symmetry

MDPI

Article

# A Cloud-Based Crime Reporting System with Identity Protection

**Tzay-Farn Shih [1], Chin-Ling Chen [1,2,3,*], Bo-Yan Syu [1] and Yong-Yuan Deng [1,*]**

[1] Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung 41349, Taiwan; tfshih@cyut.edu.tw (T.-F.S.); s10327624@gm.cyut.edu.tw (B.-Y.S.)
[2] School of Information Engineering, Changchun Sci-Tech University, Changchun 130600, China
[3] School of Computer and Information Engineering, Xiamen University of Technology, Xiamen 361005, China
* Correspondence: clc@mail.cyut.edu.tw (C.-L.C.); allen.nubi@gmail.com (Y.-Y.D.); Tel.: +886-4-23323000 (ext. 4761) (C.-L.C.)

Received: 2 January 2019; Accepted: 13 February 2019; Published: 18 February 2019


**Abstract:** Criminal activities have always been a part of human society, and even today, in a world of extremely advanced surveillance and policing capabilities, many different kinds of crimes are still committed in almost every social environment. However, since those who commit crimes are not representative of the majority of their community, members of these communities tend to wish to report crime when they see it; however, they are often reluctant to do so for fear of their own safety should the people they report identify them. Thus, a great deal of crime goes unreported, and investigations fail to gain key evidence from witnesses, which serves only to foster an environment in which criminal activity is more likely to occur. In order to address this problem, this paper proposes an online illegal event reporting scheme based on cloud technology, which combines digital certificates, symmetric keys, asymmetric keys, and digital signatures. The proposed scheme can process illegal activity reports from the reporting event to the issuing of a reward. The scheme not only ensures informers' safety, anonymity and non-repudiation, but also prevents cases and reports being erased, and ensures data integrity. Furthermore, the proposed scheme is designed to be robust against abusive use, and is able to preclude false reports. Therefore, it provides a convenient and secure platform for reporting and fighting crime.

**Keywords:** citizen digital certificate; public key; private key; illegal event; crime; digital signature

## 1. Introduction

In today's technologically advanced society, mechanisms for fighting crime are extremely advanced, from remote, automatic surveillance to sophisticated dedicated laboratories and evidence analysis, yet crime still has a significant presence in our world, both globally and in local communities, including sexual assault, drugs and violent crimes, all of which endanger the public. While some people may be willing to actively report illegal acts, others choose not to do so, as they are worried about the fallibility of the policing, reporting and criminal justice systems, based on previous failings in all three departments [1–3]. People are afraid for their own safety should those they report identify them, or they are worried that law enforcement officials may simply erase any case they report. Moreover, people afraid of intimidation may choose not to offer information, or stand as a witness to criminal acts, despite a high reward being offered for such information. All of these concerns have, in the past, contributed to an environment in which crime is more difficult to address, and in which crime is more likely to be committed. However, recent years have seen rapid developments in Internet technology, in particular cloud technology, which have made possible an online crime reporting system with identity protection. In fact, the high degree of identity protection offered by these technological advances is a necessity for any such online crime reporting system [4].

User identities must be as secure as possible for any such reporting system, as informers are required to use their real names; understandably, this information must be kept secret to ensure the informer's safety [5]. Informers are required to provide their real identities, as the use of pseudonyms would make them difficult to contact, and cases may not be accepted as a result. However, an informer's real identity is always vulnerable to exposure through human error.

There are two primary requirements for an online crime reporting system: Informers must provide their real identities, and their identities must be well protected. With these requirements in mind, several online crime reporting systems have been proposed for different applications in recent years [1,2,6,7]. In order to ensure that the informer's identity is protected during reporting, anonymity can effectively protect victims and witnesses; however, the security mechanisms involved in identity verification and data transmission are important issues to be addressed.

As a result, this paper presents a novel reporting system using a cryptographic mechanism for improved security and identity confidentiality. The proposed scheme also combines digital certificates, symmetric keys, asymmetric keys, digital signatures and a design verification mechanism to achieve integrity, privacy and un-falsification of transmitted data. In addition, the system not only ensures the legitimacy of a user's identity, but also protects informers' privacy and security [7] in an anonymous manner. Rewards can also automatically be remitted to informers. In addition, the proposed system prevents administration problems, such as cases being deleted or lost, or malicious abuse of the reporting system.

The proposed scheme uses a network online reporting mechanism to improve reporting and reduce policing costs [2], combined with digital certificates for authentication [8–10] to ensure that reports cannot be made anonymously. The proposed system is thus able to use an impartial third-party organization to confirm an informer's identity, and protect the informer's privacy and security. In addition, if cases reported are not accepted within a specified time, the system is equipped with an automatic upward reporting mechanism to prevent late investigations or the erasure of cases. If reported information leads to the successful resolution of a case, a reward will be automatically remitted to the informers via the system, so that the process is completely hidden and safe, thus offering complete informer identity protection, and preventing a variety of security threats.

Network service applications have increased rapidly with the recent rapid growth of information technology, giving rise to the development of powerful, high-capacity cloud computing systems that can satisfy various user demands and offer shared resources online [11,12]. According to the literature [13], many enterprises employ cloud services and their applications provided through a browser offering access to online programming applications, software and data. These computing services can be implemented in the cloud platform. In addition, [14] noted that the cloud services are an important future trend.

Many online reporting systems have been proposed to date, and research into such systems has provided several requirements for such systems [6,15–18]. For example: trusted third-parties are used to verify legitimate informer identities using digital certificate technology to prevent abuse of the system by impostor attacks [15,16]; authentication mechanisms are crucial to such systems [19–21].

Informers may wish to remain anonymous during the online reporting process [6] because they are afraid for their own safety should their identity become known to those being reported [17]. Therefore, it is important to protect informer identity. In addition, as Martín et al. [18] noted, messages must be secure against tampering during transmission. It is also important to ensure that the identity of the informer is not even known to the auditor or the system in the event of a malicious digital attack.

Another important requirement is non-repudiation. The system server saves information signed by all personnel; thus, if disputes occur, users cannot deny that the record has been signed [18].

Other concerns include:

(1) That reported cases may be erased or delayed due to external intervention. Therefore, if reported cases have not been accepted within a specified time, the proposed scheme is equipped with an automatic upward reporting mechanism to avoid reported cases being suppressed.

(2) That informers' identities may be disclosed in the reward procedure. The system must protect the privacy of informers in any actions, so the proposed scheme includes a precautionary mechanism to ensure that managers or databases are not leaked, as there is no record to track the identity of a person making a report.

(3) That reported information may be intercepted or leaked, revealing the informer's identity. Therefore, it is essential to ensure complete transmission confidentiality.

To sum up, an online reporting system should meet the following requirements: authentication, anonymity, integrity, and non-repudiation, preventing cases from being erased, avoiding the disclosure of informer identity in the award procedure, protecting the privacy of informers, and preventing the reported information from being intercepted.

## 2. Methodology

This section describes how the proposed online crime reporting system with identity protection protects informer identity and privacy during the reporting process, how the proposed system prevents cases being erased, and the automatic reward process.

### *2.1. Notations*

$U_x$—user $x$ is categorized as: informer $U_i$, investigator $U_t$, superior $U_s$
$U_i$—informer
$U_t$—investigator
$U_s$—superior
$Server_{PLA}$—reporting server
$Server_{CA}$—certificate authority server
$TF_{Gateway}$—cooperating payment server
$ID_x$—the reporting system account of $U_x$
$PW_x$—the reporting system password of $U_x$
$PW_{HASH}$—the hash value of a password
$SN_{event}$—the serial number of a case
$ACC_i$—the bank account of $U_i$
$Cash$—the reward amount
$SN$—the serial number of an IC (Integrated Circuit) card
$IDNO$—the ID number of an IC card (last four digits)
$PUK_{Ux}$—the public key of $U_x$
$PRK_{Ux}$—the private key of $U_x$
$Msg_{event}$—attached data for reporting (e.g., photos and related documents)
$Msg_{suc}$—success response from reporting server
$Msg_{unsuc}$—unsuccessful response from reporting server
$Msg_{CA}$—the result of verification from the CA (Certificate Authority) server
$Msg_{ver}$—the audit result of reporting case form $U_t$ or $U_s$
$Msg_{BANKsuc}$—notification of remit
$Sig_x$—the signature of $x$
$V_{PUKUx}(Sig_x)$—use the public key $PUKUx$ to verify signature $Sig_x$
$S_{PRKUx}(M)$—use the private key $PRKUx$ to sign message $M$
$E_{KEY}(M)$—encrypt message $M$ by symmetric key $KEY$
$D_{KEY}(C)$—decrypt ciphertext $C$ by symmetric key $KEY$
$E_{PUKSERVERPLA}(M)$—encrypt message $M$ by public key $PUK_{SERVERPLA}$
$D_{PRKSERVERPLA}(C)$—decrypt ciphertext $C$ by server's private key $PRK_{SERVERPLA}$
$H(\ )$—one way hash function

$X \rightarrow Y$—send a message from $X$ to $Y$
$A \stackrel{?}{=} B$—determine if $A$ is equal to $B$
——▶—insecure channel
- - - - - - - - ▶—secure channel

### 2.2. System Structure

The system structure and operation processes of the proposed system are shown in Figure 1. The main interactive roles are informers, investigators and superiors. The servers include the reporting server, the cooperating payment server, and the certificate authority server. The platform uses digital certificates on personal identification IC (Integrated Circuit) cards, which verify the identity of the user, thus preventing reports by impostors. The user (e.g., informer, investigator and superior) must apply for a personal identification IC card in person at the digital certificate management center. In all operations, the verification of a personal IC card is issued by the reporting platform to the digital certificate management center. In the following descriptions, it is assumed that the user has registered successfully and has logged in to the reporting platform.

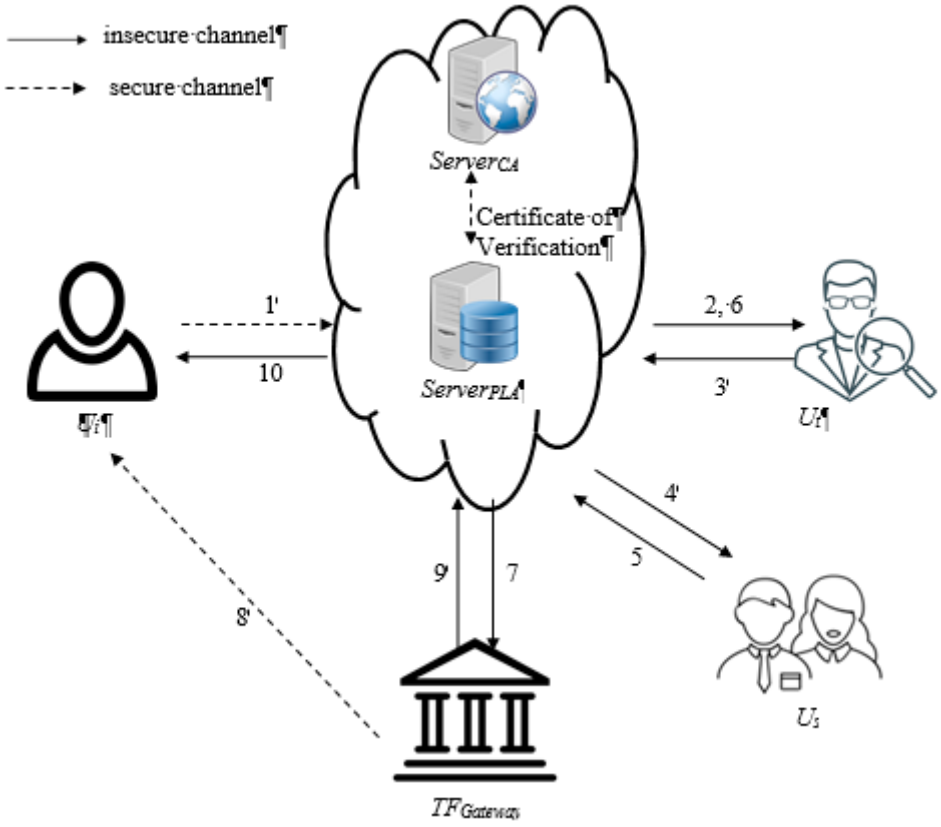


**Figure 1.** System structure and operations of reporting cloud.

(1) Informer logs in to the system to make a report, or to process other related operations.
(2) The reporting server assigns an investigator to conduct an investigation, and the investigator receives the report of a crime, and determines whether the preliminary evidence is sufficient to open a case.
(3) The investigator transmits the result of the audited case to the reporting server.
(4) The reporting server transmits the reports audited by the investigator to a superior. In addition, if the investigator does not receive or audit reports within a specified period, the system will automatically notify the superior of the reports. If the upward notification confirms the reports are sufficient to open cases, with a reward to be issued, the reports will be sent to the upper superiors

for confirmation. When all the superiors confirm that the details of the report are sufficient for the reward, the financial system will automatically remit the reward to the informer's account. On the other hand, if the investigator determines that a report is abusing the system, then the superior will re-confirm whether the case is rejected or must be re-investigated to avoid a wrong judgment.

