Authenticating compromisable storage systems

Jiangshan Yu
Interdisciplinary Center for Security, Reliability and Trust
University of Luxembourg
Email: jiangshan.yu@uni.lu

Mark Ryan
School of Computer Science
University of Birmingham
Email: m.d.ryan@cs.bham.ac.uk

Liqun Chen
Department of Computer Science
University of Surrey
Email: liqun.chen@surrey.ac.uk

Abstract—A service may be implemented over several servers, and those servers may become compromised by an attacker, e.g. through software vulnerabilities. When this happens, the service manager will remove the vulnerabilities and re-instate the server. Typically, this will involve regenerating the public key by which clients authenticate the service, and revoking the old one.

This paper presents a scheme which allows a storage service composed of several servers to create a group public key in a decentralised manner, and maintain its security even when such compromises take place. By maintaining keys for a long term, we reduce the reliance on public-key certification. The storage servers periodically update the decryption secrets corresponding to a public key, in such a way that secrets gained by an attacker are rendered useless after an update takes place. An attacker would have to compromise all the servers within a short period lying between two updates in order to fully compromise the system.

Index Terms—Post compromise security, Proactive security, Self-healing system, Authentication, Information security.

I. INTRODUCTION

a) Motivation: Services across the internet authenticate themselves to clients by means of public keys. If a server becomes compromised by an attacker, the attacker may obtain the secret key corresponding to its public key. If this happens, in a real situation, the service manager will eventually become aware of it, and can then shut down the service, repair the damage, and generate a new key pair. The service manager also has to revoke the old public key. In this scenario, clients of this server will need to switch from the old revoked public key to the newly updated key.

This paper introduces a technique which allows a service composed of several servers to create a a service level public key in a decentralised manner in a way that tolerates compromise of the secret key. Specifically, even if the servers that run the service are compromised and the attacker obtains their secrets, the service owner is (in situations satisfying our assumptions) able to re-establish the servers with new secrets, and securely run the service with the same public key as before.

By allowing public keys to survive possible compromises of the services that own them, the technique reduces the reliance on certificate authorities [1], and avoids the complexities and uncertainties of public key revocation. Data storage systems [2], [3], industrial control systems [4], and corporate servers [5] whose clients are other corporate servers are examples of situations in which one could benefit from having long-lived public keys.

We develop these ideas in the context of an enterprise backup service. We assume a platform which offers a storage service provided collectively by a set of independent servers. Each server generates its private/public key pair without requiring recourse to a trusted dealer. A client Alice selects a group of servers, and requests that they collaborate using the protocol of this paper to compute a public key (which we call the “group public key”). The system provides features such that

- Alice can always authenticate the service (and encrypt her backup\(^1\)) by using the fixed group public key that she obtained securely in the initialisation;
- Alice is not required to maintain any decryption key for later data recovery;
- in the event of a disaster that destroys her local data, Alice can recover the encrypted backup by providing her identity to each server;
- Alice can be guaranteed that the outsourced encrypted backup remains secure even if an attacker compromises all the servers over a long time period.

b) Overview of our solution: To apply the technique, we assume that the storage service is composed of several servers. Each server creates a key pair independently. The servers collectively run a protocol to compute a group public key based on the public part of their individual key pairs. We call the secret part of each server’s individual key pair a “share” of the decryption secret w.r.t. their group public key. The full decryption secret is never reconstructed in the protocol.

Time is divided into epochs. At each epoch, the servers engage in a protocol to proactively update their individual key pairs in a way that connects them back to the group public key. In particular, (A) the group public key remains unchanged regardless to the update process ensuring that it can still be authenticated; (B) data encrypted using the fixed group public key can still be decrypted by using the new secrets; and (C) each update renders useless all previously generated shares of the decryption secrets. So, an attacker cannot recover an encrypted data without compromising all servers’ shares of the decryption secrets in the same epoch.

\(^1\)In practice, Alice can use hybrid encryption: she encrypts her backup with a fresh symmetric key, and that symmetric key becomes the data encrypted with the group public key. The symmetric key will be destroyed after the encryption, and Alice is not required to remember any secret.
At any time, one or more of the servers may become compromised by an attacker. In that case, the attacker obtains all the data (including secrets) stored on the server. Our solution ensures that the attacker is not able to perform any decryption, provided that in any epoch at least one of the servers remains uncompromised.

