*Journal of Advances and Scholarly Researches in Allied Education*
*Vol. XV, Issue No. 2, (Special Issue) April-2018, ISSN 2230-7540*

# IOT Transaction Security

**Gopal Jogdand[1]* Shubham Kadam[2], Kiran Patil[3], Gaurav Mate[4]**

[1,2,3,4] Student, Computer Engineering, JSPM's ICOER, Pune, India

***Abstract – There are a continuously growing number of customers who use Internet banking because of its convenience. But the security and privacy of Information may be one of the biggest concerns to the Online Banking users. The problem with Online banking applications is that they send data directly to customer in plain text form compromising with security. The solutions to the security issues require the use of software-based solutions that involve the use of encryption algorithms. Proxy plays the role of interface between client and Server. It can also decrypt the received message and encrypt data according to the used security transport protocol of the other side. The vulnerability appears during this phase, especially, where the proxy is not confident or supervised by an illegitimate entity. Consequently, passing through the proxy communication node, security services like confidentiality and integrity can easily be compromised. Exploiting advantages of studied cryptographic algorithms, we focus on our customized security objectives regarding proxy element and DTLS-TLS translation. We detail, in this paper, the algorithm and the sequence diagram of secure communication of our proposal adapted for CoAP architecture. As an encryption strategy, we follow the cryptographic envelope principle based on ID-KEM and Three-pass Protocol. As a hypothesis, we assumed that the communication deploys our recent IDMS (Identity management System) contribution for IoT, relying on the EAP OAuth2.0 (Extensible Authentication Protocol and Open Authorization Protocol) protocols via DTLS, as the starting phase in order to keep authentication and authorization services.***

***Keywords—CoAP,DTLS,TLS,vulnerabilities,security,proxy,IBE,IOT,ID-KEM***

----------X----------

## 1. INTRODUCTION

The Internet is an integral part of our daily lives, and the proportion of people who expect to be able to manage their bank accounts anywhere, anytime is constantly growing. As such, Internet banking has come of age as a crucial component of any financial institution's multichannel strategy. Information about financial institutions, their customers, and their transactions is, by necessity, extremely sensitive; thus, doing such business via a public network introduces new challenges for security and trustworthiness. Any Internet banking system must solve the issues of authentication, confidentiality, integrity, and nonrepudiation, which means it must ensure that only qualified people can access an Internet banking account, that the information viewed remains private and can't be modified by third parties, and that any transactions made are traceable and verifiable. For confidentiality and integrity, Secure Sockets Layer/Transport Layer Security (SSL/TLS) is the de facto Internet banking standard, whereas for authentication and nonrepudiation, no single scheme has become predominant yet.

Internet banking systems must authenticate users before granting them access to particular services. More precisely the banking system must determine whether a user is, in fact, who he or she claims to be by asking for direct or indirect proof of knowledge about some sort of secret or credential. With the assumption that only an authentic user can provide such answers, successful authentication eventually enables users to access their private information.

## 2. RELATED WORK

**Implementation of Methods for Transaction in Secure Online Banking:**

Security is a concept similar to being cautious or alert against any danger. Network security is the condition of being protected against any danger or loss. Thus safety plays a important role in bank transactions where disclosure of any data results in big loss. We can define networking as the combination of two or more computers for the purpose of resource sharing. Resources here include files, database, emails etc. It is the protection of these resources from unauthorized users that brought the development of network security. It is a measure incorporated to protect data during their transmission and also to ensure the transmitted is protected and authentic. Security of online bank transactions here has been improved by increasing the number of bits while establishing the SSL

connection as well as in RSA asymmetric key encryption along with SHA1 used for digital signature to authenticate the user.

**A Novel algorithm for Secure Internet Banking with finger print recognition:**

Now a days, the banking and financial systems have been totally changed due to the environment and globalization changes and competition of business services (Majid Karimzadeh and Dastgir Alam, 2012). Web Banking or Internet Banking is used to describe banking transactions through internet application. But there are many security problems like fraudulent websites, fake emails from banks, capturing user IDs and passwords, hacking personal bank accounts and steal money etc. To overcome these problems, this research paper gives a solution through novel algorithm with finger print recognition.