(5) Each superior sends the results of the case to the reporting server.

(6) When the reporting server receives a superior's determination that the case needs re-investigating, the case will be reassigned to a new superior.

(7) When the reporting server receives the confirmation and agrees to issue the reward, the server will notify the financial institution.

(8) The cooperating payment server of the financial institution will automatically remit the reward to the informer's account.

(9) When the cooperating payment server has remitted the reward, it will notify the reporting server.

(10) The reporting server notifies the informer that the remittance has been completed.

#### 2.2.1. Registration Phase

Before a user is granted access to the platform for the first time, they must go to the digital certificate management center to get a personal identification IC card, which they will then use to register and access the platform. Figure 2 is the flow chart of the registration verification phase. The steps of the registration phase are as follows:

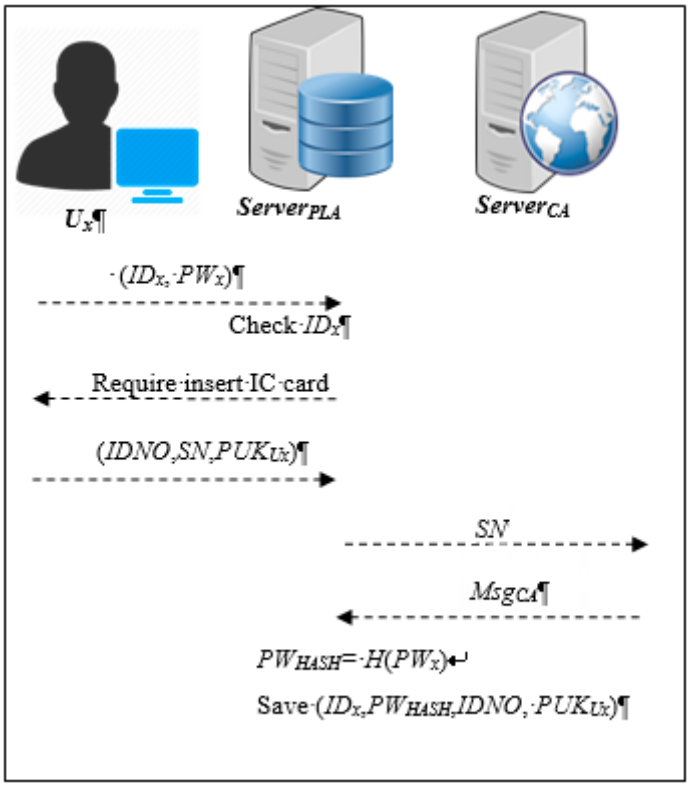


**Figure 2.** The flow chart of the registration phase.

**Step 1**: $U_x \rightarrow Server_{PLA}$

User $U_x$ must first register and provide basic information, such as account $ID_x$ and password $PW_x$. The user $U_x$ will transmit $ID_x$ and $PW_x$ to the reporting server $Server_{PLA}$.

**Step 2**: $Server_{PLA} \rightarrow U_x$

After receiving the $ID_x$ and $PW_x$, the reporting server verifies the account $ID_x$ of the user $U_x$. If the user account $ID_x$ is approved by the server, then user $U_x$ will be asked to insert his/her personal identification IC card to determine whether the IC card is valid.

**Step 3**: $U_x \rightarrow Server_{PLA}$

User $U_x$ must insert the personal identification IC card and enter the PIN code. If the PIN code is correct, then user $U_x$ will receive the *SN* number of the IC card, the public key $PUK_{Ux}$ and his/her personal data (for example, the last four digits of the ID card number *IDNO*) and the system will send *IDNO*, *SN*, and $PUK_{Ux}$ to the reporting server.

**Step 1**: $Server_{PLA} \rightarrow Server_{CA}$

After receiving the the user's *IDNO*, *SN* and public key $PUK_{Ux}$, the reporting server will transmit the *SN* and authentication data to the OCSP (Online Certificate Status Protocol) service of the certificate authority server $Server_{CA}$ to check the validity of *SN*.

**Step 2**: $Server_{CA} \rightarrow Server_{PLA}$

The certificate authority server $Server_{CA}$ will verify the *SN* sent by the reporting server $Server_{PLA}$, and send the result $Msg_{CA}$ back to the reporting server.

**Step 3**: $Server_{PLA}$

After receiving the $Msg_{CA}$ that $Server_{CA}$ has already sent back, the $Server_{PLA}$ can determine whether $Msg_{CA}$ is valid. If it is valid, then user $U_x$ is a legal user. The reporting server will then convert the user's password $PW_x$ into $PW_{HASH}$ with SHA-256:

$$PW_{HASH} = H(PW_x) \tag{1}$$

Finally, the registration information $ID_x$, encrypted $PW_{HASH}$, *IDNO* and public key $PUK_{Ux}$ of the user $U_x$ are stored in the database, completing the registration process.

### 2.2.2. Login Verification Phase

Once a user passes the verification phase, s/he will be allowed to log into the system. The following Steps (1) and (2) describe the login processes and verification steps. Figure 3 shows the flow chart of the login verification phase.

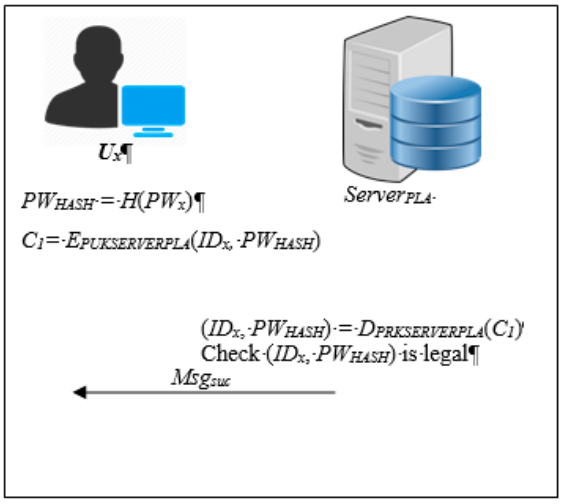


**Figure 3.** The flow chart of the login verification phase.

**Step 1**: $U_x \rightarrow Server_{PLA}$

The user $U_x$ logs into the reporting platform and enters the account $ID_x$ and password $PW_x$, and then sends this information. This will convert the password $PW_x$ into $PW_{HASH}$:

$$PW_{HASH} = H(PW_x) \tag{2}$$

Then the $Server_{PLA}$ uses the public key $PUK_{SERVERPLA}$ to encrypt $ID_x$ and $PW_{HASH}$. After this, the encrypted message $C_1$ is transmitted to the reporting server:

$$C_1 = E_{PUKSERVERPLA}(ID_x, PW_{HASH}) \tag{3}$$

**Step 2**: $\text{Server}_{\text{PLA}} \rightarrow \text{U}_{\text{x}}$

When the reporting server receives the encrypted message $C_1$, the server $Server_{PLA}$ will use its own private key $PRK_{SERVERPLA}$ to decrypt $C_3$:

$$(ID_x, PW_{HASH}) = D_{PRKSERVERPLA}(C_1) \tag{4}$$

The user $U_x$, account $ID_x$ and password $PW_{HASH}$ will be obtained, and then compared with the data stored in the database. If $ID_x$ and $PW_{HASH}$ match the database, $Server_{PLA}$ will respond with a success message $Msg_{suc}$ that the login is successful.

#### 2.2.3. Reporting Phase

In the reporting phase, the informer can log into the system and fill in a crime report by entering the identity of the offender, the related documents and the details of the violation. The informer's identity is not required. The informer simply needs to insert his/her IC card and verify his/her identity. If the informer's identity is correct, the system will allow him/her to submit a report. The flow chart of the reporting phase is shown in Figure 4.

**Step 1**: $\text{U}_{\text{i}} \rightarrow \text{Server}_{\text{PLA}}$

The informer $U_i$ logs into the reporting platform, enters his/her account $ID_i$ and password $PW_i$, and then submits them. This will convert the $PW_i$ into $PW_{HASH}$:

$$PW_{HASH} = H(PW_i) \tag{5}$$

After this, $PUK_{SERVERPLA}$ uses the public key to encrypt $ID_i$ and $PW_{HASH}$ and then send the encrypted message $C_4$ to the reporting server:

$$C_2 = E_{PUKSERVERPLA}(ID_i, PW_{HASH}) \tag{6}$$

**Step 2**: $\text{Server}_{\text{PLA}} \rightarrow \text{U}_{\text{i}}$

When the reporting server receives the encrypted message $C_2$ from the informer $U_i$, the server will use the private key $PRK_{SERVERPLA}$ to decrypt message $C_2$:

$$(ID_i, PW_{HASH}) = D_{PRKSERVERPLA}(C_2) \tag{7}$$

The informer $U_i$ account $ID_i$ and password $PW_{HASH}$ will be obtained and then compared with the data stored in the database. If $ID_i$ and $PW_{HASH}$ match the related data in the database, $Server_{PLA}$ will reply $Msg_{suc}$ to inform $U_i$ that they have successfully logged in.

**Step 3**: $\text{U}_{\text{i}} \rightarrow \text{Server}_{\text{PLA}}$

Then, the informer $U_i$ enters the report event $Msg_{event}$ and encrypts $ID_i$ and $Msg_{event}$ by public key $PUK_{SERVERPLA}$. The encrypted message $C_3$ will be sent to the reporting server:

$$C_3 = E_{PUKSERVERPLA}(ID_i, Msg_{event}) \tag{8}$$

**Step 4**: $\text{Server}_{\text{PLA}} \rightarrow \text{U}_{\text{i}}$

The reporting server $Server_{PLA}$ uses its own private key $PRK_{SERVERPLA}$ to decrypt $C_3$, and then gets the informer's $ID_i$ and report event $Msg_{event}$:

$$(ID_i, Msg_{event}) = D_{PRKSERVERPLA}(C_3) \tag{9}$$

It then checks that the form is completed. If the information is completed, the $Server_{PLA}$ will request the informer $U_i$ to insert his/her IC card.

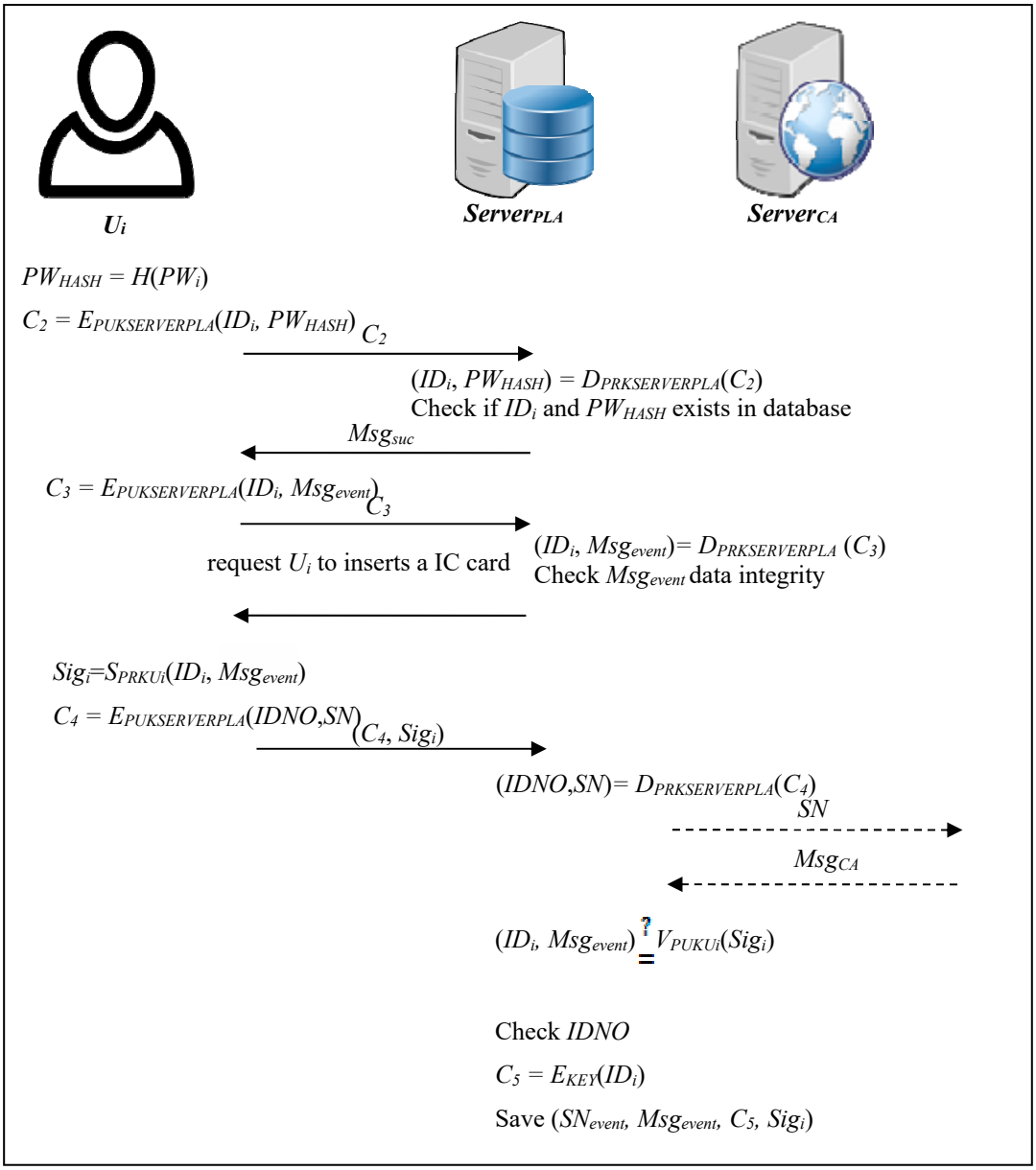


**Figure 4.** The flow chart of the reporting phase.

**Step 5**: $U_i \rightarrow Server_{PLA}$

After this, $U_i$ inserts his/her IC card and enters his/her PIN code. If the PIN code is correct, it will use the informer's private key $PRK_{Ui}$ to sign the reported event $Msg_{event}$:

$$Sig_i = S_{PRKUi}(ID_i, Msg_{event}) \tag{10}$$

Next, $SN$ and $IDNO$ are obtained from the informer $U_i$'s IC card, and the public key $PUK_{SERVERPLA}$ is used to encrypt the $SN$ and $IDNO$:

$$C_4 = E_{PUKSERVERPLA}(IDNO, SN) \tag{11}$$

Finally, $Server_{PLA}$ sends the encrypted message $C_4$ and the informer's signature $Sig_i$ to the reporting server.

