International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 09
August 2017

Off-Line Small-Payments Using Fraud Flexible Technique

Boya Sripriya & M.Chaitanya Kishore Reddy
Asst.Professor St.Peters Engineering College,
chkishore.0007@gmail.com & priya679.k@gmail.com

ABSTRACT: *Online shopping payment scheme is one of the popular in recent years. During payment process the attackers aim to stealing the customer data by targeting the Point of Sale (PoS) system. Increasing malware that can steal card data as soon as they are read by the device. As such, in cases where customer and vendor are steadily or intermittently disconnected from the network and there is no secure during off-line payment. The proposed work is to provide secure fully off-line work is interactivity between multiple client - server. This server is identified from legal to illegal control is provided to customer key approach. Once collect the Coin details at customer side and automatically erases after the transaction. It include that limited activity is ensured referred as server to client transaction is secured. Further, an exhaustive investigation of FRoDO utilitarian and security properties is given, demonstrating its viability and plausibility. As an exhaustive extension to the project further investigated with possibility to allow digital change to be spent over multiple off-line transactions while maintaining the same level of security and usability.Providing an exhaustive Coin Management in framing and creating On Mobile Move Coins.*

INTRODUCTION

Credit and Debit card data stealing is most popular problem in cybercrime. Slashers goal at stealing the consumer information with the aid of aiming the Point of Sale systems, i.e.The factor at which the seller cope with the customers facts. Modern POS structures having specialized software program inbuilt in card reader. Often consumer gadgets are external input to the POS. In these ideas, malware steal the card information must examine by using tool has proliferated. Like this case, connection between client and seller being intermediately stopped and there at ease online fee isn't feasible. This initiatives supplying FRODO concepts for a relaxed off-line micro-payment is bendy to POS statistics breaches. Solution consists of flexibility and security. Still, FRODO is the primary solution that may provide fully cozy off-line payments while being bendy to all presently regarded POS failures. In certain, it includeFRODO architecture, components, and protocols. Thereby, complete details of FRODO functional, security properties are provided, showing its effectiveness and viability. Mobile micro payments are famous and they are traditional in marketing fields. The classic credit card approaches may be implemented in banking such as mobile-based payments. Even though many technologies developed, many unexpected problems faced in the field for that the crypt-currencies and de-centralized payment systems are used. Due to several unresolved problems, including a lack of widely-accepted standards, limited interoperability among systems and security the payment schemes are not get successful in the payment system. The vendor have been victims of information security breaches and payment data theft targeting consumer payment card data and Personally Identifiable Information(PII).The user data can be used by the criminals for fraud operations. For improving security, the credit card and debit card holders use Payment card industry Security Standard Council. PoS system always handle critical information and requires remote management. PoS System acts as gateways and require network connection to work with external credit card processors. However, a network connection not be available due to either a temporary network service or due to permanent lack of network coverage. On solutions are not very efficient since remote communication can introduce delays in the payment process. Brute forcing rem in PoS intrusions. The FRoDO introduces a secure off physical unclonable function. FRoDO introduces coin element and identity element. Vendor only communicate with the identity to identify the user. Identity element I the security of users. Market analysts have anticipated that cellular bills will overtake the conventional market, therefore supplying more convenience to customers and new resources of revenue to many companies. This state of affairs produces a shift in purchase techniques from classic credit score playing cards to new techniques which include cellular-based totally bills, giving new market entrants novel enterprise

probabilities. Widely supported by using latest hardware, cellular charge generation is still at its early tiers of evolution but it's miles predicted to upward thrust inside the near destiny as validated through the developing interest in crypto-currencies,

The main benefit is a simpler, faster, and more secure interaction between the involved actors/entities. Among other properties, this two-steps protocol allows the bank or the coin element issuer to design digital coins to be read only by a certain identity element, i.e., by a specific user. Furthermore, the identity element used to improve the security of the users can also be used to thwart malicious users. In proposed solution that can provide secure fully off-line payments while being resilient to all currently known PoS breaches.

