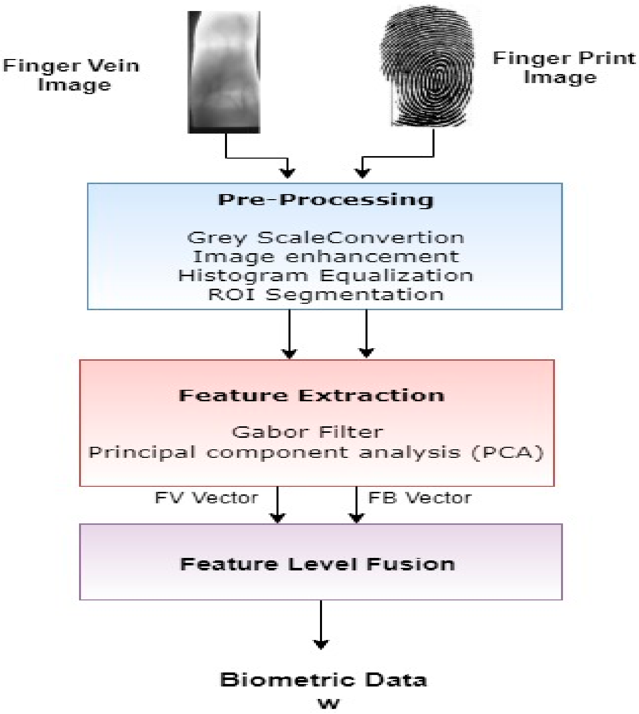

Figure 5. Schematic diagram of the fingerprint and finger vein biometric key extraction. ROI: Regions of interest.

3.2.1. Pre-Processing

The user fingerprint and finger vein images are converted into greyscale images. The main reason why grayscale representations are often used for extracting descriptors instead of operating on color images directly is that grayscale simplifies the algorithm and reduces computational requirements. Then, the image enhancement technique is used to improve the contrast and brightness properties of the images, followed by histogram equalization to eliminate the noise from the images [37]. In order to reliably exploit texture details, stable ROIs corresponding to the fingerprints and finger veins should be extracted at an early stage.

In this scenario, various methods of ROI extraction should be practiced. Core point detection using fingerprint orientation field was used for fingerprint ROI extraction [38], measured using gradient-based technology, and optimized neighborhood averages to produce a smoother field of orientation. Herein, the fingerprint image is cropped into 168 × 168 pixels. For the extraction of finger veins, inter-phalangeal joint prior to finger vein segment ROI is being used [39]. The finger vein image is cropped into 160 × 80 pixels. Some results are shown in Figure 6.

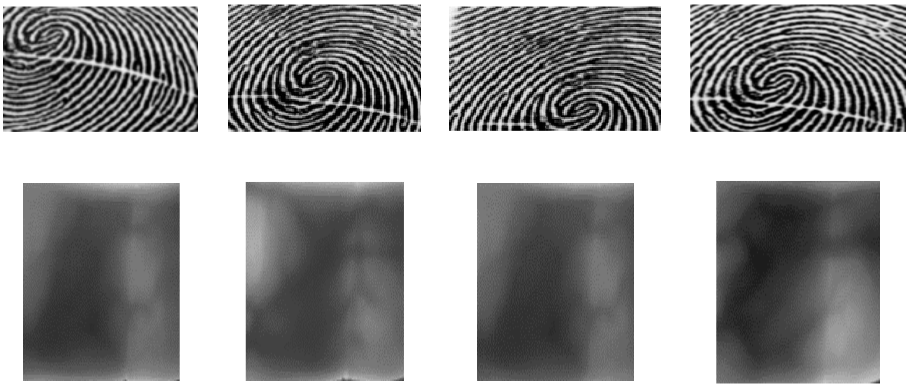

Figure 6. ROI extraction. (**Top row**) ROIs of four fingerprint image samples. (**Bottom Row**) ROIs of four finger vein image samples.

3.2.2. Feature Extraction

Gabor filters were commonly utilized in the spatial domain for study of texture information and recognition functionality. Gabor filters may be divided into a true and imaginary component with the aid of the Euler formula. The real part, also referred to as the Gabor symmetric filters, can be calculated at the border (ridge) of the image [40], while the imaginary part, generally referred to as the Gabor symmetric filters, can be used to detect the border [41]. In order to achieve the optimum effects, the symmetric Gabor filters should also be built according to all styles of textures. Gabor filter-based feature extractor is a Gabor filter bank defined by its parameters, including frequencies, orientations, and smooth parameters of the Gaussian envelope. See [42,43] for more details. Eight filtered images can be generated according by a two-dimensional (2D) convolution between an ROI and Gabor filtered at eight directions. With the Average Absolute Deviation (AAD) of each block 8 × 8/16 × 8, we can construct two features, Up and Uv, which each reflect the local features of a filtered fingerprint/finger-venal image. The matrix Up and Uv of eight orientations are easily rearranged in a row through two one-dimensional (1D) vectors called the fingerprint code FP_{code} and finger vein code FV_{code}.

