IMPLEMENTATION OF SECURITY ON NET BANKING

Dr.V.Kavitha[1], Manthra.T[2] , Anupriya.M[3], Aishwarya.R[4]
[1]Assistant Professor (Sr.Gr) / CSE, Velalar College of Engineering and Technology, Erode.
[2]Final year CSE, Velalar College of Engineering and Technology, Erode.
[3]Final year CSE, Velalar College of Engineering and Technology, Erode.
[4]Final year CSE, Velalar College of Engineering and Technology, Erode.

ABSTRACT:

The main objective of the project is to develop online Banking system for banks. In present system all banking work is done manually. Users have to visit bank to Withdrawal or Deposit amount. In present bank system it is also difficult to find account information of account holder. In this bank management system we will automate all the banking process. In our bank management system user can check his balance online and he can also transfer money to other account online. In this Software you can keep record for daily Banking transactions. The main purpose of developing bank management system is to design an application, which could store bank data and provide an interface for retrieving customer related details with 100% accuracy. This bank management system also allow user to add new customer account, delete account and user can also modify existing user account information. Using this system user can also search any individual account in few seconds. Using our bank management system user can also check any translation in any account. Our system also provides security check to reduce fraud. The system will check the user's existence in the database and provide the set of services with respect to the role of the user.

KEYWORDS: Withdrawal, deposit, transaction, retrieving, security.

---

1. INTRODUCTION

Cryptography or **cryptology** is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics. Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.

Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent sense. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons from doing the same.

Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances, e.g., improvements in integer factorization algorithms, and faster computing technology require these solutions to be continually adapted. There exist information-theoretically secure schemes that probably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms.

The growth of cryptographic technology has raised a number of legal issues in the information age. Cryptography's potential for use as a tool for espionage and sedition has led many governments to classify it as a weapon and to limit or even prohibit its use and export. In some jurisdictions where the use of cryptography is legal, laws permit investigators to compel the disclosure of encryption keys for documents relevant to an investigation. Cryptography also plays a major role in digital rights management and copyright infringement of digital media.

2. LITERATURE SURVEY

2.1 On k-Anonymity and the Curse of Dimensionality

In recent years, the wide availability of personal data has made the problem of privacy preserving data mining an important one. A number of methods have recently been proposed for privacy preserving data mining of multidimensional data records. One of the methods for privacy preserving data mining is that of *anonymization*, in which a record is released only if it is indistinguishable from *k* other entities in the data. We note that methods such as *k*-anonymity are highly Depend upon spatial locality in order to effectively implement the technique in a statistically robust way. In high dimensional space the data becomes sparse, and the concept of spatial locality is no longer easy to define from an application point of view. In this paper, we view the *k*-anonymization problem from the perspective of inference attacks over all possible combinations of attributes. We show that when the data contains a large number of attributes which may be considered quasi- identifiers, it becomes difficult to anonym zed the data without an unacceptably high amount of information loss. This is because an exponential number of combinations of dimensions can be used to make precise inference attacks, even when individual attributes are partially specified within a range. We provide an analysis of the effect of dimensionality on *k*-anonymity methods. We conclude that when a data set contains a large number of attributes which are open to inference attacks, we are faced with a choice of either completely suppressing most of the data or losing the desired level of anonymity. Thus, this paper shows that the curse of high dimensionality also applies to the problem of privacy preserving data mining.

2.2 Practical Privacy: The SULQ Framework

We consider a statistical database in which a trusted administrator introduces noise to the query responses with the goal of maintaining privacy of individual database entries. In such a database, a query consists of a pair (S, f) where S is a set of rows in the database and f is a function mapping database rows to {0, 1}. The true answer is Pi ∈S f (di), and a noisy version is released as the response to the query. Results of Dinar, Dwarf, and Nazism show that a strong form of privacy can be maintained using a surprisingly small amount of noise – much less than the sampling error – provided the total number of queries is sub linear in the number of database rows. We call this query and (slightly) noisy reply the SULQ (Sub-Linear Queries) primitive. The assumption of sub linearity becomes reasonable as databases grow increasingly large. We extend this work in two ways. First, we modify the privacy analysis to real-valued functions f and arbitrary row types, as a consequence greatly improving the bounds on noise required for privacy. Second, we examine the computational power of the SULQ primitive. We show that it is very powerful indeed, in that slightly noisy versions of the following computations can be carried out with very few invocations of the primitive: principal component analysis, k means clustering, the Perceptron Algorithm, the ID3 algorithm, and (apparently!) all algorithms that operate in the in the statistical query learning model

