Information Science Letters
An International Journal

Efficiency Analysis in Outsourced Database using One Time Signature Scheme

Nabila Kanwal[1] and Aihab Khan[2]

[1]*Department of Software Engineering, Fatima Jinnah Women University, Rawalpindi, Pakistan*
[2]*Department of Computing and Technology, Iqra University, Islamabad, Pakistan.*

Email: nabila_kanwal@ymail.com, aihabkhan@yahoo.com
Received*: 8 Feb. 2012; Revised 15 May. 2012; Accepted 23 Jul. 2012*

Abstract: In the outsourced database model (ODB) entities need third party service providers. As the third party service provider is being untrusted, so there should be a mechanism to determine the integrity and authenticity in the query result which is given to the actual client, by the service provider. In the digital signature schemes, verification is efficient. In this many separate signatures can be combined into a single signature, but the problem with digital signatures (for RSA 1024 bits) is that they have storage overhead. To overcome this weakness, we use one way hash chain that requires little storage as compare to digital signatures. One of the types of hash chain is comb skipchain which can be used to reduce the storage overhead. Winternitz one time signature scheme which is the type of one time signatures scheme is use to generate the public key. In this paper, the comb skipchain construction is use to construct the hash chain by using the public key of the one-time signature schemes and the signature produced is use to authenticate the last value of another comb skipchain. By using this technique the problem of storage overhead in outsourced database model is overcome.

Keywords: Outsourced database (ODB); Digital signature algorithm (DSA).

Introduction

In this modern trend, the information technology services are being outsourced by the increasing number of enterprises through the third party service provider, due to economy of scale who can offer these services for a much lower cost.[1] As the third party service provider being untrusted so there should be a mechanism to determine the integrity and authenticity in the query which is given by the service provider to the actual client. Particularly in the digital signature schemes verification is efficient. In this many separate signatures combined into a single signature, but the problem with digital signatures (for RSA 1024 bits) is that they have storage overhead. Typically the size of digital signature for DSA is between 320 bits and for RSA the size is 1024 bits.[2] In many applications related to security, one way hash chains are being used for the security of data. Figure 1 shows graphical representation of one way hash chain. It's one of the type is "Comb Skipchain Construction", use to reduce the storage overhead and also use to improve the one way hash chain's efficiency.[3] In this research, the Winternitz one time signature scheme is use to generate the public key. The comb skipchain construction is use to construct the hash chain by using the public key of the one-time signature scheme which is used to authenticate the last value of another comb skipchain.[3] So, the problem of storage overhead which is due to digital signatures will be solve by using the proposed technique.

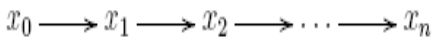

Figure 1. One way hash chain[3].

There are some advantages of the "Comb Skip chain Construction" as it provides the fast and efficient verification as compared to the typical hash chains and on authentication values it has resistance against DOS attacks and also, as it is a type of one way hash chain so it can be used to reduce the storage overheads.[4] As the digital signature has storage overheads in the outsourced database model, "comb skipchain construction" is used to reduce the storage overhead in the proposed technique. In the database outsourcing, the important security concern is with the integrity as when a query result receives from the service provider to client, he wants to be assured that the query result is both complete and correct. Jian et al.[5] Insert tuples to monitor the integrity of the database, if an inserted tuple that satisfies from the reply the query is absent it means integrity is not achieved. In ODB, authentication and integrity is provided by MHT (Markle Hash Tree). It is assumed that for a relation data

owner has built an MHT, where the records have been sorted based on one of the relation attribute values. MHT is given to the untrusted outsourced database server after the root has been signed by the owner.