LITERATURE SURVEY: A literature survey or literature review means study of references papers and old algorithms that we have read for designing the proposed methods. It also helps in reporting summarization of all the old references papers, their drawbacks. The detailed literature survey for the project helps in comparing and contrasting various methods, algorithms in various ways that have implemented in the research. The literature study prescribed in this research of the project, supports high availability of data, Various algorithms, Various old references papers, comparison of the methods. This design supports various types of jamming attacks preventions like combined cryptography methods, strong commitment methods, elliptic method and all or nothing methods

Pay word andmicro mint: two simple micropayment schemes

- The Basic Pepper coin method can be implemented in a variety of ways, to maximize ease of use for the customer in a given situation. While the basic peppercoin method requires that each consumer have digital signature capability, one can easily eliminate this requirement by having a party trusted by the consumer sign payments for him as a proxy, this might be a natural approach in a web services environment.
- The pepper coin method can also be implemented so that it feels to the consumer as a natural extension of his existing credit-card processing procedure, further increasing consumer acceptance and ease of use.

Secure POS & KIOSKAUTHOR: BOMGAR

Limited interfaces and location within local networks, supporting kiosks and point of sale (POS) terminals can be challenging. Often they are located on networks that are not connected to the internet, making direct access impossible for most remote support tools.

And even when an employee is present at the terminal, access restrictions and/or lack of technical knowledge makes communicating the solution to a problem difficult. To add complications, hackers are ramping up their efforts to steal payment card data by gaining access to POS systems and kiosks.

Reliable OSPM schema for secure transaction using mobile agent in micropayment system

- The paper introduces a novel offline payment system in mobile commerce using The case examine of micro-payments. The gift paper is an extension model of our earlier look at addressing on implication of at ease micropayment system deploying system orientated structural design in cellular network. The preceding device has large utilization of SPKI and hash chaining to supply reliable and cozy offline transaction in cellular commerce.
- However, the contemporary paintings has attempted to provide an awful lot more mild weight comfy offline fee device in micro-payments by designing a new schema termed as Offline Secure Payment in Mobile Commerce (OSPM). The empirical operation are accomplished on three types of transaction process considering most situation of actual time offline cases. Therefore, the modern idea introduces two new parameters i.e. Cellular agent and mobile token which can ensure higher protection and comparatively much less network overhead.

Lightweight and Secure PUF Key Storage Using Limits of Machine Learning

A lightweight and comfy key storage scheme using silicon Physical Unclonable Functions (PUFs) is described. To derive strong PUF bits from chip manufacturing variations, a light-weight errors correction code (ECC) encoder / decoder is used. With a check in count of sixty nine, this codec middle does now not use any conventional errors correction strategies and is 75% smaller than a previous provably cozy implementation, and yet achieves sturdy environmental overall performance in 65nm FPGA and zero.13µ ASIC implementations. The security of the syndrome bits uses a new protection argument that is based on what cannot be found out from a device gaining knowledge of attitude. The range of Leaked Bits is decided for each Syndrome Word, reducible the usage of Syndrome Distribution Shaping.

The layout is at ease from a min-entropy point of view against a device-gaining knowledge of-prepared adversary that, given a ceiling of leaked bits, has a type error bounded by ε. Numerical examples are given the usage of modern-day gadget learning results.

Building robust m-commerce payment system on offline wireless network

- Mobile commerce is one of the upcoming research areas with focus on mobile payment systems. Unfortunately, the current price systems is at once depending on constant infrastructure of network (cellular network), which fails to facilitate most excellent level of safety for the price machine. The proposed device highlights a singular technique for constructing a cozy, scalable, and bendy e-fee systems within the dispensed situation of Wi-Fi adhoc community in offline mode of conversation for superior safety on transaction and charge method.
- The proposed device uses Simple Public Key Infrastructure for supplying the safety in price procedures. The performance evaluation of the proposed model suggests that the system is noticeably strong and at ease ensuring anonymity, privateness, non-repudiation offline payment device over Wi-Fi adhoc network.

SYSTEM ANALYSIS: Systems Analysis is a detailed study of project information through various steps, procedures, functions and entities which including in getting the analysis of computer Information, Project Information, Algorithm Information and Other Inner and Outer information related to the proposed study. System Analysis provides a series of scientific methods to understand the various requirements required for designing the project work. In System analysis we study about various functional, non-functional requirements needed for the designing the proposed system. In the current System Analysis is we have studied various papers related to the project work and planned the design using various tools such as Class Diagrams, Sequence Diagrams, data flow diagrams and data dictionary are used in developing a logical model of system.

