A Database Watermarking Service with a Trusted Authority Architecture for Cloud Environment

Nour El-Zawawi Mohamed Hamdy

Raina El-Gohary Mohamed F.Tolba

Faculty of Computer and Information Sciences,

Ain Shams University,
El-Kalifa Al Ma'moun st., Abbasyia 11565
Cairo, Egypt

ABSTRACT

Providing cloud services gets an increasing interest of both scientific and industrial applications today. Storage services are the fundamental component of the Cloud computing paradigm. Exploiting such storage services enables users to outsource their data into the cloud. Not only is the reduction of storage and maintenance costs achieved but gets rid of the required infrastructure burden as well. How to prevent data abuses it by the cloud remains a hot point of the research. As there is a lack of trust between the service providers and clients, a set of challenges of securing the outsourced data against being abused is popped up. In this article, an enhanced secure data scheme for Cloud environments, Enhanced Watermarking Technique for Rational Database with non repudiation (EWRDN), is proposed. It is based on a set of enhancements for the WRDN approach. It improves space complexity by 56% of original WRDN system with the same time complexity.
EWRDN Service works as a trusted third party between clients and service providers. It guarantees data integrity, privacy, and non repudiation with the ability to recover data to its origin. Moreover, it gives data owner more controlling capabilities for their data, by tracing users' activities. Besides, it adds a user signature over data being processed. A proposed architecture for EWRDN service is illustrated to prove data integrity and save copyright with the ability to trace the data and recover it to its origin if unauthorized changes take place.

General Terms:

Design, Security

Keywords:

Cloud computing, middleware services, establishing trust in Clouds,privacy, trustworthy computing, security

1. INTRODUCTION

Cloud computing is currently an important set of technologies and computing paradigms for both scientific and industrial applications. Dynamic, scalable and often virtualized resources are provided in Cloud environments as services via the Internet [18,28]. It allows new business opportunities and capabilities without investing in infrastructure, training new personnel or licensing new software. Moreover, it offers pay per use charge for the different required services. Essential characteristics of Cloud Computing [28] are on demand self service, broad network access, resource pooling, rapid elasticity, and measured service.
In general, there are three known types of Clouds: Infrastructure as a service (Iaas), Platform as a service (PaaS) and Software as a service (SaaS). IaaS refers to the provision of virtualized hardware on which the client can run their operating system and software stack. In PaaS, the operating system and environment are provided and maintained for the client, who then runs their applications. In SaaS the Cloud provider runs and organizes the entire software system and provides software services [44].
Organization gains new features when moving to the cloud [9]. In spite of the potential benefits that could be gained, the model has challenges [13,22,43,48] that affect the model credibility like Data Integrity, which is the consistency and accuracy of the data stored in cloud, privacy and confidentiality, which is the people's right to control what happens with personal information over the internet.
The privacy issues differ according to different cloud scenarios, and can be divided into three subcategories [33,34,42], which include: (a) how to make users control their data when it is stored and processed in cloud, (b) how to avoid data loss, leakage and unauthorized modification, and (c) who is responsible for ensuring legal requirements for personal information.
However, previously mentioned challenges data security is the major concern that affects the adoption of the cloud computing model where security is the way to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non repudiation [10, 30, 43]. To protect Cloud data resources such as storage services, traditional security techniques, such as encryption and authorization which provide a good solution, but they fail when helping entities act maliciously due to the nature of cloud connections.
Trust as a security solution can work against such security threats; achieving the missing trust here enables the parties in a cloud environment to operate their applications and services.

Trusting issues in cloud computing environments can be divided into four subcategories [33,42], which include: (a) how to define and evaluate trust, (b) how to handle changed information, (c) how to consider and provide difference security level of service according to the trust degree, (d) how to manage and monitor trust.

In this article, one proposes architecture for a trusted service. To be used by organizations or individuals determines moving their critical data to the cloud; moreover they need to ensure data security and privacy. The proposed architecture uses EWRDN (An Enhanced Watermarking Approach for Secure database Service) as a service as a trusted authority. It is based on the enhancement of WRDN [47] (watermarking technique for rational database with non repudiation) technique. It works as a trusted third party Service between user and service provider. Besides, it guarantees data integrity, privacy, and non repudiation with the ability to recover data to its origin. Moreover, it gives users more monitoring capabilities over their data. These features come from the missing trust between service providers and clients. According to Top Threats to the Cloud Computing Report, clients do not trust database services providers on Cloud due to: Abuse and immoral use of cloud computing, insecure application interfaces, malicious insiders, weakness of shared technologies, data loss or leakages, account and service hijacking and Risk profiles which are not available [20]. Trusted account authority service is used to solve the previous problems. EWRDN Service uses a Trusted Authority (TA) service to distribute private and public keys between users to add a user signature to trace users' activities. Lots of protocols are used to arrange access, facilities and resources for the customers' need to work on site. In the proposed system, Service Level Agreement (SLA) is used to share private and public keys between users without being exposed [15,19,27].

The rest of the article is organized as follows: Section 2 presents the proposed system architecture assumed in this work with the proposed and current scenarios. The proposed EWRDN algorithm - Enhanced Watermarking Approach for Secure database Service - with an analysis in the traditional environment is described in section 3. Meanwhile, the application of EWRDN algorithm as a Service is presented in section 4. Finally, section 5 concludes the achievements made.

2. SYSTEM ARCHITECTURE

Cloud databases service can offer significant advantages over their traditional counterparts [12], including increased accessibility, automated scaling, maintenance of hardware, and better performance. At the same time, cloud databases have their share of potential drawbacks, including security and privacy issues as well as the potential loss of or inability to access critical data in the event of a disaster or bankruptcy of the cloud database service provider [29]. Database Service structure is not the key point in this research. One concentrates on encouraging users to move their tuples over the cloud, by providing a secure and trusted service which gives users more control over his data, traces users' activity, and recovers data to its origin if unauthorized changes take place. Before applying cloud service, there are architectural requirements needed to be considered [37].