**Smart transaction and automation system for banks:**

The main purpose of this manuscript is to make the banking process a completely automatic system, which will increase security features and at the same time increase the efficiency in the working of the banks to a great extent. The entire transaction system will be completely automatic, which will make the banking process much faster, thus saving the time of the customers and also making the system error-free to a great extent. Aims have also been made to increase the security of these banks with the help of image processors, sensors and GSM. Various other features like aid for handicapped, speech recognition for senior citizens have also been implemented. Apart from these features, several other features like automatic fire extinguishing have also been introduced in the system. Hence, the main aim of the manuscript is to make the banking process completely user-friendly, secure and automated, without the requirement of any kind of human intervention.

**Recognizing debit card fraud transaction using CHAID and K-nearest neighbor:**

Indonesian Bank case: his paper presents a preliminary study on debit card fraud transaction recognition, whose cards are issued by Indonesian bank, based on actual ATM transaction records. The premise of this research is fraudulent transaction contains `anomaly' from the pattern of non-fraudulent transactions so that the anomalous pattern can be detected and separated at some point using classification models. Less availability dataset for research, non-stationary distribution of the data, highly imbalanced class distributions, and continuous streams of transactions become the main driven of using CHAID and k-NN classification method. Empiric result using actual debit card transaction using ATM services shows that Accuracy of CHAID model is 0.8 and F = 0.7; and k-NN model (for k=3) is 0.7 and F = 0.6 These results are comparable to previous studies using Hidden Markov Models.

Transaction authorization from Know Your Customer (KYC) information in online banking: - Online banking is getting popularity due to location independence, 24/7 services and responsiveness. Financial services through the internet are running under various threats like phishing, pharming (cyber-attack intended to redirect a website's traffic to another fake site), malware, Man-In-The-Middle (MITM) attack and the evolving sophistication of compromise techniques. One time password (OTP) in online banking system alleviate the risk and make it secure. In various methods of OTP and Mobile Transaction Authentication Number (mTAN), device can be lost or stolen, delivery in delay, etc. Compliance with Anti-Money Laundering (AML), Know Your Customer (KYC) and sanctions requirements continues to be a key focus area for financial institution (FI) management, and firms must ensure they are following appropriate compliance procedures to meet the increasing regulatory demands (Xia, et. al., 2012), (Castillejo, et. al., 2013). Addressing existing limitation of OTP, this paper proposes Challenge Question (CQ) from dynamic KYC database for transaction authorization before committing any financial transaction from online banking application. Analysis and simulation results show that the proposed method provides equal control as existing OTP/mTAN.

**Big Data of Bank Card Transactions as the New Proxy for Human Mobility Patterns and Regional Delineation. The Case of Residents and Foreign Visitors in Spain:**

Increasing availability of big data, which documents human activity in space and time, offers new solutions to well-known operational problems. Recent studies have demonstrated how topological community detection in large-scale networks of human interactions and mobility can produce geographically cohesive regions, which are meaningful for the regional division of countries. So far, those networks have mainly been built based on the country-wide datasets of telephone calls, typically available for residents of a country. However, it is natural to expect that foreign visitors explore a country in a different way, with patterns that vary depending on nationality. Understanding those differences can be of a great importance for the touristic industry and transportation planning. In this study, we demonstrate the potential of a new type of extensive data, namely bank card transactions executed in a variety of businesses by the domestic and foreign customers of a Spanish bank. We confirm applicability of this data to the regional delineation in line with other datasets and reveal new opportunities related to the distinction of customers by their origin. We point out the important

differences between the optimal regional structure derived from the mobility of residents and of foreign visitors. The definition of the mobility network appears to be a crucial component of the methodology, and is potentially sensitive to the dataset being used. While a reasonable comparison of results obtained based on different data of course requires the consistency of such definition. We propose a novel, consistent way of constructing mobility networks using transactional data, a way transposable to a variety of other datasets. Finally, we perform a quantitative study of the impact of tourists' nationality on their mobility behavior. We find a surprisingly consistent trend between the distance from a given country to Spain, and the mobility characteristics of visitors coming from this country, i.e. the parameters of the gravity model estimation.

