

# Performance Enhancements of Wireless Body Area Networks with Authentication by Encrypted Negative Password

Sai Divya Kalagatla<sup>#1</sup>, Arun Sahayadhas<sup>\*2</sup>

<sup>1</sup>Research Scholar, <sup>2</sup>Professor

<sup>1,2</sup>Department of Computer science and Engineering,

VELS Institute of Science, Technology & Advanced Studies, Pallavaram, Chennai, India

**Abstract** — Although password authentication is still the most popular method of authentication, in spite of certain security vulnerabilities, secure password storage is an essential component of systems that rely on it. In this study, we present a framework for password authentication that can be readily integrated into current authentication systems and is intended for safe password storage. First, our framework uses a cryptographic hash algorithm (SHA-256) to hash the plain password that a client sends. Next, a negative password is created using the hashed password. Lastly, a symmetric-key method (AES) is used to encrypt the negative password into an encrypted negative password (ENP). Multi-iteration encryption may be used to increase security even further. It is challenging to decipher passwords from ENPs due to the symmetric encryption and cryptographic hash function. In addition, a given plain password has several associated ENPs, making pre-computation attacks (such as lookup table and rainbow table assaults) impractical. According to comparisons and studies of algorithm complexity, the ENP might withstand lookup table attacks and offer more robust password security against dictionary attacks. In addition to not adding additional components (salt), it is important to note that the ENP is still resistant to pre-computation attacks. Most notably, the ENP is the first password protection technique that just requires the plain password and combines the symmetric-key algorithm, the negative password, and the cryptographic hash function.

**Keywords:** Password Authentication; Negative Password; Offline Attacks; Wireless Body Area Networks.

## 1. Introduction

Due to its affordability and ease of use, password authentication is the most popular authentication method among the plethora of online services that have arisen as a result of the Internet's development. As a result, both industry and academia are constantly very interested in password security. For example, a lot of users choose weak passwords frequently and utilize them across multiple systems. To make their passwords easier to remember, they typically create them using well-known words. It is really challenging to get passwords from extremely secure systems. One the one hand, it is challenging to steal authentication data tables in high security systems, which store usernames and passwords.

However, there is typically a cap on the amount of login attempts made during an online guessing assault. Passwords, however, might leak from unreliable systems. Adversaries can launch offline attacks if they have access to authentication data tables from vulnerable systems. Typically, the passwords in the authentication data table are hashed passwords.

However, hashed passwords are not immune to pre-computation techniques like rainbow table attack and lookup table assault because CPU and storage resources are become more and more plentiful.

## 1.1 Overview of Attack Tools ENP

A number of features, including numerous hash algorithms, multiple attack models, multiple operating systems, and multiple platforms, are offered by certain potent attack tools like hashcat, Rainbow Crack, and John the Ripper. Attacks under these circumstances are typically conducted as follows.

Initially, adversaries pre-compute a lookup table, with the records being the corresponding plain passwords in the password list and the keys being the hash values of elements in a password list comprising commonly used passwords.

They then get an authentication data table from systems with low security. Then, by comparing hashed passwords in the authentication data table with the keys in the lookup database, they search the lookup table for plain passwords. Ultimately, the adversaries utilize compromised usernames and passwords to gain access to higher security systems in order to steal more sensitive user data and accomplish other goals.

As a result, there is a high success rate in breaking hashed passwords since the lookup table can be swiftly generated and has a large enough size.