DOMAIN ANALYSIS: The selected area or domain analysis is the process studying which a software to be selected for designing the project work. The word 'domain' in the case means the general field of business or technology in which the customers expect to be using the software. As per our requirement the project is related to cryptographic and wireless protocol management, to design these specifications we selected java technology because it provides wireless, security and network packages. **REQUIREMENT ANALYSIS:**A requirement analysis is a study of various methods and functions like man power, software, inputs, outputs and processing to be implemented for the development of proposed system. In this study we have performed functional and non-functional requirements for the project.

EXISTING SYSTEM: In the current system, the system describes FRoDO, a secure off-line micro-payment solution that is resilient to PoS data breaches. FRoDoprovides a fixed architecture in creating and maintenance of coins. The FroDO solution cannot

improves over up to date approaches in terms of flexibility and security required by user. The FRoDO introduces a secure off physical function. FRoDO introduces coin element which are static in nature and cannot be changed on Move or on Requirement. In particular current FRoDO architecture, components, and protocols does not provides effectiveness and viability

.**DISADVANTAGES:**The system implemented called FRoDO, was built using a static coin architecture which are easier to hack. Current FroDo Does not provides Coins Management. Frodo is a weak prevention strategy based on data obfuscation and did not address the most relevant attacks aimed at threatening customer sensitive data, thus being vulnerable to many advanced attack techniques.

PROPOSED SYSTEM: Project is proposed with advanced investigation and possibility to allow extensive digital change to be spent over multiple off-line transactions while maintaining the same level of security and usability. Project can be extended with Coin Management in framing and creating On Mobile Move Coins. Project is extended with UMC Frodo (User Management of Coins with Fraud Resilient Device for Off-line micro-Payments).

ADVANTAGES: The system Extended with UMC FRoDO, with a changed architecture for user coin management.UMC FroDo provides On Mobile Coins Management.UMC FroDo is provides prevention strategy based on data obfuscation and address the most relevant attacks aimed at threatening customer sensitive data, thus being vulnerable to many advanced attack techniques.Creating on Mobile Coins provides user in generating and managing coins when needed.

MODULES AND ITS DESCRIPTION

In the proposed system there are four modules they are:

- System Construction Module
- Identity Element
- Coin Element
- Attack Mitigation

System Construction Module

In the first module, develop the System Construction module with the various entities: Vendor, User, FRoDO, PUF, Attacker. This process is developed completely on Offline Transaction process. Develop the system with user entity initially. The options are available for a new user to register first and then login for authentication process. Then develop the option of making the Vendor Registration, such that, the new vendor should register first and then login the system for authentication process. Accounts, nor trusted devices to provide resiliency against frauds based on data breaches in a fully off-line electronic payment systems. Furthermore, by allowing FRoDO customers to be free from having a bank account, makes it also particularly interesting as regards to privacy. In fact, digital coins used in FRoDO are just a digital version of real cash and, as such, they are not linked to anybody else than the holder of both the identity and the coin element. FRoDO assumes that only the chips built upon PUFs can take advantage from the tamper evidence feature. As a consequence project assumptions are much less restrictive than other approaches.

Identity Element

In this module, develop the Identity Element module functionalities. FRoDO does not require any special hardware component apart from the identity and the coin element that can be either plugged into the customer device or directly embedded into the device. Similarly to secure elements, both the identity and the coin element can be considered tamperproof devices

with a secure storage and execution environment for sensitive data. Thus, as defined in the ISO7816-4 standard, both of them can be accessed via some APIs while maintaining the desired security and privacy level. Such software components (i.e., APIs) are not central to the security of solution and can be easily and constantly updated. This renders infrastructure maintenance easier.