**Step 6**: $\text{Server}_{\text{PLA}} \rightarrow \text{Server}_{\text{CA}}$

The reporting server receives $C_4$ and $Sig_i$ of $U_i$, and then uses the server's private key $PRK_{SERVERPLA}$ to decrypt $C_4$, and obtains the *IDNO* and *SN* of $U_{i.}$.

$$(IDNO, SN) = D_{PRKSERVERPLA}(C_4) \tag{12}$$

The reporting server will transmit the *SN* to the OCSP service of the certificate authority server through a secure channel to check the validity of *SN*.

**Step 7**: $\text{Server}_{\text{CA}} \rightarrow \text{Server}_{\text{PLA}}$

The certificate authority server $Server_{CA}$ will verify the *SN* from the reporting $Server_{PLA}$ and send the result $Msg_{CA}$ back to $Server_{PLA}$.

**Step 8**: $\text{Server}_{\text{PLA}}$

When the reporting server receives the result of the certificate authority server $Server_{CA}$ and it is effective, it will then compare the information in signature $Sig_i$ and messages ($ID_i$, $Msg_{event}$):

$$(ID_i, Msg_{event}) \stackrel{?}{=} V_{PUKUi}(Sig_i) \tag{13}$$

If the signature is correct, the server will compare the *IDNO* of the IC card with the *IDNO* stored in the database. If the comparison is successful, the system will generate an event number $SN_{event}$. This event number $SN_{event}$ will be associated with the identity of the informer. Therefore, the system will encrypt the $ID_i$ of the $U_i$ with symmetric key from $Server_{PLA}$:

$$C_5 = E_{KEY}\ (ID_i) \tag{14}$$

Finally, the $SN_{event}$, $Msg_{event}$, $C_5$ and $Sig_i$ are saved in the database.

#### 2.2.4. The Superior Verification Phase

Upon logging into the system, the investigator will conduct an investigation of reported crimes randomly assigned by the system. If the reported case is illegal and has a reward, it will be forwarded to the superior to issue the reward. On the other hand, if it is a non-reward case, the investigator will indicate the case processing status as "closed". This phase verifies individual identification of the IC card as in the case reporting phase steps (6)–(7). The case before the superior will only receive and display relevant documents and content, and does not contain the identity of the informer because the identity of the informer was confirmed at the beginning of the reporting phase, which means the informer is a legal user, and the whole process of the report is guaranteed to be anonymous. The following steps (1)–(4) describe the auditing process and give an overview of verification, as shown in Figure 5.

**Step 1**: $\text{U}_{\text{t}} \rightarrow \text{Server}_{\text{PLA}}; \text{U}_{\text{t}} \rightarrow \text{U}_{\text{s}}$

When the investigator $U_t$ receives the report event $Msg_{event}$ assigned by the system, the investigator investigates that event. If the investigation shows that it is an illegal event with reward, the investigator $U_t$ will be requested to insert his/her IC card and enter his/her PIN code. If the PIN code is correct, the server will use the investigator $U_t$'s private key $PRK_{Ut}$ to sign the case. The signature of the investigator $Sig_t$ includes the identity of the investigator $ID_t$, event number $SN_{event}$, reporting event $Msg_{event}$, event verification result $Msg_{ver}$ and the reward amount *Cash*:

$$Sig_t = S_{PRKUt}(ID_t, SN_{event}, Msg_{event}, Msg_{ver}, Cash) \tag{15}$$

The investigator will close it, and the $ID_t$, $SN_{event}$, $Msg_{event}$, $Msg_{ver}$, *Cash* and $Sig_t$ are stored directly in the database.

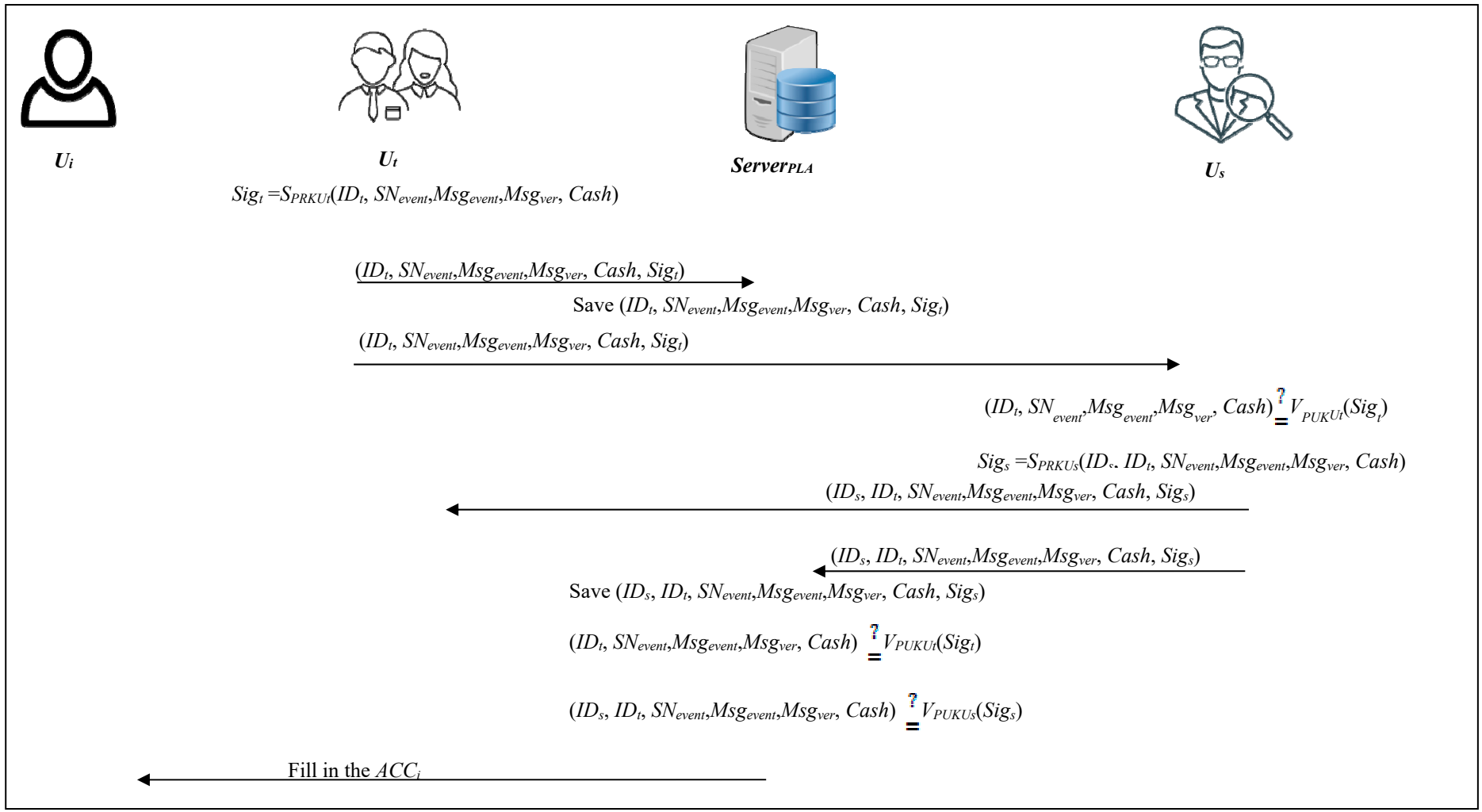


**Figure 5.** The flow chart of the superior verifying phase.

**Step 2**: $\text{Server}_{\text{PLA}}$

When the reporting server receives the signature of the undertaker, the $ID_t$, $SN_{event}$, $Msg_{event}$, $Msg_{ver}$, $Cash$ and $Sig_t$ will be stored in the database.

**Step 3**: $\text{U}_\text{s}\rightarrow\text{Server}_{\text{PLA}}$;$\text{U}_\text{s}\rightarrow\text{U}_\text{t}$

When the superior receives the signature of the investigator, the superior $U_s$ will use the public key $PUK_{Ut}$ of the undertaker $U_t$ to check whether the signature is correct. If it is correct, then the illegal event has passed the undertaker's audit:

$$(ID_t, SN_{event}, Msg_{event}, Msg_{ver}, Cash) \stackrel{?}{=} V_{PUKUt}(Sig_\text{t}) \tag{16}$$

At this point, the superior $U_s$ audits the case checked by the investigator $U_t$ again. If the superior agrees to issue the reward, then the case will be decided by signature. The reporting server will then request that the superior $U_s$ insert the IC card and enter the PIN code. If the PIN code is correct, the superior will use the IC card private key $PRK_{Us}$ to sign the case:

$$Sig_s = S_{PRKUs}(ID_s, ID_t, SN_{event}, Msg_{event}, Msg_{ver}, Cash) \tag{17}$$

The superior then sends $ID_s$, $ID_t$, $SN_{event}$, $Msg_{event}$, $Msg_{ver}$, $Cash$ and $Sig_s$ to the reporting server and the investigator.

However, reward amounts differ from case to case. When the superior thinks the case requires further evaluation, this means the reward amount is higher than the superior thought. The superior thus sends $ID_s$, $ID_t$, $SN_{event}$, $Msg_{event}$, $Msg_{ver}$, $Cash$ and $Sig_s$ to the upper superior to audit. The upper superior will follow the above steps to audit the case.

**Step 4**: $\text{Server}_{\text{PLA}}\rightarrow\text{U}_\text{i}$

When the reporting server receives the signature of the superior, it will store $ID_s$, $ID_t$, $SN_{event}$, $Msg_{event}$, $Msg_{ver}$, $Cash$ and $Sig_s$ in the database, and then check whether the audited case has been signed one by one. The reporting server uses the investigator's public key $PUK_{Ut}$ to verify the signature $Sig_t$. If it is correct, then the investigator has already audited the case:

$$(ID_t, SN_{event}, Msg_{event}, Msg_{ver}, Cash) \stackrel{?}{=} V_{PUKUt}(Sig_\text{t}) \tag{18}$$

The reporting server then verifies the signature of the superior $U_s$ using the superior's public key $PUK_{Us}$ to verify signature $Sig_s$. If it is correct, then the reward has already been issued by the superior. In addition, if the reporting server receives all superiors' signatures $Sig_s$, it will verify all signatures $Sig_s$ by the following equation:

$$(ID_s, ID_t, SN_{event}, Msg_{event}, Msg_{ver}, Cash) \stackrel{?}{=} V_{PUKUs}(Sig_\text{s}) \tag{19}$$

When the reporting server verifies the signature of the superior, it will automatically transmit a notification to the informer. Therefore, when the informer $U_i$ logs into the platform, s/her will receive a notification to enter his/her the banking details $ACC_i$.

#### 2.2.5. Reward Issuing Phase

When the informer logs into the system and receives a remittance notification from the reporting server, the informer must fill in the remittance account within the effective period, beyond which the reward will not be issued. The reporting server will remit the reward through the designated payment server according to the existing remittance mechanism of the cooperating financial institution. Steps (1)–(4) describe the reward issuing process. The flow chart of reward issuing is shown in Figure 6.