3.2.3. Feature Level Fusion

In feature-level fusion, feature vectors must be fused into a template to improve human recognition by integrating several features. We use the principal component analysis (PCA) feature fusion to orthogonally turn measurements of a series of correlated variables into a collection of values of linearly uncorrelated variables [44]. PCA is a very popular way to speed up a Machine Learning algorithm by extracting associated variables that do not contribute to decisions. Algorithm training time reduces significantly with fewer features. PCA helps with overfitting by reducing the number of features. Because we deal with a private blockchain where all members have identities, in traditional permissioned blockchain they use public key infrastructure to generate cryptographic certificates that are tied to organizations, network components, and end user's applications. In our proposed scheme, we are developing a biometric key infrastructure with a biometric certificate authority to validate participant identities to determine specific resource rights and access to information on the blockchain network.

3.3. Registration Phase

The user's biometric private key K_w is produced from the user's biometric data w in this process, and its public key associated with the private key is also developed and certified, and recorded in the blockchain network. This is a four-step phase [29,31–34]: (1) Confirming the User Identity. Biometric Certificate Authority (BCA) confirms the identity of the user, and then obtains the biometric information after fused into a vector w_{fused}. (2) Generating Public key and Master Key. To setup the system, first, choose $g_1 = g^y$, $g_2 \epsilon$ G, where G is the prime order p, where p is a large prime number. From this, the value $A = e(g_1, g_2)$ is calculated. Next, choose $t_1, \ldots\ldots\ldots, t_{n+1}$ uniformly at random from G. Finally, choose y uniformly at random in Z_q, where Z_q denotes the group $\{0, 1, \ldots\ldots, q-1\}$ under addition modulo q. (3) Generating Biometric Information Combined with a Private Key. (4) Granting a Public Key Certificate. The Biometric Certificate Authority (BCA) issues a Public Key Certificate (PKC) by assigning the public key to the digital signature, which is a collection of certificate holder attributes such as a user ID (UID), expiry date, and other information. All these features are encrypted by the BCA's private key to invalidate the certificate. Then, the BCA signs and publishes a PKC in the file and publishes it to the network.

3.4. Transaction Generation Phase

Herein, the sender creates a new blockchain transaction that includes the owner's PKC (the receiver's PKC), content, and hash value H. Herein, the user signs the message by the hash value for the identity w with using his private key k_w to create the new blockchain transaction. After that, the biometric signature S is generated from the hash value H using his biometric information w (fuzzy signature). The sender adds its biometric signature S to the latest blockchain transaction, thus, this new block transaction is added to the ledger waiting for validation or rejection [44].

3.5. Transaction Verification Phase

In this step, we use the PP public parameters verification algorithm, a w' identity so that $|w \cap w'| \geq d$, Hash message H, and the corresponding signature S as an input. It returns a bit b, where b = 1 implies that the signature is correct. The verification is achieved through hierarchical verification with two stages. (1) A transaction verifier checks the expiration date and other attributes of the owner's PKC from the previous blockchain transaction and verifies it using the BCA public key. (2) The transaction verifier calculates a signature verification result. Successful verification means that a blockchain transaction is generated using a correct private key corresponding to the public key. Our scheme does not need to store a user's private key in any device or cloud servers as the user's biometric information acts as a user's private key [45–47].

4. Results and Discussion

No accessible database currently holds fingerprint and finger vein images for the same user. The prepared fingerprint and finger vein database are selected from the University of Shandong SDUMLA-HMT database [48]. We assume that the same individual has different biometric characteristics. Fingerprint and finger vein images from 106 participants have been obtained. The fingerprint archive contains images from both hands' thumb finger, finger index, and middle finger. In total, eight impressions for each of the six fingers were recorded. The finger vein database comprises images obtained from both hands' index finger, middle finger, and ring finger. The set is repeated for each finger six times in order to achieve six finger vein images per finger.

The assessment is carried out using IoT specifications: CPU: Intel Core i7 7500U Processor 2.7 GHz and Memory: 8 GB. Device type: 64-bit Business as an operating system. MATLAB has been used to implement the biometric aspect of the key extraction. The blockchain component of the Hyperledger Fabric [45] open-source blockchain framework was used to build and implement cross-industry blockchain technologies and systems. In addition, in this evaluation, we use the fuzzy identity-based signature as a digital signature algorithm [46].

4.1. Security Evaluation

In our framework, we limit the installation of malicious software on the IoT system by automating the assessment on the whitelist and smart contract of the security score and then applying blockchain recording. Our suggested scheme guarantees optimum scalability when the security score is strong and scalability is limited when the security score is poor. We also carry out our tests with the adversary's attacks. The opponent has two common attacks to get these data. One attacks the private key, the other forges the signature.