The solution we present requires all the selected servers to participate. At the end of the paper, we discuss how it can be extended to a threshold-based solution.

c) Contribution: We introduce a system which allows a family of servers to maintain decryption secrets corresponding to a group public key, with the following properties:

- The secrets are proactively maintained. This means that the servers periodically engage in a protocol to update the secrets, defending from attackers that could potentially compromise all the servers over a long period.
- The group public key remains fixed, even though the decryption secrets of the servers change in each time period. We achieve this in a simple and decentralised manner without requiring a trusted dealer.
- There is no time during our protocol at which an entire decryption key corresponding to the group public key is generated, stored, reconstructed or used.

We present the system as a self-healing storage service, though this construction can be used as a building block to solve the problem of authenticating a compromisable service in other applications. Self-healing means servers can be attacked and their secrets compromised, but after attacks the service can continue with the same public key as before.

We formalise an adversary model for this kind of system. Since there might be robust malware that cannot be removed from a server, our adversary model allows the adversary to permanently compromise servers. We also define the security of a distributed storage system against our model through a security game. We provide a rigorous formal security proof of the proposed system under the defined security model. Our proof also shows that the proposed scheme provides IND-CCA2 security. Due to space limitations, the security proof is not presented in this paper. We refer readers to our technical report [6] for a fully detailed formal security analysis.

d) Efficiency: The system is also optimal in round communication between a client and a group of servers, i.e. it requires only one round communication per-server in both phases for data encryption/distribution and for data reconstruction, and does not require any client involvement for the periodic update. In addition, it requires only two exponentiation operations on the client side for encryption or decryption.

II. SECURITY MODEL

This section first presents an informal attacker model and security goal, in Section II-A and Section II-B, respectively. It then defines the formal security model in Section II-C.

We consider the scenario that an attacker wants to steal the sensitive data of users on cloud servers, by gradually breaking into servers of the system.

A. Attacker model

Suppose an attacker compromises a server. Then the attacker can fully control the server and has access to all its stored secrets. Suppose sometime later, the maintainer of the server applies software patches and malware removal. Depending on the nature of the compromise, that action might restore the server into a secure state, or it might not.

As shown in Table I, we use $S_{PAC}$ to represent the set of permanently attacker-controlled servers; $S_{TAC}$ to represent the set of temporarily attacker-controlled servers (as illustrated in Figure 2); and $S_{Sec}$ to represent the set of secure servers.

Figure 1 shows the possible transformation between different types of servers. Generally, any secure server in $S_{Sec}$ may become a temporarily attacker-controlled server; any server in $S_{TAC}$ may become a secure server; and any server in $S_{Sec}$ or $S_{TAC}$ may become a permanently attacker-controlled server.

![Figure 1](image-url)  
Fig. 1. A figure presenting the possible transformation between different types of participants.
servers in of Alice, provided the total number of attacker-controlled temporarily attacker-controlled servers in $T_{\text{AC}}$ is less than the number of servers chosen by Alice, i.e. $|S_{\text{PAC}}(T')| + |S_{\text{TAC}}(T)| + |S_{\text{TAC}}(T')| < |S_{\text{Alice}}|.$

Remark 1: Loosely speaking, it says that the system should be secure if the total number of compromised servers in any epoch is less than the number of servers chosen by Alice. Note that $S_{\text{PAC}}(T)$ is the set of permanently compromised servers at epoch $T$, and these servers will be included in the set of permanently compromised servers in future epochs as well. So we have $|S_{\text{PAC}}(T)| < |S_{\text{PAC}}(T')|$. However, this is not true for $S_{\text{TAC}}(\cdot)$.

C. Formal Model

We first define the scenario we are considering, i.e. attackers can periodically compromise cloud servers for storage. Then we formally define the ability of an attacker, and the security of a self-healing distributed storage system.

Definition 1: A periodically compromised system environment (PCSE) is an environment in which an attacker can periodically control participants of a protocol. It consists of

1) Protocol II: the underlying security protocol;

2) Security checking oracle $\text{SecurityCheck}(\Pi, S)$: given a server $S \in S$ in protocol II, it outputs a value $V_S$ to indicate if $S$ is compromised. If $V_S = \text{comp}$, then an attacker has compromised $S$; otherwise, $S$ is secure. This models the security status of a server.

3) Security action oracle $\text{SecurityAction}(\Pi, S)$: given a server $S$, it outputs a strategy for $S$ such that if $S$ is a temporarily attacker-controlled server, i.e. $S \in S_{\text{TAC}}$, and it executes the strategy, then the server will become a secure server, i.e. $\text{SecurityCheck}(\Pi, S) = \text{secure}$.

We define our security model through a game with two participants, namely a challenger and a probabilistic polynomial time (PPT) adversary $A$. The attacker’s goal is to win the game that is initialized by the challenger. $A$ is able to ask the following oracle queries.