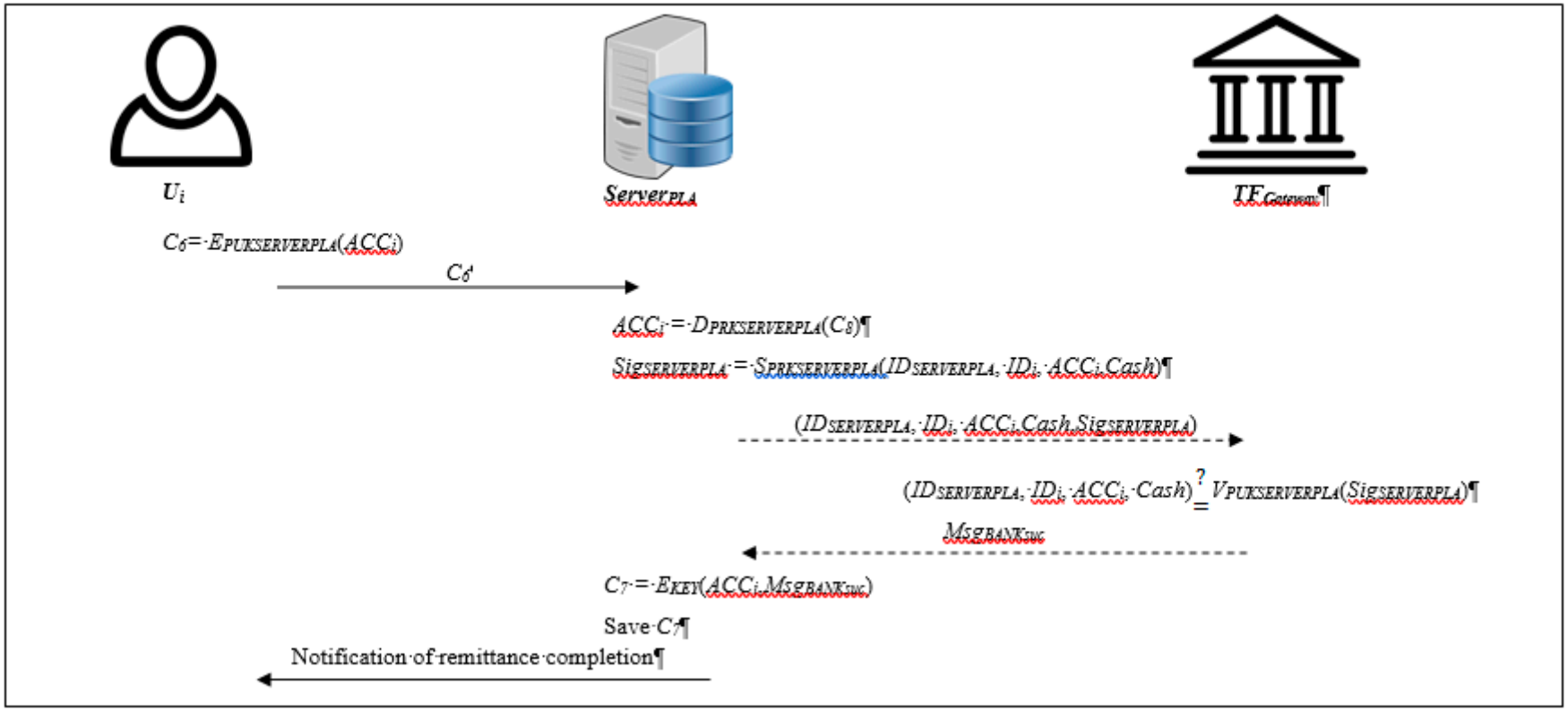


**Figure 6.** The flow chart of the reward issuing phase.

**Step 1**: $U_i \rightarrow Server_{PLA}$

The informer $U_i$ logs into the system and receives a remittance notification, and then enters the bank account $ACC_i$. $Server_{PLA}$ uses the public key $PUK_{SERVERPLA}$ to encrypt the bank account $ACC_i$ and sends the encrypted message $C_8$ to the reporting server:

$$C_6 = E_{PUKSERVERPLA}(ACC_i) \tag{20}$$

**Step 2**: $Server_{PLA} \rightarrow TF_{Gateway}$

The reporting server receives $C_8$ from the informer $U_i$, then $Server_{PLA}$ uses the private key $PRK_{SERVERPLA}$ to decrypt $C_8$, and obtain the bank account $ACC_i$ of $U_i$:

$$ACC_i = D_{PRKSERVERPLA}(C_6) \tag{21}$$

The $Server_{PLA}$ then uses its private key $PRK_{SERVERPLA}$ to sign the remittance information:

$$Sig_{SERVERPLA} = S_{PRKSERVERPLA}(ID_{SERVERPLA}, ID_i, ACC_i, Cash), \tag{22}$$

and sends the remittance information and signature to the designated cooperating payment server $TF_{Gateway}$, and starts the payment.

**Step 3**: $TF_{Gateway} \rightarrow Server_{PLA}$

When the payment server $TF_{Gateway}$ receives the remittance information and signature $Sig_{SERVERPLA}$, it uses the server's public key $PUK_{SERVERPLA}$ to verify the signature:

$$(ID_{SERVERPLA}, ID_i, ACC_i, Cash) \stackrel{?}{=} V_{PUKSERVERPLA}(Sig_{SERVERPLA}) \tag{23}$$

If the verification is successful, the server will issue the reward to the informer $U_i$, and send a message $Msg_{BANKsuc}$ to the reporting server.

**Step 4**: $Server_{PLA} \rightarrow U_i$

When the reporting server receives the reply message $Msg_{BANKsuc}$ of remittance from the cooperating payment server $TF_{Gateway}$, the server will verify the remittance information. If it is correct, then the remittance has been successful. After this, the server will send a message to inform the informer $U_i$ that the reward has been remitted to the designated account. Finally, the reporting server uses the symmetric key $KEY$ of $Server_{PLA}$ to encrypt $ACC_i$ and $Msg_{BANKsuc}$, and then stores the encrypted message $C_9$ in the database:

$$C_7 = E_{KEY}(ACC_i, Msg_{BANKsuc}) \tag{24}$$

#### 2.2.6. The Judgment of and Punishment for Abusing the System

If a report is judged by the investigator $U_t$ to be abuse of the system, the report will be sent upward to the superior $U_s$ for further evaluation. When the reporting server receives confirmation from all the superiors that the report is abuse, it will suspend the informer, denying them access to the system for a period of time. If the user repeatedly abuses the system, and reaches the maximum threshold of abuse instances, the informer will be permanently banned from the system. On the other hand, as long as one superior $U_s$ confirms that the requires further evaluation, the reporting server will assign it to another investigator to re-check. This not only prevents bad judgments, but also prevents cases being erased.

## 3. System Implementation

### *3.1. Hardware and Software Environment*

1. IC Reader, personal identity IC card
2. Apache

3. PHP (Personal Home Page)
4. Mysql
5. Microsoft Windows Server

### *3.2. Implementation*

#### 3.2.1. Registration Phase

In the registration phase, the user can click the register button and enter the registration page, as shown in Figure 7. On this page the user must enter his/her account and password for registration. The system will then ask the user to insert his/her personal identity IC card and enter his/her PIN code, as shown in Figure 8. If the PIN code is correct, the system will send the SN to the certificate authority center via SSL (Secure Socket Layer) secure channel, and verify the user's identity. If the verification result is correct, then the registration is complete.

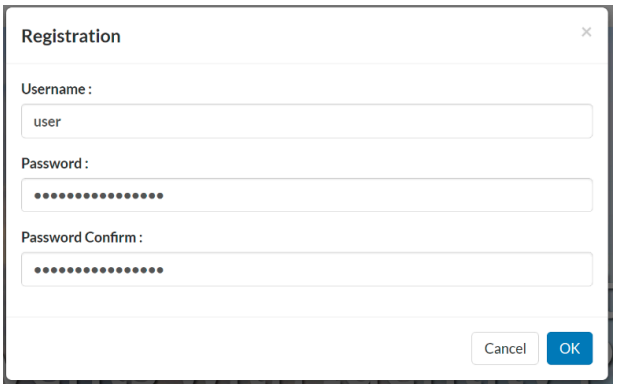


**Figure 7.** Resistration.


**Figure 8.** Integrated Circuit card verification.

#### 3.2.2. Login Phase

After the user (informer, investigator, superior) completes the registration, s/he can log into the reporting system by entering his/her account and password, as shown in Figure 9.


**Figure 9.** Login page.

### 3.2.3. Reporting Phase

The informer can fill in the crime report form, inquire about the progress of cases, or modify personal data when logged into in the system. Figure 10 shows the flowchart of the reporting process. To report a crime, the informer selects the "Report" option, as shown in Figure 11 and fills out the form, as shown in Figure 12. When the informer submits the report form, the system asks the informer to insert his/her identity IC card (as shown in Figure 13) to verify his/her identity. If his/her identity is verified, the reporting procedure is completed.