Figure 1 illustrates the proposed architecture to support a trusted database service in cloud. This service helps users to trust cloud database service. It represents three layers as follows:

—Client Application layer refers to client frontend that runs at the users computer. It communicates with infrastructure layer via an XML based protocol to let applications exchange information over HTTP (SOAP - Simple Object Access Protocol) [7,35].

—Infrastructure layer refers to managing the hardware and software providing the service on the cloud. It controls two types of servers: Database Server, which contains user private data on the cloud and Web server, which provides the application responsible for communicating between users and cloud provider. Both servers are strongly decoupled via a SOAP channel allowing flexibility, which is envisioned to be useful in a Cloud environment.

—Physical layer refers to cloud physical machines. It works from storage and server infrastructure and working up through the application and network layers. It defines mechanical, electrical, optical, radio, procedural, and functional standards to enable the transmission of data to cloud virtual machines.

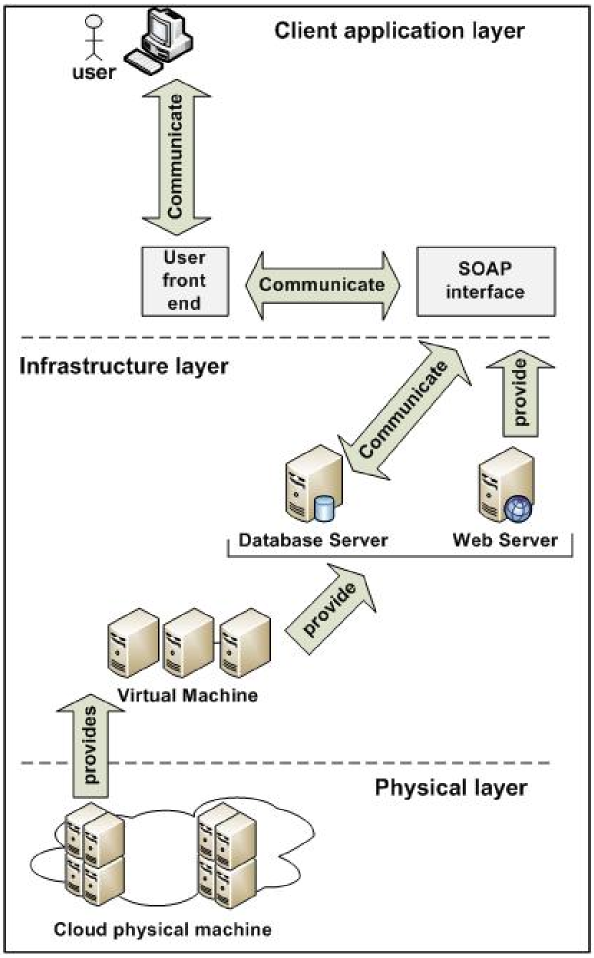


Fig. 1. Proposed Service prototype

Different threats emerge with the appearance of technology that represents current Cloud environment. These threads appear to be more difficult due to the infrastructure change in a Cloud environment, where security boundaries may be needed to be modified as well as the rate of change and level of scale in the Cloud environment [42].

Cloud Security problems could be summarized due to three problems: Loss of control, where users have no control over their private and personal data, Lack of trust (mechanisms), due to lack of Service Level Agreement (SLA) standards availability between users and providers, and the Multi tenancy, which refers to a single instance of a software application serving multiple customers. There is a number of key security elements that should be considered as an integral part of the Cloud application development and deployment process. In the meantime, there are few technical issues like browser security, Secure Browser Based Authentication and Attacks on Browser Based Cloud Authentication that needs to be built [4].

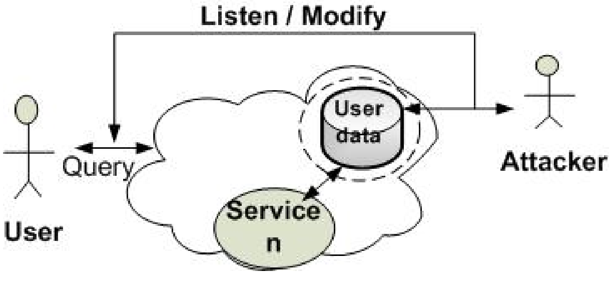


Fig. 2. Current Scenario

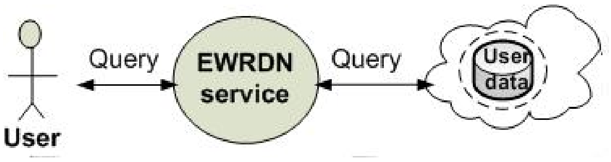


Fig. 3. Proposed Scenario

As shown in Figure 2, one will see the problems that prevent data owners from moving to the cloud; The main problem that arises is the trust. Trust is the degree which clients will rely on for the assertions or security services provided by the cloud provider. In Database Management Systems (DBMS), Database Administrators DBAs have full control over their data and structures hosted inside their databases. Therefore, they have the ability to restore or hide data in order to prove data integrity and ownership, as appearing on WRDN system. However, problems happened when trying to apply WRDN as a cloud service, due to the lack of guaranties between users and cloud provider to hide the watermark data or lock column. So, enhancement needs to be made to apply WRDN as a service on the cloud. Regardless of trust challenges, the others could be:

- Cloud Provider has complete authorities over user data.
- Data Leakage: data being revealed between nodes running on a Cloud system
- Threat amplification: which means that a problem spreads faster and farther through a Cloud environment rather than supposed. This also has the effect of potentially reducing time response and recovers data threat. It can be addressed by ensuring complete and well managed security processes.
- Distributed Denial of Service (DDoS) attacks: a user or application becomes unavailable or non serviceable because it stopped running down of the operated resources.
- Guaranties to recover data if any are missing.
- Cloud provider has no records about data usage.
- Complexity: more components mean more attack surfaces and more interactions among components. Time and Space complixty is important to be considered.

