IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 5, May 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105125|

SeCRYPT- A Password Manager

Aditya Gupta[1], Aniket Sahu[2], Animesh Tarodia[3], Shubham Choudhari[4]

BCA-CTIS, Ajeenkya D Y Patil University, Pune, Maharashtra, India [1]

BCA-CTIS, Ajeenkya D Y Patil University, Pune, Maharashtra, India [2]

BCA-CTIS, Ajeenkya D Y Patil University, Pune, Maharashtra, India [3]

BCA-CTIS, Ajeenkya D Y Patil University, Pune, Maharashtra, India [4]

ABSTRACT: Password-protected systems are still vulnerable to a variety of assaults, even decades after they were first introduced. SeCRYPT is an end-to-end encrypted password manager which emphasizes on security and privacy. It protects users' web service account passwords on a password file on a cloud service. The application will function as SaaS over cloud which increases the availability and reliability of the application. All the password stored in our application will be encrypted and stored in database over cloud. The encrypted password and keys will be stored in different database which would further increase the security.

KEYWORDS: Password manager, AWS, Security, Cryptography, Software

I. INTRODUCTION

Password-protected systems are still vulnerable to a variety of assaults, including shoulder surfing, even decades after they were first introduced. online guessing (brute force) attacks, and offline dictionary attacks. Several of these attacks are entirely based on the passwords' entropy[11]. Users like to use memorable passwords; nevertheless, because of the memorability issue, such easy passwords often indicate easier assaults, whilst safe and random passwords open up new avenues of attack. (e.g., writing down, storing electronically, and less frequent updates). Furthermore, users frequently re-use the same password to access several web services, increasing security issues because the breach of one service threatens the accounts of other services [6].

Online password managers save users' (encrypted) web service account passwords on a password file on a cloud service to address these difficulties. By recommending complex and unique account passwords for each web service, these password managers help to reduce the risk of password leaks. Current online password managers, on the other hand, do not protect the "account password" or the "master password" from the password manager itself, leaving them vulnerable to malicious insider and outsider attacks that compromise the password management service, which is especially dangerous given its online nature. Several reports reveal that this critical vulnerability in password managers has been exploited.

To address this problem, we introduce SeCRYPT. SeCRYPT is an end-to-end encrypted password manager which emphasizes on security and privacy. All the password stored in our application will be encrypted and stored in database over cloud in which encrypted password and keys will be stored in different database which would further increase the security of the application[10]. The application will function as SaaS over cloud which increases the availability and reliability of the application.

What is AES and why is it used? AES is a key cypher with symmetric keys. This means that the same secret key is used for encryption and decryption, and the sender and recipient of the data both need a copy of the key. The US National Institute of Standards and Technology (NIST) published a standard for electronic data encryption in 2001. Despite being more complex to construct, AES is still widely used today due to its superior strength than DES and triple DES[8][9].

With the help of AES we are going to encrypt the password which are we going to store on cloud server.

Points to Keep in Mind -

•The AES cypher is a block cypher.

•The key can be 128/192/256 bits in length.

•Data is encrypted in 128-bit chunks.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105125|

What does the acronym SHA stand for? The abbreviation for secure hashing algorithm (SHA) is secure hashing algorithm. MD5 is the basis for SHA, which is a hashing algorithm. It is employed in the hashing of data and certificates[1]. A hashing method compresses the input data into a smaller form that cannot be interpreted using bitwise operations, modular additions, and compression functions.

II. LITERATURE SURVEY

1. AES – 256

The Advanced Encryption Standard (AES) algorithm is a symmetric block encryption technique that is extensively utilized across the world. This technique, which has its unique structure for encrypting and decrypting sensitive data, is used in hardware and software all around the world. When using the AES method to encrypt data, it is exceedingly difficult for hackers to decrypt the data. To yet, there is no evidence that this algorithm is broken. AES can handle three alternative key sizes: 128, 192, and 256 bits, with each of these ciphers having a 128-bit block size. The number of people using the internet and networks is continually expanding. Every day, a large amount of digital data is exchanged among users. Some data is sensitive and must be safeguarded against attackers. Encryption methods are crucial in preventing unauthorised access to original data. Encryption algorithms come in a variety of forms. The Advanced Encryption Standard (AES) method is one of the most efficient, and it is widely accepted and implemented in both hardware and software.[1]