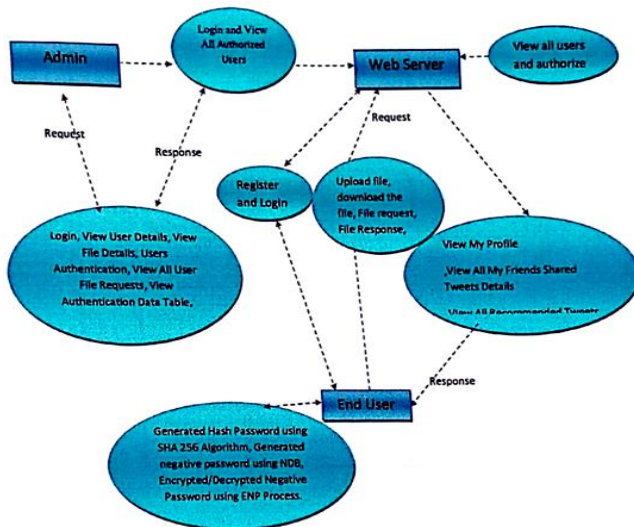


Fig.1: Information flow functional

Hashed passwords, salted passwords, and key stretching are common password protection strategies. Hashed passwords would progressively be removed from these SCHCMCCs due to their susceptibility to pre-computational assaults. uncomfortable to use. To strengthen password security, dynamic salt creation and placement are employed in. In essence, this method is also a variation on the salted password technique, in which the salt is a randomly generated string that depends on the original password. As a result, it could withstand lookup table attacks, but it was unable to fend off dictionary attacks and added another element (salt). For password storage, an enhanced dynamic Key-Hashed Message Authentication Code function—abbreviated as d-HMAC—was presented in.

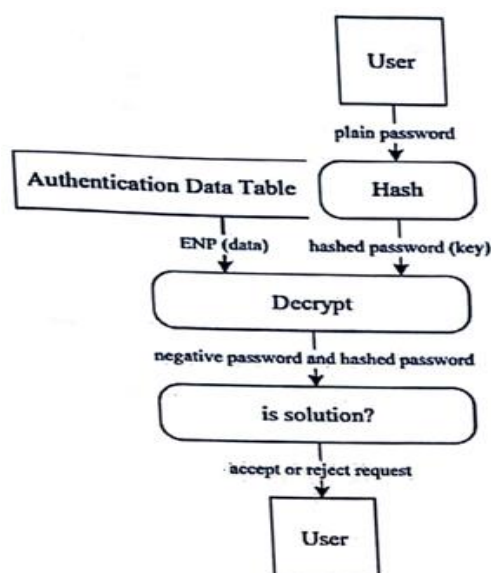


Fig.2: Data Flow Diagram Level

## 1.2 Objectives Of ENP'S

- Input Design is the process of converting a user-oriented description of the input into computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.
- It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates be performed. It also provides record viewing facilities.
- When the data is entered it will check for its validity. Data can be entered with the of screens. Appropriate messages are provided as when needed so that the user will noo be in maize of instant. Thus, the objective of input design is to create an input layout that is easy to follow.

As a result, these passwords are instantly vulnerable. Nonetheless, the secret key in the ENP is the hash value of each user's password; as a result, it is nearly always unique and does not require specific generation or storage.

## 2. Literature Review

Theory on passwords has lagged behind practice, where large providers use back-end smarts to survive with imperfect technology. Simplistic models of user and attacker behaviours have led the research is community to emphasize the wrong threats. Authentication is a classification problem amenable to machine learning, with many signals in addition to the password available to large Web services. Pass-words will continue as a useful signal for the foreseeable future, where the goal is not impregnable [1].

Authentication supported passwords is employed for the most part in applications for pc security and privacy. but act like selecting dangerous passwords Associate in Nursing inputting passwords in an insecure approach are considered "the weakest link" within the authentication chain. Within the projected system, a unique authentication system Pass Matrix, supported graphical passwords to resist shoulder water sport attacks. With a valid login indicator and travel horizontal; and vertical bars covering the complete scope of pass pictures. Within the modification method, deploy Graphical primarily based countersign authentication except for Pass Matrix implementation. Users are going to be registering with 2 pictures and with its Pixels. User is attested provided that each PassMatrix and Graphical countersign is matched. It doubtless assist you hunt down the hacker and report them to the authorities. Programs that

are enables to visualize the IP address that the user is connected from. This IP address may be wont to realize their approximate geographic location, presumably login names from their pc, and identity clues from their host names. We are able to then use this data to report them to the authorities or enforcement [2].

A probabilistic password model assigns a probability value to each string. Such models are useful for research into understanding what makes users choose more (or less) secure passwords, and for constructing password strength meters and password cracking utilities. Guess number graphs generated from password models are a widely used method in password research. In this paper, we show that probability-threshold graphs have important advantages over guess-number graphs. They are much faster to compute, and at the same time provide information beyond what is feasible in guess-number graphs. We also observe that research in password modeling can benefit from the extensive literature in statistical language modeling. We conduct a systematic evaluation of a large number of probabilistic password models, including Markov models using different normalization and smoothing methods, and found that, among other things, Markov models, when done correctly, perform significantly better than the Probabilistic Context-Free Grammar model proposed in Weir et al., which has been used as the state-of-the-art password model in recent research [3].