4.1.1. Experiment 1: Private key Attack or Leakage

In a typical Blockchain network, the private key is the critical value that decides the ownership of the transaction especially if the transaction is serious. Thus, this experiment is run to analyze the robustness when the user's private key has been leaked from an IoT device due to IoT device theft, cyber-attack, etc. Multimodal biometrics based on feature level fusion algorithm are implemented in this study in order to find the most important features to extract a unique private key that helps to make our framework more robust and secure. In the first set of experiments, we analyze the security of our proposed scheme and confirm their effectiveness against common attacks in the blockchain system; additionally, we compare the security level against three signature schemes. In the first experiment, we examined the security and efficacy of our proposed scheme against typical attacks in the blockchain environment and compared the safety level with three signature schemes: the conventional private key based signature scheme (PKSS), the fuzzy key signature scheme based on unimodal biometrics (FKSSU), and our proposed fuzzy identity key signature scheme based on multimodal biometrics (FIKSSM). From Table 1, it can be seen that the proposed model is more secure than the previous methods when it comes to a private key leakage.

Table 1. Security Level Comparison. PKSS: conventional private key based signature scheme; FKSSU: fuzzy key signature scheme based on unimodal biometrics; FIKSSM: fuzzy identity key signature scheme based on multimodal biometrics.

Signature Approach	Leakage of Private Key	Digital Signature Forgery
PKSS	Low	Middle
FKSSU	Middle	Middle-High
FIKSSM	High	High

In PKSS, the IoT device, a cloud service, or wallet controls the long-term private key. Therefore, an adversary threatens to capture the private key by producing a digital signature and making an illicit blockchain transaction. Losing the secret key involves losing the asset's possession permanently, since the private key cannot be restored. This leaves PKSS susceptible to security breaches or cyber threats and offers inadequate security in today's connected and data-driven environment. In FKSSU, however, the private key is not handled in the IoT device. The user's private key arises from biometric knowledge. Thus, FKSSU finds a stable scheme based on just one biometric trait. FKSSU has many challenges in capturing clean data, including noisy data concerns, inter-class variations, spoof attacks, and unreasonable error rates [48]. The FKSSU is not absolutely safe against this attack. In our FIKSSM, the IoT device does not manage the private key like FKSSU. However, we use the user's fingerprint and finger knuckle print to derive a unique private key; using multimodal biometrics increases the amount of data evaluated, helps verify the match accurately, and makes spoofing exponentially more difficult for the opponent, since incorporating several modalities allows identifying and utilizing all the biometric data required to spoof the algorithm harder. This allows our device to be more stable and efficient and can prevent spoofing attacks.

4.1.2. Experiment 2: Forgery of Digital Signatures

This threat is to fake a digital signature in order to create an illicit blockchain transaction and to effectively validate a digital signature. It is possible to manage this threat if we adopt a safe algorithm to create key pairs. When a stable signature algorithm is used in PKSS and FKSSU, which is difficult to forge, these signature schemes are protected. Table 1 indicates that the proposed model is safer in digital signature forgery than the previous approaches. We use a stable fuzzy identity signature algorithm in the FIKSSM, which was proved safe under EUF-CMA (Existential Unforgeability against Chosen Adaptive Message Attacks) [31]. The likelihood of adversaries generating a legitimate signature for a message under a new private key is insignificant in the EUF-CMA model.

4.1.3. Experiment 3: Security Score Evaluation

We have deployed a simulation network of 200 IoT device nodes randomly arranged at a known location to test the efficiency of our proposed model in terms of security score with the number of Unverified Software. The security score is set to all 200 nodes and the agent and the smart contract are believed to be registered in the blockchain. Based on the whitelist upgrade, we determine the security score. All verified software exists in the whitelist; if unverified software is installed on the IoT device, it is said to be infected with a virus and the security score will automatically drop according to the number of unverified software programs. Additionally, when viruses are removed by the whitelist update, it is set to improve scalability by increasing the security score. Table 2 illustrates the connection range comparison of our proposed scheme against the FKSSU signature scheme. The lower the score is, the more restriction to the IoT device to extend to other devices in the network. That is why our proposed system offers different connection ranges depending on the security score of the device. The other comparative scheme is set to extend the IoT device to all the devices within the same connection range regardless of the security score of the device.

Table 2. Security Score Evaluation.