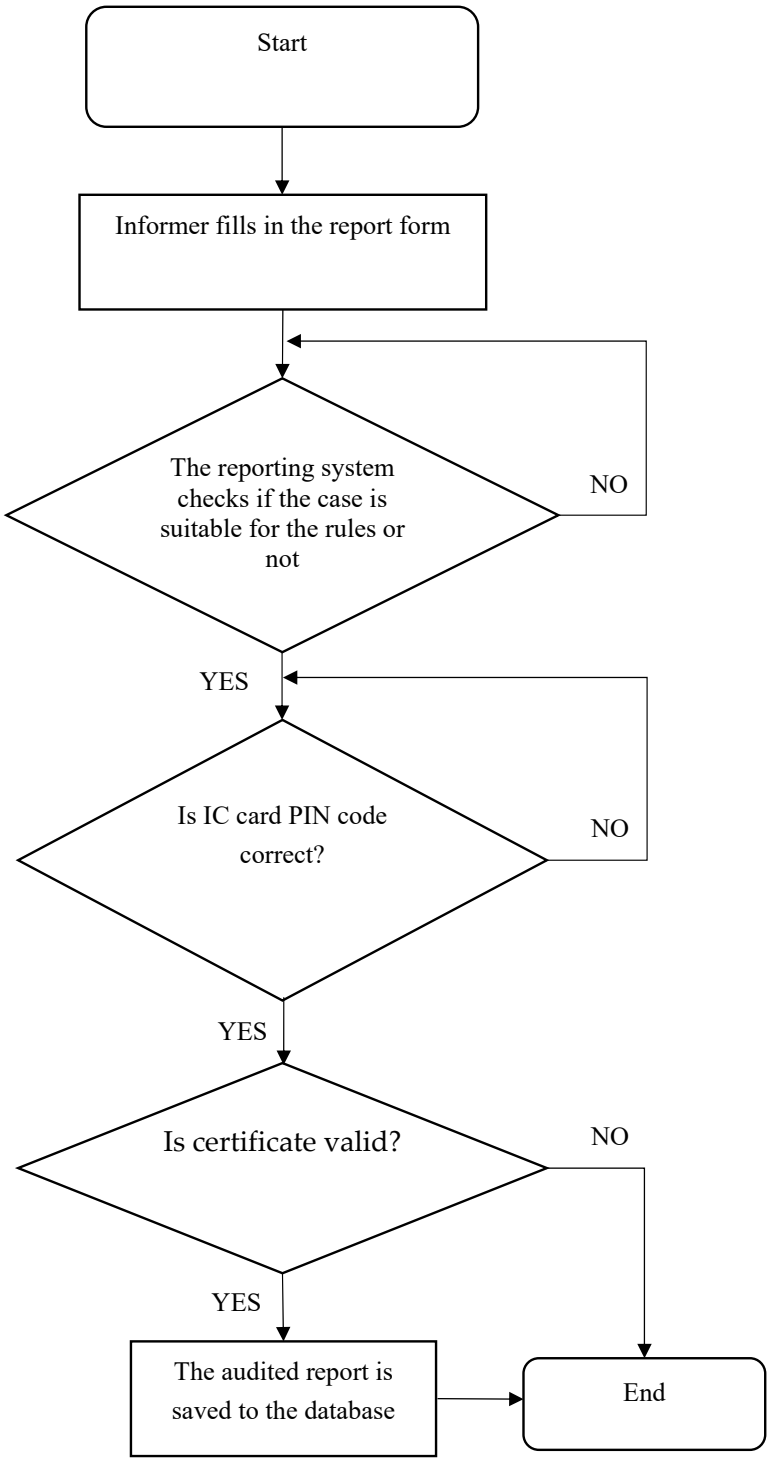


**Figure 10.** Flowchart of informer's reporting Figure 7 Registration process form.

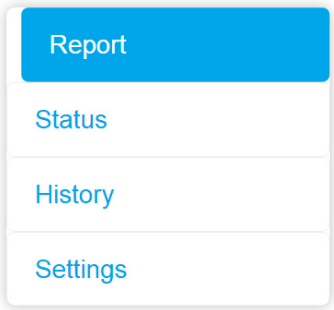


**Figure 11.** Informer menu page.

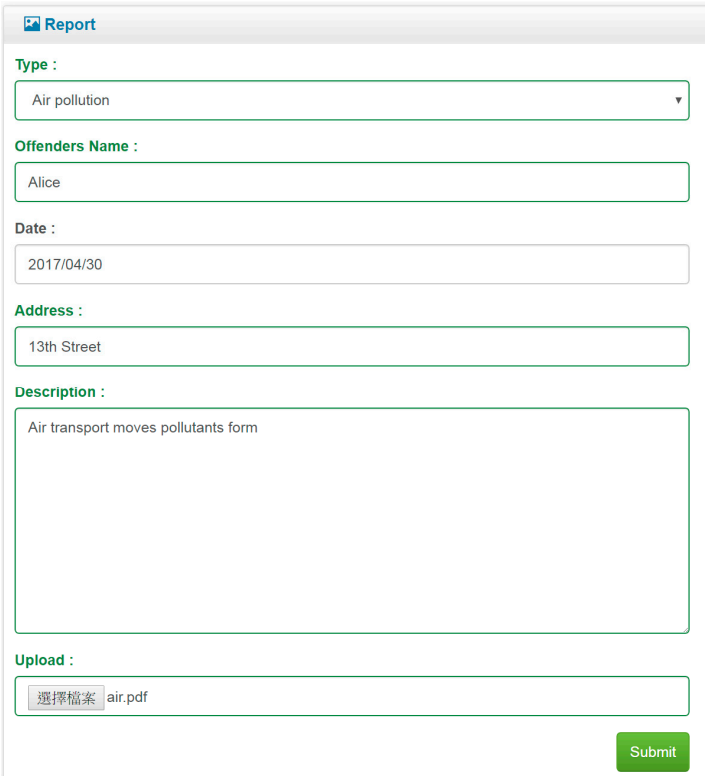


**Figure 12.** Report form.


**Figure 13.** Informer IC card verification page.

### 3.2.4. Contracting the Events

The flowchart of the investigator's auditing process is shown in Figure 14. Figure 15 shows the main investigator page. The investigator can click the "pending" button in the menu of Figure 16 to check all cases pending investigation. All the pending cases are randomly assigned by the system to investigators. Figure 17 shows the list of pending cases. Clicking the last column of each case will open the auditing page, which shows the details for each case (see Figure 18). There are three notification choices in Figure 18 to indicate the auditing result. The meanings of these three choices are detailed as follows:

(1) 【Abuse】button: If the reported case is not within the scope of contracting, or the reported content is not real, this choice will be used to report it to the system.
(2) 【Reward】button: If the reported case is verified as real and must be rewarded, clicking the button will authorize the reward being issued.
(3) 【Closed】button: If the reported case is verified as real and without reward, then clicking this button closes the case.

When the auditing result is submitted, the system will verify the IC card of the investigator, as shown in Figure 19.

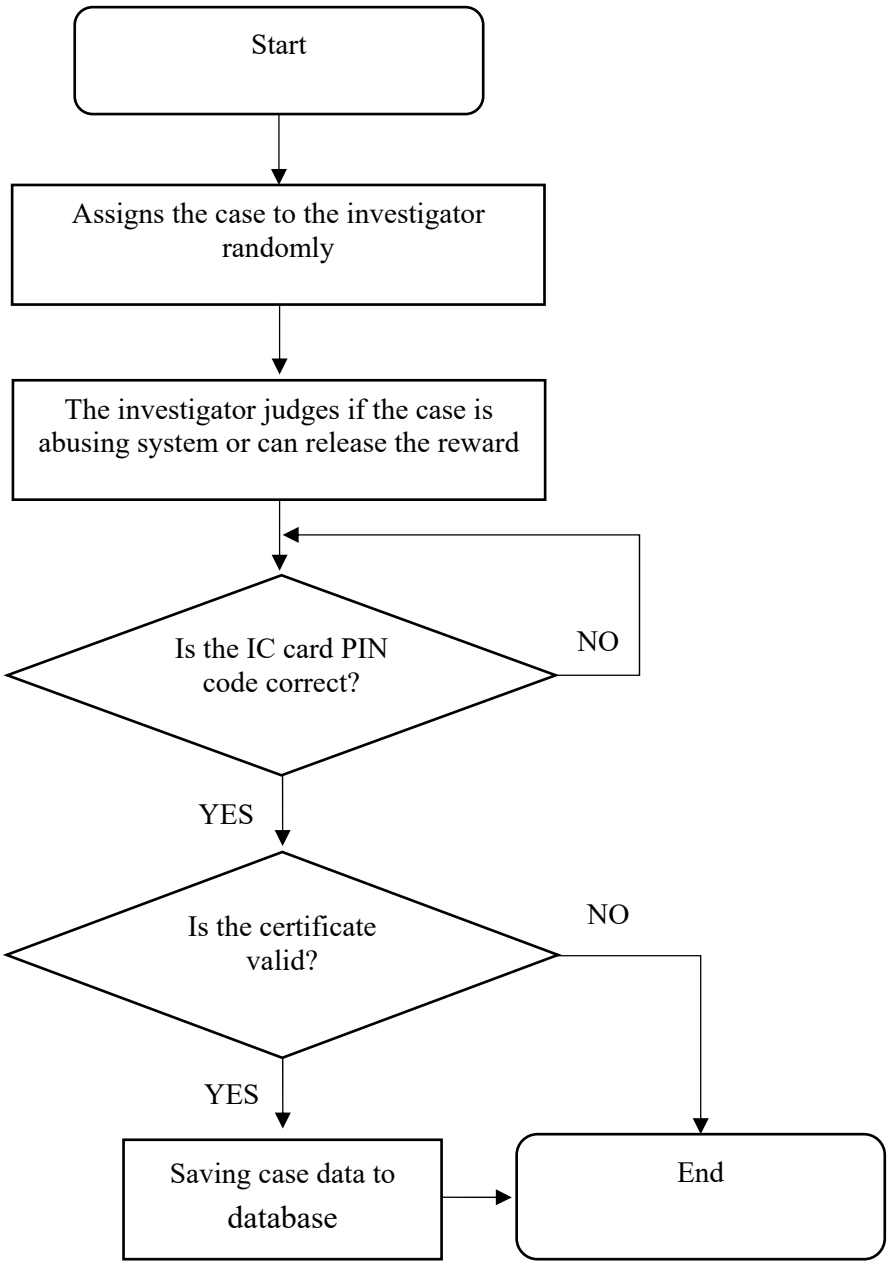


**Figure 14.** Flowchart of investigator's auditing process.

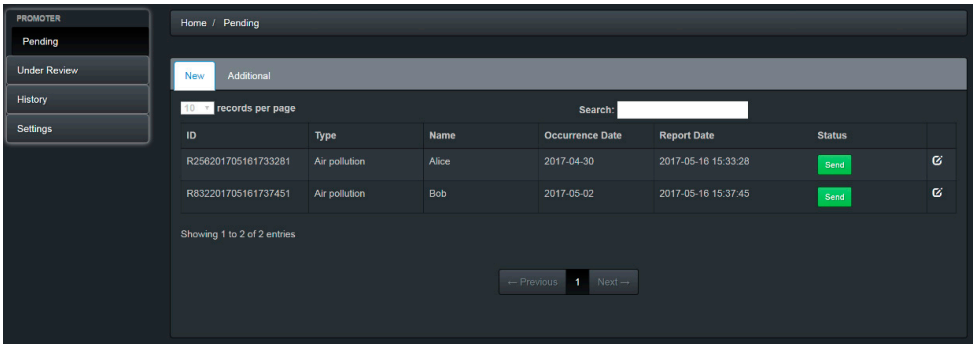


**Figure 15.** The main investigator page.

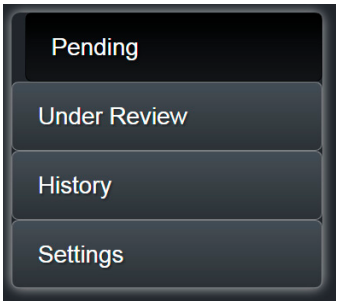


**Figure 16.** Investigator menu page.

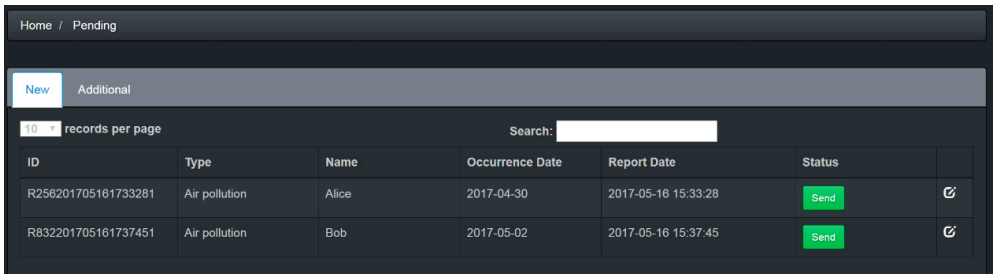


**Figure 17.** List of the pending cases for investigators.

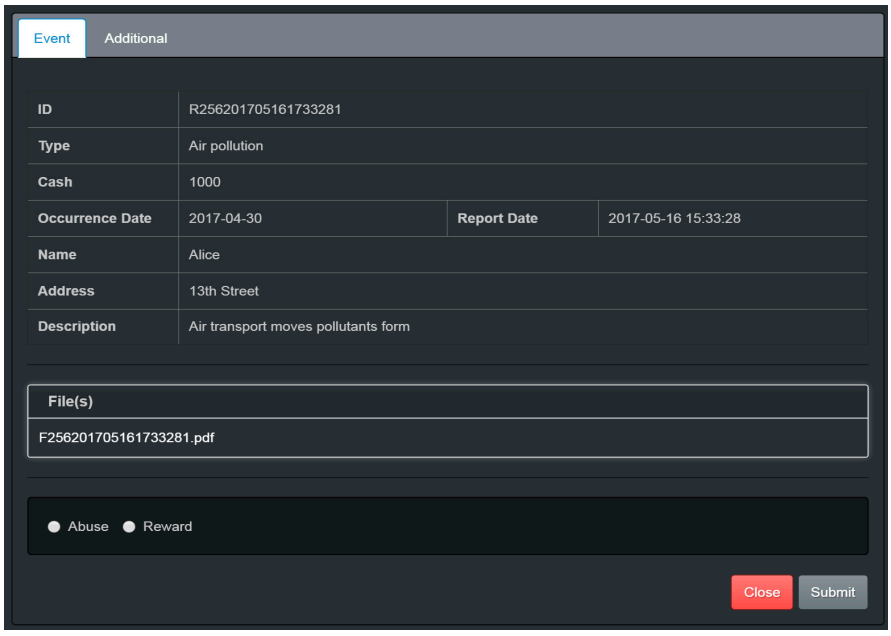


**Figure 18.** Auditing page of pending case for investigator.

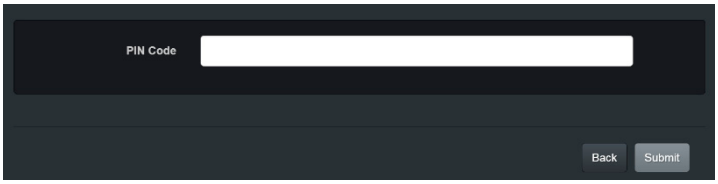


**Figure 19.** Investigator IC card verification page.

### 3.2.5. Upper Superior

Figure 20 shows the flowchart of the superior's auditing process. The flowchart of the reward issuing process is shown in Figure 21. Figure 22 shows the main page when the superior logs into the system. On this page, the superior can check audited cases, and whether the cases are over time. If a case has not been audited by an investigator within the specified time, the system will automatically report it to the upper superior. The superior can select the "Expired" item in Figure 23 to recheck or reassign the expired case. In addition, the superior can click the "Pending" button to review audited abuse or reward cases, as shown in Figure 24.

