IORD Journal of Science & Technology
E-ISSN: 2348-0831
Volume 3, Issue 3 (MAR-APRIL 2017) PP103 -107
IMPACT FACTOR 1.719
www.iord.in

"Encryption Using Hidden Markov Model to Broadcast Encryption and Short Cipher text"

Ms. Asfiya Shireen Shaikh Mukhtar
(PG Student,VITNagpur)

Abstract

Today data mining is used in many applications areas medical, scientific research, banking and many more. From last decade, Internet has given rise to many privacy issues. To solve these issues many theoretical and practical solutions to the classification problem have been proposed using different security models. However, cloud computing allow users to outsource their data to cloud. User prefers to encrypt the data before storing it on cloud, but performing any classification on encrypted data is main issue. Today's privacy-preserving classification techniques are not useful for encrypted data, so here we uses k-NN classifier over encrypted data in the cloud. The proposed technique protects the security of data, privacy of user's input query, and hides the access patterns. Our aim is to develop a secure k-NN classifier on encrypted data using the semi-honest model. Also, efficiency of K nearest neighbor classification is analyzed using real world data set under different parameters conditions. The proposed protocol protects the confidentiality of data, privacy of user's input query, and hides the data access patterns. To the best of our knowledge, our work is the first to develop a secure k-NN classifier over encrypted data under the semi-honest model. Also, we empirically analyze the efficiency of our proposed protocol using a real-world dataset under different parameter settings.

Keywords—

(HMM,Ciper Text ,Existing System,Proposed System,Implementation, KNN,Hybrid KNN,Result Analysis)

1. Introduction

In this research, we apply Hidden Markov Models (HMMs) to classic cryptanalysis problems. We show that with sufficient ciphertext, an HMM can be used to break a simple substitution cipher. We also show that when limited ciphertext is avail-able, using multiple random restarts for the HMM increases our chance of successful decryption In this application we will make a system where there will be all multiple users can create their accounts, and admin of the application will be able to broadcast the message that message will be displayed to each user who is an authorized user of the application. The Encryption with Cipher text will be used in this application. With the fast advance and pervasive deployment of communication technologies, there is an increasing demand of versatile cryptographic primitives to protect group communications and computation platforms. These new platforms include instant-messaging tools, collaborative computing, mobile ad hoc networks and social networks. These new applications call for cryptographic primitives allowing a sender to securely encrypt to any subset of the users of the services without relying on a fully trusted dealer. Broadcast encryption (BE) [1] is a well-studied primitive intended for secure group-oriented communications. It allows a sender to securely broadcast to any subset of the group members. Nevertheless, a BE system heavily relies on a fully trusted key server who generates secret decryption keys for the members and can read all the communications to any members.Traditional broadcast encryption (BE) schemes allow a sender to securely broadcast to any subset of members but require a trusted party to distribute decryption keys. Group key agreement (GKA) protocols enable a group of members to negotiate a common encryption key via open networks so that only the group members can decrypt the cipher texts encrypted under the shared encryption key, but a sender cannot exclude any particular member from decrypting the ciphertexts. In this paper, we bridge these two notions with a hybrid primitive referred to as contributory broadcast encryption (ConBE). In this new primitive, a group of members negotiate a common public encryption key while each member holds a decryption key. A sender seeing the public group encryption key can limit the decryption to a subset of members of his choice. Following this model, we propose a ConBE scheme with short ciphertexts. The scheme is proven to be fully collusion-resistant under the decision n-

IORD Journal of Science & Technology
E-ISSN: 2348-0831
Volume 3, Issue 3 (MAR-APRIL 2017) PP103 -107
IMPACT FACTOR 1.719
www.iord.in

Bilinear Diffie-Hellman Exponentiation (BDHE) assumption in the standard model. Of independent interest, we present a new BE scheme that is aggregatable. The aggregatability property is shown to be useful to construct advanced protocols.It allows a sender to securely broadcast to any subset of the group members.