About the existence of a particular attribute value v, a client then wishes to query the server. If v is present in the tree, it will be represented by one of the leaves and the server will return the nodes from the particular leaf node to the co-path. On the co-path, the nodes are defined as those needed to enable the client to re-compute the root of the tree to verify its signature (which was generated by the data owner). If the signature is valid, the client can be assured that correct response is returned by the server, and therefore it will confirm that the attribute value is present.[1] For record level integrity the intuitive and natural solution is to use the Message Authentication Codes (MAC-s) as they are efficiently verified and computed. In the digital signature schemes, many separate signatures are combined into a single signature. If that single signature is verified, it means that all the separate signatures are also verified. The advantage is that, particularly in digital signature schemes, verification is efficient and the limitations are the storage, computation and bandwidth overheads.[2] To keep guarantee of data integrity and data confidentiality bucket based authentication is used. Bucket based index is basically consist of (1) Bucket Identifier (BID) (2) size of bucket (3) lower bound. In the "Naive Solution", when new tuples are inserted in the bucket, it will again and again recalculate bucket checksum so it has overhead on client and very heavy network traffic. After receiving the query by the server in ODB model, it runs the query to find the corresponding signatures as well as their tuples matching the query predicate. To find the aggregated signature and returns the set of results comprising of the tuples and the aggregated signature, server securely combines individual tuple signatures. When the querier receives the set of tuples with the aggregated signature, then the querier simply verifies it. By including the all of immediate predecessor's hashes, a tuple signature is computed to provide completeness, thereby explicitly chaining (linking) the signatures.[7]

In this paper Section **II** is related to Materials and Methods which consist of (Section II. A) Framework Overview. Section **III** is related to Mathematical Model which consists of (Section III. A) Problem, (Section III. B) Identify Real Problem, (Section III. C) Formulate Mathematical Model, (Section III. D) List of Factors, (Section III. E) Obtain Mathematical Solution. Then Section **IV** consists of Construction of Comb Skipchain. Finally, Section **V** consists of Results and Discussion. Tentative conclusion is also given bellow.

I. Materials and Methods

II. A. Framework Overview

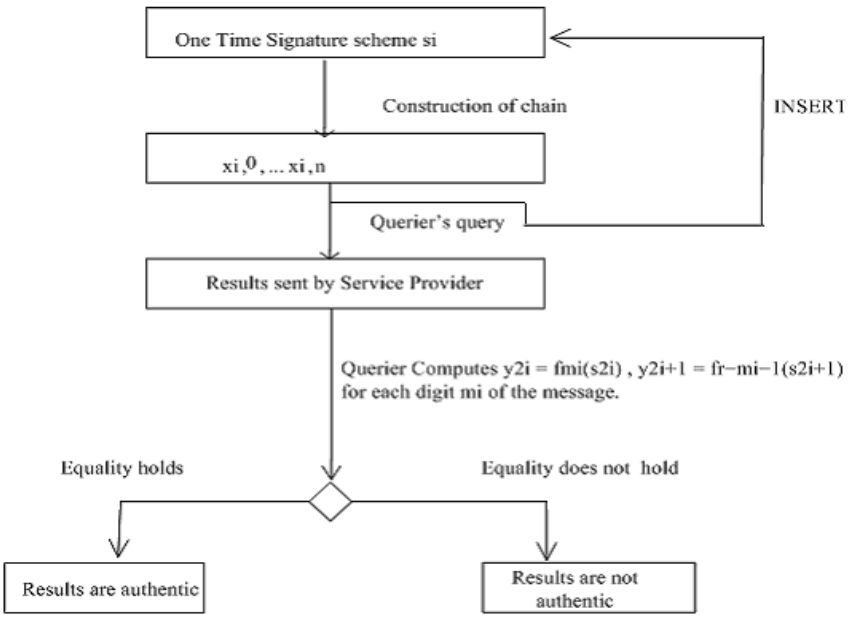

Figure 2. Proposed Model for the solution of storage overhead[8].

Figure 2 showing that the comb skipchain is constructed with the public key of Winternitz one time signature scheme. If the querier asks any query, so the results are given by the third party service provider to the actual client. Now the querier computes $Y_{2i} = f^{(m)}_{i}(s_{2i})$ *and* $Y_{2i+1} = f^{(r-m_i-1)}(s_{2i+1})$ *for each digit* m_i *of the message. If equality holds so results are authentic else results are not authentic.*

II. Mathematical Model

III. A. Problem

In this modern trend database outsourcing plays an important role. For database outsourcing third party service provider is used. The service provider may be untrusted or compromised so there should be a mechanism through which it determine that the integrity and authentication of results which sent by the service provider. Digital signatures are used for this purpose, but digital signature (for RSA 1024 bits) causes storage overhead. In this the size of DSA is 320 bits and for RSA 1024 bits. The problem is how integrity and authentication of results will be achieved using less memory than RSA (1024bits).