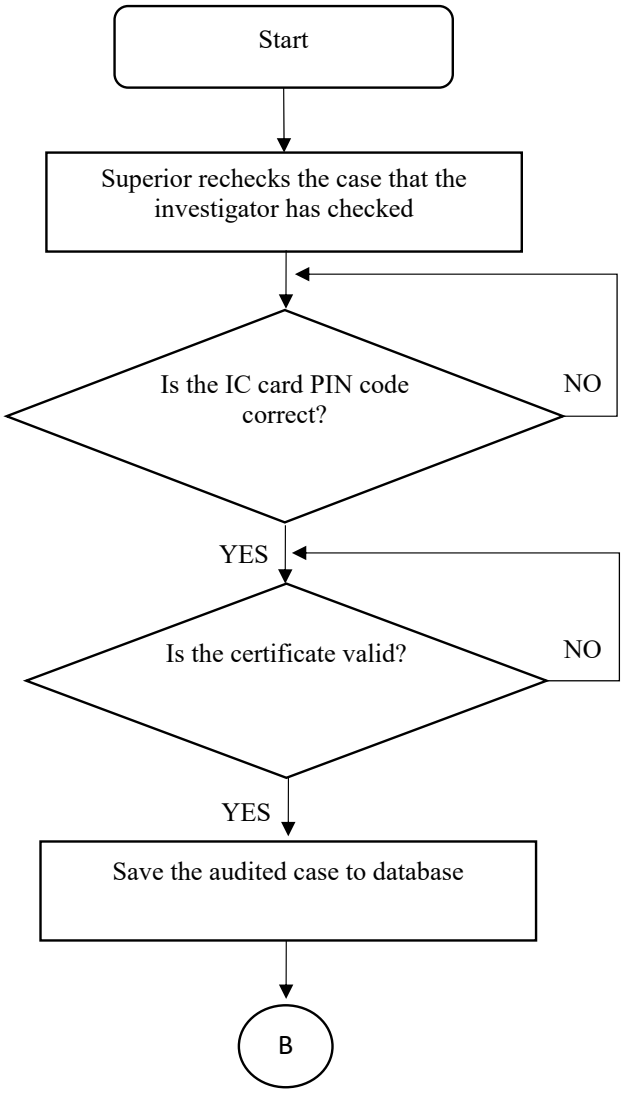


**Figure 20.** Flowchart of superior's auditing process.

The Reward button is on the reward page, and the Abuse and Retrial buttons are on the abuse page. The functions of the three items are as follows:

1. 【Reward】: When the reward has been confirmed for issue, the superior clicks the 【Reward】button, as shown in Figure 25.
2. 【Abuse】: When the superior clicks the 【Abuse】 button in Figure 26, this means the case is an abusive reporting case.
3. 【Retrial】: When a case is in doubt, it must be re-investigated. Such cases are called "retrial cases" and will be randomly assigned to a new investigator. The upper superior can designate a case in which there is cause for doubt as a retrial case by pressing the 【Retrial】 button, shown in Figure 26. The system will automatically reassign the retrial case to another investigator.