Using EWRDN Service solves the previous problems, by building a trusted authority (TA) service. Clients use EWRDN service to have control over their private data and restore data to its origin if any error occurs. EWRDN Service does not reduce Cloud provider control over data; instead it gives users the ability to trace the changes made over data.

The main idea of using EWRDN Service is based on building a trusted cloud service [17]. That works as a third party that ensures the data privacy. The proposed system has the ability to communicate with other security services, to ensure the data security and privacy. Figure 3 illustrates the proposed scenario. It shows that EWRDN is a reliable service. It takes tuples from users, then communicates with the available database service on the cloud. It overcomes all problems shown in the previous discussion. EWRDN Service has two actors and two services as follows:

- Actors: cloud customer (CC); database users responsible for updating and querying over data or data owner who needs just reports about users' activities and service, if the system is automatically maintaining and updating itself. Both actors send tuples to EWRDN Service to store it over the cloud. The communication channel between actors and EWRDN Service is secured by Service Level Agreement (SLA).
- Services: EWRDN Service; a trusted authority (TA) service which provides data privacy and database Service, which is part of cloud database provider (CP) responsible for storing and processing data over virtual machines (VM) or it could be a security service to encrypt data content. EWRDN service does not need to know the nature of database service and its applications. Moreover, it communicates with cloud provider instead of customers.

3. ENHANCED WRDN

In this section, EWRDN approach (Enhanced Watermarking Approach for secure database Service) is introduced and discussed to prove data integrity and localizing any changes made with the ability to restore data to its origin and to establish a layer of trust between providers and clients.

A Novel Watermarking Approach for Data Integrity and Non-Repudiation in Rational Databases (WRDN) is published in [47]. WRDN prevents the impacts of tampering dataset and localizing any changes made, by giving the database owner more control over his data. Besides, it concentrates on proving their ownerships or integrity of database against any type of attackers. An Enhancement model of WRDN (EWRDN) is presented. It does not prevent copying, but it deters illegal copying by providing a means of establishing the ownership of a redistributed copy. The main idea is to apply WRDN system as a trusted security service on cloud. But problems arise when trying to apply it - discussed in section 2. To overcome these problems, an enhancement model of WRDN system is proposed.

This service prevents the worse impacts of tampering data set by localizing any changes made. Besides, it has the ability to recover data to its origin if any changes appear, which will give database owner more control over his data. The data is prevented from any type of attacks by tracing users work to recognize authorization from unauthorized users. EWRDN relies on changing database schema by adding two new columns. The function is used in constructing the new record as well as the secret key (K) known only by the data owner; each user has a private key. The public key for each user is available in public. In general, the proposed models combine some important features of database security and privacy like Non Repudiation, Integrity, Copyright protection and Recovery.

The following Subsections are organized as follows: subsection 3.1 introduces EWRDN insertion mechanism while subsection 3.2 introduces detection mechanisms. EWRDN performance analysis is presented in subsection 3.3. Finally, probability analysis of the results is described in subsection 3.4.

3.1 EWRDN insertion Algorithm

Table 1 shows the notations and parameters used in this paper. Algorithm 1 identifies the algorithm for watermark insertion. For the beginning, one needs to have two hidden columns. No one of the database users knows about them and has no control over. First apply special mathematical function F () over all the row values to calculate watermark value. Then, use user's private key (PrK) to add signature over each attribute. Second, use Arithmetic Coding [6, 41] technique on new signature attribute to compress value. Add compressed values into a new column.

Table 1. Notation and Parameters

n	Number of attributes in the relation
m	Number of tuples in the relation
X	Number of users
$PrK_{1..x}$	User private key
$C_{i,m-1}$	Watermarked column
$C_{i,m}$	Compressed Data
W(i,j)	Watermark value of tuple i and attribute j
WM	Watermark Calculated Value
$PuK_{1..x}$	User public key consist of p,q,g,y
K	Database embedded key
F()	Special function used to calculate values in Rn+1
k	randomly-chosen number $<$ q
M	The Signatured attributes
y	Length of Signatured attributes
L,R	Unique interval represent each M

Algorithm 1 Watermark Insertion Algorithm

```
for i=1:n do
    for j=1:m-2 do
        WM=F($Cell_{i,j}$);
        M(i,j)=ADS($Cell_{i,j}$); See Algorithm 2
    end for
    $C_{i,m-1}$=WM;
    $C_{i,m}$=ACA(M(i));See Algorithm 3
    Lock($C_{i,m-1}$&$C_{i,m}$,K);
end for
```

Algorithm 2 Add Signature

```
A signature with hash value H consists of two numbers R and S:;
R = (($g^k$ mod P ) mod q);
S = $K^{-}1$ SHA(Cell)+ $PrK_{1..x}$.R (mod q);
Send signature (R,S) with message
```

Algorithm 3 Arithmetic Encoding Algorithm

```
Initialize L := 0 and R:= 1;
for i=1:y do
    Width := R - L;
    L := L + Width * C(xi);
    R := L + W * P(xi);
end for
tag := (L+R)/2;
choose code for the tag;
```

Algorithm 4 Watermark Detection Algorithm

```
for i=1:n do
    UnLock($C_{i,m-1}$,K);
    for j=1:m-2 do
        W(i,j)=F($Cell_{i,j}$);
    end for
    if W(i,j)=$C_{i,m-1}$ then
        Ownership proved;
    else
        $C_{i,m}$=ADA(M(i)); See Algorithm 5
        $C_{i,m}$=VDS(M($C_{i,m}$),PuK); See Algorithm 6
        $C_{i,j}$=$C_{i,m}$;
    end if
end for
```

Algorithm 5 Arithmetic Decoding Algorithm

```
Initialize L := 0 and R:= 1;
tag := .$b_1b_2...b_m$000...
for i=1:y do
    Width := R - L;
    find j such that L + Width * C($aj$) < tag < L + Width * (C($aj$)+P($aj$));
    output $aj$
    L := L + Width * C(xi);
    R := L + W * P(xi);}
end for
```

Finally, both watermarking and compressed column needs to be locked using (K) which is a private key that is only known to the database owner.