**Discovering internal fraud models in a stream of banking transactions:**

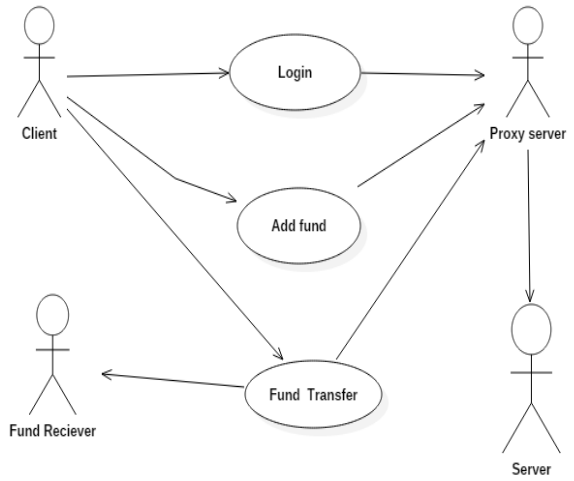
Internal frauds in the banking industry represent a huge cost and this problem is particularly difficult to solve because, by construction, swindlers being very imaginative persons, the fraud schemata evolves continuously. Fraud detection systems must then learn from the continuously new fraud schemata's, making them difficult to design. This paper proposes a new theoretical and practical approach to detect internal frauds and to model fraud schematas. This approach is based on a particular method of abstraction that reduces the complexity of the problem from $O(n^2)$ to O(n) making its implementation in a an Java program that detects and models the frauds in real time and online with a simple professional personal computer. The results of this program are presented with its application on a real-world fraud provided by a worldwide French bank.

**Intelligent phishing detection parameter framework for E-banking transactions based on Neuro-fuzzy:**

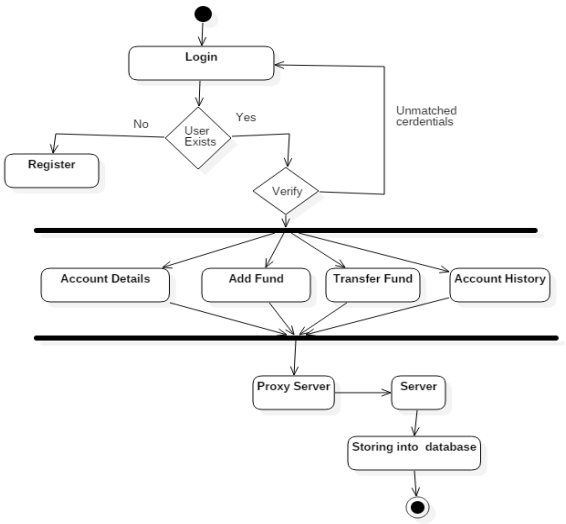
Phishing attacks have become more sophisticated in web-based transactions. As a result, various solutions have been developed to tackle the problem. Such solutions including feature-based and blacklist-based approaches applying machine learning algorithms. However there is still a lack of accuracy and real-time solution. Most machine learning algorithms are parameter driven, but the parameters are difficult to tune to a desirable output. In line with Jiang and Ma's findings, this study presents a parameter tuning framework, using Neuron-fuzzy system with comprehensive features in order to maximize systems performance. The neuron-fuzzy system was chosen because it has ability to generate fuzzy rules by given features and to learn new features. Extensive experiments were conducted, using different feature-sets, two cross-validation methods, a hybrid method and different parameters and achieved 98.4% accuracy. Our results demonstrated a high performance compared to other results in the field. As a contribution, we introduced a novel parameter tuning framework based on a neuron-fuzzy with six feature-sets and identified different numbers of membership functions different number of epochs, different sizes of feature-sets on a single platform. Parameter tuning based on neuron-fuzzy system with comprehensive features can enhance system performance in real-time. The outcome will provide guidance to the researchers who are using similar techniques in the field. It will decrease difficulties and increase confidence in the process of tuning parameters on a given problem.

