Fortifying Online Banking Transactions Against Forensic Salami Slicing with Homomorphic Encryption.

G.Swapna[1], P.Swathi[2], J.Priyanka[3]

[1] Assistant Professor, Department of CSE, Sri Indu Institute of Engineering & Technology, Hyderabad

[2] Assistant Professor, Department of CSE, Sri Indu Institute of Engineering & Technology, Hyderabad

[3] Assistant Professor, Department of CSE, Sri Indu Institute of Engineering & Technology, Hyderabad

Abstract: ***Internet banking has become one among the fastest and easiest ways of banking. The threat of cyber security attacks set a great challenge for the internet banking industries, where the security of our data has become a huge issue. This paper aims to describe a type of information attack or theft called salami slicing attack. In a nutshell, salami slicing attack occurs when a small piece of information is acquired from various sources in such a way that the victims whose information ware acquired from didn't notice. So many researches were carried out till date to solve the issue of salami attack nevertheless all of them seem to be very unrealistic. Salami attack is correspondingly called penny splinter, not observed stealing (NoS). The remedy for this kind of attack is achieved by proposing homomorphic encryption. When the info is transferred to the general public area, there are many encryption algorithms to secure the operations and therefore the storage of the info. But to process data located on remote server and to preserve privacy, homomorphic encryption is beneficial that permits the operations on the cipher text, which may provide an equivalent results after calculations because the working directly on the data. In this paper, the most focus is on public key cryptographic algorithms supported homomorphic encryption scheme for preserving security.***

Keywords: Salami Slicing Attack, Penny Splinter, Not Observed Stealing (Nos), Homomorphic Encryption, Cryptography, Encryption, Decryption

1. Introduction

The use of electronic banking is increasing day by day. Customers and businesses can interact and manage their financial transactions, paying bills, investments, e-cheques, etc. With such increase, the possibility of attacking e-banking services inherently increased as well. These attacks considerably threatens banks customers, bank reputation and trustworthy. This era of the cyber world has many intruders which makes internet vulnerable. This is the rationale we'd like to secure cyber world from various quite existent attacks are often caused by the intruders. In search of identifying those intruders which can make the security networks vulnerable, we need to find their activities or several kinds of possible attacks on data, and then only we could prevent the info to being stolen. The basic necessity for the smart banking industry is important for people to possess trust in their account accessibility and security of their privacy. Many intruders are there to attack the user's account and it's very liable to detect the cyber-crime which is occurring to the user's account. In the present competitive world of hackers where every expert is looking forward to form money or to be famous, one among the main attack used is that the salami attack, for this reason salami attack is one among the foremost discussed attack in computer classes or between security experts. Salami attack may be a process by which a private steal bit of data from numerous sources

A "salami-slicing attack" or "salami fraud" could be a technique by which cyber-criminals steal money or resources a small amount at a time in order that there's no noticeable difference in overall size. The perpetrator gets away with these little pieces from an outsized number of resources and thus accumulates a substantial amount over a period of your time. The essence of this method is the failure to detect misappropriation. The most classic approach is that the "collect-the-roundoff" technique. Stealing money electronically is that the commonest use of the salami-slicing technique, but it's not restricted to concealment. The salami technique also can be applied to collect little bits of data over a period of your time to deduce an overall picture of a corporation. This act of distributed operation could also be against a private or a corporation. Data are often collected from internet sites, advertisements, documents collected from trash cans, and therefore the like, gradually build up an entire database of factual intelligence about the target.

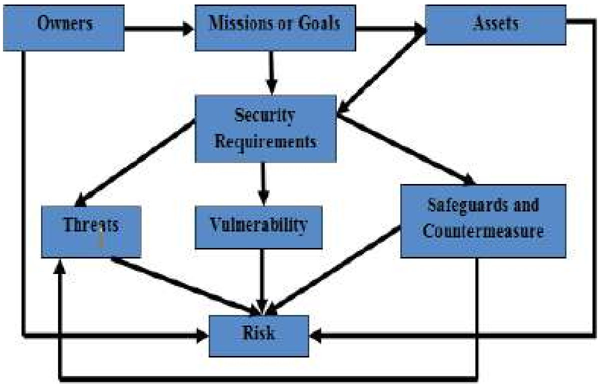

Figure 1: Risk Assessment

1.1 Types of Salami Attacks

1.1.1 Internal Attacks

This is the foremost common sort of salami attack which occurs when a private working within the organization who knows about the safety system within the organization attempt to steal from the organization and causes serious damage. For example, when an accountant of a particular bank who engaged with the bank customers on a daily basis, try to insert a program into the bank server that will divert one rupee from each customer that makes a transaction from his work station to his account, at the end of the day after transacting with five thousand customers he will get a sum of 5,000 rupees into his account.