2. Existing Methodology

We present the Contributory Broadcast Encryption (ConBE) primitive, which is a hybrid of GKA and BE. This full paper provides complete security proofs, illus-trates the necessity of the aggregatability of the underly-ing BE building block and shows the practicality of our ConBE scheme with experiments. First, we model the ConBE primitive and formalize its security definitions. ConBE incorporates the underlying ideas of GKA and BE. A group of members interact via open networks to negotiate a public encryption key whileeach member holds a different secret decryption key. Us-ing the public encryption key, anyone can encrypt any message to any subset of the group members and only the intended receivers can decrypt. We formalize collusion resistance by defining an attacker who can fully control all the members outside the intended receivers but cannot extract useful information from the cipher text. Second, we present the notion of aggregatable broadcast encryption (AggBE). Coarsely speaking, a BE scheme is aggregatable if its secure instances can be aggregated into a new secure instance of the BE scheme. Specifically, only the aggregated decryption keys of the same user are valid decryption keys corresponding to the aggregated public keys of the underlying BE instances. Finally, we construct an efficient ConBE scheme with our AggBE scheme as a building block. The ConBE con- struction is proven to be semi-adaptively secure under the decision BDHE assumption in the standard model.

3. Problem Statements

A Markov Chain or Markov Process [23] refers to the memoryless process of a stochastic process. A stochastic process possesses the Markov property if the condi- tional probability of the successive states depends only upon the present state and not the ones preceding it. A Hidden Markov Model [23] or HMM is a statistical Markov Model in which the system being modeled is assumed to be a Markov process with unobserved (hidden) states. In simpler Markov models (like a Markov chain), the state is directly visible to the state transition probabilities [23] are the only parameters. In a HMM, the internal state is not directly visible, but the output (dependent on the internal state) is visible. Each state the observer, and therefore has a probability distribution over the possible output tokens. Therefore, the sequence of tokens generated by an HMM provides some information regarding the sequence of internal states.

Notation

The components of a Hidden Markov Model can be represented using the follow-

ing notation:

The components of a Hidden Markov Model can be

represented using the follow-ing notation

= length of the observation sequence

= number of states in the model

= number of observation symbols

= { $_0$, $_1$, . . . , $_{-1}$} = distinct states of the Markov process

= {0, 1, ..., − 1} = set of

possible observations = state

transition probabilities=

observation probability matrix

= initial state distribution= ($_0$,

$_1$, . . , $_{-1}$) = observation

sequence

4. Methodology used in the paper

Double encryption with cyphertext key which will be sent to each broadcast users to decrypt the data. Web socket

IORD Journal of Science & Technology
E-ISSN: 2348-0831
Volume 3, Issue 3 (MAR-APRIL 2017) PP103 -107
IMPACT FACTOR 1.719
www.iord.in

will be used for the broadcasting. It is good to iuse socket for messaging application and broadcasting. We next define the security of a ConBE scheme. Several methods have been proposed to transform public key encryption (PKE) with security against chosen-plaintext attacks (CPA) into encryption against adaptively chosen-ciphertext attacks (CCA2) in the standard model. In [48], Canetti et al. suggested conversion from CPA-secure IBE to CCA2secure PKE using a one-time signature. In [49], Matsuda and Hanaoka proposed to obtain a CCA2-secure PKE from any CPA-secure PKE with a universal computational extractor. In 0018-9340 (c) 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.vThis article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TC.2015.2419662, IEEE Transactions on Computers 015.2419662, IEEE Transactions on Computers IEEE TRANSACTIONS ON COMPUTERS, VOL. XXX, NO. XXX, XXX 2015 4 [50], Liu et al. obtained a CCA2-secure ABE from a CPAsecure ABE without extra cryptographic primitives, but with an additional on-the-fly dummy attribute. We note that these methods are applicable to our ConBE setting with/without modification (e.g., by adding an on-the-fly dummy receiver). The cost depends on the methods, i.e., a universal computational extractor, a one-time signature or a dummy user. Hence, it is sufficient to only define the CPA security of a ConBE scheme. However, noting that ConBE is designed for distributed applications where the users are likely to be corrupted, we include full collusion resistance into our security definition.