III. B. Identify Real Problem

How computation cost in outsourced database is effected by the number of records? How integrity and authentication will be achieved?

Suppose that available data is

Numbers of records in database = n

Numbers of signatures in database = m

III. C. Formulate Mathematical Model

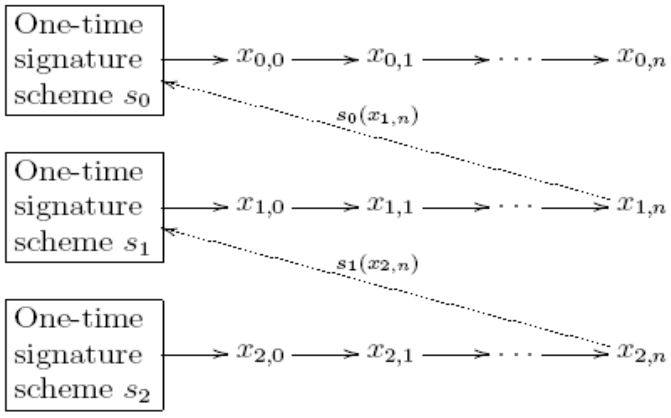

Figure 3. Comb Skipchain Construction[6].

Figure 3. *Showing that the construction of comb skipchain, by using the public key of one time signature scheme and these all are interlinked.*

III. D. List of Factors

Table 1. List of symbols used in technique.

Symbol	Description
S_n	One Time Signature Scheme of nth record
P_n	Public key of nth record
V_n	Node of hash chain of nth record

Table 1. *Showing the symbols which are used in the technique*.

Comb Skipchain construction will be completed in these steps:

III. E. Obtain Mathematical Solution

For signing messages, with the base r and with n digit hash outputs the Winternitz scheme is mostly used.

III. E. I. Key Generation

Randomly from the set $[0, 1]^n$, first signer *(A)* picks the digit uniformly $[X_0 \ldots X2n_{-1}]$.

First signer *(A)* calculates the $[Y_0 \ldots Y_{2n-1}]$

where

$$Y_i = f^{(r-1)}(X_i) \tag{1}$$

Now $[Y_{0\ldots} Y_{2n-1}]$ is consider as the first signer *(A's)* public key.

III. E. II. Signature Generation

For the each digit m_i of the message, first signer *(A)* calculates the

$$s_{2i} = f^{(r-m_i-1)}(X_{2i}) \tag{2}$$

As well as

$$s_{2i+1} = f^{(mi)}(X_{2i+1}) \tag{3}$$

Now the set $[s_0 \ldots s_{2n-1}]$ is the signature.

III. E. III. Verification

For the each of the digit m_i of the message, the verifier can easily checks

$$Y_{2i} = f^{(m_i)}(s_{2i}) \tag{4}$$

As well as

$$Y_{2i+1} = f^{(r-m_i-1)}(s_{2i+1}) \tag{5}$$

III. F. Interpret Mathematical Model

Begin
Customer enters registration information
If CNIC and Mobile number is valid then
Combskip chain is constructed and registration is successful
Else
Return invalid CNIC or mobile number
End
User enters login information
If mobile number and password are valid then
User can view profile can edit profile, change password, view packages details and can verify results
Else
Return invalid mobile number or wrong password
End

III. G. Compare with Reality

If there are small numbers of tuples in ODB then there will be less computation cost consumed. As MD5 produces hash chain of 128 bits, so the total storage = 128 * 7 = 896 bits.[8]

IV. Construction of Comb Skipchain

As shown in the figure 4, one time signature scheme is used to construct the hash chain[8] by using the one time signature scheme's public key.