1.1.2 External Attacks

As the name implies, the external attack may be a quite salami attack that happens outside the organization. A situation where the attacker leaves outside the organization but tries to steal information from the organization causing serious damage to the organization is known as an external attack.

2. Forms of Salami Attacks

In 1940s salami attack was used to lunch different kind of internet attack such as, stealing one’s internet banking information or revealing opponent’s sensitive information during political race for this reasons salami attack was also called divide and conquer.

In these present days of recent technology, there are several and different quite operational wallets where one can enhance currency to the wallet and used the added money to make online transactions (that is to buy goods or transfer the money to another wallet) it can also be used to make payments in an eatery, supermarket, to a taxi driver etc. This improvement is good technology advancement. However, this wallet can be hacked by intruders in to the wallet server to deduct a small amount of money from each wallet, for example if one rupee (1) is deducted from each wallet, would someone aware in communicating them to crisscross about the facts? If someone acquaintances them, needless to say the phone charges are going to be quite one rupee (1) if there's not a toll free facility. Maximum of us won’t cognizance loosing that one rupee (1). Now, if the hacker deduct one rupee (1) from 2 million wallets, then hacker will make a sum of 2 million rupees (2,000,000.00). Salami attack is classified in to two forms.

2.1 Intentional Form

This form of salami attack refers to stealing of one’s information knowingly, mostly for fun, fame, fund, political uses etc. For example when we go to a mall to purchase some clothes etc. On the worth tag we'll see price like 1999/- (one thousand nine hundred and nighty nine rupees) but once we give the cashier 2000\- (two thousand rupees) he will not refund the one rupee (1) change. Imagine if this were done on 5000 customers, the cashier would accumulate a sizable sum at the close of the day. These things aren't somewhat novel, but maximum of the individuals already familiar about it.

2.2 Unintentional Form

Unintentional form of salami attack occurs accidentally, mostly as a result of complexity of information that an individual is working on, singularity of information source etc.

3. Proposed Method

3.1 Homomorphic Encryption Algorithm

Security is that the prime requirement because cyber crimes are increasing nowadays. Today, the banking sectors is needed to be secure for preserving the security of data. There are many banking sectors are available but to store the data over those environments can be expensive than public area. Hence, everyone is convenient to store the data on public cloud i.e. Internet. There are many encryption algorithms are available. Homomorphic encryption enables that secure environment during which the operations are often done on the already encrypted data and therefore the same results are often obtained as on original data.

Homomorphic encryption is the encryption on the already encrypted data rather than on the original data with providing the result as it is done on the plain text. The complex mathematical operations are often performed on the cipher text without changing the character of the encryption.

Functions of homomorphic encryption homomorphic encryption h may be a set of four functions. as shown in figure 2.
H = {Key Generation, Encryption, Decryption, Evaluation}

1) Key generation: client will generate pair of keys public key PK and secret key SK for encryption of plaintext.
2) Encryption: using secret key SK client encrypt the plain text pt and generate ESK (PT) and along with public key PK this cipher text ct will be sent to the server.
3) Evaluation: server has a function f for doing evaluation of cipher text CT and performed this as per the required function using PK.
4) Decryption: generated eval (f(PT)) will be decrypted by client using its SK and it gets the original result.

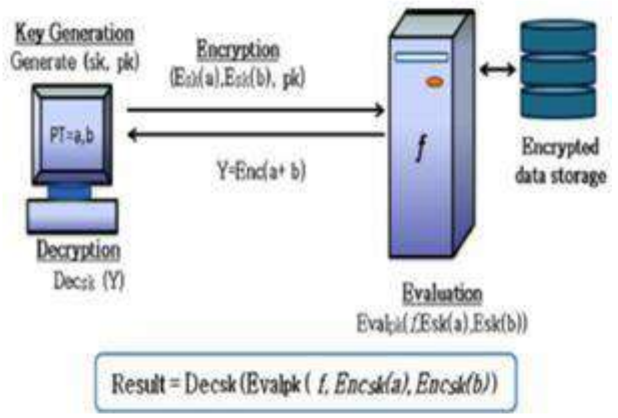

Figure 2: Homomorphic Encryption Functions

3.2 Cryptographic Techniques in Cloud Computing

Some of the significant and mostly used public key cryptosystems are presented as below:-

3.2.1 RSA Cryptosystem[Multiplicative Homomorphic Encryption]

RSA cryptosystem satisfies multiplicative homomorphic property or in other words, rsa cryptosystem is an example of partial homomorphic encryption mechanism.