### 3. Methodology

#### 3.1. Proposed System

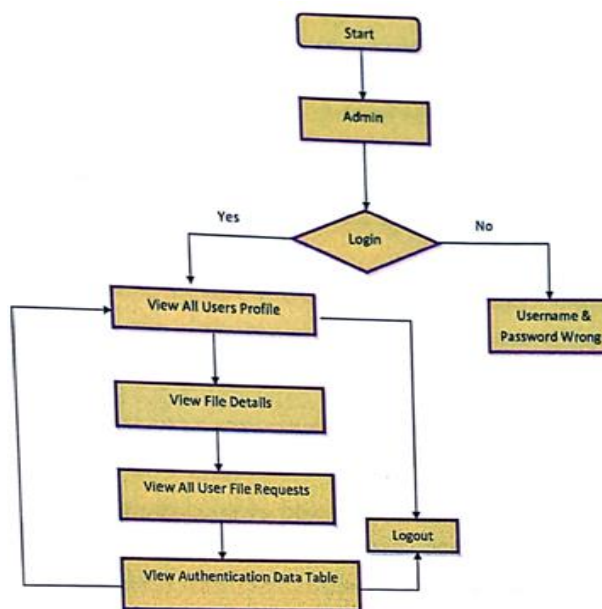


Fig.3: Class diagram: Use case

The proposed framework includes two phases: the registration phase and authentication phase. When adopting our framework to protect passwords in an authentication data table, the system designer must first select a cryptographic hash function and a symmetric-key algorithm, cryptographic hash function is equal to the key size of the selected symmetric-key algorithm.

A password protection scheme called ENP, and we propose two implementations of the ENP: ENPI and ENPII, including their generation algorithm and verification algorithms. Furthermore, a password authentication framework on the ENP is presented. We analyse and compare the attack complexity of hashed password, salted password, key stretching and the ENP. The results show that the ENP could resist lookup table attack without the need for extra elements and provide stronger password protecting under dictionary attack.

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard managed, and was created by, the Object Management Group. The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

#### 3.2. Encrypted Negative Password

Java technology is both a programming language and a platform; it is a high-level language that can be characterized by all of the buzzwords.

- ENPs could be obtained plain password (i.e., a sequence of characters) from a client is first hashed using a cryptographic hash function.
- Next, the hashed password is converted into a negative password using an NDB generation algorithm.
- Then, the negative password is encrypted using a symmetric-key algorithm- Thus, ENP is obtained. The solution of the negative password is the hash value of receive plain password.
- The NDB generation algorithm is selected for converting a hashed password to corresponding negative password.
- The NDB generation algorithm is a one-to-many mapping; simultaneously it is reversible; additionally, while keeping the one-to-many relationship, it does not introduce extra element.

#### 1.3 Open source SQL

A database is a structured collection of data. It may be anything from a simple shopping list to a picture gallery or the vast amounts of information in a corporate network. To



au access, and process data stored in a computer database, you need a database management system such as MySQL Server. Since computers are very good at handling large amounts of data, database management systems play a central role in computing, as utilities, or as parts of other applications. A relational database stores data in separate tables rather than putting all the data in big storeroom. The database structures are organized into physical files optimized 6n• speed. The logical model, with objects such as databases, tables, views, rows, and offers a flexible programming environment. You set up rules governing the relationship between different data fields, such as one-to-many, unique, required optional, and "pointers" between different tables. The database enforces these rules, so that with a well-designed database, your application never sees inconsistent, duplicate, orphan, out-of-date, or missing data. Open Source means that it is possible for anyone to use and modify the software. The MySQL software uses the GPL (GNU General Public License), <http://www.fsf.org/licenses/>, define what you may and may not do with the software in different situations. If you El uncomfortable with the GPL or need to embed MySQL code into a commercial application you can buy a commercially licensed version from us. The MySQL Database Software is a client/server system that consists of a multi-threaded SQL server that supports different backend, several different client programs and librarZ6, administrative tools, and a wide range of application programming interfaces (APIs).