Coin Element

In this module, develop Coin Element. In this coin Element broaden Key Generator and Cryptographic Element. The Key Generator is used to compute on-the-fly the personal key of the coin element. The Cryptographic Element used for symmetric and asymmetric cryptographic algorithms applied to statistics acquired in enter and send as output with the aid of the coin detail; The Coin Selector is answerable for the choice of the proper registers used together with the output price computed via the coin detail PUF with a view to gain the final coin cost; The Coin Registers used to store both PUF input and output values required to reconstruct original coin values. Coin registers contain coin seed and coin helper data. Coin seeds are used as input to the PUF whilst coin helpers are used in order to reconstruct stable coin values when the PUF is challenged

Attack Mitigation

In this module develop the Attack Mitigation process. The read-once property of the erasable PUF used in this solution prevents an attacker from computing the same coin twice. Even if a malicious customer creates a fake vendor device and reads all the coins, it will not be able to spend any of these coins due to the inability to decrypt the request of other vendors. The private keys of both the identity and coin elements are needed to decrypt the request of the vendor and can be computed only within the customer device. The fake vendor could then try to forge a new emulated identity/coin element with private/ public key pair. However, identity/coin element public keys are valid only if signed by the bank. As such, any message received by an unconfirmed identity/coin element will be immediately rejected. Each coin is encrypted by either the bank or the coin element issuer and thus it is not possible for an attacker to forge new coins

SOFTWARE REQUIREMENTS

Operating System: Windows XP/7/8

Front End: JSP 2.5

Database:MySQL 5.5

Programming language :Jdk 6

IDE: My Eclipse ,Net beans

HARDWARE REQUIREMENTS

Processor: Pentium Dual Core/ Core

to Duo/ I Core with Minimum 1.2 GHZ Speed

RAM: 1GB

GBHardDisk: 120 GB

SYSTEM DESIGN: System design or System planning is the procedure of defining the project Structure, architecture, Planning, components, modules, interfaces, and data elements for a system to satisfy the design requirements and helps to start the work in planned way. Systems design or Planning could be seen as the appliance of systems philosophy and helps to product development in a systematic manner. There is some extensions with the disciplines of systems analysis and planning, systems architecture and development engineering. System Design is broadly divided in two activities.

Logical design: The logical design of a system is concerned to an theoretical representation of the project planning using UML Flows, data flows, inputs and outputs of the system. Logical Design is also called as Graphical Modeling of System planning. In the Logical context of systems design

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 09
August 2017

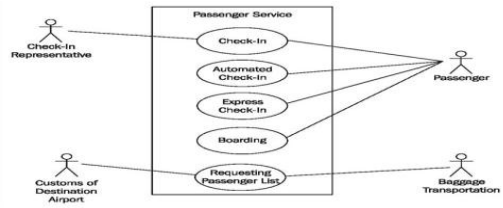
are included. For our project we have processed various UML, DFD and ER Diagrams for better planning and implementation

Physical design: The physical design and planning relates to the real and actual input and output processes to be given the system. This is process is a study of various data inputs and outputs to be processed in the system. Physical Design involves in User Interface Design Front End Screens, Data Design Back end Tables and Process Design Algorithm.

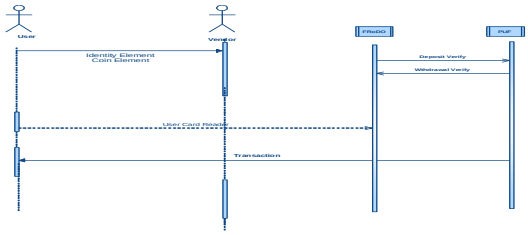
UML DIAGRAMS: The (UML) is a general and all-purpose modeling and planning language in the Software engineering field, which provides a standard way to envisage or visualize the design of a system in a pictorial format. Unified modeling language is a language for writing blueprints.

Class Diagram :A class diagram is a set of various related objects that share the same characteristics called attributes operations called activities, relationships called associations and semantics called rules. A class is a whole set of objects. Its representation is Architects look at class diagrams to see if any class has too many functions and see if they are required to be split.

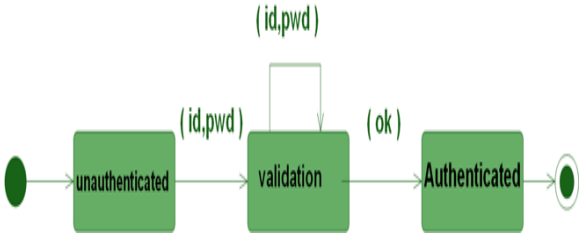
Use Case Diagram:Use case diagram is a graph of actors, a set of use cases are enclosed by a system boundary. Use case diagram are important for knowing the behavior of the element.