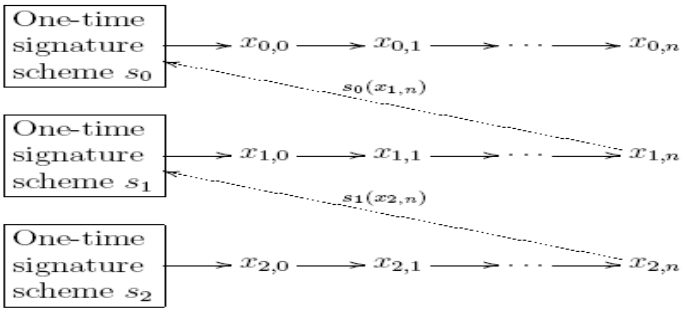

Figure 4. A Comb Skipchain Construction [3]

Figure 4. *showing the comb skipchain, which are constructed by the one way hash chain, and these are interlinked.In this technique, from one time signature scheme the signature basically used to authenticate the last value of another comb skip chain. From one initialization, an unlimited number of times it can be used to authenticate. Further the more secure channel is not required for this construction.*[3]

IV. A. The Entity Authentication Scheme

The description is given bellow as:

IV. B. I. Initialization

- First signer (A) forms a comb skipchain which is constructed from s_0 (one time signature scheme) and a hash chain $[P_0, X_{0,0} \ldots X_{0,n}]$ of the length $[n + 1]$ which constructed from P_0 which is its public key.
- First signer *(A)* sends to *B* the last value $X_{0,n}$ by using an authentic channel.

IV. B. II. Authentication of Entity

- If the end value which is sent to *B* by first signer *(A)* was $X_{i,j}$,where $j \in [1,n]$ so first signer(*A)* sends $X_{i,j-1}$ to *B*.
- If the end value which is sent to *B* by first signer *(A)* was $X_{i,0}$ so first signer(A) sends the value P_i to *B*.
- In this *B* can also verify identity of first signer's *(A's)* by taking the hash of the value which received to come to know that the result is the same or not as the previous value received.
- If the end value which is sent to *B* by first signer *(A)* was P_i so first signer *(A)* made next one time signature scheme s_{i+1} and will construct a next comb skipchain.
- First signer *(A)* will make a signature on last value of the next chain. First signer *(A)* sends signature and the value to *B*.
- Now the verification of the signature, *B* can do, against the P_i public key value. If it is successful then it will authenticated the first signer *(A)* and the value $X_{i+1,n}$.[3]