2. AWS

Cloud computing has exploded in popularity, especially among commercial web applications. The pay-as-you-go concept allows for a flexible and cost-effective access to computational resources. Because of these factors, the scientific computing community is becoming more interested in cloud computing. Cloud implementation and performance, on the other hand, differ significantly from those at traditional supercomputing centers. It is consequently necessary to assess the performance of HPC applications in today's cloud systems in order to comprehend the tradeoffs that come with cloud migration. This is the most extensive comparison of traditional HPC systems to Amazon EC2 to date, utilizing real workloads representative of a typical supercomputing center's workload. Overall, EC2 is six times slower than a normal mid-range Linux cluster and twenty times slower than a recent HPC server, according to the results. The EC2 cloud platform's connection severely limits performance and generates significant fluctuation.[2]

3. SAAS

Cloud computing is a type of internet-based distributed computing that allows a programme or application to operate on several computers at the same time. Software as a service (SaaS) is a type of service that offers various advantages to its users. To assess the quality of a SaaS cloud service, a specific quality model is required. The standard quality approach ignores SaaS characteristics like as security and service quality. SaaS is a form of cloud service that has developed as a useful repurposing paradigm. It offers service users a number of advantages, including no upfront costs for software, no maintenance/updates, Internet accessibility, high availability, and pay-per-use pricing. As a result, assessing the quality of SaaS becomes a more crucial job for effective SaaS management.[3]

4. Designing Password Policy for Strength and Usability

Service providers are growing increasingly worried about the security of internet accounts, which has resulted in password-composition regulations. These restrictions limit the number of characters that may be used in user-created passwords, making it more difficult for attackers to guess passwords. Many users, on the other hand, struggle to construct and remember passwords when they are subjected to severe password-composition standards, such as those that require passwords to have at least eight characters, various character classes, and a dictionary check. According to recent research, focusing policy requirements on password length rather than complexity is a potential approach. Only length was needed by a few of the password-composition criteria we evaluated. These policies were quite simple to implement. Many of the passwords generated as a result of these regulations were quite strong. For High-Security Service Providers, the Pattern Requirement may be appropriate. Passwords must begin and end with lowercase letters to meet the pattern requirement. Without this restriction, the great majority of research participants tended to begin or conclude with special characters that were not necessary.[4]

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105125|

5. Use of Password Manager

Cybersecurity is one of the most rapidly expanding disciplines in computer science and the technology sector. The global economy has suffered enormous costs as a result of shoddy security. Password security is frequently the stumbling block in such financial losses. Companies and individuals alike are not doing enough to enforce stringent password requirements, as recommended by the NIST (National Institute of Standards and Technology). Thousands to millions of passwords can be disclosed and kept in files as a result of large security breaches, making users vulnerable to dictionary and rainbow table attacks. These are only a couple of instances of password cracking attacks. One of the main features that Passbolt, Encryptr, and Padlock all have in common is that they are all open-source. Consumers may review the code and report any vulnerabilities or problems directly, which helps to speed up the refining process. Because open-source software is free, anybody can identify security flaws, but not everyone will disclose them. The advantage of closed source password managers is that their code is shielded from possible attackers. This means that an attacker is unlikely to be able to examine the code and exploit any flaws that may exist. A closed source password manager's biggest flaw is the person who runs it. Because the user is unaware of the intricacies of how their passwords are saved and processed, the user must believe that the organisation is safely preserving their credentials. A decent password manager would put security ahead of convenience.[5]

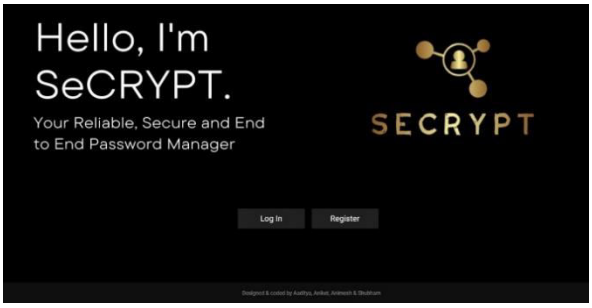
IV. PROPOSED SYSTEM

1 REQUIREMENTS

Microsoft IE 11, IE 10, IE 9, IE 8, Firefox, Safari 5.1.7 or Chrome with stable internet connection.

2 METHODOLOGY

2.1 Login Modules



The Login Module is a portal module that enables users to log in using their user name and password. To allow users to log into the system, you may add this module to any module tab. The master password and username can both be found in this module. In our suggested approach, the master password is saved in the form of a SHA-256 hash, which allows the system to authenticate the user.SHA-256 applications include hash tables, integrity verification, challenge handshake authentication, digital signatures, etc[7].