2.3 The Cost of Privacy: Destruction of Data-Mining Utility in Anonym zed Data Publishing

Re-identification is a major privacy threat to public datasets containing individual records. Many privacy protection algorithms rely on generalization and suppression of "quasi-identifier" attributes such as ZIP code and birthdate. Their objective is usually syntactic sanitization: for example, *k*-anonymity requires that each "quasi-identifier" tuple appear in at least *k* records, while *l*-diversity requires that the distribution of sensitive attributes for each quasi-identifier have high entropy. The utility of sanitized data is also measured syntactically, by the number of generalization steps applied or the number of records with the same quasi-identifier. In this paper, we ask whether generalization and suppression of quasi-identifiers offer any benefits over trivial sanitization which simply separates quasi-identifiers from sensitive attributes. Previous work showed that *k*-anonymous databases can be useful for data mining, but *k*-anonymization does not guarantee any privacy. By contrast, we measure the tradeoff between privacy (how much can the adversary learn from the sanitized records?) and utility, measured as accuracy of data-mining algorithms executed on the same sanitized records.

For our experimental evaluation, we use the same datasets from the UCI machine learning repository as were used in previous research on generalization and suppression. Our results demonstrate that even modest privacy gains require almost complete destruction of the data-mining utility. In most cases, trivial sanitization provides equivalent utility and better privacy than *k*-anonymity, *l*-diversity, and similar methods based on generalization and suppression.

2.4 Privacy Skyline: Privacy with Multidimensional Adversarial Knowledge

Privacy is an important issue in data publishing. Many organizations distribute non-aggregate personal data for research, and they must take steps to ensure that an adversary cannot predict sensitive information pertaining to individuals with high confidence. This problem is further complicated by the fact that, in addition to the published data, the adversary may also have access to other resources (e.g., public records and social networks relating individuals), which we call *external knowledge*. A robust privacy criterion should take this external knowledge into consideration.

In this paper, we first describe a general framework for reasoning about privacy in the presence of external knowledge. Within this framework, we propose a novel multidimensional approach to quantifying an adversary's external knowledge. This approach allows the publishing organization to investigate privacy threats and enforce privacy requirements in the presence of various types and amounts of external knowledge. Our main technical contributions include a multidimensional privacy criterion that is more intuitive and flexible than previous approaches to modeling background knowledge. In addition, we provide algorithms for measuring disclosure and sanitizing data that improve computational efficiency several orders of magnitude over the best known techniques.

2.5 Revealing Information while Preserving Privacy

We examine the tradeoff between privacy and usability of statistical databases. We model a statistical database by an *n*-bit string $d1,..,dn$, with a query being a subset $q \subseteq [n]$ to be answered by $\Sigma i \varepsilon q di$. Our main result is a polynomial reconstruction algorithm of data from noisy (perturbed) subset sums. Applying this reconstruction algorithm to statistical databases we show that in order to achieve privacy one has to add perturbation of magnitude $(\Omega \sqrt{n})$. That is, smaller perturbation always results in a strong violation of privacy. We show that this result is tight by exemplifying access algorithms for statistical databases that preserve privacy while adding perturbation of magnitude $\tilde{O}(\sqrt{n})$.For time-*T* bounded adversaries we demonstrate a privacy preserving access algorithm whose perturbation magnitude is $\approx \sqrt{T}$.

3. METHODOLOGY

Minimum Identity Key Exposure (MIKE) Technique

Used to maintain the customer details in the manner so that no all the details of the customers are exposed to unauthorized users. It maintains the term and limitation for the data to be published so that no customer details could be misused.

CDA document generation system that generates CDA documents on different developing platforms and CDA document integration system that integrates multiple CDA documents scattered in different banks for each customer.

The benefits of adopting this system are as follows.

1. The system is accessible through an Open API and developers can continue working on their developer platforms they specialize in such as Java, .NET, or C/C++.

2. Banking systems can simply extend their existing system rather than completely replacing it with a new system.

3. It becomes unnecessary for bank to train their personnel to generate, integrate, and view standard-compliant CDA documents.

4. The cloud CDA generation service produces documents in the CDA format approved by the National Institute of Standards and Technology (NIST).

5. If this service is provided for free at low price to bank, existing EHR are more likely to consider adoption of CDA in their practices.

Algorithm:

MIKE (Minimum Identity Key Exposure) algorithm is used to encrypt and decrypt the password in database by two level process which is shown in figure 1.