Adding a user signature is shown in algorithm 2. Digital Signature Algorithm (DSA) [1, 31, 39]is the algorithm used to sign attributes. In DSA, a digital signature is generated by applying $PrK_{1..x}$ to hash function to sign a message.

Algorithm 3 shows arithmetic encoding technique. Arithmetic encoding is especially suitable for small alphabet (binary sources) with highly distorted probabilities. The basic idea of the arithmetic encoding is to use a high precision fractional number to encode the probability of the message, to represent M of length y by a unique interval [L,R] in]0,1]. As the interval becomes smaller, the number of bits needed to specify it grows. It assumes an explicit probabilistic model of the source.

3.2 EWRDN detection Algorithm

The watermark detection algorithm is shown in Algorithm 4, which shows EWRDN detection technique. First, apply mathematical function F () over all the row values to calculate watermark value W1 (i,j). Then use private key (K) to unlock the watermark and compressed column. Finally compare the new calculated result W1(i,j) with the original watermark value. If they match, then data is tampered free. Otherwise, it proves which rows are changed. To recover data, decompress values in the row that contains tampered data. Then restore data in order to restore to its origin.

Algorithm 5 shows Arithmetic decompression technique, where, decoding strategy is based on decoding the elements in the sequence in such a way that the upper and lower limits will always contain the tag value for each cell. In order to recover the original data M, the decoder must know the model of the source used by the encoder (eg., the source messages and associated ranges) and a single number within the interval determined by the encoder.

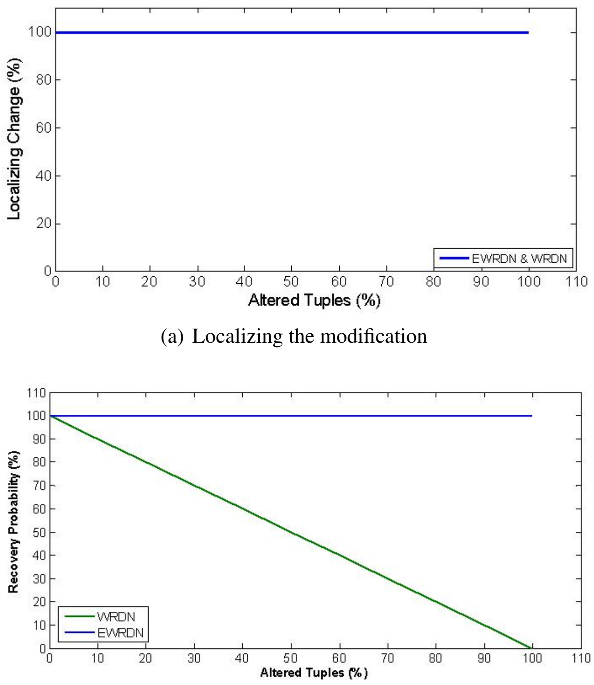
Verifying a message signature is illustrated in algorithm 6. The security of DSA is based on the computational infeasibility of finding a solution to equation S.

3.3 Performance Analysis

EWRDN is resilient against attacks to prove integrity. The database used for the implementation contains 100000 tuples, where there are 31 attributes for each tuple. Data Cleaning and Reduction is applied over the data. The preprocessing of the data used is processed to be complete, not noisy and consistent [23]. So, after preprocessing, it became 5000 tuples and 30 attributes. Figure 4(a) shows that both systems (WRDN and EWRDN) have the same ability to localize changes, but WRDN failed to recover data to its origin. Figure 4(b) demonstrates that WRDN fails each time the number of altered tuples increase. At the same time, EWRDN has a recovery factor equal to 100% even if all the available tuples have been altered. Performance Metrics: To measure the performance of EWRDN, three factors need to be considered: the first is the time needed for EWRDN to add watermark and recover data; the second is the amount of space needed to apply EWRDN system; and the third is Robustness where it is the ability to operate despite abnormalities in input, calculations, etc. Previous factors only affect the system when an alternation happens to database. EWRDN will have a static time performance of O(n) where n is the number of rows. But, if unauthorized changes take place, the time will be affected. Fig-

Algorithm 6 Verifing Signature

```
To verify the signature, a recipient must compute a value V from the known information:;
W = $S^{-}1$ mod q;
U1=(SHA(M).W)(mod q);
U2=R.W(mod q);
V=(($g^U1$. $y^U2$)mod p)mod q;
if V=R then
    data Signed by person with the public key (p, q, g, y);
end if
```



(a) Localizing the modification

(b) Recovery Factor

Fig. 4. Difference between WRDN and EWRDN

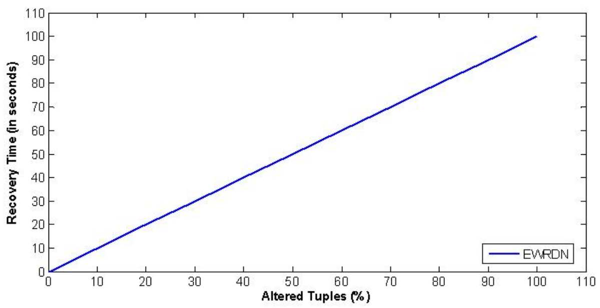


Fig. 5. EWRDN time performance

ure 5 shows the time EWRDN takes to restore data to its origin, where each time altered tuples numbers increase, the time EWRDN takes to restore data will also increase.

Space depends on compressed values. It has a complexity of O(1+β)×n where β is the compressed value between]0...1] and n is the number of attribute. Figure 6 shows that the value of compressed ratio β does not depend on the number of types available. Instead it depends on attributes value. Average value of compression ratio β is nearly fixed = 0.56 for tested data set. In the same time, compressed value changes depend on data types. Figure 7 shows the relation between the number of changed tuples and overhead space. One found that EWRDN consumed less space than WRDN. That is because WRDN depends on the number of attributes available, while EWRDN uses compression technique. Moreover, value of overhead space in EWRDN is nearly a fixed number.