Result Analysis

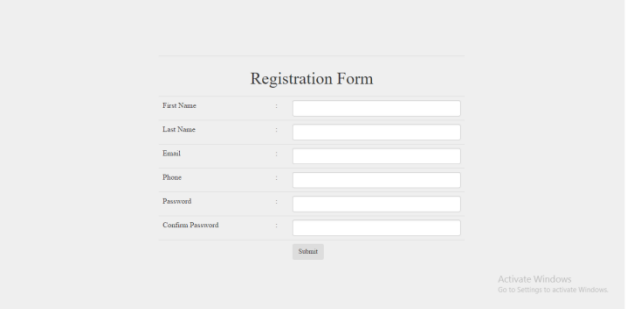

Fig: ***Registration Page***

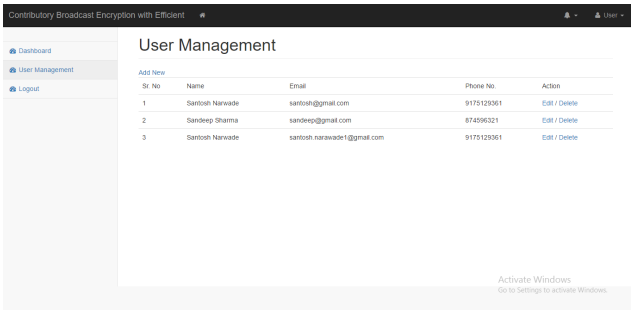

Fig:***User Management Page***

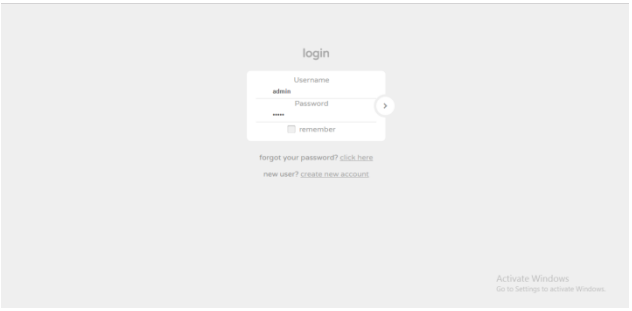

Fig:Login Page

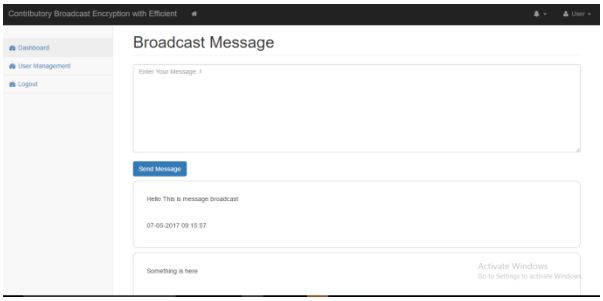

Fig:Dashboard Page

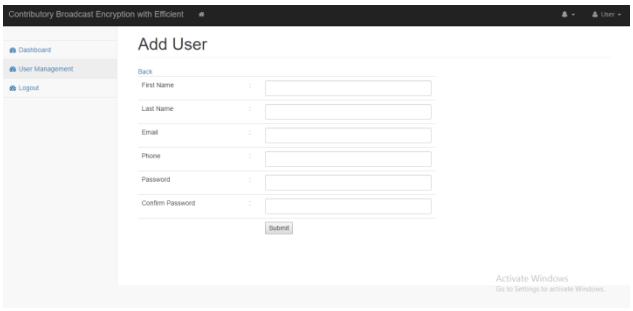

Fig:Add new user

***Reference*.**

1. D. H. Phan, D. Pointcheval and M. Strefler, “Decentralized Dynamic Broadcast Encryption,” in Proc. SCN 2012, 2011, vol. LNCS 7485, Lecture Notes in Computer Science, pp. 166-183
2. [7] M. Steiner, G. Tsudik and M. Waidner, “Key Agreement in Dynamic Peer Groups,” IEEE Transactions on Parallel and Distributed Systems, vol. 11, no. 8, pp. 769-780, 2000.
3. [8] A. Sherman and D. McGrew, “Key Establishment in Large Dynamic Groups Using One-way Function Trees,” IEEE Transactions on Software Engineering, vol. 29, no. 5, pp. 444-458, 2003.
4. [9] Y. Kim, A. Perrig and G. Tsudik, “Tree-Based Group Key Agreement,” ACM Transactions on Information System Security, vol. 7, no. 1, pp. 60-96, 2004.
5. [10] Y. Mao, Y. Sun, M. Wu and K.J.R. Liu, “JET: Dynamic Join-ExitTree Amortization and Scheduling for Contributory Key Management,” IEEE/ACM Transactions on Networking, vol. 14, no. 5, pp. 1128-1140, 2006.
6. [11] C. Boyd and J.M. Gonz´alez-Nieto, “Round-Optimal Contributory Conference Key Agreement,” in Proc. PKC 2003, 2003, vol. LNCS 2567, Lecture Notes in Computer Science, pp. 161-174.
7. [12] W.-G. Tzeng and Z.-J. Tzeng, “Round Efficient Conference Key Agreement Protocols with Provable Security,” in Proc. Asiacrypt 2000, 2000, vol. LNCS 1976, Lecture Notes in Computer Science, pp. 614-627.
8. [13] R. Dutta and R. Barua, “Provably Secure Constant Round Contributory Group Key Agreement in Dynamic Setting,” IEEE Transactions on Information Theory, vol. 54, no. 5, 2007-2025, 2008.
9. [14] W.-G. Tzeng, “A Secure Fault-Tolerant Conference-Key Agreement Protocol,” IEEE Transactions on Computers, vol. 51, no.4, pp. 373-379, 2002.