1) $\mathcal{O}_1$: $\text{Settings}(\Pi)$. By sending this query, $A$ is given all the public parameters of $\Pi$.

2) $\mathcal{O}_2$: $\text{Execute}(\Pi, \mathcal{P})$. Upon receiving this query, the set of participants $\mathcal{P} \subseteq \mathcal{P}$ executes protocol II, if applicable (where $\mathcal{P}$ is the set of all participants, as defined in Table I). The exchanged messages will be recorded and sent to $A$. This oracle query models an attacker’s ability to eavesdrop communications between participants in $\Pi$.

3) $\mathcal{O}_3$: $\text{CreateAttackerControlledClient}(\Pi, C)$. Upon receiving this query with a fresh identity $C$, the oracle creates an attacker-controlled client $C$ in $\Pi$ according to the attacker’s choice. After this query has been made, we have that $C_{\text{AC}} := C_{\text{AC}} \cup \{C\}$. We say an identity is “fresh” if and only if the identity is unique and has not been previously generated. This oracle models an attacker’s ability to register a new client of its choice.

4) $\mathcal{O}_4$: $\text{CreateAttackerControlledServer}(\Pi, S)$. Upon receiving this query, the oracle creates a fresh server $S$, and sends the corresponding secret key and public key to the attacker. (The created secret key will be used as this server’s share of the group decryption secret.) After this query has been made, we have that $S_{\text{PAC}} := S_{\text{PAC}} \cup \{S\}$. This oracle allows $A$ to adaptively register permanently attacker-controlled servers of its choice.

5) $\mathcal{O}_5$: $\text{CreateSecureClient}(\Pi, C)$. Upon receiving this query, the oracle creates a fresh client $C$ in $\Pi$. After this query has been made, we have that $C_{\text{Sec}} := C_{\text{Sec}} \cup \{C\}$. This oracle query allows an attacker to introduce more clients, which are initially secure.

6) $\mathcal{O}_6$: $\text{CreateSecureServer}(\Pi, S)$. Upon receiving this query, the oracle creates a fresh server $S$ in $\Pi$. After this query has been made, we have that $S_{\text{Sec}} := S_{\text{Sec}} \cup \{S\}$. This oracle query allows an attacker to introduce more servers, which are initially secure.

7) $\mathcal{O}_7$: $\text{CompromiseClient}(\Pi, C)$. Upon receiving this query for some $C \in C_{\text{Sec}}$ in $\Pi$, the oracle forwards all corresponding secrets of $C$ to $A$. From now on the attacker controls $C$ so that $C \in C_{\text{AC}}$ and $C \notin C_{\text{Sec}}$ after this query has been made. This oracle query allows $A$ to adaptively and permanently compromise a client of its choice.

8) $\mathcal{O}_8$: $\text{TakeOwnershipServer}(\Pi, S)$. Upon receiving this query for some $S \in S_{\text{Sec}}$ or $S \in S_{\text{TAC}}$ in $\Pi$, the oracle forwards all corresponding secrets of $S$ to $A$, and from now on the attacker controls $S$. So, $S$ is moved from its current set in to $S_{\text{TAC}}$ after this query has been made. This oracle query allows $A$ to adaptively and permanently compromise a server of its choice.
9) \(O_9\): \textit{CompromiseServer}(I, S). Upon receiving this query, the oracle outputs all secrets of \(S \in S_{\text{Sec}}\) in \(I\). We have \(S \notin S_{\text{Sec}}\) and \(S \in S_{\text{TAC}}\) after this query has been made. This oracle query models \(A\)'s ability to adaptively and temporarily compromise an attacker-controlled server of its choice.

10) \(O_{10}\): \textit{Dec}(I, \textit{Enc}(M, PK_{S_{\text{C}}}), C). Upon receiving this query for some client \(C \in C_{\text{Sec}}\) with data \(M\), the set \(S_C\) of servers collectively executes the decryption protocol to decrypt the encrypted data \(\textit{Enc}(M, PK_{S_{\text{C}}})*\), and sends the decryption result \(M\) to the attacker, where \(PK_{S_{\text{C}}}\) is the group public key of the set \(S_C\) servers selected by \(C\) for encryption/decryption.

We now consider the distributed storage scenario. If a powerful attacker \(A\) can fully control a data owner’s device when the device is creating or recovering data \(M\), then \(A\) can easily learn \(M\). As mentioned before, we do not consider this case as there is nothing we can do and it is not interesting. To focus on the more interesting cases, we only consider that \(A\) cannot learn \(M\) by compromising the data owner’s device during the secret creation or recovery time.