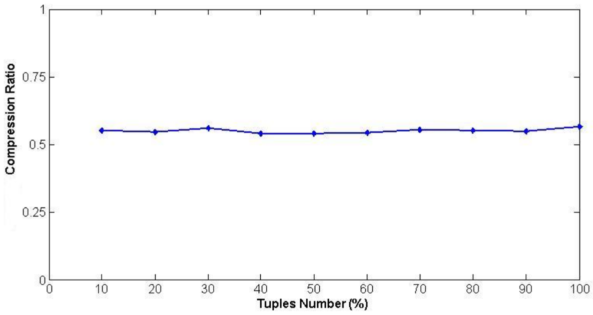


Fig. 6. Relation between β and number of tuples

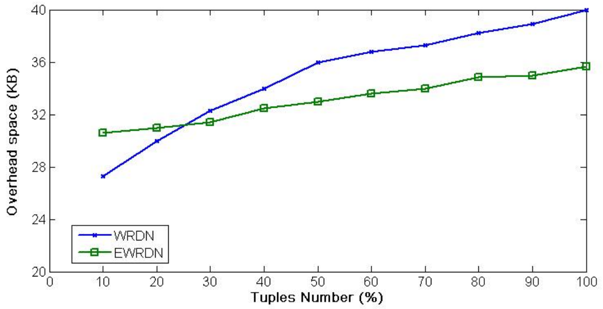


Fig. 7. Difference between WRDN and EWRDN in overhead space

3.4 EWRDN Results Analyis

Analyzing the results of EWRDN scheme is made by Bernoulli trials and binomial probability. The probability that the outcome of an experiment that consists of n Bernoulli trials has k successes and n - k failures is given by the binomial distribution

$$b(n, k, p) = \binom{n}{k} p^k (1-p)^{n-k} \tag{1}$$

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}\ 0 \leqslant k \leqslant n \tag{2}$$

where the probability of success on an individual trial is given by p.

The probability of having at least k successes in n trials, the cumulative binomial probability, can be written as

$$B(n, k, p) = \sum_{i}^{k} b(n, k, p) \tag{3}$$

Discussing the results is based on Robustness condition which is based on two parameters false hit and false miss.

False hit is the probability of a valid watermark being detected from non watermarked data. The lower the false hit, the better the robustness. On EWRDN, it never happened because each data has its own watermark. That is due to hiding the watermark data. Therefore, all detected strings will match their watermark, and the false hit is zero.

False miss is the probability of not detecting a valid watermark from watermarked data that has been modified in typical attacks. The less the false miss, the better the robustness. When applying equation 1 to get the value for one trial, it will be found that the value of p=1; whatever changes happen in the values of n and k. So, by applying equation 3, it will be found that the probablity of false miss will be equal to zero. Two cases are considered when trying to calculate the false miss.

—In case of deletion: The watermark value associated with the deleted tuples or attributes will not be detected. However, the other tuples or attributes will not be affected. Therefore, all detected watermark will match their counterparts in the data, and the false miss is zero.

—In case of adding: Suppose an attacker inserts 'c' new tuples to replace 'c' watermarked tuples with their primary key values unchanged. Watermark detection will never return a false answer, because new added values will fail to have corresponding watermarkes.

From the above observation, EWRDN improves watermarking robustness by 100%, due to its results in case of false hit and false miss.

4. EWRDN AS A SERVICE

Services are software function designed to exchange machine-to-machine interaction over a network. It provides potential fulfilling their requirements, but they need to be intentionally designed to do so [16, 32]. Services offer systems with many benefits over other types of distributed computing. They can be summarized as:

—Interoperability: It works outside of private networks, offering developers a non-proprietary route to their solutions. Besides, let developers use their preferred programming languages and they are platform-independent.

—Usability: It allows the business logic of many different systems to be exposed over the Web. This gives applications the freedom to choose the Services that they need. This allows developing services and/or client-side code using the languages and tools that developer wants.

—Reusability: It is easy to reuse Service components as appropriate in other services. It also makes it easy to deploy legacy code as a Web Service.

—Deployability: it is possible to deploy Web Services even over the fire wall to servers running on the Internet. Besides thanks to the use of proven community standards, underlying security (such as SSL) is already built-in.

The prime revolutionary aspect of Cloud Computing is its ability to deploy location independent services. At the same time, Service consumers (SCs) are no longer locked in with their providers. Cloud services take full advantage of the service oriented paradigm with a focus on the key attributes of statelessness, low coupling, modularity, and semantic interoperability. In this section, one talks about transferring EWRDN to real service. By applying EWRDN as a service, it inherits all features of web services plus their own benefits.

Data security in the cloud has been extensively studied. Despite the necessity and importance, security and privacy research in cloud database environment is still in its early stages, especially with respect to trusted framework. The issue of establishing trust in the Cloud has been discussed by many authors. Much of the discussion has been centered on the reasons for trusting the Cloud or not.

The work proposed by Aradhana and Chana [3] determines process for managing trust with specifying trust policies for different cloud scenarios. At the same time, trust policies are represented in the form of decision table that help in the implementation of these policies. The work in [2] considers Clouds resources management and infrastructure properties and differentiates between secure management of infrastructures data and users applications data.