**Applying Bayesian game theory to analyse cyber risks of bank transaction systems:**

Bayesian game theory is an interesting field within cyber security. Applying it to bank transfer systems can be very useful in finding risks in time and to dynamically adapt to them. It can not only provide insight about the best threat control methods, but also gives insights in how confidential certain core information and actions within the system are. By defining key points for bank transfer systems, an abstract `meta model' is created. Due to the key constraints and the relation with `classic' Bayesian game theory, the validity of the abstract model can be proven for the more specific models



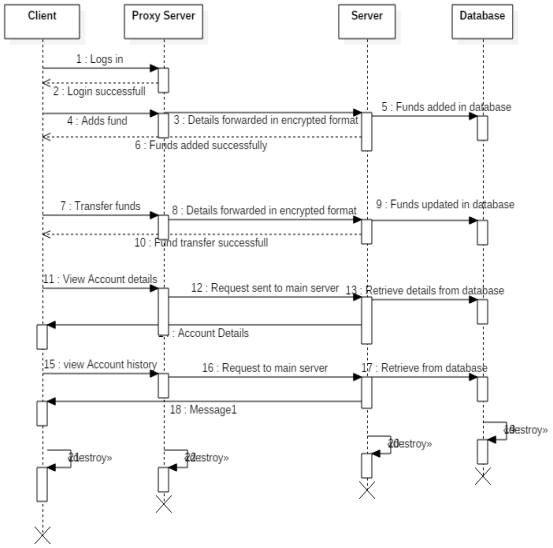

**ARCHITECTURE OF IOT TRANSACTION:-**




**AES (Advanced Encryption Standard) Algorithmn**:-

All of the cryptographic algorithms we have looked at so far have some problem. The earlier ciphers can be broken with ease on modern computation systems. The DES algorithm was broken in 1998 using a system that cost about $250,000. It was also far too slow in software as it was developed for mid-1970's hardware and does not produce efficient software code. Triple DES on the other hand, has three times as many rounds as DES and is correspondingly slower. As well as this, the 64 bit block size of triple DES and DES is not very efficient and is questionable when it comes to security. What was required was a brand new encryption algorithm. One that would be resistant to all known attacks. The National Institute of Standards and Technology (NIST) wanted to help in the creation of a new standard. However, because of the controversy that went with the DES algorithm, and the years of some branches of the U.S. government trying everything they could to hinder deployment of secure cryptography this was likely to raise strong skepticism. The problem was that NIST did actually want to help create a new excellent encryption standard but they couldn't get involved directly. Unfortunately they were really the only ones with the technical reputation and resources to the lead the effort. Instead of designing or helping to design a cipher, what they did instead was to set up a contest in which anyone in the world could take part. The contest was announced on the 2nd of January 1997 and the idea was to develop a new encryption algorithm that would be used for protecting sensitive, non-classified, U.S. government information. The ciphers had to meet a lot of requirements and the whole design had to be fully documented (unlike the DES cipher). Once the candidate algorithms had been submitted, several years of scrutinisation in the form of cryptographic conferences took place. In the first round of the competition 15 algorithms were accepted and this was narrowed to 5 in the second round. The fifteen algorithms are shown in table 7 of which the 5 that were selected are shown in bold. The algorithms were tested for efficiency and security both by some of the world's best publicly renowned cryptographers and NIST itself. After all this investigation NIST finally chose an algorithm known as Rijndael. Rijndael was named after the two Belgian cryptographers who developed and submitted it - Dr. Joan Daemen of Proton World International and Dr. Vincent Rijmen, a postdoctoral researcher in the Electrical Engineering Department of Katholieke Universisteit Leuven. On the 26 November 2001, AES (which is a standarised version of Rijndael). The AES cipher Like DES, AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. However, AES is quite different from DES in a number of ways. The algorithm Rijndael allows for a variety of block and key sizes and not just the 64 and 56 bits of DES' block and key size. The block and key can in fact be chosen independently from 128, 160, 192, 224, 256 bits and need not be the same. However, the AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES256 respectively. As well as these differences AES differs from DES in that it is not a feistel structure. Recall that in a feistel structure, half of the data block is used to modify the other half of the data block and then the halves are swapped. In this case the entire data block is processed in parallel during each round using substitutions and permutations. A number of AES parameters depend on the key length. For example, if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14 for 192 and 256 bits respectively. At present the most common key size likely to be used is the 128 bit key. This description of the AES al Chapter 7 The AES Algorithm implementation.