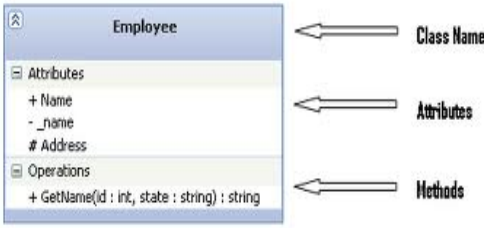


Sequence Diagram: It is an interaction diagram that emphasizes the time ordering of messages. A sequence diagram shows objects participating in the interaction by their lifetime and the messages that they exchange/arranged in the time sequence



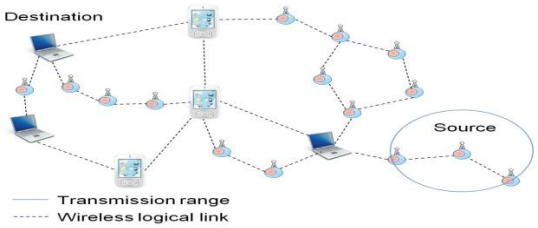
STATE CHART DIAGRAM:A State Chart diagram shows the state machine focusing on the flow of control from state to state. In the UML these are used to model the behavioral aspects of a system. A state chart diagram comprises states and events. A state is defined as the situation in the life of an object. An event can trigger a state transition. The relationship between the states can be represented by a transition. Objects have behaviors and state. A state chart diagram can have the similar properties of other diagram. It has an initial and final states, action states, objects, forks, joins etc…





SYSTEM ARCHITECTURE

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 09
August 2017



IMPLEMENTATION

Java Server Pages (JSP) is a Advanced Internet Server Language that helps Application and Internet developers in creating a statical and dynamically web pages based on DHTML,HTML, XML. The language was introduced in the year 1999 by the software Company named Sun Microsystems. The language uses the Java Compiler. To deploy and run JSP Pages, a suitable web server with a inbuilt servlet container, such as Apache Tomcat, Weblogic or Blazix.The Java Server Pages have an enhanced dynamic scripting facility that works in connection with Hyper Text Markup Language code, dividing the page logic from the static elements related to dynamic actions, the proposed or actual design of pages provides a help to make the Hyper language more functional. A Java Server Page is translated into servlet before being executed, and it processes Hyper Transfer Protocol requirements and creates responses like any servlet. The Java technology imparts a more flexible way to code a servlet. The JSP Translation occurs the first time the application as it run. A Java Page translator is produced to trigger the java page file name extension in a unified resource locator. The java pages are fully attached with servlets in execution of the code. The JSP pages include getting the output from a servlet or sending the output to a servlet, and a servlet can include both input and output from a java page.

TESTING: Testing Software is a critical process which includes many activities, elements of software excellence assertion and represents the ultimate review of specification, design and coding, Software Testing presents a wide nature of an interesting variance for the software developers.

Unit Testing: In software testing, Unit testing mainly focuses on verification effort on the smallest unit of program or software design that is also called a module. In unit testing the procedural or functional design provides a detailed description as a guide, focal the control paths are tested to uncover errors occurred in the designed software within the boundaries of the module. The unit testing of software is normally white box or open testing oriented and the series of steps can be conducted in corresponding or parallel for multiple modules or functions.

Integration Testing:Integration testing is another Testing for systematic technique and product module integrating which constructs the program structure and makes the data flow between the modules, while conducting Integration Testing it requires to uncover errors associated with various interfaces. The main objective is to take unit tested methods and activities to build a program structure that have been dictated by design

Validation Testing: The Validation Testing is integration testing for software which is completely assembled as a package. The Validation testing is the next stage in Testing Activities, which can be defined as successful testing process for the software functions in the manner reasonably expected by the customer. The validation Testing is mainly performed at the end approach of the user needs in testing the information inputed to the product and information contained in those sections are to validated through various testing approaches.The sensible prospect is defined in the software development with a requirement specification, and a document that gives de tailed information of all uservisible attributes of the software methodologies. The document of specification contains a section titled Validation Criteria in which the end user should follow various indications in give the inputs.