10. [15] X. Yi, “Identity-Based Fault-Tolerant Conference Key Agreement,” IEEE Transactions Dependable Secure Computing vol. 1, no. 3, 170178, 2004.
11. [16] M. Burmester and Y. Desmedt, “A Secure and Efficient Conference Key Distribution System,” in Proc. Eurocrypt 1994, 1994, vol. LNCS 950, Lecture Notes in Computer Science, pp. 275-286.
12. [17] A. Joux, “A One Round Protocol for Tripartite Diffie-Hellman,” Journal of Cryptology, vol. 17, no. 4, pp. 263-276, 2004.
13. [18] D. Boneh and A. Silverberg, “Applications of Multilinear Forms to Crytography,” Contemporary Mathematics, vol. 324, pp.71-90, 2003.
14. [19] E. Bresson, O. Chevassut and D. Pointcheval, “Provably Authenticated Group Diffie-Hellman Key Exchange – The Dynamic Case,” in Proc. Asiacrypt 2001, 2001, vol. LNCS 2248, Lecture Notes in Computer Science, pp. 290-309.
15. [20] E. Bresson, O. Chevassut and D. Pointcheval, “Dynamic Group DiffieHellman Key Exchange under

Standard Assumptions," in Proc. Eurocrypt 2002, 2002, vol. LNCS 2332, Lecture Notes in Computer Science, pp. 321-336.

16. [21] E. Bresson, O. Chevassut, D. Pointcheval and J.-J. Quisquater, "Provably AuthenticatedGroupDiffie-HellmanKeyExchange,"in Proc. ACM CCS 2001, 2001, pp. 255-264.
17. [22] J. Snoeyink, S. Suri and G. Varghese, "A Lower Bound for Multicast Key Distribution," in Proc. INFOCOM 2001, 2001, pp. 422-431.
18. [23] H.J. Kim, S.M. Lee and D. H. Lee, "Constant-Round Authenticated Group Key Exchange for Dynamic Groups," in Proc. Asiacrypt 2004, 2004, vol. LNCS 3329, Lecture Notes in Computer Science, pp. 245259.
19. [24] M. Abdalla, C. Chevalier, M. Manulis and D. Pointcheval, "Flexible Group Key Exchange with On-demand Computation of Subgroup Keys," in Proc. Africacrypt 2010, 2010, vol. LNCS 6055, Lecture Notes in Computer Science, pp. 351-368.
20. [25] S. Jarecki, J. Kim and G. Tsudik, "Flexible Robust Group Key Agreement," IEEE Transactions on Parallel Distributed Systetems, vol. 22, no. 5, pp. 879-886, 2011.

1.