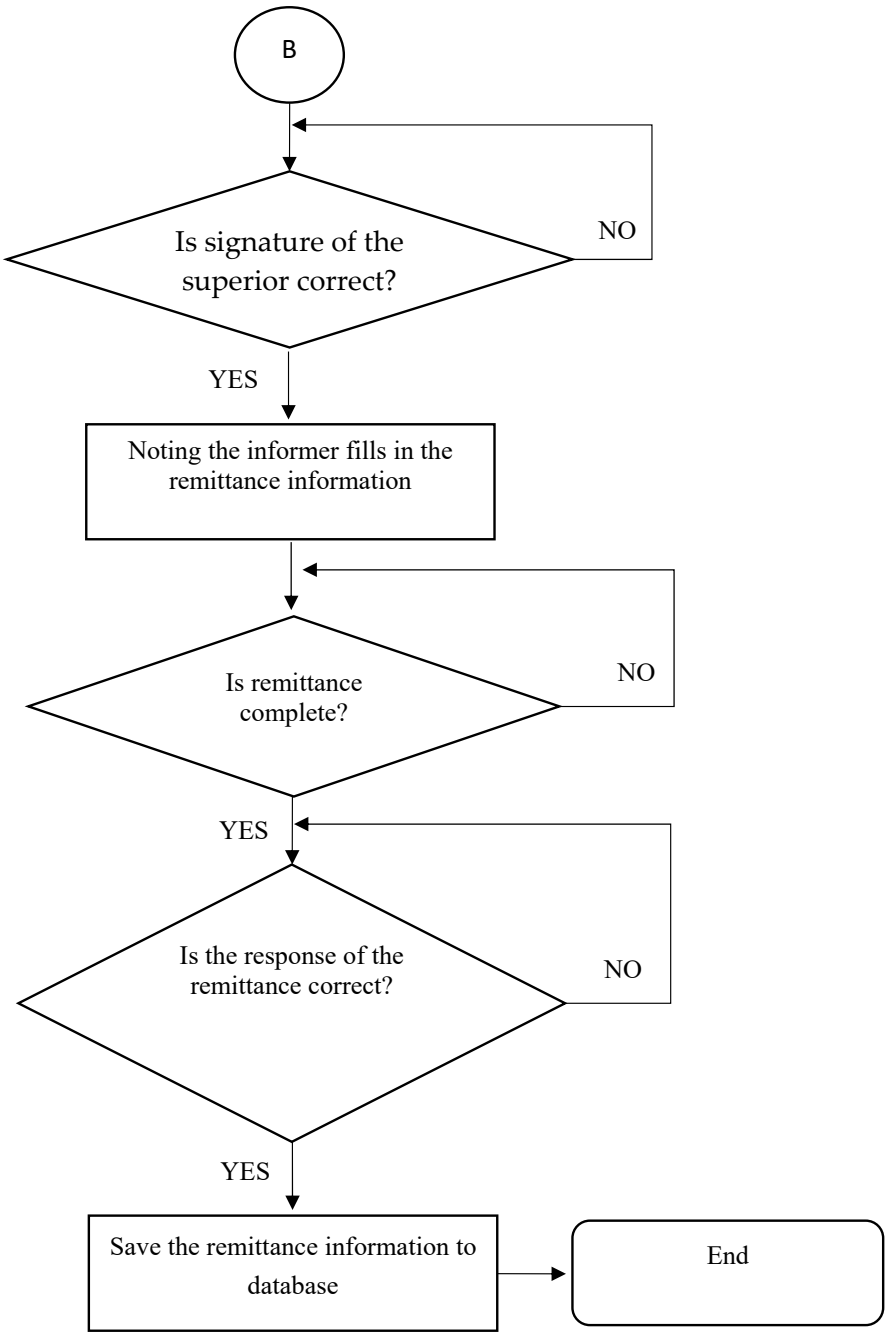


**Figure 21.** Flowchart of reward issuing process.

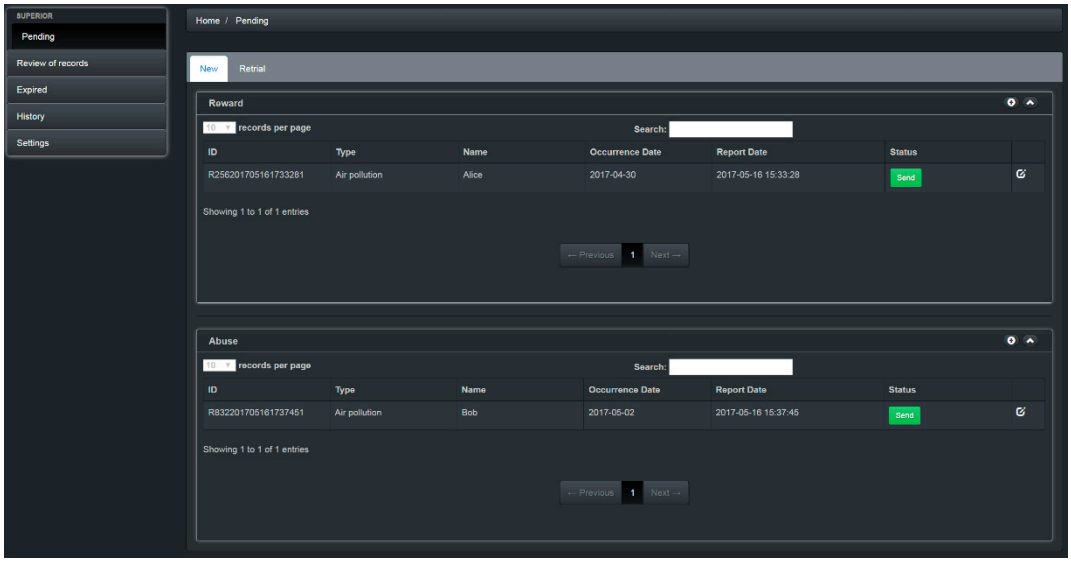


**Figure 22.** The main page of the superior.

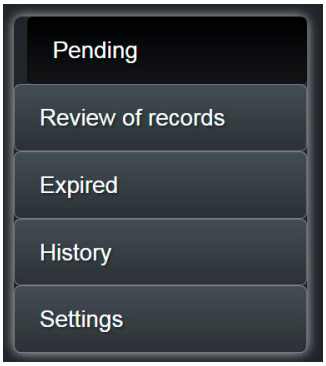


**Figure 23.** Menu of the superior page.

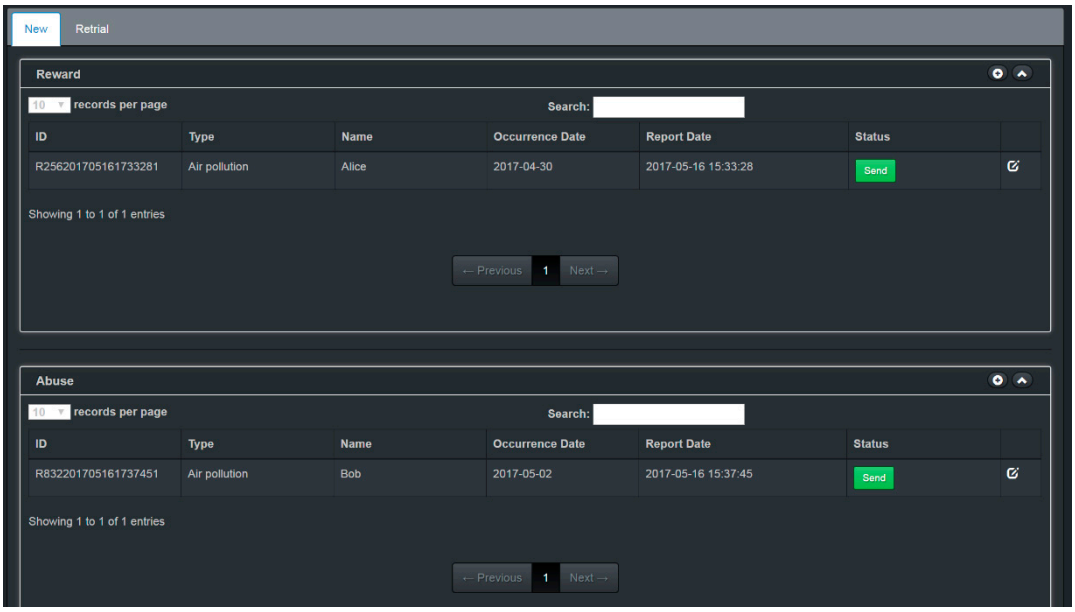


**Figure 24.** List of pending cases for superior.

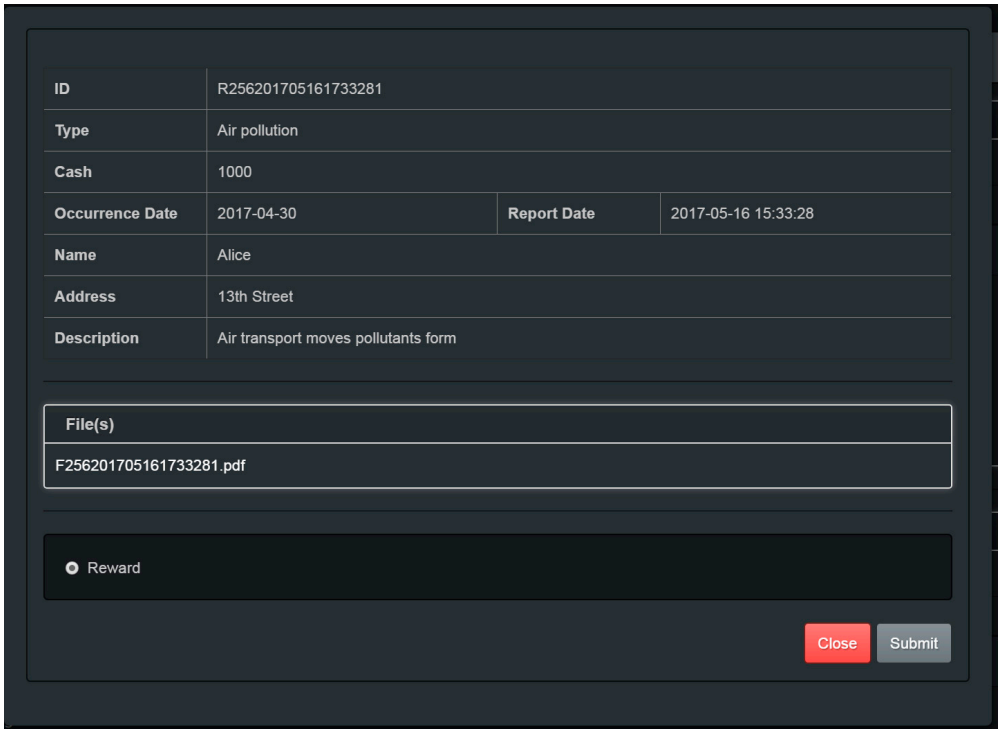


**Figure 25.** Reward audit page of superior.

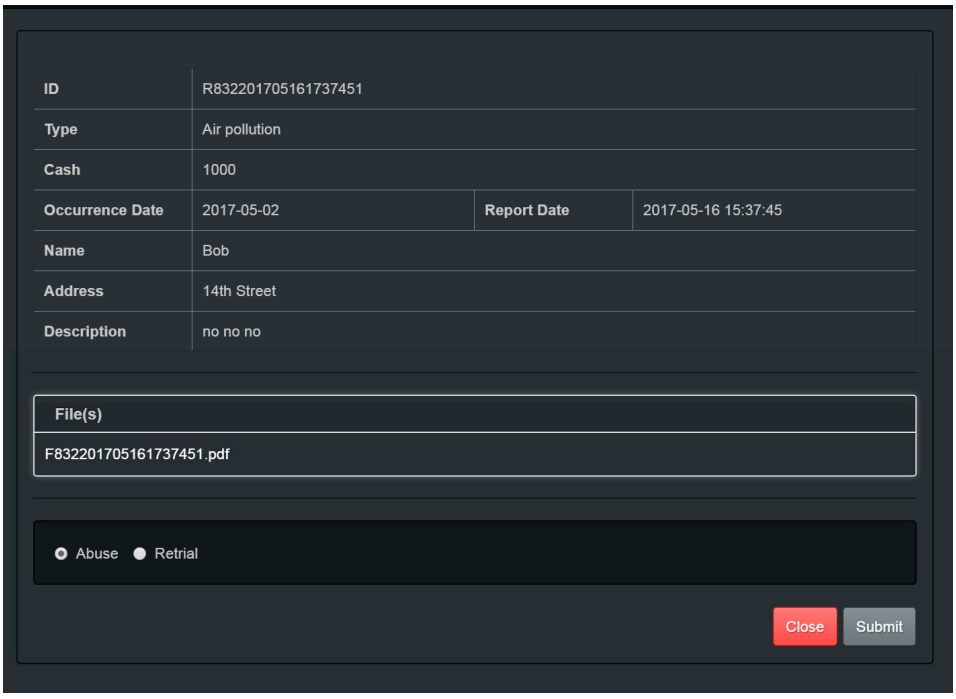


**Figure 26.** Abuse and retrial audit page of superior.

## 4. Discussion

### *4.1. The Identity of the Informer*

To ensure the legality of the user' identity, the system will verify the informer's account $ID_i$ and password $PW_{HASH}$ when the informer logs into the system:

$$C_2 = E_{PUKSERVERPLA}(ID_i, PW_{HASH}) \quad (25)$$

$$(ID_i, PW_{HASH}) = D_{PRKSERVERPLA}(C_2) \tag{26}$$

Moreover, when the informer reports a crime, the informer must have an IC card. The system will obtain the SN and the last four digits of *IDNO* from the informer's IC card. The SN will then be sent to $Server_{CA}$ via SSL secure channel for verification:

$$C_4 = E_{PUKSERVERPLA}(IDNO, SN) \tag{27}$$

$$(IDNO, SN) = D_{PRKSERVERPLA}(C_4) \tag{28}$$

**Scenario**: Malicious users may continue to make false reports in an attempt to crash the reporting system's server.

**Analysis**: The attack will fail because when an informer reports a crime; s/he must use their physical ID card, which includes the serial number SN and the ID number *IDNO* of the IC card. When the number of malicious reports exceeds the system threshold, the user's reporting permission will be suspended. The proposed scheme can thus protect legal users' identities from being abused, and can also prevent malicious reporting behavior.

### *4.2. Anonymous Reporting*

In the reporting procedure, the system verifies the informer's identity by certificate authority center so that the informer does not have to fill in personal information. When the center has checked the identity, it generates a case number. The content and $ID_i$ will be encrypted and stored in the database:

$$C_5 = E_{KEY}(ID_i) \tag{29}$$

Therefore, the crime reports are stored in the database in such a way that the identity of informers is protected.

**Scenario**: If an informer's true identity is leaked during the reporting process, his/her safety may be at risk as a result.

**Analysis**: Any attempt to obtain an informer's the true identity will fail, as in the proposed scheme, the key message is encrypted with the asymmetric key of the reporting server. Only the legal reporting server can know the true identity of the informer. Therefore, malicious users will not be able to obtain the true identity of the informer and threaten their safety.

### *4.3. The Integrity of the Data*

1. The reporting server uses the following formula to confirm whether the case has been reported by the informer him/herself:

$$(ID_i, Msg_{event}) \stackrel{?}{=} V_{PUKUi}(Sig_i) \tag{30}$$

**Scenario**: Malicious users may try to intercept the report in order to modify its content.

**Analysis**: The attack will fail because the message is encrypted with the public key of the reporting server $C_3 = E_{PUKSERVERPLA}(ID_i, Msg_{event})$, and signed with the private key of the informer $Sig_i = S_{PRKUi}(ID_i, Msg_{event})$. Thus, malicious users cannot modify report content.

2. An investigator attaches their signature when a case has been audited. The following formula can then be used to verify the signature to ensure the case is signed by the investigator correctly:

$$(ID_t, SN_{event}, Msg_{event}, Msg_{ver}) \stackrel{?}{=} V_{PUKUt}(Sig_t) \tag{31}$$

**Scenario**: Malicious users may try to intercept the investigator's audit results in order to modify them.

**Analysis**: The attack will fail because the message is signed with the private key of the investigator $Sig_t = S_{PRKUt}(ID_t, SN_{event}, Msg_{event}, Msg_{ver}, Cash)$. Thus, malicious users cannot modify audit results.

3. The reporting server can ensure that the reward is issued by the superior using the following equation:

$$(ID_s, ID_t, SN_{event}, Msg_{event}, Msg_{ver}) \stackrel{?}{=} V_{PUKUs}(Sig_s) \quad (32)$$

**Scenario**: Malicious users may try to intercept the reward information from the superior in order to modify it.

**Analysis**: The attack will fail because the message is signed with the private key of the superior $Sig_s = S_{PRKUs}(ID_s, ID_t, SN_{event}, Msg_{event}, Msg_{ver}, Cash)$. Thus, malicious users cannot modify the reward information.

### *4.4. Non-Repudiation*

In order to ensure non-repudiation, the proposed system has a completion verification mechanism, as shown in Table 1, which achieves non-repudiation as follows:

- The reporting server will verify the informer's signature $Sig_i$; therefore, the informer cannot deny the signature.
- The reporting server will verify the investigator's signature $Sig_t$; therefore, the investigator cannot deny the signature.
- The superior receives the $Sig_t$ of a reward case form an investigator, and the superior will verify the $Sig_t$; therefore, the investigator cannot deny the signature.
- The reporting server receives the $Sig_s$, which means the superior agrees to issue the reward; therefore, the superior cannot deny that they confirmed the reward.
- The cooperating payment server will receive the $Sig_{SERVERPLA}$ issued by the reporting server; therefore, the reporting server cannot deny that it confirmed the reward.

**Table 1.** The verifiable proofs of non-repudiation.

| Evidence | Evidence Issuer | Evidence Holder | Verification Equation |
|---|---|---|---|
| $(C_3, Sig_i)$ | $U_i$ | $Server_{PLA}$ | $(ID_i, Msg_{event}) = D_{PRKSERVERPLA}(C_3)$ $(ID_i, Msg_{event}) \stackrel{?}{=} V_{PUKUi}(Sig_i)$ |
| $(ID_t, SN_{event}, Msg_{event}, Msg_{ver}, Cash, Sig_t)$ | $U_t$ | $Server_{PLA}$ | $(ID_t, SN_{event}, Msg_{event}, Msg_{ver}, Cash) \stackrel{?}{=} V_{PUKUt}(Sig_t)$ |
| $(ID_t, SN_{event}, Msg_{event}, Msg_{ver}, Cash, Sig_t)$ | $U_t$ | $U_s$ | $(ID_t, SN_{event}, Msg_{event}, Msg_{ver}, Cash) \stackrel{?}{=} V_{PUKUt}(Sig_t)$ |
| $(ID_s, ID_t, SN_{event}, Msg_{event}, Msg_{ver}, Cash, Sig_s)$ | $U_s$ | $Server_{PLA}$ | $(ID_s, ID_t, SN_{event}, Msg_{event}, Msg_{ver}, Cash) \stackrel{?}{=} V_{PUKUs}(Sig_s)$ |
| $(ID_{SERVERPLA}, ID_i, ACC_i, Cash, Sig_{SERVERPLA})$ | $Server_{PLA}$ | $TF_{Gateway}$ | $(ID_{SERVERPLA}, ID_i, ACC_i, Cash) \stackrel{?}{=} V_{PUKSERVERPLA}(Sig_{SERVERPLA})$ |

### *4.5. Preventing the Case Being Erased*

The proposed system is equipped with an automatic notification mechanism to prevent investigators ignoring cases. If an investigator does not audit a case within a default period of time, the reporting server will automatically send the case to an upper superior.

### *4.6. Secure Reward Issuing*

The secure issuing of the reward is shown in Figure 27, and the processes are as follows:

(1) Auditing phase:

The $U_t$ and $U_S$ send $Sig_t$ and $Sig_s$ to $Server_{PLA}$, respectively:

$$Sig_t = S_{PRKUt}(ID_t, SN_{event}, Msg_{event}, Msg_{ver}, Cash) \quad (33)$$

$$Sig_s = S_{PRKUs}(ID_s, ID_t, SN_{event}, Msg_{event}, Msg_{ver}, Cash) \quad (34)$$

$Server_{PLA}$ can verify each signature of the superior by the following equations:

$$(ID_t, SN_{event}, Msg_{event}, Msg_{ver}, Cash) \stackrel{?}{=} V_{PUKUt}(Sig_t) \quad (35)$$

$$(ID_s, ID_t, SN_{event}, Msg_{event}, Msg_{ver}, Cash) \stackrel{?}{=} V_{PUKUs}(Sig_s) \quad (36)$$

According to Formulae (39) and (40), only if the signature verification is successful will the $Server_{PLA}$ instruct the $U_i$ to enter the remittance account.

**Scenario**: The informer attempts to modify the survey results, change the survey failure to success, or change the reward amount.

**Analysis**: The attack will fail to modify the survey results or reward information because the message is signed with the private key of the investigator $Sig_t = S_{PRKUt}(ID_t, SN_{event}, Msg_{event}, Msg_{ver}, Cash)$ and superior $Sig_s = S_{PRKUs}(ID_s, ID_t, SN_{event}, Msg_{event}, Msg_{ver}, Cash)$. The reporting server will verify $(ID_t, SN_{event}, Msg_{event}, Msg_{ver}, Cash) \stackrel{?}{=} V_{KUt}(Sig_t)$ and $(ID_s, ID_t, SN_{event}, Msg_{event}, Msg_{ver}, Cash) \stackrel{?}{=} V_{KUs}(Sig_s)$. Thus, the informer cannot modify the survey results or reward information.

(2) Remitting phase:

When $U_i$ receives the notice from $Server_{PLA}$, $U_i$ provides the remittance account $ACC_i$. Then, the account $ACC_i$ is encrypted by Formula (41) and the encryption $C_8$ is sent to $Server_{PLA}$. When the reporting server $Server_{PLA}$ receives $C_8$, it decrypts $C_8$ by Formula (42) to obtain the $ACC_i$ of the $U_i$:

$$C_6 = E_{PUKSERVERPLA}(ACC_i) \quad (37)$$

$$ACC_i = D_{PRKSERVERPLA}(C_6) \quad (38)$$

Then, $Server_{PLA}$ signs the remittance information by Formula (43) and sends it to the $TF_{Gateway}$ via SSL, and begins the payment:

$$Sig_{SERVERPLA} = S_{PRKSERVERPLA}(ID_{SERVERPLA}, ID_i, ACC_i, Cash) \quad (39)$$

$$(ID_{SERVERPLA}, ID_i, ACC_i, Cash) \stackrel{?}{=} V_{PUKSERVERPLA}(Sig_{\mathrm{SERVERPLA}}) \quad (40)$$

The server uses Formula (44) to verify the signature. If the signature is correct, the cooperating payment server will remit to the $U_i$, and then send the completed message to the $Server_{PLA}$, thus preventing an incorrect amount being paid, or payment being made to the wrong person.

From the above analysis, the reward mechanism cannot be corrupted or altered. Therefore, it ensures the security of the identity of the informer. In addition, the system uses an automatic remittance mechanism. The signature mechanism ensures the identity of the superior, and this mechanism therefore not only ensures the identity, but also the confirmation of the reward. This shows that the system uses digital signatures, asymmetric key, and SSL to achieve the remittance operations.

**Scenario**: Malicious users attempt to modify the bank account information, and try to get the rewards of the informer.