#### 4. Results & Discussions

The purpose of testing is to discover errors. Testing is the process to fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

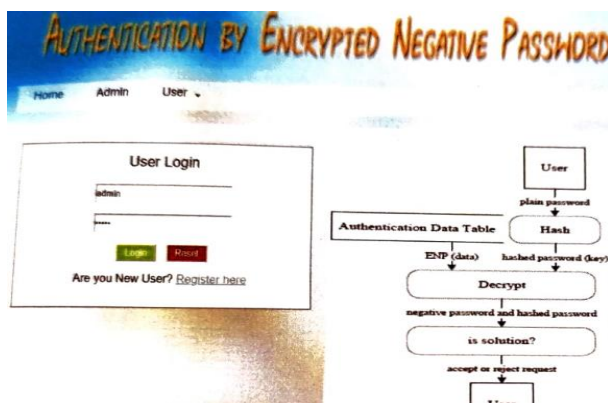


Fig.4: ENP Registration

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches internal code flow should be validated. It is the testing of individual software units of the application. It is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

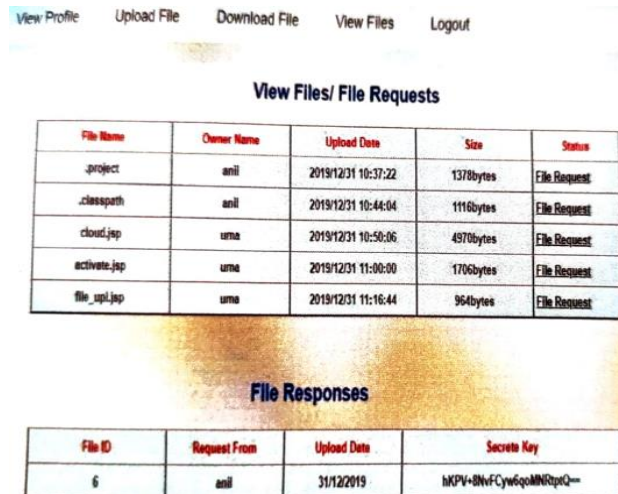


Fig.5: User login



Fig.6: User Page

Integration tests are designed to test integrated software components to determine if actually run as one program. Testing is event driven and is more concerned with the outcome of screens or fields. Integration tests demonstrate that although the components individually satisfaction, as shown by successfully unit testing, the combination of component is correct and consistent. Integration testing is specifically aimed at exposing that arise from the combination of components.



The screenshot shows a web application with a navigation bar containing 'View Profile', 'Upload File', 'Download File', 'View Files', and 'Logout'. Below the navigation bar, there are two sections: 'View Files/ File Requests' and 'File Responses'.

**View Files/ File Requests**

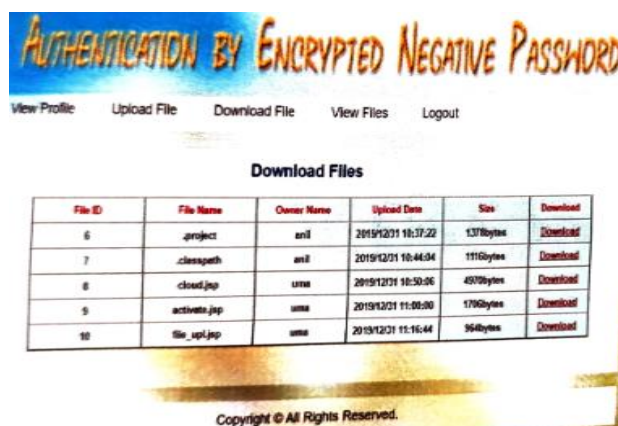
File Name	Owner Name	Upload Date	Size	Status
.project	anil	2019/12/31 10:37:22	1378bytes	File Request
.classpath	anil	2019/12/31 10:44:04	1116bytes	File Request
cloud.jsp	uma	2019/12/31 10:50:06	4970bytes	File Request
activate.jsp	uma	2019/12/31 11:00:00	1706bytes	File Request
file_up.jsp	uma	2019/12/31 11:16:44	964bytes	File Request

**File Responses**

File ID	Request From	Upload Date	Secret Key
6	anil	31/12/2019	hKPV+8NvCYw6qoMNRQpQ=

Fig.7: File Upload

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is configuration oriented system integration test. System is based on process descriptions and flows, emphasizing pre-driven process links and integration points. White Box Testing is a testing in which in which the software tester has knowledge of at inner workings, structure and language of the software, or at least its purpose. It is purport is used to test areas that cannot be reached from a black box level.