V. Results and Discussion

V. A. Bit Lengths of RSA, MD5, Comb skipchain

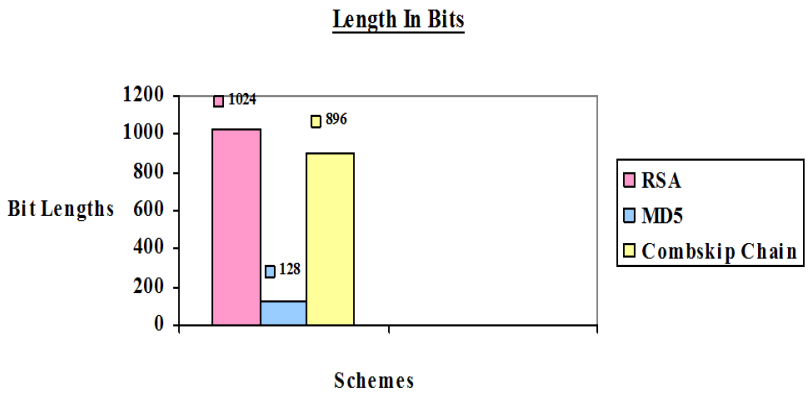

Figure 5. Bit Lengths of RSA, MD5 and Comb Skipchain

V. B. Storage of RSA and Comb skipchain

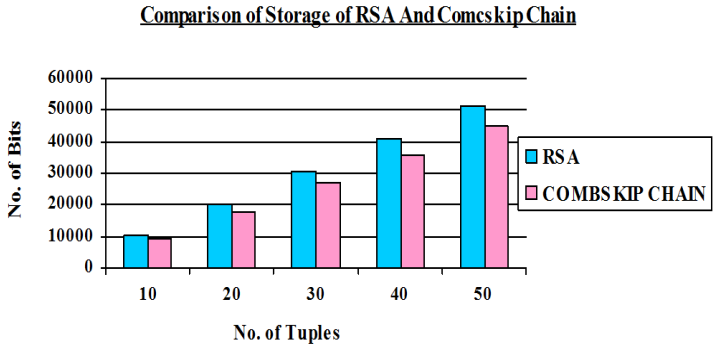

Figure 6. Storage of RSA and Comb Skipchain

Figure 6. *shows number of bits used by n tuples i.e (n tuples x no of bits). As combskip chain consumes less number of bits than RSA so our proposed technique is better than RSA (in terms of bits) to achieve authentication and integrity in ODB.*

V. C. Construction Time of Comb skipChain

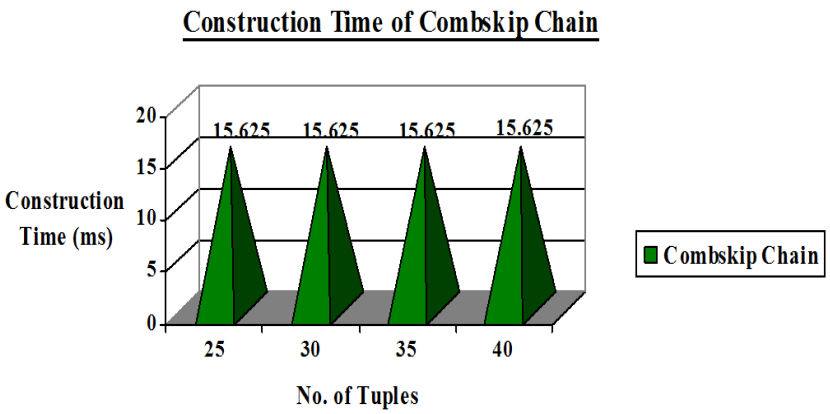

Figure 7. Construction Time of Comb Skipchain.

Figure 7. *shows time (ms) used for construction of combskip chain. As combskip chain is constructed on entire table so increase in number of tuples the construction time of combskip chain will be same.*

V. D. Mean Construction Time of RSA, Comb Skipchain

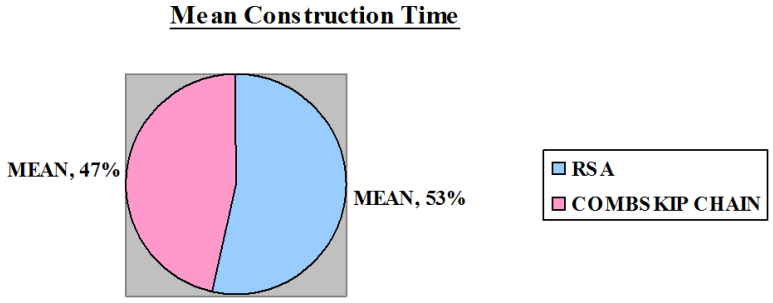

Figure 8. Mean Construction Time of RSA, Comb Skipchain

Figure 8. *Shows mean construction time of RSA and Comb skipchain. As Comb skipchain consumes less number of bits than RSA, so its mean construction time is also less than RSA.*

V. E. Comparison of Standard Deviation, Standard Error of RSA, Comb skipchain

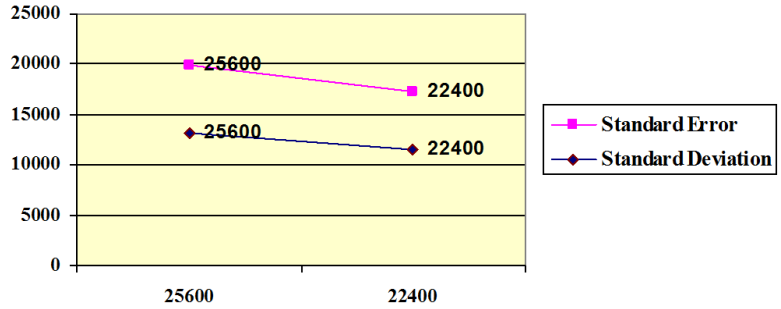

Figure 9. Comparison of Standard Deviation, Standard Error of RSA and Comb Skipchain