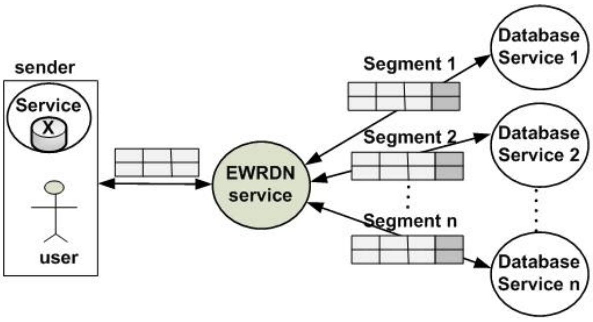


Fig. 8. Storing and Retrieving Mechanism

Roy H. Campbell et al. [8] proposed the properties and building blocks of a middleware for assured critical missions cloud computing, where, the middleware in such systems needs to manage the configuration and the dynamic systems with trusted and partially trusted resources. The work proposed by Bajpai et al. [5] proposed an authentication and authorization interface for accessing a cloud service through Security Service Level Agreements.

Some researchers proposed the usage of a Trusted Platform Module (TPM) to establish trust in Clouds and to provide remote attestation [38, 45]. Wang et al. [45] proposed an approach that combines the public key authenticator with random masking to achieve the privacy for public cloud auditing system. Meanwhile, the work in [38] establishes trust between Cloud entities based on their dynamic behavior. At the same time, Sato et el. [40] proposed a new cloud trust model based on predicting trust models and tight trust that controls cloud service providers. Li and Ping [26] introduced a novel cloud trust model to solve security issues in cross clouds environment. In the meantime Ko et el. [25] presented the TrustCloud framework, which addresses liability in cloud computing via technical and policy based approaches.

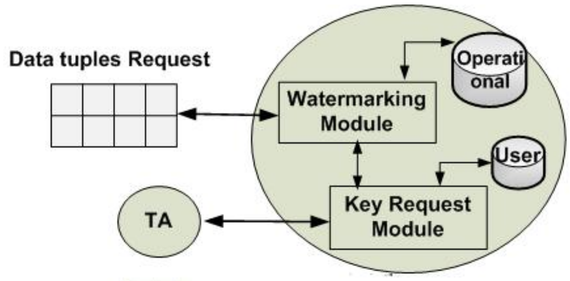
The work in [46] proposed a new security model which partitions data in unencrypted form to distributed secure database servers. Itani et al. [21] proposed Privacy as a Service (PaaS), a set of security protocols for ensuring the privacy of customer data. Moreover, it allows secure storage and processing of users' confidential data by leveraging the tamper proof capabilities of cryptographic coprocessors.

Meanwhile, Ranchal et el. [36] provides an approach for Identity Management with the ability to use identity data on untrusted hosts. It is based on the use of predicates over encrypted data. In the meantime, Corradi [11] presented a real use case of home healthcare SaaS application deployed on Amazon AWS, and discussed the challenges and changes needed to add cryptography and key management capabilities to enable SaaS data protection.

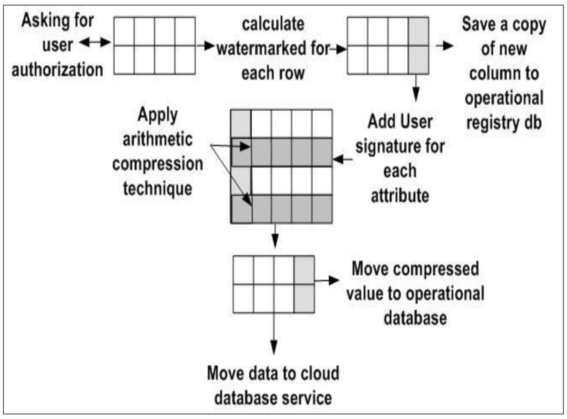
One's work differs from the previous research in which the proposed design approach does not require users to understand Cloud infrastructure and database service structure (most importantly a Cloud's dynamic nature). Besides, this model concentrates on database privacy over the cloud. It gives data owner the ability to trace users' activities and restore data if any errors occur. Moreover, it does not need the understanding of database service structure.

4.1 EWRDN Service Scenario

Figure 8 shows the mechanism of storing and retrieving data in EWRDN Service, where, the users send tuples to EWRDN Service as a message. First, it calculates watermark for each tuple and adds a user signature for each attribute. Then, it divides data to segment. Each segment has its own watermark value. Finally, the proposed service communicates with cloud database service to store data. Applying EWRDN service enables users to



(a) EWRDN Service general Architecture


Asking for user authorization
calculate watermarked for each row
Save a copy of new column to operational registry db
Apply arithmetic compression technique
Add User signature for each attribute
Move compressed value to operational database
Move data to cloud database service

(b) Watermarking module architecture

Fig. 9. EWRDN Service Architecture

recover the tuples if unwanted changes take place. Moreover, it provides evidences if the tuples are changed by any of the Cloud providers.

4.2 EWRDN Service Architecture

EWRDN Service architecture is represented in Figure 9. Figure 9(a) shows an overall system architecture, where the following steps will be applied inside the service in case of sending tuples to service; 1- Calculate watermark for each tuple; 2- Communicate with key request module to check over trusted authorization with trusted authority (TA) Service; 3- Key request module goes to user registry database to get user keys; 4- Use keys sent to watermarking module to add user signature; 5- Save a copy of watermarked data in operational registry database.

In Figure 9(b) the architecture of watermarking module is represented. The proposed service will be applied in two cases: 1- The query and 2- Recovery. It can be summarized into the following steps: a. Calculate watermark value for each row; b. Add a user fingerprint over each attribute. Any Digital Signature Schema (DSS) insertion algorithm using the user private key (PrK) could be applied; c. Save a copy of watermarked row in operational registry database; d. Apply compression technique over a new column; e. Move compressed values to operational registry database.

4.3 EWRDN Service Coordination

Every Web service task differs in the nature of the application executed and the role played by the service in the execution. Service coordination aims at the coherent and efficient discovery, composition, negotiation, and execution of Web Services in a given environment and application context [14, 24]. EWRDN service requires the transmission of multiple messages. The challenge lies in coordinating these messages in sequence where the actions performed by the message are executed properly with configuration of overall task. These messages are called Message exchange path (MEP).

