Privacy Preserving for Efficient Authentication in Pervasive and Mobile Computing

M. Srilatha¹, K. Sruthi², V. Gouthami³

¹Student, Computer Science & Engineering-Department, JNTU Hyderabad
India
srilathamekala5@gmail.com

²Assistant Professor, Computer Science & Engineering Department, Auroras Research & Technological Institute,
Warangal, India
shruthi.kandukuri@gmail.com

³Associate Professor, Computer Science & Engineering Department, Auroras Research & Technological Institute,
Warangal, India
gautami.velakanti@gmail.com

Abstract— In the present computer era and advancement in mobile communication system where many applications rely on the existence of small devices and small applications which can exchange data in any communication networks where the main challenging is to provide security where the significant portion of applications is based on the confidentiality and integrity of messages that are communicated by short encrypted messages that are based on advance encryption cryptographic systems directed to meet the requirements of mobile devices and pervasive applications by authenticating the message with accuracy to secure the communication the proposed message authentication technique.

In this paper we implement the MAC algorithm and the aim to utilize the security based on the encryption algorithm which can provide to design more efficient authentication mechanisms using the standalone authentication primitives with high risk for sender input data where the transmitter and receiver will exchange the data by evaluating the real time scenarios.

Keywords—Authentication, pervasive computing, Privacy, Mobile Computing.

I. INTRODUCTION

In the present computer era where the Pervasive Computing Environments (PCEs) consists of various interconnected devices with an abundant services that tends to promises greater integration for implementation of digital infrastructure in many aspects that converts us into physical selves [1].

Due to availability of huge number of communicating devices in any network we need to provide seamless access to multiple dynamic networks at any span of time from any location where the users and autonomous agents will be able to communicate the data between each other and by which a environment will be created with ubiquitous based intelligent computing environment getting into existence.

Due to the As the networking technologies are becoming more and more commonplace day by day and getting specified as a core or the central part of our everyday life where different organizations and individuals are utilizing the service are becoming increasingly dependent on electronic means and the technology to process information that provides relevant services by taking advantage of ambient intelligence in PCEs as the transactions will be considered to be sensitive and critical due to which we mainly emphasize on access control for preventing information leakage and service capabilities.

![Fig.1. System Architecture](image-url)
Every customized tool that uses queries on database to attain some data either by implementing a simple SQL query or may be a complex cursor or trigger uses distinct mechanisms to develop customized queries which are totally based on manual editing’s of various user that relies on hundreds and thousands of data attribute which may sometimes confuse the user.

When a query is considered to be a non-familiar to the targeted database schema available in advance as the non-technical users make use of the available relational databases where the main challenging task is considered to be attaining the data from very recent years that is done by many researchers who tends to focused on distinct database interfaces for assisting various users for querying the relational databases without using the structured query language.

II. RELATED WORK

Most of the researchers have published many papers in this area where few of the major concerns which we recognized are:

In the reference provided by Linden provides us with the process of identifying and discovering the related items in an entity our work must be similar to the research which is based on the recommender systems that comprises of recommend query for a possible user where the recommender system mainly rely on similarities between queries and or its available or derived statistical correlations that are directly based on the user log data [1].

In the reference provided by Ravichandran provides us with the recommended queries to attain the data of customers that are based on their own purchase histories for similar customers who previously have the purchase histories and similarity search is performed between various products where the recommending of an item is not considered to be equivalent for finding a comparable purchase data items [2].

In the reference provided by Kozareva provides us with the process of proposing various recommendations is to identify their proposed customers for performing addition of more item sets to perform shopping and analyzing the shopping carts which is suggested by most of the similar or related item sets which later tends to compare various products that are centrally available in the proposed system [3].

In the reference provided by Jeh provides us with the process of comparing various cases of comparison which would like to help users to explore various alternatives and for helping them to make an appropriate decision making process among various comparable item sets and the possible comparative questions that are intended and are posted by users which are considered to be predicted and are simply based on the item similarity [4].

In the reference provided by Jindal provides us with the process of mining comparative sentences and their relations as the method that is proposed users the class sequential rules that are intended to perform various label sequential rules that is learned from annotated corpora to identify various comparative sentences and extract comparative relations on every possible domain [5].

The process of ensuring high recall is considered to be crucial in the intended application based scenario where every user can raise or issue any number of arbitrary queries for addressing the problem for developing weakly supervised bootstrapping pattern or the learning method that is based on the process of effectively leveraging unlabeled questions that are imposed [6].

In the reference provided by Smeulders provides us with a classic content based question retrieval (CBQR) system that takes a solo query image as requesting source for retrieving similar images based on the localized content based image retrieval system as CBIRs primary task where a user creates a interested portion of the image as input set and will leave the rest as irrelevant content and then the user will explicitly mark the region of interest domain as a localized CBIR which must rely on more number of images that are labeled as positive or negative based on the criteria to learn what portion of the image is considered to be an interest to the end user as the challenge is further localized to represent the image[7].