Suppose, CT1 and CT2 are two cipher texts. MSG1 and MSG2 are the plain texts.

CT1 = MSGE 1 MOD N

CT2 = MSGE 2 MOD N

Where, E: is public key exponent; N = P.Q: is product of two large prime numbers P and Q.

CT1 . CT2 = MSGE1 .MSGE 2 MOD N

So, multiplicative homomorphic property is: (MSG1.MSG2) **E**MOD**N**. So, if the encryption of a message MSG is given by –
E(MSG) = MSGE MOD N

Homomorphic property is then –
E(MSG1) . E(MSG2) = MSGE 1 . MSGE 2 MOD N = (MSG1.MSG2) E MOD N = E(MSG1.MSG2)

3.2.2 Paillier Cryptosystem [Additive Homomorphic Encryption]

In paillier cryptosystem, encryption function is additively homomorphic

GIVEN, **E(M1) AND E(M2),**

Where, M1 and M2 are plain texts. The computation of cipher text (encryption method) in paillier cryptosystem is as –

C = GM.R N MOD N 2

We cannot get **E (M1.M2). We can only get E(M1 + M2).**

4. Problem Identification

Today, data privacy and security becomes an essential part of various cloud based applications, multiparty computation scenarios etc. Homomorphic encryption is a recently evolved technique, which solves the problems of confidentiality and privacy of the stored data. Still, there exist many complications to practically apply these homomorphic encryption mechanisms. The core problems, which we have identified in the present existing system are as below for some cryptographic algorithms, after applying the encryption algorithm on plain text data, the size of cipher text is more as compare to original plain text. The reason may be due to some padding procedure. So, to perform computations on this encrypted data, will take more computational time. Cipher text may comprise some noise elements in it that becomes relatively massive with the subsequent homomorphic multiplication computations, and only those cipher texts, whose noise estimation remains within a certain threshold value, can be decrypted accurately.

5. Conclusion

Today's banking sectors (including the business environment) has benefited immensely from the exponential growth of the internet. E-banking revolutionized the banking business through the provision of many customer-related benefits and new business platforms for banks. However, it came with a price, mainly in terms of banking risks, challenges, and security issues. To protect against various forms of frauds, the security aspect must be considered at all levels of financial organizations. Many researchers have proposed several methods for fraud prevention and detection. Homomorphic encryption provides the best solution for data security. By using this homomorphic encryption user sensitive information secured from intruder and salami slicing attack.

References

[1] Abdul Rasheed, A., Babaita, I.S. And Yinusa, M.A., 2012. Fraud and its Implications for Bank Performance in Nigeria. International Journal of Asian Social Science, 2(4), Pp.382-387.

[2] Abu-Shanab, E. And Matalqa, S., 2015. Security and Fraud Issues of E-Banking. Int. J. Comput. Netw.Appl, 2, pp.179- 187.

[3] Anthala, H.R., 2018. Banking System in India a Legal Study with Special Reference to Fraud and Forgery in Public Sector Banks in Ambala City Haryana.

[4] Bhasin, M., 2007. Mitigating Cyber Threats to Banking Industry. The Chartered Accountant, 50(10), pp.1618-1624.

[5] Bhasin, M.L., 2015. An Empirical Study of Frauds in the Banks.

[6] Bhasin, M.L., 2015. Menace of Frauds in the Indian Banking Industry: An Empirical Study.

[7] Bhasin, M.L., 2016. Challenge of Mitigating Bank Frauds by Judicious Mix Of Technology: Experience of A Developing Country. Economics, Management and Sustainability, 1(1), pp.23-41.

[8] Bhasin, M.L., 2016. Integration of Technology to Combat Bank Frauds: Experience of a Developing Country. Wulfenia Journal, 23(2), pp.201-233.

[9] Bhasin, M.L., 2016. The Fight against Bank Frauds: Current Scenario and Future Challenges. Ciencia E Tecnicavitivinicola Journal, 31(2), pp.56-85.

[10] Morgado, M., Rolo, S., Macedo, A.F., Castelo-Branco, M.Association of Statin Therapy With Blood Pressure Control in Hypertensive Hypercholesterolemic Outpatients in Clinical Practice(2011) Journal of Cardiovascular Disease Research, 2 (1), pp. 44-49.