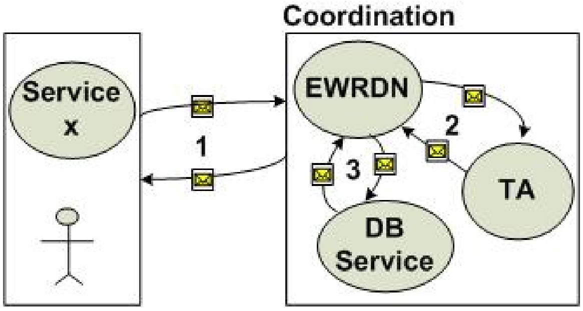


Fig. 10. Service Coordination Example

MEP represents a set of models that provide a group of sequences for the exchange of messages. The more complex an activity, the more context information it will bring with. Every activity introduces a level of context into an application runtime environment. Something executing has meaning during its lifetime, and the description can be classified as context. So, a framework is required to provide a means for context information in complex activities to be managed, updated, and distributed to activity participants. Coordination which establishes such a framework is shown in Figure 10.

5. CONCLUSION

This article presented an Enhanced Watermarking Approach for Secure database Service (EWRDN Service), a security service for ensuring privacy of customer data in cloud by trusted system (TA). The main idea is to build a watermarking (for supporting trust) security service. The security solution relies on making changes to traditional database watermarking technique (WRDN). In order to be applied as a service, EWRDN adds watermark data and user signature in order to trace data and provides recovery capabilities, if it is required. EWRDN as compared with WRDN proved to be better. EWRDN saves space between 55% and 56% of WRDN data size. Besides, it gives data owner more control of his data. Moreover, it has the same time WRDN takes to be executed.

EWRDN Service architecture is built to prove data integrity. It works as a part of the trusted third party coordination. It provides monitoring capabilities and then trust between clients and database service provider in the cloud. It helps users to overcome problems of trust that stop them from moving to the cloud. Moreover, it guarantees data integrity, privacy, and non repudiation with the ability to recover data to its origin. Also, it gives users more control over their data by, tracing authorized users activity over database. For future work, techniques of optimization for executing queries and their related operators are being proposed. The relation between query, EWRDN Service and other database security services on different service parties needs to be specified and polished.

6. REFERENCES

[1] *Digital signature standard (DSS)*. National Institute of Standards and Technology (NIST), 2009. Federal Information Processing Standard 186-3.

[2] Imad M. Abbadi and Muntaha Alawneh. A framework for establishing trust in the cloud. *Computers and Electrical Engineering*, 2012.

[3] Aradhana and I. Chana. Developing trust policies for cloud scenarios. In *2nd International Conference on Computer*

and Communication Technology, ICCCT, pages 389– 393, 2011.

[4] L. D. Dhinesh Babu, P. Venkata Krishna, A. Mohammed Zayan, and Vijayant Panda. An analysis of security related issues in cloud computing. In *4th International Conference Contemporary Computing*, IC3. Springer, 2011.

[5] Durgesh Bajpai, Manu Vardhan, and Dharmender Singh Kushwaha. Authentication and authorization interface using security service level agreements for accessing cloud services. In *5th International Conference on Contemporary Computing-IC3*, volume 306 of *Communications in Computer and Information Science*, page 370:382. Springer, 2012.

[6] Eric Bodden, Malte Clasen, and Joachim Kneis. Arithmetic coding revealed a guided tour from theory to praxis. Technical report, McGill University, 2007.

[7] Don Box, David Ehnebuske, Gopal Kakivaya, Andrew Layman, Noah Mendelsohn, Henrik Frystyk Nielsen, Satish Thatte, and Dave Winer. Simple object access protocol (soap) 1.1. W3c note, World Wide Web Consortium, 2000.

[8] Roy H. Campbell, Mirko Montanari, and Reza Farivar. A middleware for assured clouds. *JOURNAL OF INTERNET SERVICES AND APPLICATIONS*, 3:87–94, 2012.

[9] Mariana Carroll, Paula Kotzé, and Alta van der Merwe. Secure cloud computing: Benefits, risks and controls. In *Information Security South Africa*, ISSA, pages 1– 9. IEEE Computer Society, 2011.

[10] WilliamY. Chang, Hosame Abu-Amara, and JessicaFeng Sanford. Security for enterprise cloud services. In *Transforming Enterprise Cloud Services*, chapter 9, pages 341–384. Springer Netherlands, 2010.

[11] Antonio Corradi. Database security management for healthcare saas in the amazon aws cloud. In *Proceedings of the IEEE Symposium on Computers and Communications*, ISCC '12, pages 812–819. IEEE Computer Society, 2012.

[12] Jean-Daniel Cryans, Alain April, and Alain Abran. Criteria to compare cloud computing with current database technology. In *International Workshop On statistical Modelling (IWSM)*, 2008.

[13] Tharam Dillon, Chen Wu, and Elizabeth Chang. Cloud computing: Issues and challenges. In *IEEE International Conference on Advanced Information Networking and Applications*. IEEE Computer Society, 2010.

[14] Thomas Erl. *Web Services and Contemporary SOA*, chapter 6. Pearson Education, 2005.

[15] W. Fawaz, B. Daheb, O. Audouin, M. Du-Pond, and G. Pujolle. Service level agreement and provisioning in optical networks. *IEEE Communications Magazine*, 42:36–43, 2004.

[16] Prof. Dieter Fensel, Dr. Federico Michele Facca, Dr. Elena Simperl, and Ioan Toma. Service science. In *Semantic Web Services*, chapter 3, pages 25–35. Springer, 2011.

[17] M. Fugini and G. Hadjichristofi. Security and trust in cloud scenarios. In *1st International Workshop on Securing Services on the Cloud*, IWSSC, pages 22– 29, 2011.

[18] Tyrone Grandison, E. Michael Maximilien, Sean S. E. Thorpe, and Alfredo Alba. Towards a formal definition of a computing cloud. In *6th World Congress on Services, SERVICES*, pages 191–192. IEEE Computer Society, 2010.