\textbf{Definition 2:} A self-healing distributed storage protocol \(\Pi\) comprises a group of data owners, and a group \(S\) of decryptors. It consists of two algorithms and three protocols, namely key generation algorithm \(\textit{KeyGen}\), encryption algorithm \(\textit{Enc}\), encryption key construction protocol \(\Pi_{PK}\), decryption key construction protocol \(\Pi_{SK}\), and decryption protocol \(\Pi_{dec}\).

- \(\textit{KeyGen}(\lambda)\): Taking security parameter \(\lambda\) as input, it outputs a pair \((s_i, P_i)\) of private and public keys for the decryptor \(S_i \in S\).
- \(\Pi_{PK}\): It is run by a group \(S' \subseteq S\) of decryptors. The decryptor \(S_i\) has private input \(s_i\). After the completion of the protocol, each \(S_i \in S'\) outputs the same long term public key \(PK_{S'}\) of group \(S'\).
- \(\Pi_{SK}\): It is run by a group \(S' \subseteq S\) of decryptors at each time period \(j\). After the completion of the protocol, each \(S_i \in S'\) outputs a share \(s_{ij}\) of the corresponding group private decryption key for time period \(j\). If \(j = 0\), then the private input of \(S_i\) is \(s_i\). If \(j > 0\), then the input of \(S_i\) is \(s_{i(j-1)}\).
- \(\textit{Enc}(M, PK_{S'})\): Taking data \(M\) and the public key \(PK_{S'}\) of group \(S'\) as input, it outputs the ciphertext of \(M\) encrypted under \(PK_{S'}\).
- \(\Pi_{dec}\): It is run by a data owner with encrypted \(M\), and a group \(S' \subseteq S\) of decryptors with their private input \(s_{ij}\) for each \(S_i \in S'\) at time period \(j\). After the completion of the protocol, the data owner outputs \(M\).

\textbf{Remark 2:} The self-healing feature is defined by the decryption key construction protocol \(\Pi_{SK}\), as it enables decryptors to update their keys periodically.

\textbf{Definition 3:} A self-healing distributed storage protocol \(\Pi\) is \((k, n)\)-secure if the advantage \(Adv_t^{A,n,k}(\lambda) = |Pr[b = b'] - \frac{1}{2}|\) of \(A\) to win the following game, denoted \textit{Game-PCSE}, is negligible in the security parameter \(\lambda\).

\textbf{Game-PCSE:}

- \(\textit{Setup}(\Pi, \lambda)\): The challenger sets up protocol \(\Pi\) according to the security parameter \(\lambda\). Initially, \(S = C = \emptyset\).
- \(\textit{Query}\) phase. The attacker can ask a polynomially bounded number of oracle queries \(O_i\) for \(i \in \{0, 1, \ldots, 10\}\). Let \(j_4, j_8, j_9\) be counters counting the total number of \(O_1, O_8, O_9\) queries asked by the attacker, respectively. We have that \(j_4 + j_8 + j_9 < k\).
- \(\textit{Security action}\) phase. The challenger makes security checking oracle queries on all servers, and then makes security action oracle queries on the servers that are temporarily controlled by the attacker. At the end of this phase, the counter \(j_9\) will be reset to “0”.
- The query phase and the security action phase are repeated a polynomially bounded number of times.
- \(\textit{Challenge}(C_b, C)\): The attacker selects a target client \(C\) who has not been asked through \(O_i\) for \(i \in \{3, 7\}\), i.e. \(C \in C_{\text{Sec}}\), and selects two messages \(M_0\) and \(M_1\), s.t. \(|M_0| = |M_1|\). The attacker then sends them to the challenger. The challenger tosses a coin. Let \(b \in \{0, 1\}\) be the result of the coin toss. The challenger then encrypts \(M_b\) according to \(\Pi\), and sends the ciphertext \(C_b = \textit{Enc}(M_b, PK_{b})\) back to the attacker.
- The query phase and the security action phase are repeated a polynomially bounded number of times. Additionally, we require that the target client \(C\) cannot be asked through \(O_3\) and \(O_7\), and \(\textit{Dec}(\Pi, C_b, C)\) cannot be queried through \(O_{10}\).
- \(\textit{Guess}(b)\): The attacker makes a guess \(b'\) of the value of \(b\), and outputs \(b'\). The attacker wins if \(b = b'\).

\textbf{Remark 3:} In the game defined above, the execution of a query phase followed by a security action phase simulates an epoch of the protocol.