Number of Unverified Software	Security Score	Connection Range of Comparative Signature Scheme	Connection Range of Our Proposed Signature Scheme
0	100–81	4 hop	4 hop
1	80–61	4 hop	3 hop
2	60–41	4 hop	2 hop
3	40–0	4 hop	1 hop

4.2. *Performance Evaluation*

4.2.1. Experiment 4: Throughput

For all of the experiments below, the average end-to-end latency and the average throughput are measured to get the ideal results by firstly assuming an ideal network, then assuming infected devices in the network, and next measuring the vulnerability of the total network. Throughput is defined as the result of the successfully transmitted packets divided by the packets' transmission time [49]. As shown in Figure 7, the number of transmitted packets is reduced when the update period becomes longer, resulting in poor network performance, because network scalability is restricted when the update period is set to be excessively long, resulting in a decrease in throughput. On the other hand, the number of transmitted packets is improved only when the update period increases to a certain level. Therefore, based on the simulation results, we will set the basic update period to 10 times as the highest throughput was achieved when 10 connection failures were accumulated, after which the whitelist was updated. As shown in Figure 8, we set the update period to be 10 times to get the highest throughput; in our FIKSSM proposed model, the throughput results measured for a network size of 200 IoT devices achieved a higher throughput performance within the available network resource compared to the other signature schemes, which is a desirable goal in any network.

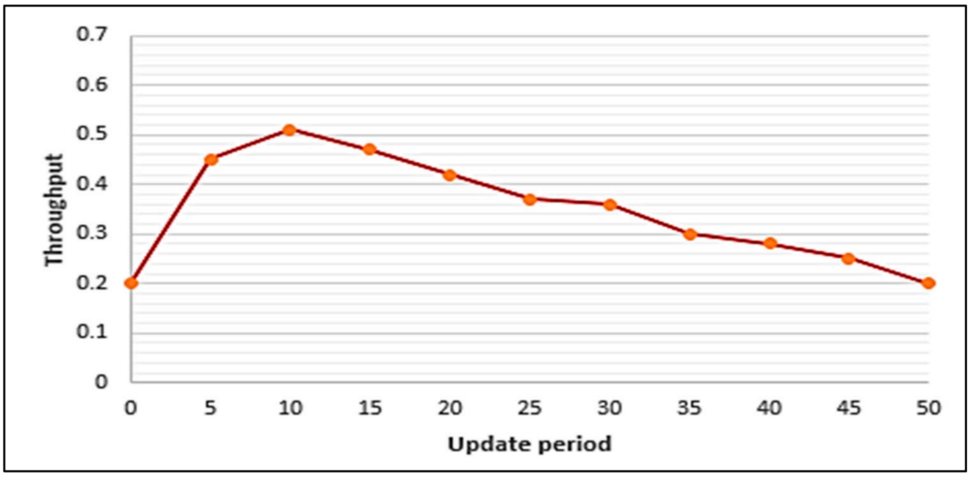

Figure 7. Throughput results when changing the update period for the proposed model.

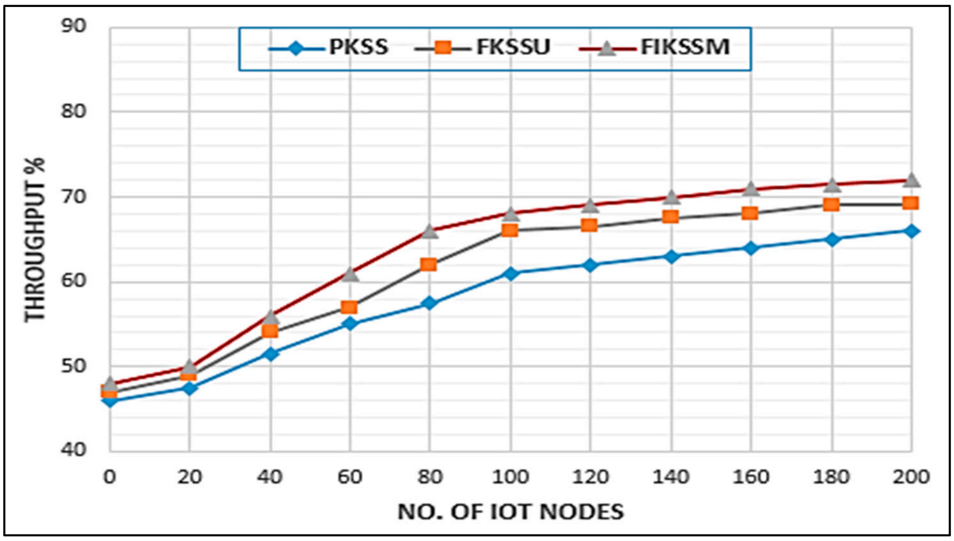

Figure 8. Comparison results of throughput.