[19] Asit Dan and Richard King and Richard Franck Heiko Ludwig and, Alexander Keller and. A service level agreement language for dynamic electronic services. *Electronic Commerce Research*, 3:43–59, 2003.

[20] Dan Hubbard and Michael Sutton. Top threats to cloud computing. Technical report, Cloud Security Alliance, 2010.

[21] Wassim Itani, Ayman Kayssi, and Ali Chehab. Privacy as a service: Privacy-aware data storage and processing in cloud computing architectures. In *IEEE International Conference on Dependable, Autonomic and Secure Computing*, 2009.

[22] Meiko Jensen, Jorg Schwenk, and and Luigi Lo Iacono Nils Gruschka. On technical security issues in cloud computing. In *IEEE International Conference on Cloud Computing*. IEEE Computer Society, 2009.

[23] Jian Pei Jiawei Han and, Micheline Kamber and. *Data Mining Concepts & Techniques*, chapter 3. Elsevier (Morgan Kaufmann), 3 edition, 2011.

[24] Matthias Klusch. Semantic web service coordination. In *CASCOM: Intelligent Service Coordination in the Semantic Web*, Whitestein Series in Software Agent Technologies and Autonomic Computing, chapter 4, pages 59–104. Birkhuser Basel, Springer, 2008.

[25] Ryan K L Ko, Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg, Qianhui Liang, and Bu Sung Lee. Trustcloud: A framework for accountability and trust in cloud computing. In *IEEE World Congress on Services (SERVICES)*. IEEE Computer Society, 2011.

[26] Wenjuan Li and Lingdi Ping. Trust model to enhance security and interoperability of cloud environment. In *First International Conference, CloudCom*, volume 5931, pages 69–79, 2009.

[27] Zhen Liu, Mark S. Squillante, and Joel L. Wolf. On maximizing service-level-agreement profits. In *Proceedings of the 3rd ACM conference on Electronic Commerce*, EC '01, page 213:223. ACM Digital Library, 2001.

[28] Peter Mell and Tim Grance. The nist definition of cloud computing, 2011.

[29] Rafael Moreno-Vozmediano, Rubn Montero, and Ignacio Llorente. Key challenges in cloud computing to enable the future internet of services. *IEEE Internet Computing*, PP:1, 2012.

[30] Mohamed Al Morsy, John Grundy, and Ingo Mller. An analysis of the cloud computing security problem. In *Proceedings of Asia-Pacific Software Engineering Conference 2010 Cloud Workshop*. IEEE Computer Society, 2010.

[31] CORPORATE NIST. The digital signature standard. *Communications of the ACM*, 35, 1992.

[32] M.P. Papazoglou. Service-oriented computing: concepts, characteristics and directions. In *Proceedings of the Fourth International Conference on Web Information Systems Engineering*, WISE 2003., pages 3–12. IEEE Computer Society, 2003.

[33] Scott Paquettea, Paul T. Jaegerb, and Susan C. Wilsonb. Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly*, 37:245253, 2010.

[34] S. Pearson and A. Benameur. Privacy, security and trust issues arising from cloud computing. In *IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom)*, pages 693 –702, 2010.

[35] R. Perrey and M. Lycett. Service-oriented architecture. In *Proceedings. 2003 Symposium on Applications and the Internet Workshops*, pages 116–119. IEEE Computer Society, 2003.

[36] Rohit Ranchal, Bharat Bhargava, Lotfi Ben Othmane, Leszek Lilien, Anya Kim, Myong Kang, and Mark Linderman. Protection of identity information in cloud computing without trusted third party. In *IEEE Symposium on Reliable Distributed Systems,*, SRDS, pages 368–372, 2010.

[37] Bhaskar Prasad Rimal, Admela Jukan, Dimitrios Katsaros, and Yves Goeleven. Architectural requirements for cloud computing systems: An enterprise cloud approach. *Grid Computing*, 9:3–26, 2011.

[38] Anbang Ruan and Andrew Martin. Repcloud: achieving fine-grained cloud tcb attestation with reputation systems. In *Proceedings of the sixth ACM workshop on Scalable trusted computing*, STC '11, page 3:14. ACM Digital Library, 2011.

[39] Kazue Sako. Digital signature schemes. In *Encyclopedia of Cryptography and Security (2nd Ed.)*, pages 343–344. Springer, 2011.

[40] H. Sato, A. Kanai, and S. Tanimoto. A cloud trust model in a security aware cloud. In *10th IEEE/IPSJ International Symposium on Applications and the Internet (SAINT)*, pages 121 –124, 2010.

[41] Khalid Sayood. *Lossless Compression Handbook*, chapter 5, page 101152. Academic Press, 2004.

[42] S. Subashini and V.Kavitha. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34:1–11, 2011.

[43] Hassan Takabi, James B. D. Joshi, and Gail-Joon Ahn. Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, 8(6):24–31, 2010.

[44] WILLIAM VOORSLUYS, JAMES BROBERG, and RAJKUMAR BUYYA. introduction to cloud computing. In *Cloud Computing: Principles and Paradigms*, chapter 1, page 144. Wiley Press, 2011.

[45] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou. Privacy-preserving public auditing for data storage security in cloud computing. In *IEEE INFOCOM*, page 1:9, 2010.

[46] Yu Yonghong. Privacy protection in secure database service. In *International Conference on Networks Security, Wireless Communications and Trusted Computing*. IEEE Computer Society, 2010.

[47] Nour Zawawi, Rania El-Gohary, Mohamed Hamdy, and Mohamed F. Tolba. A novel watermarking approach for data integrity and non-repudiation in rational databases. In *First International Conference on Advanced Machine Learning Technologies and Applications (AMLTA12)*, 2012.

[48] Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, and Aoying Zhou;. Security and privacy in cloud computing: A survey. In *Sixth International Conference on Semantics Knowledge and Grid*, SKG. IEEE Computer Society, 2011.