In the reference provided by Cristianini provides us with Training support vector machine that requires resolving of quadratic programming problem in a number of coefficients that are equal to the total number of training examples from the numeric techniques for a specific QP which is considered to be infeasible for very large dataset by implementing the practical techniques for decomposing the problem [8].

In the reference provided by Basel Alomair and Radha Poovendran proposes us by examining encrypted data and authenticate based generic work for protected all the available channels by launching E-MACs which is a new symmetric key based cryptographic approach which can be utilized for dynamic creation of E&A variations after considering various benefits of the proposed E&A structure by utilizing the E-MACs that are exposed for progressing the effectiveness and precautions of the specified authentication process [9].
III. EXISTING SYSTEM

In the present computer era the usage of internet and world wide web is being dramatically increasing at a lightning speed due to immense usage of internet either through computers or through mobile phones and the web or internet acts as a medium of exchange for most of the user for obtaining more services for lesser or cheaper costs and the information that is available in the web useful not only to an individual user but also helpful to most of the business organizations or hospitals or educational purposes and many more research areas.

The Blind signature scheme is considered to be a variant that is based on the digital signature concept where the content of message is encrypted with its signer where the blind signature schemes can implement using a number of well known digital signature schemes like RSA algorithm to produce a signature on the message itself where the user first blinds the message with a blinding function b which combines with a random blinding factor k and later forwards the blinded message to the signer to perform digital signature.

Then the signer signs on the blinded message using a standard signing algorithm such as RSA which is depicted as SA(msg) that denotes the digital signature of A on msg (message) and later sends the result back to the user who then unblinds it by using the unblinding function g for obtaining the signer’s signature on the original message.

In order to yield a compressed result table a cluster is generated where the cluster is a set of actual instances that are represented by each and every instance in the compressed table that is dynamically generated for viewing the comprehensive data instances where the user can briefly click through interested clusters that are generated by various users where every user is capable of generating it.

For attaining the efficiency issues we have to chosen the incremental data clustering model or the framework where the implementation represents a different set of compressed tables or views for each and every user who tends to propose different data clustering methods and frameworks where distinct types of data are being implemented on various clusters by just offering the better aspect of generating the query results for all the available users.

Many statistical tools that generate multiple regression for neural networks that tends to provide various methods for creating and developing the static query forms where the structural model is specified elaborately to a certain extent where the query forms user can raise or generate a query and obtain the relevant information that satisfies the query regarding to each and every query that is generated.

IV. PROPOSED SYSTEM

In this paper we propose privacy preserving for efficient authentication in pervasive and mobile computing environments where various forms of database queries are implemented on pervasive computing and as well as on mobile computing for implementing the privacy preserving aspects.

We need to consider mainly two different observations that makes use for the existing MAC algorithms that are designed independently of handing other operations that are required to be performed whenever we want the messages to be specifically authenticated and also for encrypting those messages using the existing MAC values that are not designed to utilize the main functionality such that it can provide the underlying encryption formulas and implement algorithm. And secondly the other observation is based on the most frequent MAC values that are designed for implementing general computer communication to be performed independently by using the properties for every message and can possess its implementation.

![Fig.2. proposed system architecture](image)

All the random strings that are used for performing different operations between sender and receiver are considered to be independent based on the proposed authentication algorithm which can benefit from its implementation simplicity for performing unconditional secure authentication for allowing faster and more efficient authentication algorithm that tends to manage one time keys or session keys or time based keys that makes a hackers assumption out of his or her reach.

One of the important assumption is to make a messages authentic is by making it non deterministic predefined length by including applications that makes a fixed length oriented which uses RFID based systems for implementing sensor based nodes that reports of happening of events or specifications of measurements within a certain range as the proposed scheme utilizes the encryption algorithm for delivering a random string and uses the same to reach the simplicity and efficiency of authentication.
V. RESULTS

We have implemented our proposed system in java and some of the screens are:

Fig. 3. Login page of the proposed system

Fig. 4. Mobile Login Page

Fig. 5. Send Short Message Screen

Fig. 6. Mail Sent Screen

Fig. 7. Email Verification Screen

Fig. 8. Emails Sent Screen
VI. CONCLUSION

In this paper we have proposed the privacy preserving for efficient authentication in pervasive and mobile computing is used for validating small encrypted messages where the truth is based on the message which is to be validated and must need to be encrypted for providing an arbitrary nonce to the proposed receiver using the cipher text which permits the design of a validation code based on the profits from the simplicity of absolutely secure validation implementation using the approach of one-time keys that are proposed in this paper.

REFERENCES


AUTHOR

M. Srilatha, is presently pursuing her M.Tech degree in Software Engineering of Computer Science and Engineering department from Aurora’s Research & Technological Institute affiliated to JNTU Hyderabad.

K. Shruth, is presently working as Assistant Professor in department of Computer Science & Engineering at Aurora’s Research & Technological Institute.

V. Gouthami, is presently working as Associate Professor and HOD in department of Computer Science & Engineering at Aurora’s Research & Technological Institute and she has a total teaching experience of 8 years.