\textbf{Remark 4:} In a \((k, n)\)-threshold cryptosystem, an attacker can break the security if the attacker is able to compromise \(k\) secrets/parts during the lifetime of the system. However, in the above defined \((k, n)\)-secure system in the PCSE, an attacker cannot break the security even if the attacker can compromise all \(n\) parties in the lifetime of the system, provided at any time point \(t\) between two updates, at most \(k - 1\) parties are compromised by the attacker.

### III. OUR SOLUTION

We present our solution, first in a non-threshold form (i.e., we stipulate that the minimum number \(k\) of servers needed for performing decryption is equal to \(n\), the total number of servers). Later, in section VI-A, we generalise it to a threshold-based solution where we allow one to choose \(k < n\).

\textbf{A. Basic idea}

A client Alice selects a set of servers, and requests that they collaborate using the Initialisation protocol (detailed later) to compute a public key for a storage service. She encrypts her sensitive data using this group public key. Each selected server stores a copy of the encrypted data. (Of course, in practice, this makes sense only if the data is small. If a large amount of
data is required to be stored, we assume that a fresh session key is generated. The large data is encrypted with the session key and stored on an (untrusted) cloud service; and the session key is encrypted using the group public key and stored on the selected servers.)

Time is divided into epochs. At the end of each epoch, the servers execute a protocol during which they generate new decryption keys and destroy the old ones.

If a server is compromised in an epoch, the attacker obtains all its (shares of) decryption keys. However, the protocol ensures that decryption keys from a server in one epoch cannot be used together with decryption keys from a server in a different epoch. Each change of epoch renders useless the decryption keys obtained by the attacker in previous epochs.

Thus, to decrypt the secret, an attacker would have to compromise a threshold number of servers within the same epoch.

B. Abstract construction

Our protocol is based on bilinear map, as defined below.

**Definition 4 (Bilinear Map):** Let $G_1$, $G_2$ be two cyclic groups of a sufficiently large prime order $q$. A map $e: G_2^* \rightarrow G_2$ is said to be bilinear if $e(g^a, g^b) = e(g, g)^{ab}$ is efficiently computable for all $g \in G_1$ and $a, b \in \mathbb{Z}_q$; and $e$ is non-degenerate, i.e. $e(g, g) \neq 1$.

We now explain the protocol with three servers, $S_A$, $S_B$, and $S_C$. Let $g \in G_1$ be a fixed public value and $Z = e(g, g) \in G_2$. The data associated with the servers at different stages of the protocol are presented in Fig. 3.

**Setup and zero-th epoch.** $S_A$ generates a private key $a$, and a public key $g^a$. Similarly, $S_B$ and $S_C$ generate $(b, g^b)$ and $(c, g^c)$. Then $S_A$, $S_B$, $S_C$ collectively compute and publish their joint public key $g^{abc}$.

Next, $S_A$ generates a new key $a_0$ and public key $g^{a_0}$, and similarly $S_B$ and $S_C$ generate $(b_0, g^{b_0})$ and $(c_0, g^{c_0})$. Then $S_A$, $S_B$, $S_C$ collectively compute and publish helper data $H_0 = g^{(a_0/a)}(b_0/b)(c_0/c)$ with proofs that they have correctly performed the computation. They destroy the secrets $a, b, c$.

**At the end of the $(j-1)$-th epoch.** The servers replace their decryption keys $a_{j-1}$, $b_{j-1}$, and $c_{j-1}$ with new ones $a_j$, $b_j$, and $c_j$. Then $S_A$, $S_B$, $S_C$ collectively compute and publish helper data $H_j = g^{(a_j/a)}(b_j/b)(c_j/c)$ with proofs that they have correctly performed the computation. The values $a, b, c$ are not required to compute $H_j$. They destroy the secrets $a_{j-1}$, $b_{j-1}$, $c_{j-1}$.

**Encryption of data $M$.** At any time during the server lifecycle (i.e. any epoch $j$), a client Alice can encrypt her data $M$ by using the (unchanging) public key $g^{abc}$. She selects a new random $k$, and computes $C = (\alpha = g^{abc k}, \beta = MZ^k)$.

**Decryption of ciphertext $(\alpha, \beta)$ at the $j$-th epoch.** After authenticating client Alice’s request for decryption, the servers can collectively decrypt a ciphertext $(\alpha, \beta)$ during any epoch. To decrypt $(\alpha, \beta)$, the servers compute $\gamma = e(\alpha, H_j) = Z a_j b_j c_j k$. Then the servers use their secrets $a_j$, $b_j$, and $c_j$ to collectively compute $Z^k$, and then they can recover the data $M$ from $\beta = MZ^k$. Note that during this decryption process, Alice should apply masking to the $\gamma$ to prevent servers from learning the plaintext. More details are presented in the next section.