4.2.2. Experiment 5: Scalability

Scalability is defined as the ability of an IoT device to work gracefully without any undue delay and non-productive resource consumption. It is the result of dividing the number of connected IoT devices by the number of physically available connections. As shown in Figure 9, in our FIKSSM proposed model, the scalability is low at the start of the simulation time compared to other signature schemes PKSS and FKSSU; the IoT devices with low-security scores are restricted from extension to the network, as they contain malicious software, resulting in a continuous whitelist update to remove the unverified software. After a certain period of time, the security score increased and restricted devices are able to extend to the network. It took 0.19 s for our proposed scheme to extend the devices' scalability to 90% and above.

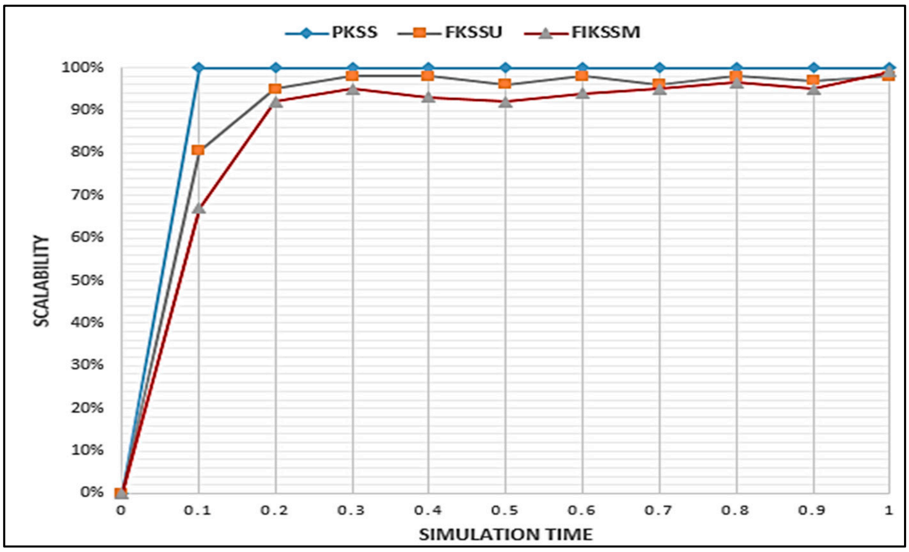

Figure 9. Comparison results of scalability.

4.2.3. Experiment 6: Vulnerability

Vulnerability in an IoT system is described as the faults or vulnerabilities that expose it to threats. It comes from dividing the number of infected devices by the number of devices in the network. In Figure 10, the horizontal axis reflects the simulated time and, through the relation to other peripheral malicious appliances, the vertical axis represents the amount of infected IoT computers. In PKSS, malicious devices are explicitly connected to all IoT devices in the network, which renders the scheme susceptible to a Distributed Denial of Service (DDOS) attack, in which an intruder uses many infected IoT devices to overload the target node. The FKSSU is still not adequately confident, as the security score of the device when applied to the internet, which renders the device susceptible to malicious applications installed by the user's carelessness or by the hacker, depends only on the security of the user authentication and verification with a unimodal biometric key. Our suggested FIKSSM scheme decreases the number of machines attached to malicious devices to 4%. Compared to PKSS, the number of malicious devices has decreased to 49%. As the link depends on the security level and the agent, and the whitelist continuously checks the software, there is a decrease in the number of malicious devices after the whitelist update.

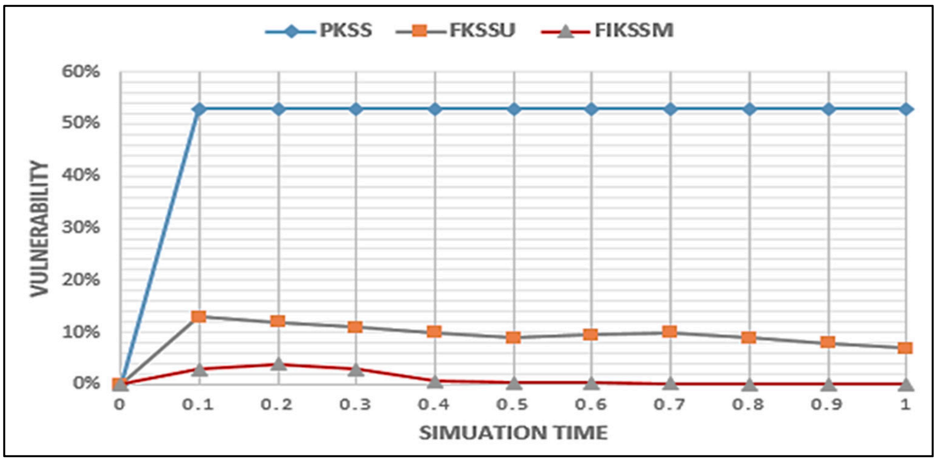

Figure 10. Comparison Results of Vulnerability.