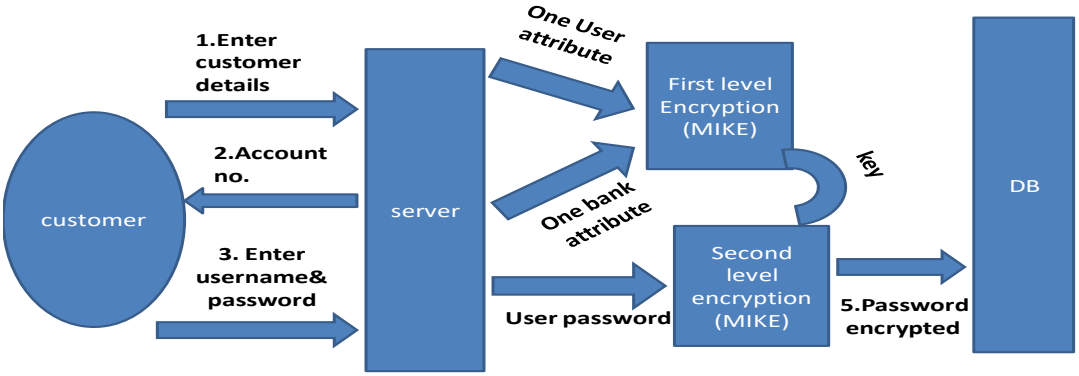

Figure 1.system design

Assumption:

- n is the number of digits in the password
- k_0 and k_1 are integers fixed by the protocol.
- m is the password, an $(n - k_0 - k_1)$-bit string
- G and H are typically some cryptographic hash functions fixed by the protocol.
- $\oplus$ is an XOR operation.

To encode,

- r is a randomly generated k_0-bit string
- $X = m \oplus G(r)$
- H reduces the $n - k_0$ bits of X to k_0 bits.
- $Y = r \oplus H(X)$
- The output is $X \parallel Y$ where X is shown in the diagram as the leftmost block and Y as the rightmost block.

To decode

- recover the random string as $r = Y \oplus H(X)$
- recover the message as $m = X \oplus G(r)$

4. CONCLUSION

This project is developed to nurture the needs of a user in a banking sector .Future version of this project will enhance the security of data than the current version. Registration and login are the essential steps to open an account, transaction, checking the balance etc, but advancements in technology have added the feature to protect the password. All banks have rules about how to open and close an account, how to perform transaction such as withdraw, deposit, fund transfer and how to check the balance. Banks are providing internet banking services so, that the customers can be attracted. By asking the bank employs to know that maximum numbers of internet bank account holders are youth and business man. Online banking is an innovative tool that is fast becoming a necessity, so the security for the password stored in the database is became one of important threads in banking .It is a successful strategic weapon for banks to remain profitable in a volatile and competitive marketplace of today. If proper security is provided to the password then the customer details in database is maintained securely. Secondly the website should be made friendlier from where the first time customers can directly make and access their accounts. Thus the Bank Management System it is developed and executed successfully.

5. REFERENCES

1. Arnold, M. (6 Oct. 2014) ; "Banks Face Rising Threat from Cyber Crime," *Financial Times*, www.ft.com /content/5fd20f60-4d67-11e4-8f75 -00144feab7de.

2. Article: Online banking, Website: https://en.wikipedia.org/wiki/Online_banking (June 29, 2015), 12.30 Am.

3. Crosman, P. (23 Sept. 2015) ; "Hackers to Bankers: Pay Up or We Attack Your Website," *American Banker*, www.americanbanker.com/news/bank technology /hackers-to-bankers -pay-up-or-we-attack-your-website -1076912-1.html.

4. Cuomo, A.M. and Lawsky, B.M. (May 2014) ; *Report on Cyber Security in the Banking Sector*, New York State Dept. of Financial Services, www.dfs.ny.gov /reportpub/dfs_cyber_banking _report_052014.pdf.

5. Kshetri , N. (21 Oct. 2009) ; "Hacking the Odds," *Foreign Policy*, foreign-policy .com/2009/10/21/hacking -the-odds.

6. Learning MYSQL, JavaScript, J Query, PHP, HTML, CSS3, (2014-2015) Website: http://www.w3schools.com,

7. Messmer, E. (4 Apr. 2014) ; "New Federal Rule Re-quires Banks to Fight DDoS Attacks," *Network World*, www.networkworld.com/article/2175847 /network-security/new-federal -rule-requires-banks-to-fight-ddos -attacks.html.

8. Nir kshetri, (January 2017) university of north carolina at Greensboro IEEE-Banking on Availiability-