Figure 9. *Shows Standard Deviation, Standard Error of RSA and Comb skipchain at their mean.*

V. F. Verification Time

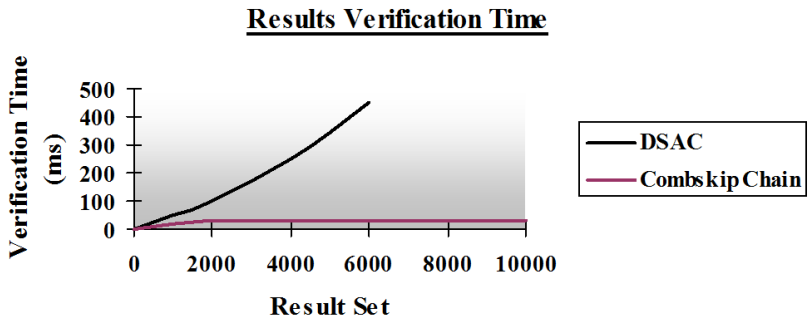

Figure 10. Verification Time

Figure 10. *Shows verification time is constant for tuples of comb skipchain where as when DSAC is used, verification time increases with the increase in number of tuples.*[8]

VI. Summary and Conclusion:

In this modern trend, database outsourcing plays an important role. In the Outsourced Database model (ODB) for the outsourcing, entities need third party service providers. Service provider provides the hardware, software and network resources to operate its client's databases and also use to update, creates and access (query) outsourced data. As the third party service provider is being untrusted, so there should be a mechanism to determine the integrity and authenticity in the query result which is given to the actual client, by the service provider. In the previous approaches (Digital signatures for RSA 1024 bits) there was large storage overhead, to reduce that storage overhead one way hash chain used. As the Comb Skipchain construction is one of the types of one way hash chain. It is use to construct the hash chain by using the public key of the one time signature scheme. In this the signature is basically used to authenticate the last value of another comb skipchain. So, the problem of storage overhead which is due to digital signatures will be solve by using this technique.

References

[1] M. Narasimha, and E. Mykletun, Providing Authentication And Integrity In Outsourced Database Using Merkle Hash Tree's, IEEE Symposium on Research in Security and Privacy, California, Irvine, 1-7 (1980).

[2] M. Narasimha, E, Mykletun, and G. Tsudik, Authentication and Integrity in Outsourced Databases, Journal ACM Transactions on Storage (TOS), 2(2), 1-10 (2006).

[3] Technical Report RHUL–MA–2009–18, Royal Holloway, 1-234, 4 August 2009, Department of Mathematics Royal Holloway, University of London Egham, Surrey TW20 0EX, England.

[4] M. Jakobsson, Y. Hu, and A. Perrig, Efficient Constructions for One-Way Hash Chains, In Proceedings of ACNS (Applied Cryptography and Network Security)', Newyork, 3531, 423-441(2005).

[5] J. Yin, X. Mengy, M. Xiey, and H. Wang, Integrity Auditing of Outsourced Data, In Proceedings of the 33rd International Conference on Very large data bases VLDB '07, Beijing, China, 782–793 (2007).

[6] J. Lu, W. Lu, J. Wang, and Xiaoyong, Bucket-Based Authentication for Outsourced Databases, 22(9), 1160–1180 (25 June 2010).

[7] G. Tsudik, and M. Narasimha, DSAC: An Approach to Ensure Integrity of Outsourced Databases Using Signature Aggregation and Chaining, CIKM '05, In Proceedings of the 14th ACM International Conference on Information and knowledge management, California, Irvine, 1-10 (November 2005).

[8] Nabila Kanwal, Efficiency analysis in outsourced database using one time signature scheme, BSE (Bachelors in Software Engineering), Thesis, Fatima Jinnah Women University, the Mall, Rawalpindi, Pakistan, (2011).