4.2.4. Experiment 7: Complexity

Herein, the objective is to evaluate the execution factors that influence the complexity of the suggested model. We execute different signature methods and evaluate them in terms of the size of files and processing time. First, we evaluate the file size of the Private Key, Public Key, Public Key Certificate, and the signature in a blockchain transaction. A Private Key includes a fused vector form and a fingerprint and a finger vein pattern, and the file size of a Private Key is 10 Kbyte. This file size is larger than a traditional private key. However, 10 Kbyte is small enough for practical use. The public key includes the public parameters assumed by our scheme and the file size is 1 Kbyte. The file sizes of a public key certificate and signature are the same in all methods, and they are 1 Kbyte and 71 bytes, respectively.

As revealed from Table 3, the processing time of the public key generation is executed one time in initial user registration. Thus, the processing time of 400 ms is fast enough compared to the one used by unimodal biometrics which is 499 ms. We perform signature generation every blockchain transaction generation. The processing time of signature generation is in the PKSS is 78 ms. In the FKSSU, the processing time of signature generation is 1306 ms; this is slower than the PKSS and the FIKSSM, whereas in FIKSSM, the processing time is 74 ms, which is significantly faster. We perform signature verification every blockchain transaction verification. The processing time of signature verification in the FIKSSM is 60 ms, which is faster compared to other blockchain procedures. In this way, you can see that our proposed scheme achieves practical file size and processing time. Therefore, we can use our scheme for a practical IoT blockchain system.

Table 3. Implementation comparative results in terms of file size and processing time.

Execution Factors	**Algorithm**	**PKSS**	**FKSSU**	**FIKSSM**
File Size	Private Key	1 Kbyte	10 Kbyte	10 Kbyte
	Public Key	1 Kbyte	1 Kbyte	1 Kbyte
	Public key Certificate	1 Kbyte	1 Kbyte	1 Kbyte
	Signature in a Blockchain Transaction	71 byte	71 byte	71 byte
Processing Time	Public key Generation	300 ms	499 ms	400 ms
	Signature Generation	78 ms	1306 ms	74 ms
	Signature Verification	70 ms	70 ms	60 ms

5. Conclusions and Future Work

In this work, we present a new signature scheme that tackles security and scalability concerns in IoT devices focused on blockchain technologies and multimodal biometrics. The suggested model safely expands the network communication of IoT devices and guarantees that the individual who creates the blockchain transaction is not a fraud. The model suggested increased security in two steps. One is to use multimodal biometric as a private key to authenticate and validate a blockchain transaction using the fuzzy identity signature. Two of them include the implementation of whitelist applications on IoT, and then a smart contract to record all installed software in the blockchain. A list of available software is recorded in the IoT manufacture, and when the IoT devices are used, their security score is evaluated by checking the number of unverified software programs on the whitelist with the manufactured list. This restricts the infected IoT devices; by automatically updating the whitelist, unverified software programs are removed, and the security score is raised, which leads to adding IoT devices to the network. Experiments show that our proposed model reduces the addition of infected devices to the network up to 49% compared to the conventional schemes. The proposed scheme practically achieves high performance in terms of security against spoofing and signature forgery and provide high throughput and low latency. Future work may include (1) Enhancing the biometric authentication accuracy by applying multiple biometric traits; it is expected that it will extract a wider range of information and this leads to a better result, (2) different approaches for feature level fusion and extraction of biometric for private key extraction, and (3) extend the number of peers in the blockchain network to accurately test the scalability of the permissioned network, and its effects on performance.