Remark 5: Note that the public key used by clients for encryption remains constant regardless of the secret updates on the server side. Also, the update procedure is independent of the number of stored ciphertexts. That is because in the update phase the servers need only collectively compute the helper data. The ciphertext $(\alpha, \beta)$ of each data item remains unchanged.

C. Detailed construction

**Initialisation:** Setup. Let $G_1$, $G_2$ be two groups of a sufficiently large prime order $q$, such that $|q| = \lambda$, with a bilinear map $e: G_2^* \rightarrow G_2$, and $g \in G_1$ is a random generator and $Z = e(g, g) \in G_2$.

Let $S_1, S_2, \ldots , S_n$ be the servers selected by Alice. $S_i$ performs $KeyGen(\lambda)$ to create set-up key pair $(s_i, g^{s_i})$, for some $s_i \in \mathbb{Z}_q$, respectively. They also run $\Pi_{PK}$ to compute a group public key $PK = g^{\Pi_{s_i}}$, which is available to the client in an authentic matter, e.g., via a certificate. This key can be established as follows:

- Each $S_i$ computes and publishes $P_i = g^{s_i}$.
- $S_2$ computes $PK_{12} = (P_1)^{s_2}$. This computation can be verified by other servers by checking $e(PK_{12}, g) = e(P_1, P_2)$.
- $S_i$ computes $PK_{1..i} = (PK_{1..(i-1)})^{s_i}$, which again can be verified by other servers by checking $e(PK_{1..i}, g) = e(PK_{1..(i-1)}, P_i)$.

Now, each $S_i$ has a secret key $s_i$ and a group public key $PK$. Fig. 3. The data associated with the servers $S_A$, $S_B$ and $S_C$ at different stages of the protocol, and the encryption and decryption computations.
Zero-th epoch. This epoch is to generate shares of the first decryption key through Π_{SK}. Each S_i chooses another secret s_i0, computes u_{i0} = s_{i0}/s_i, computes and publishes P_{i0} = g^{s_{i0}}P_0 = g^{u_{i0}} and deletes s_i. The correctness of these values can be checked as e(P_{i0}^P_0, P_i) = e(P_{i0}, g).

By using u_{i0}, S_i works with other servers to get H_0 = g^{\Pi s_{i0}/s_i}, in the same way as computing PK, and then deletes u_{i0}.

At the end of the initialisation, S_i only holds its share s_{i0} at secret. This value can be used for decryption (if needed) and is used for the next decryption key update. In addition, S_i also holds two public values, namely a helper data H_0 and a group public key PK.

Note that the group public key is used for data encryption by the clients. This implies that the clients do not have to follow the server key updating processes, and they will keep using the key PK for a reasonably long time.

Updating the decryption keys (Π_{SK}): The decryption key update process is similar to the computation of the first decryption keys presented in the previous phase. At the end of the \((j-1)\)-th epoch for some \(j \geq 1\), the servers replace their decryption keys s_{i(j-1)} with new ones, s_{ij}. This is achieved as follows.

- With the input s_{i(j-1)}, S_i chooses s_{ij}, computes u_{ij} = s_{ij}/s_{i(j-1)}, computes and publishes P_{ij}^j = g^{s_{ij}} and P_{ij}^j = g^{u_{ij}}, and deletes s_{i(j-1)}.
  The correctness of these values can be checked as e(P_{ij}^j, P_{(j-1)}) = e(P_{ij}, g).

- By using u_{ij}, S_i works with other servers to get H_j = H_{ij-1} = g^{\Pi s_{ij}/s_i}, and then deletes u_{ij}.
  The correctness of these values should also be verified in the same way as computing PK.

At the end of \((j-1)\)-th update, S_i only holds s_{ij}. This value is used for both decryption and update in the \((j)\)-th epoch.

Encryption: To encrypt data M, Alice selects a new random \(k\), and computes PK = g^{k}\Pi s_i and MZ = k. Alice sends (\(\alpha = PK, \beta = MZ\)) to each server.

Servers only accept (\(\alpha, \beta\)) as some encrypted data from Alice if a valid proof of knowledge of \(M\) (or \(k\)) is provided. This is used to prevent replay attacks in which an attacker who has observed (\(\alpha, \beta\)) sets up an account with the servers, and provides (\(\alpha, \beta\)) as the attacker’s encrypted data, then requests servers to decrypt it for the attacker. Any secure zero knowledge proof of knowledge of ZKP can be used. For example, the proof can be a Schnorr ZKP of \(k\), where the prover knows \(k\) and the verifier knows \(PK\). If the prover shows knowledge of \(k\), this implies that she also knows \(M\).