System Testing: To check system activities related to computer we process system testing which is actually a series of different tests whose primary purpose is to test the functionalities of computer based system. Even though each test has a different purpose of checking the validations and integrations

of product, all work is to verify that all system elements and system activities which have been properly integrated to perform allocated functions.

Security Testing: Attempts to verify the protection and security mechanisms built into the system for protecting the data, program and other integrations related to system.

Performance Testing: In software engineering, performance testing is processed to check the workload, usage of system, memory, processing, network and other system functionalities. It can also serve to investigate measure the program structure and its process activities inside the system

SCREENS/ FORMS

CONCLUSION:

In this paper we have introduced FRoDO that is, to the bestof our knowledge, the first data-breach-resilient fully offlinemicro-payment approach. The security analysis showsthat FRoDO does not impose trustworthiness assumptions.Further, FRoDO is also the first solution in the literaturewhere no customer device data attacks can be exploited tocompromise the system. This has been achieved mainly byleveraging a novel erasable PUF architecture and a novelprotocol design. Furthermore, our proposal has been thoroughlydiscussed and compared against the state of the art.Our analysis shows that FRoDO is the only proposal thatenjoys all the properties required to a secure micro-paymentsolution, while also introducing flexibility when consideringthe payment medium (types of digital coins).Finally, some open issues have been identified that are leftas future work. In particular, we are investigating the possibilityto allow digital change to be spent over multipleoff-line transactions while maintaining the same level ofsecurity and usability

REFERENCES

[1] J. Lewandowska. (2013). [Online]. Available: http://www.frost.com/prod/servlet/press-release.pag?docid=274238535

[2] R. L. Rivest, "Payword and micromint: Two simple micropaymentschemes," in Proc. Int. Workshop Security Protocols, 1996, pp. 69–87.

[3] S. Martins and Y. Yang, "Introduction to bitcoins: A pseudoanonymouselectronic currency system," in Proc. Conf. Center Adv.Stud. Collaborative Res., 2011, pp. 349–350.

[4] Verizon, "2014 data breach investigations report," Verizon, Tech.Rep., 2014, http://www.verizonenterprise.com/DBIR/2014/

[5] T. Micro, "Point-of-sale system breaches, threats to the retail andhospitality industries," University of Zurich, Department of Informatics,2010.

[6] Mandiant, "Beyond the breach," Mandiant, 2014, https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf

[7] Bogmar, "Secure POS & kiosk support," Bogmar, 2014, http://www.bomgar.com/assets/documents/Bomgar_Remote_Support_for_POS_Systems.pdf

[8] V. Daza, R. Di Pietro, F. Lombardi, and M. Signorini, "FORCEFullyoff-line secure credits for mobile micro payments," in Proc.11th Int. Conf. Security Cryptography, 2014, pp. 125–136.

[9] W. Chen, G. Hancke, K. Mayes, Y. Lien, and J.-H.Chiu, "Using 3Gnetwork components to enable NFC mobile transactions andauthentication," in Proc. IEEE Int. Conf. Progress Informat.Comput.,Dec. 2010, vol. 1, pp. 441–448.

[10] S. Golovashych, "The technology of identification and authentication of financial transactions. from smart cards to NFC-terminals,"in Proc. IEEE Intell. Data Acquisition Adv. Comput. Syst., Sep. 2005,pp. 407–412.

BoyaSripriya received B.Tech in computer science and engineering from JNTUH Hyderabad and M.Tech in computer science and engineering from JNTUH Hyderabad, She is currently pursuing Mtech, Department of Computer Science and Engineering at St.peters Engineering college, Hyderabad, TS, INDIA.

Maddireddy Chaitanya Kishore Reddy received M.Tech in computer science and Engineering from Jawaharlal Nehru technological university, KAKINADA. He is currently working As Asst.Professor, Department of Computer Science and Engineering at St.peters Engineering College, Hyderabad, TS, INDIA. He has published papers at international conference on Research Advancement in Computer Science and communication (ICRACS),Intenational Conference on Recent Trends in Engineering, Science and Technology (ICRTEST),International Conference on Communications, Signal Processing Computing and Information Technologies (ICCSPCIT),International Journal of Engineering and Computer Science (IJECS),International Journal and Magazine of Engineering and Technology, management and Research (IJMETMR) in Mobile Ad-hoc Networks and Wireless sensor networks.