Author Contributions: Conceptualization, S.M.D. and O.A.H., and A.A.A.; Methodology, S.M.D., O.A.H., Y.A.L. and Z.A.O.; Software, O.A.H., A.A.A., and Y.A.L.; Validation, S.M.D., A.A.A., O.A.H., and Z.A.O.; Formal analysis, S.M.D., A.A.A. and O.A.H.; Investigation, S.M.D., Z.A.O., O.A.H., and S.T.; Resources, O.A.H., A.A.A., Y.A.L. and S.T.; Data curation, O.A.H., A.A.A. and S.T.; Writing—original draft preparation, S.M.D., A.A.A., and O.A.H.; Writing—review and editing, S.M.D.,O.A.H. and Z.A.O.; Visualization, O.A.H., A.A.A., Y.A.L. and S.T.; Supervision, S.M.D., Z.A.O. and A.A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Bozic, N.; Pujolle, G.; Secci, S. A Tutorial on Blockchain and Applications to Secure Network Control-Planes. In Proceedings of the 3rd IEEE International on Smart Cloud Networks & Systems (SCNS), Dubai, UAE, 19–21 December 2016; pp. 1–8.
2. Cai, Y.; Zhu, D. Fraud detections for online businesses: A perspective from blockchain technology. *Financ. Innov.* **2016**, *2*, 20. [CrossRef]
3. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. *Future Gener. Comput. Syst.* **2020**, *107*, 841–853. [CrossRef]
4. Zyskind, G.; Nathan, O.; Pentland, A.S. Decentralizing Privacy: Using Blockchain to Protect Personal Data. In Proceedings of the 2015 IEEE Security and Privacy Workshops, San Jose, CA, USA, 21–22 May 2015; pp. 180–184.
5. Davenport, A.; Shetty, S. Air Gapped Wallet Schemes and Private Key Leakage in Permissioned Blockchain Platforms. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 541–545.
6. Min, X.; Li, Q.; Liu, L.; Cui, L. A Permissioned Blockchain Framework for Supporting Instant Transaction and Dynamic Block Size. In Proceedings of the 15th IEEE International Trust. Security and Privacy in Computing and Communications, Tianjin, China, 23–26 August 2016; pp. 90–96.
7. Sato, M.; Matsuo, S.I. Long-Term Public Blockchain: Resilience against Compromise of Underlying Cryptography. In Proceedings of the 2nd IEEE European Symposium on Security and Privacy Workshops, Vancouver, BC, Canada, 31 July–3 August 2017; pp. 1–8.
8. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
9. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564.
10. Dmitrienko, A.; Noack, D.; Yung, M. Secure Wallet-Assisted Offline Bitcoin Payments with Double-Spender Revocation. In Proceedings of the 2017 ACM on Conference on Information and Knowledge Management, Abu Dhabi, UAE, 4–6 April 2017; pp. 520–531.
11. Bonneau, J.; Miller, A.; Clark, J.; Narayanan, A.; Kroll, J.A.; Felten, E.W. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In Proceedings of the 2015 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 17–21 May 2015; pp. 104–121.
12. Sikorski, J.J.; Haughton, J.; Kraft, M. Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Appl. Energy* **2017**, *195*, 234–246. [CrossRef]
13. Mettler, M. Blockchain technology in healthcare: The revolution starts here. In Proceedings of the 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, Germany, 14–16 September 2016; pp. 1–3.
14. Murakami, T.; Ohki, T.; Takahashi, K. Optimal sequential fusion for multibiometric cryptosystems. *Inf. Fusion* **2016**, *32*, 93–108. [CrossRef]
15. Yang, P.; Cao, Z.; Dong, X. Fuzzy identity based signature with applications to biometric authentication. *Comput. Electr. Eng.* **2011**, *37*, 532–540. [CrossRef]