At the end, Alice destroys \(M\) and \(k\) after all servers are convinced and accepted the ciphertext.

Decryption (Π_{dec}): The basic idea of the decryption process is presented in Fig. 4.

In more detail, in the \(j\)-th epoch for some \(j \geq 0\), Alice sends a request to a selected server for retrieving the encrypted data. After successfully authenticating Alice, the server calculates \(\gamma = e(\alpha, H_j) = Z^{k}\Pi^{s_{ij}}\), and sends (\(\beta, \gamma\)) to Alice.

Alice selects a new random \(k' \in \mathbb{Z}_q\), sends \(Z^{k'}\) to each of the servers as her commitment on \(k'\), computes \(\gamma'k' = Z^{kk'}\Pi^{s_{ij}}\), and asks each server to remove its \(s_{ij}\) from the exponent by calculating \(\gamma'k'\). The final output should be \(Z^{kk'}\). She then can recover \(Z^k\) by computing \((Z^{kk'})^{1/k'}\), and thus be able to decrypt \(MZ^k\).

Before a server decrypts some message requested by a user, the server expects a proof that the requested decryption is indeed a step to help the user to recover a key that the user actually owns, i.e. to prove that

\[ (Z, Z^{k'}, Z^{kk'}\Pi^{s_{ij}}, Z^{kk'}\Pi^{s_{ij}}) \]

is a DDH tuple. This can be done by using classic non-interactive ZKP schemes, for proving that \((g, g^{r}, g^{k}, g^{\Pi r})\) is a DDH tuple (e.g. Chaum-Pedersen protocol [7]). Each server also needs to check the received values from other servers in the same way.

IV. Security analysis

The full formal security proof can be found in our technical report [6] (Section 4, page 6-9). Here we provide a summary of our security analysis. Our goal is to prove the security of our protocol per Definition 3; that is, we prove that the advantage that a probabilistic polynomial-time (PPT) adversary \(A\) has to win the Game-PCSE is negligible.

To provide a rigorous security proof, we formally define our hardness assumption, and define a cryptographic game accordingly. To better simulate our protocol, the defined game
supports multiple rounds simulating the epochs in our protocol. We call such a game with \( j \) rounds as \( j \)-round modified decisional bilinear Diffie-Hellman inversion game, denoted \( \text{Game}-j\text{-R-MDBDHI} \). We then prove in a lemma that if an adversary can win \( \text{Game}-j\text{-R-MDBDHI} \) with a non-negligible advantage, then we can break our hardness assumption.

Finally, we prove in our theorem that if an adversary can win \( \text{Game-PCSE} \) with a non-negligible advantage, then we can make use of this adversary to win \( \text{Game}-j\text{-R-MDBDHI} \) with advantage \( \frac{(1+2\epsilon)(N-1)(N-N^\prime)}{N-N''} \), which is also non-negligible. (Here, the values \( N, N' \) and \( N'' \) are quantities of servers participating in the protocol.)

### V. PERFORMANCE EVALUATION

This section evaluates the performance of the proposed system in two aspects, namely the number of communication rounds and the computational cost. We define some notations to facilitate our evaluation, as presented in Table II.

The number in front of a notation means the number of times this computation is required, e.g., \( 3 \text{Mul} \) means that \( \text{Mul} \) operation has been calculated three times in this phase. Note that since the initialisation phase will only be run once at the beginning of the system, our performance evaluation ignores it here. In addition, we assume that the zero knowledge proof uses Schnorr NIZK scheme [8], and costs \( 1 \text{Exp} + 1 \text{Mul} \) for proof generation and \( 2 \text{Exp} + 1 \text{Mul} \) for verification [9].

Table III presents the number of communication rounds in each phase in three figures. In brief, our evaluation shows that the protocol for updating the decryption keys, which will be run periodically, does not require the involvement of any client. In addition, only one communication round is needed for a client to communicate with each group member for data encryption/distribution and for data reconstruction. This results in \( N \) rounds for data encryption, and \( N + 1 \) rounds for data decryption, where \( N \) is the number of servers. The reason that the data decryption requires \( N + 1 \) rounds (rather than \( N \) rounds) is that apart from one communication round with each of the \( N \) servers, an additional communication round is required between the client and the first server that the client communicates with for computing \( \gamma \), as shown in the Figure 4. However, as we will see later, although the number of communication rounds that a client is involved is dependent on the number of servers, a client’s computational cost is independent of the number of servers.

Table IV presents the computational cost, for a client and for a server, in different protocol phases. Our evaluation shows that all bilinear pairing operations are done on the server side. Due to limited space, we refer readers to our full version [6] for a more detailed analysis.