**Analysis**: The attack will fail because the message is signed with the private key of the reporting server $Sig_{SERVERPLA} = S_{PRKSERVERPLA}(ID_{SERVERPLA}, ID_i, ACC_i, Cash)$. After the designated cooperating payment server $TF_{Gateway}$ receives the message via secure channel, it will verify $(ID_{SERVERPLA}, ID_i, ACC_i, Cash) \stackrel{?}{=} V_{PUKSERVERPLA}(Sig_{SERVERPLA})$. Thus, the attacker cannot modify the bank account information to get the rewards.

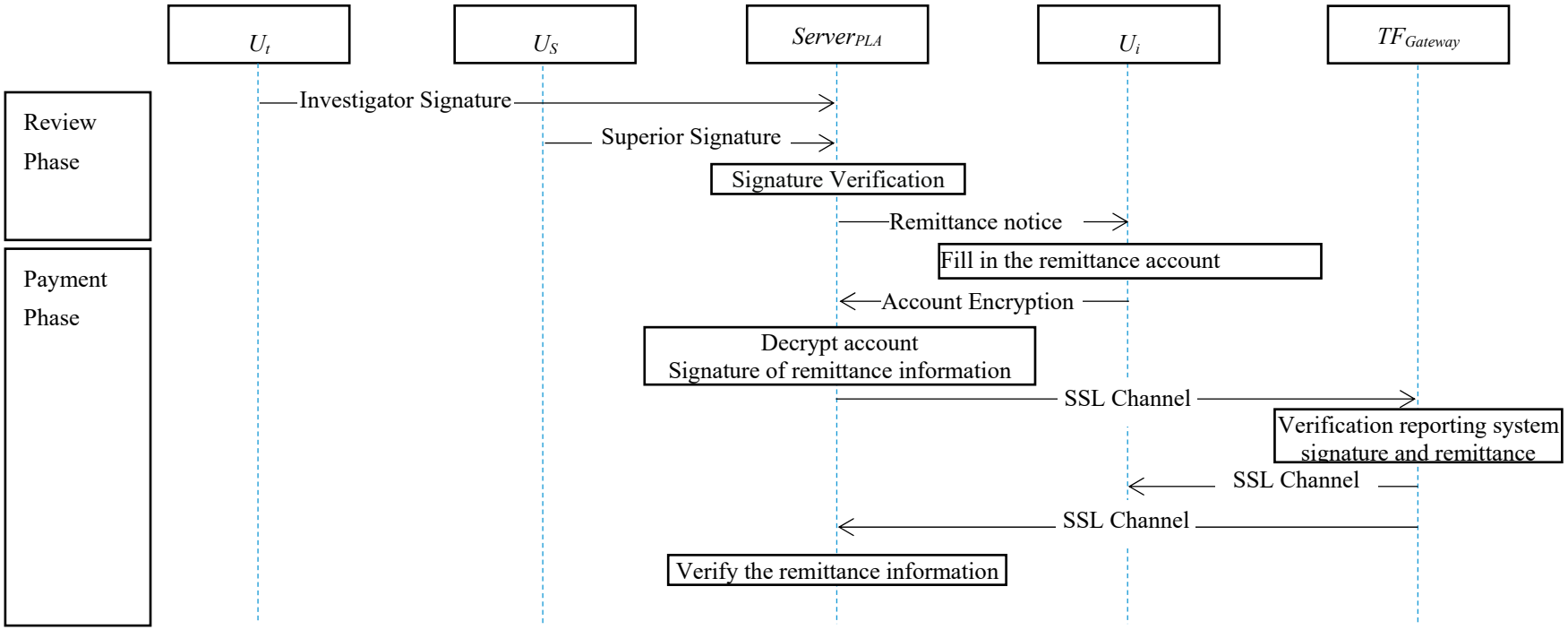


**Figure 27.** The flowchart of the reward payment phase.

### *4.7. Untraceability*

In order to protect the privacy of informers in any actions, the proposed system uses a symmetric key algorithm to encrypt its database, further protecting the identity of the informer:

$$C_5 = E_{KEY}(ID_i) \tag{41}$$

### *4.8. Confidentiality*

(1) The reporting server uses the SSL security protocol to ensure secure data transmission. In the registration phase, a one-way hash function is used to convert $PW_x$ into $PW_{HASH}$, which prevent user passwords being leaked:

$$PW_{HASH} = H(PW_x) \tag{42}$$

(2) The system encrypts the $ID_i$ of the $U_i$ with the symmetric key of $Server_{PLA}$ to protect the identity of the informer in the event of a database security breach:

$$C_5 = E_{KEY}(ID_i) \tag{43}$$

(3) In the auditing and reward phases, the server uses the asymmetric key of $Server_{PLA}$ to encrypt $ACC_i$, and $Msg_{BANKsuc}$ to protect sensitive informer information:

$$C_7 = E_{KEY}(ACC_i, Msg_{BANKsuc}) \tag{44}$$

### *4.9. Comparison*

The following compares the work in this study with the literature relating to online crime reporting systems with identity protection, as shown in Table 2.

**Table 2.** The comparison of related works.

| | Ku et al. [1] | Iriberri and Leroy [2] | Sakpere et al. [6] | Eugene [7] | The Proposed Scheme |
|---|---|---|---|---|---|
| Authenticity | N/A | N/A | N/A | N/A | YES |
| Anonymous reporting | YES | YES | YES | YES | YES |
| Data integrity | N/A | N/A | YES | YES | YES |
| Non-repudiation | N/A | N/A | NO | N/A | YES |
| Smother a reported case prevention | NO | NO | N/A | NO | YES |
| Untraceable | NO | NO | NO | NO | YES |
| Reward mechanism | NO | NO | N/A | NO | YES |
| Confidentiality | N/A | N/A | N/A | N/A | YES |
| Preclude false reports | NO | NO | NO | NO | YES |
| Theoretical analysis | NO | NO | NO | NO | YES |
| Implementation | YES | NO | YES | YES | YES |

Table 2 shows that [1,2,6,7] respectively proposed an anonymous on-line crime reporting system. However, these systems mostly do not support authentication, data integrity, non-repudiation, prevention of case deletion, untraceability, the reward mechanism, confidentiality, preclusion of false reports and theoretical analysis etc. Thus, the proposed scheme is a more secure and practical reporting system based on cryptography.

## 5. Conclusions

Despite its continued presence in many (if not all) communities, some people are still afraid to report crimes, as they fear for their own safety should their identities become known to those they report. This results in an environment in which it is difficult to combat crime, and in which crime is even more likely to occur. In order to address this problem, this study proposes a cloud-based online crime reporting system with identity protection. The system not only addresses the concern that an informer's identity may be revealed, but in doing so unites communities in combating crime. The proposed system combines digital certificates, encryption and decryption technology, and the credibility of a third party with the necessary certification. Thus it is able to verify informer identities, prevent the exposure of those identities, as well as preventing reports being erased. Using this simple and safe online reporting system, people can safely report criminal activity, thus improving and protecting the quality of life in their communities. The proposed scheme addresses all the security requirements to allow the reporting of crimes, while ensuring informers' safety, security, anonymity and convenience. Furthermore, the proposed scheme is designed to be robust against abusive use, and is able to preclude false reports. Table 2 shows that the proposed method outperforms other related schemes. This study developed the reporting system for testing, and future work will collect data and evaluate its performance for system improvement. Finally, the authors hope that the proposed reporting system will be an effective and widely used tool in the ongoing fight against crime.

**Author Contributions:** Conceptualization, T.-F.S. and B.-Y.S.; validation, C.-L.C. and Y.-Y.D.; writing—original draft preparation, B.-Y.S.; writing—review and editing, T.-F.S., C.-L.C.; supervision, T.-F.S., C.-L.C.

**Acknowledgments:** This research was supported by the Ministry of Science and Technology, Taiwan, R.O.C., under contract numbers MOST 106-2221-E-324-013, MOST 106-2622-E-305-001-CC2 and MOST 103-2632-E-324-001-MY3.

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

## References

1. Ku, C.H.; Iriberri, A.; Leroy, G. Crime Information Extraction from Police and Witness Narrative Reports. In Proceedings of the 2008 IEEE International Conference on Technologies for Homeland Security, Westin Hotel, Waltham, MA, USA, 12–13 May 2008; pp. 12–13.
2. Iriberri, A.; Leroy, G. Natural Language Processing and e-Government: Extracting Reusable Crime Report Information. In Proceedings of the IEEE International Conference on Information Reuse and Integration, Las Vegas, NV, USA, 13–15 August 2007; pp. 221–226.
3. Simon, I.S. The Fear of Reprisal and the Failure of Victims to Report a Personal Crime. *J. Quant. Criminol.* **1988**, *4*, 289–302.
4. Iriberri, A.; Leroy, G.; Garrett, N. Reporting On-Campus Crime Online: User Intention to Use. In Proceedings of the 39th Hawaii International Conference on System Sciences, Kauia, HI, USA, 4–7 January 2006; pp. 1–10.
5. USA.gov-Home. Available online: https://www.usa.gov/ (accessed on 15 May 2018).
6. Sakpere, B.A.; Kayem, A.V.D.M.; Ndlovu, T. A Usable and Secure Crime Reporting System for Technology Resource Constrained Context. In Proceedings of the 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops (WAINA), Gwangiu, Korea, 24–27 March 2015; pp. 424–429.
7. Eugene, F.F. Anonymous Reporting System. U.S. Patent 9135598 B2, 15 September 2015. Available online: https://www.google.com/patents/US9135598 (accessed on 15 February 2019).
8. Sánchez-García, J.; García-Campos, J.M.; Reina, D.G.; Toral, S.L.; & Barrero, F. On-site DriverID: A Secure Authentication Scheme Based on Spanish eID Cards for Vehicular Ad Hoc Networks. *Future Gener. Comput. Syst.* **2016**, *64*, 50–60. [CrossRef]
9. Zwattendorfer, B.; Slamanig, D. The Austrian eID Ecosystem in the Public Cloud: How to Obtain Privacy While Preserving Practicality. *J. Inf. Secur. Appl.* **2016**, *27–28*, 35–53. [CrossRef]

10. Cernian, A.; Olteanu, A.; Mateescu, G.; Vladescu, M.; Stamatescu, G.; Ropot, A.; Plesca, C.; Togan, M.; Sgarciu, V.; Carstoiu, D.; et al. The Design and Implementation of An Experimental Model for Secure Management of Personal Data Based on Electronic Identity Card and PKI Infrastructure. *IFAC Proc. Vol.* **2016**, *45*, 1697–1701. [CrossRef]
11. Bajpai, D.; Vardhan, M.; Gupta, S.; Kumar, R.; Kushwaha, D.S. Security Service Level Agreements Based Authentication and Authorization Model for Accessing Cloud Services. *Adv. Comput. Inf. Technol.* **2012**, *176*, 719–728. [CrossRef]
12. Hwang, J.J.; Chuang, H.K.; Hsu, Y.C.; Wu, C.H. A Business Model for Cloud Computing Based on A Separate Encryption and Decryption Service. In Proceedings of the 2011 International Conference on Information Science and Applications, Jeju Island, Korea, 26–29 April 2011; pp. 26–29.
13. Wang, H.; He, W.; Wang, F.K. Enterprise Cloud Service Architectures. *Inf. Technol. Manag.* **2012**, *13*, 445–454. [CrossRef]
14. Tsai, Y.L. Cloud Computing Security. *Commun. CCISA* **2012**, *18*, 62–68.
15. Karuppiah, M.; Saravanan, R. A Secure Remote User Mutual Authentication Scheme Using Smart Cards. *J. Inf. Secur. Appl.* **2014**, *19*, 282–294. [CrossRef]
16. Maliki, T.E.; Seigneur, J.M. Chapter 4–Online Identity and User Management Services. In *Managing Information Security*, 2nd ed.; Syngress: Rockland, MA, USA, 2014; pp. 75–118.
17. Zhu, B.; Setia, S.; Jajodia, S.; Wang, L. Providing Witness Anonymity Under Peer-to-Peer Settings. *IEEE Trans. Inf. Forens. Secur.* **2010**, *5*, 324–336. [CrossRef]
18. Vigil, M.; Buchmann, J.; Cabarcas, D.; Weinert, C.; Wiesmaier, A. Integrity, Authenticity, Non-repudiation, and Proof of Existence for Long-term Archiving: A Survey. *Comput. Secur.* **2015**, *50*, 16–32. [CrossRef]
19. Sergio, M.; Esther, L.M.; Africa, L.R.; Joaquin, C.; Alexis, M.P.; Manuel, C. Analysis of New Technology Trends in Education: 2010–2015. *IEEE Access* **2018**, *6*, 36840–36848. [CrossRef]
20. Tan, H.; Chung, I. A Secure and Efficient Group Key Management Protocol with Cooperative Sensor Association in WBANs. *Sensors* **2018**, *18*, 3930. [CrossRef] [PubMed]
21. Tan, H.; Choi, D.; Kim, P.; Pan, S.; Chung, I. Secure Certificateless Authentication and Road Message Dissemination Protocol in VANETs. *Wirel. Commun. Mob. Comput.* **2018**, 7978027. [CrossRef]