16. Novo, O. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet Things J.* **2018**, *5*, 1184–1195. [CrossRef]
17. Yu, Y.; Li, Y.; Tian, J.; Liu, J. Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things. *IEEE Wirel. Commun.* **2018**, *25*, 12–18. [CrossRef]
18. Rodriguez-Zurrunero, R.; Utrilla, R.; Rozas, A.; Araujo, A. Process Management in IoT Operating Systems: Cross-Influence between Processing and Communication Tasks in End-Devices. *Sensors* **2019**, *19*, 805. [CrossRef]
19. Fernandez-Carames, T.M.; Fraga-Lamas, P. A Review on the Use of Blockchain for the Internet of Things. *IEEE Access* **2018**, *6*, 32979–33001. [CrossRef]
20. Schuff, D.; Louis, R.S. Centralization vs. decentralization of application software. *Commun. ACM* **2001**, *44*, 88–94. [CrossRef]
21. Dai, W.; Deng, J.; Wang, Q.; Cui, C.; Zou, D.; Jin, H. SBLWT: A Secure Blockchain Lightweight Wallet Based on Trustzone. *IEEE Access* **2018**, *6*, 40638–40648. [CrossRef]
22. Winter, J. Trusted Computing Building Blocks for Embedded Linux-Based ARM Trustzone Platforms. In Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks—SASN '05, Association for Computing Machinery (ACM), Alexandria, VA, USA, 31 October 2008; pp. 21–30.
23. Da Xu, L.; He, W.; Li, S. Internet of Things in Industries: A Survey. *J. IEEE Trans. Ind. Inf.* **2014**, *10*, 2233–2243.
24. Samaniego, M.; Jamsrandorj, U.; Deters, R. Blockchain as a Service for IoT. In Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, 15–18 December 2016; pp. 433–436.
25. Balfanz, D. FIDO U2F Implementation Considerations. 2017. Available online: https://fidoalliance.org/what-is-fido/ (accessed on 30 May 2020).
26. Shingala, K. An Alternative to the Public Key Infrastructure for the Internet of Things. Master's Thesis, Norwegian University of Science and Technology (NTNU), Trondheim, Norway, 2019.
27. Biswas, S. Enhancing the Privacy of Decentralized Identifiers with Ring Signatures. Master's Thesis, Aalto University, Espoo, Finland, 2020.
28. Raikwar, M.; Gligoroski, D.; Kralevska, K. SoK of Used Cryptography in Blockchain. *IEEE Access* **2019**, *7*, 148550–148575. [CrossRef]
29. Dery, S. Using Whitelisting to Combat Malware Attacks at Fannie Mae. *IEEE Secur. Priv. Mag.* **2013**, *11*, 90–92. [CrossRef]
30. Lotfy, Y.A.; Darwish, S.M. A Secure Signature Scheme for IoT Blockchain Framework Based on Multimodal Biometrics. In *Proceedings of the International Conference on Advanced Intelligent Systems and Informatics*; Springer Science and Business Media LLC: Berlin, Germany, 2020; pp. 261–270.
31. Li, Y.; Yu, Y.; Min, G.; Susilo, W.; Ni, J.; Choo, K.K. Fuzzy identity-based data integrity auditing for reliable cloud storage systems. *IEEE Trans. Dependable Secure Comput.* **2017**, *16*, 72–83. [CrossRef]
32. Waters, B. *Efficient Identity-Based Encryption Without Random Oracles*; Lecture Notes in Computer Science Book Series; Springer: Berlin, Germany, 2005; Volume 3494, pp. 114–127. [CrossRef]
33. Boneh, D.; Franklin, M. Identity-Based Encryption from the Weil Pairing. *SIAM J. Comput.* **2003**, *32*, 586–615. [CrossRef]
34. Joux, A. Separating Decision Diffie—Hellman from Computational Diffie—Hellman in Cryptographic. *J. Cryptol.* **2003**, *16*, 239–247. [CrossRef]
35. Choi, Y.-J.; Kang, H.-J.; Lee, I.-G. Scalable and Secure Internet of Things Connectivity. *Electronics* **2019**, *8*, 752. [CrossRef]
36. Ross, A.; Govindarajan, R. Feature Level Fusion Using Hand and Face Biometrics. In *Biometric Technology for Human Identification II*; International Society for Optics and Photonics: Bellingham, WA, USA, 2005; Volume 5779, pp. 196–204.
37. Wang, Z.; Tao, J. A Fast Implementation of Adaptive Histogram Equalization. In Proceedings of the 2006 8th International Conference on Signal Processing, Beijing, China, 16–20 November 2006; Volume 2, pp. 3–6.
38. Kekre, H.B.; Bharadi, V.A. Fingerprint's core point detection using orientation field. In Proceedings of the International Conference on Advances in Computing, Control, and Telecommunication Technologies, Trivandrum, Kerala, India, 28–29 December 2009; pp. 150–152.

39. Yang, J.; Li, X. Efficient Finger Vein Localization and Recognition. In Proceedings of the 2010 20th International Conference on Pattern Recognition, Istanbul, Turkey, 23–26 August 2010; pp. 1148–1151.
40. Yang, J.; Liu, L.; Jiang, T.; Fan, Y. A modified Gabor filter design method for fingerprint image enhancement. *Pattern Recognit. Lett.* **2003**, *24*, 1805–1817. [CrossRef]
41. Zhu, Z.; Lu, H.; Zhao, Y. Scale multiplication in odd Gabor transform domain for edge detection. *J. Vis. Commun. Image Represent.* **2007**, *18*, 68–80. [CrossRef]
42. Yang, J.; Zhang, X. Feature-level fusion of fingerprint and finger-vein for personal identification. *Pattern Recognit. Lett.* **2012**, *33*, 623–628. [CrossRef]
43. Jain, A.K.; Prabhakar, S.; Hong, L. A multichannel approach to fingerprint classification. *IEEE Trans. Pattern Anal. Mach. Intell.* **1999**, *21*, 348–359. [CrossRef]
44. Srivastava, S. Accurate Human Recognition by Score-Level and Feature-Level Fusion Using Palm—Phalanges Print. *J. Sci. Eng.* **2017**, *2*, 543–554.
45. Cachin, C. Architecture of the Hyperledger Blockchain Fabric. In Proceedings of the 2016 Workshop on Distributed Cryptocurrencies and Consensus Ledgers, Chicago, IL, USA, 25 July 2016.
46. Wang, C. A provable secure fuzzy identity based signature scheme. *Sci. China Inf. Sci.* **2012**, *55*, 2139–2148. [CrossRef]
47. Yao, Y.; Li, Z. A novel fuzzy identity based signature scheme based on the short integer solution problem. *Comput. Electr. Eng.* **2014**, *40*, 1930–1939. [CrossRef]
48. Shandong University. SDUMLA. Available online: http://mla.sdu.edu.cn/info/1006/1195.htm (accessed on 30 May 2020).
49. Rodrigues, R.N.; Kamat, N.; Govindaraju, V. Evaluation of biometric spoofing in a multimodal system. In Proceedings of the 2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), Washington, DC, USA, 27–29 September 2010; pp. 1–5.

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).