<table>
<thead>
<tr>
<th>Entity/phase</th>
<th>Updating the decryption keys</th>
<th>Encryption</th>
<th>Decryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>-</td>
<td>3 Exp + 2 Mul</td>
<td>4 Exp + 1 Mul + 1 Inv</td>
</tr>
<tr>
<td>Server</td>
<td>1 Inv + 3 Exp + 4(N-1) BP</td>
<td>2 Exp + 1 Mul</td>
<td>1 BP* + 3 Exp + 1 Mul + (N-1) BP**</td>
</tr>
</tbody>
</table>

Note:
* Only 1 out of \( N \) servers need to perform this operation (for computing \( \gamma \) with cost \( 1 \text{BP} \)).
** The number of correctness checks is different for each server depending on their network position, where \( (N-1) \text{BP} \) is the cost in average.

### VI. DISCUSSION AND RELATED WORK

#### A. Extension to a threshold system

As mentioned in previous sections, our system requires the presence of all servers for recovering a secret. However, it can be easily extended to a threshold-based system, by using any classical (verifiable) secret sharing schemes to back-up all ephemeral secret keys of servers.

To be more precise, let ‘key servers’ be the servers in our protocol and ‘back-up servers’ be the secret sharing servers. Each time a new key of a key server is generated, the key will be distributed to a set of back-up servers through secret sharing schemes, and the shares associated to the old keys will be destroyed. So, when a key server is dead, our system can still continue by recovering the dead server’s secret keys from shares, and take actions from there to re-build the server.

Intuitively, the extended threshold system is secure even if we additionally allow an attacker to compromise less than a threshold number of back-up servers at any epoch, provided that the set of back-up servers does not overlap with the set of key servers, and all key servers uses the same threshold with the same set of back-up servers for sharing their keys. Loosely speaking, since the shares of different epochs are independent each other, the compromise of shares in an epoch does not help an attacker to recover secrets shared in other epochs.

In fact, we can easily improve the security guarantee of the extended threshold system by letting key servers use different
sets of back-up servers for sharing their keys. In this way, an attacker would need to compromise a threshold number of back-up servers to only obtain the secret of a single key server, rather than being able to recover all key servers’ secrets. A more rigorous security analysis of the extended threshold system will be our future work.

B. Related work

Outsourcing storage is a growing industry, it enables users to remotely store their data into a cloud, reduces users’ burden of in-house infrastructure maintenance, and offers economies of scale. However, due to concerns over data privacy and security [10], users are not willing to outsource their sensitive data in the cloud [11]. For example, many recent attacks have been perpetrated on cloud systems [12], [13]. We discuss related proactively secure systems that have been designed to secure against compromised servers.

Proactive secret sharing (PSS) (e.g., [14]–[18]) is a technique for sharing a secret among a set of servers; it is secure against an attacker that can compromise servers, one by one, over a long period. In PSS, as in our protocol, time is divided into epochs. In each epoch, the servers that hold shares of the secret engage in a protocol to update their shares. An attacker may compromise some servers in a given epoch, but the learnt secrets are useless in other epochs. Thus, even if all the servers are eventually compromised over different epochs, the secret remains intact provided that in each epoch there was at least one server that remained honest.

Proactively secure cryptographic systems (e.g., [19]–[25]) apply the ideas of proactively secure secret sharing to sharing decryption or signing secrets among several servers. Such systems have been achieved by combining a proactively secure secret sharing scheme with an encryption or signature scheme. However, these constructions make use of a trusted dealer, who creates the secret key and distributes shares of some secrets to the servers. Unfortunately, the creation of the secret key in a single location by the dealer prevents the decentralisation required and achieved in our protocol. Although it is mentioned in a number of papers (e.g. [25] can be extended to a dealer-less protocol by using [26]) that the function of the trusted dealer in these schemes can be done by the servers, it is well known that both distributing a secret in Shamir’s secret sharing scheme and creating and distributing an RSA (or a DL) key, amongst multiple players without a trusted dealer, are complicated and very expensive. In this paper, we propose a decentralised distributed decryption scheme, which does not have such a trusted dealer and is efficient.

VII. CONCLUSION

Increasing numbers of attacks on cloud servers challenge the security of cloud storage. We have introduced a provably secure distributed storage system as a security enhanced approach to this challenge. Because the system updates decryption secrets on servers, it remains secure even if all the servers are compromised over a long time, provided that no more than a threshold number of servers are compromised in a single epoch. The storage system maintains a fixed public key; the key can be used securely even after such compromises. This solves an important problem of how to authenticate servers when they are compromised, without having to rely on PKI.