**Flow Diagram:-**



## CONCLUSION

The intended objectives were successfully achieved in the prototype model developed. The developed product is easy to use, economical and does not require any special training. Though the project showcases the proof of concept, there are a few aspects that can be included to this project to make it more robust. To begin with, in this project the latency time of the wireless communication with the server may need to be considered. Secondly, the communication is not very secure. The transaction done is safe from phising which is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. We have successfully deployed this project by using AES(Advanced Encrypting Standard) Algorithm.

## REFERENCES

Birgit Mager (2008). Design Dictionary published by Birkhäuser, Basel URL: http://uk.service-design-network.org/?page_id=257

Chris Spear (2008). “System Verilog for Verification”, Springer, 2008

D. Klabjan and J. Pei (2011). “In-store one-to-one marketing,” Journal of Retailing and Consumer Services, vol. 18, no. 1, pp. 64–73.

D. M. Dobkin (2012). The RF in RFID: uhf RFID in practice. Newnes, 2012.

DeSai, J. (2008). Mastering innovation: Roadmap to sustainable value creation

Edgett (1994). The traits of successful new service development, Journal of Services Mar-keting, Vol. 8 No.

Edvardsson (1997). Quality in new service development: Key concepts and a frame of reference, Int. J. Production Economics 52 (1997), Elsevier Science

Egils Milbergs & Vonortas (2008). Innovation Metrics: Measurement to Insight, Center for Accelerating Innovation2008, pp. 2-3.

F. Xia, L. T. Yang, L. Wang, and A. Vinel (2012). “Internet of things,” International Journal of Communication Systems, vol. 25, no. 9, p. 1101.

Fritillaria (2010). Service design and the customer's journey [e-article]. Fritillaria blog [cited on 27.4.2012]. Available at: http://fritillaria.blogspot.com/2010/04/service-design-and-customersjourney.html.

Gube, J. (2010). What is User Experience Design? Overview, Tools and Resources [earticle]. UX Design. 2010 [cited on 13.4.2012]. Available at: http://uxdesign.smashingmagazine.com/2010/10/05/what-is-userexperience-design-overviewtools-and-resources/.

Joan Daemen and Vincent Rijmen (2002). "The Design of Rijndael: AES - The Advanced Encryption Standard." Springer, 2002. ISBN 3-540-42580-2

N. Mitton, S. Papavassiliou, A. Puliafito, and K. S. Trivedi (2012). “Combining cloud and sensors in a smart city environment,” EURASIP journal on Wireless Communications and Networking, vol. 2012, no. 1, p. 1, 2012.

National Institute of Standards and Technology (2001). “Federal Information Processing Standards Publication 197”.

P. Castillejo, J.-F. Martinez, J. Rodriguez-Molina, and A. Cuerva (2013). “Integration of wearable devices in a wireless sensor network for an e-health application,” IEEE Wireless Communications, vol. 20, no. 4, pp. 38–49.

S. Shepard (2005). RFID: radio frequency identification. McGraw Hill Professional, 2005.

Samir Palnitkar (2003). “Verilog HDL, A Guide to Digital Design and Synthesis”, Prentice Hall, 2003

Stuart Sutherland (2006). “Systen Verilog for Design”, Springer, 2006

T. Shanmugapriyan (2013). “Smart cart to recognize objects based on user intention,” International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, no. 5.

T. Song, R. Li, X. Xing, J. Yu, and X. Cheng (2016). “A privacy preserving communication protocol for iot applications in smart homes,” in to appear in International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI) 2016, 2016.

**Corresponding Author**

**Gopal Jogdand***

Student, Computer Engineering, JSPM's ICOER, Pune, India

**E-Mail – gopaljogdand07@gmai.com**