The screenshot shows a web application with a navigation bar containing 'View Profile', 'Upload File', 'Download File', 'View Files', and 'Logout'. Below the navigation bar, there is a section titled 'Download Files'.

**Download Files**

File ID	File Name	Owner Name	Upload Date	Size	Download
6	.project	anil	2019/12/31 10:37:22	1378bytes	Download
7	.classpath	anil	2019/12/31 10:44:04	1116bytes	Download
8	cloud.jsp	uma	2019/12/31 10:50:06	4970bytes	Download
9	activate.jsp	uma	2019/12/31 11:00:00	1706bytes	Download
10	file_up.jsp	uma	2019/12/31 11:16:44	964bytes	Download

Copyright © All Rights Reserved.

Fig 8: File save

Black Box Testing is testing the software without any knowledge of the inner work— structure or language of the module being tested. Black box tests, such as specification requirements document, such as specification or requirements document. It is a testing in the software under test is treated, as a black box .you cannot "see" into it. Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by defects. The task of the integration test is to check that component of software applications. User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements. Test Results; All the test cases mentioned above passed successfully. No defects encountered.

## 5. Conclusion

A Password protection scheme called ENP, and presented a password authentication framework based on the ENP. In our framework, the entries in the authentication data table are ENPs. In the end, we analysed and compared the attack complexity of hashed password, salted password, key stretching and the ENP. The results shown that the ENP could resist lookup table attack and provide stronger password protection under dictionary attack, it is worth mentioning that the ENP does not need extra element (e.g. salt)while resisting lookup table attack.

## References

- [1] Nazish Khalid a, Adnan Qayyum (2023) "Privacy-preserving artificial intelligence in healthcare: Techniques and applications" 158,106848
- [2] Syed Jawad Hussain, Muhammad Irfan (2020) "Performance Enhancement in Wireless Body Area Networks with Secure Communication" <https://doi.org/10.1007/s11277-020-07702-7>
- [3] Jehangir Arshad, Talha Ahmad Siddiqu (2023) "Deployment of an intelligent and secure cattle health monitoring system", Egyptian Informatics Journal, Vol. 24, pp265-275.
- [4] Jean-Paul A. Yaacoub a , Ola Salman (2020) " Cyber-physical systems security: Limitations, issues and future trends", Microprocessors and Microsystems. Vol. 77, 10320
- [5] Victor Chang, Le Minh Thao Doan (2023) "Digitalization in omnichannel healthcare supply chain businesses: The role of smart wearable devices", Journal of Business Research. Vol. 156, 113369
- [6] Carmen Camara, Pedro Peris (2015) "Security and privacy issues in implantable medical devices: A comprehensive survey" Journal of Biomedical Informatics, Vol. 55, pp.272-289.
- [7] Moustafa Mamdouh , Ali Ismail Awad (2021) "Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions" Computer & Security, 111, 102491
- [8] Morteza Safaei Pour, Christelle Nader (2023) "A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security" Computers & Security, 128, 03123
- [9] Pablo Najera , JavierLopez (2011) "Real-time location and inpatient care systems based on passive RFID" Journal of Network and Computer Applications. Vol. 34, pp.980-989.
- [10] Andrew J, Deva Priya Isravel (2023) "Blockchain for healthcare systems: Architecture, security challenges, trends and future

- directions”, Journal of Network and Computer Applications 215, 103633.
- [11] Matan Kintzlingera,c, Nir Nissima (2019) “Keep an eye on your personal belongings! The security of personal medical devices and their ecosystems, Journal of Biomedical Informatics Vol. 95, 103233
- [12] Reyazur Rashid Irshad, Shahab Saquib Sohail (2023) “Towards enhancing security of IoT-Enabled healthcare system” Heliyon 9, e22336.
- [13] Sushovan Chaudhury, Kartik Sau (2023) “A blockchain-enabled internet of medical things system for breast cancer detection in healthcare” Healthcare Analytics 4, 100221