- 'Challenge handshake authentication' (or 'challenge hash authentication') prevents passwords from being shown in the clear - a client can submit the hash of a password over the internet for confirmation by a server without the danger of the original password being intercepted.
- Anti-tamper – connect a message's hash to the original, and the receiver may re-hash the message and compare it to the given hash: if they match, the message is unmodified; this can also be used to ensure no data is lost during transmission.
- Digital signatures are more complicated, but in principle, you may sign a document's hash by encrypting it with your private key, resulting in a digital signature. Anyone else may then verify that you authenticated the

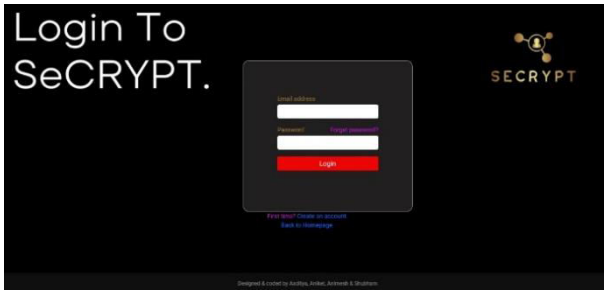
| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105125|

content by decrypting the signature with your public key and comparing the original hash to their own hash of the text

2.2 Development Of Login Module



Node.js

Node.js is a server environment that is free to use. Node.js is a free runtime environment. Node.js may be used on a variety of systems (Windows, Linux, Unix, Mac OS X, etc.). On the server, Node.js employs JavaScript. Opening a file on the server and returning the contents to the client is a common activity for a web server.

A file request is handled in PHP or ASP like this:

- Sends the task to the file system on the computer.
- Waits for the file system to open the file and read it.
- The client is given the content back.
- I'm all set to take on the next task.

A file request is handled in Node.js as follows:

- Sends the task to the file system on the computer.
- I'm all set to take on the next task.
- The server returns the file's content to the client when the file system has opened and read it.

Node.js skips the waiting and moves on to the next request instead. Node.js is a memory-efficient single-threaded, non-blocking, asynchronous programming language.

Express.js

Express.js, or simply Express, is a back-end web application framework for Node.js that was distributed under the MIT License as free and open-source software. It is intended for the development of web applications and APIs. It's been dubbed Node.js' de facto standard server framework[4].

Express is a Node.js web application framework that offers a rich collection of functionalities for developing web and mobile apps. It allows for the quick creation of Node-based Web applications. The characteristics of the Express framework are listed below:

- Allows middlewares to reply to HTTP requests to be configured.
- Defines a routing table that can be used to conduct various actions depending on the HTTP Method and URL.
- Allows giving arguments to templates to dynamically render HTML pages.

BCrypt

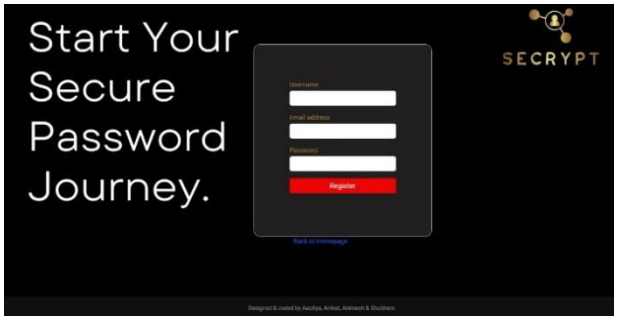
The problems present in traditional UNIX password hashes led naturally to a new password scheme which we call *bcrypt*, referring to the Blowfish encryption algorithm. Bcrypt uses a 128-bit salt and encrypts a 192-bit magic value. It takes advantage of the expensive key setup in *eksblowfish*.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105125|

- BCrypt is based on the Blowfish block cipher cryptomatic algorithm and takes the form of an adaptive hash function. But why should you use it to protect your data and resources? To explain, we're going to need to get a little technical…
- Using a Key Factor, BCrypt is able to adjust the cost of hashing. With Key Factor changes, the hash output can be influenced. In this way, BCrypt remains extremely resistant to hacks, especially a type of password cracking called rainbow table.
- This Key Factor will continue to be a key feature as computers become more powerful in the future. Why? Well, because it compensates for these powerful computers and slows down hashing speed significantly. Ultimately slowing down the cracking process until it's no longer a viable strategy.
- If you have sensitive data or information that you need to be protected, ensuring it is secured correctly is vital. As we have seen, there are many ways to secure this information through various password methods, but only BCrypt offers a truly robust solution.



JSON web token

JSON Web Token (JWT) is an open standard (RFC 7519) for securely sending information between parties as a JSON object. Because it is digitally signed, this information can be checked and trusted. JWTs can be signed with either a secret (HMAC) or a public/private key pair (RSA or ECDSA).

Although JWTs can be encrypted to guarantee party-to-party confidentiality, we'll concentrate on signed tokens. Signed tokens can be used to verify the validity of the claims they contain, whilst encrypted tokens keep those claims hidden from others. When public/private key pairings are used to sign tokens, the signature also verifies that only the party who holds the private key signed it[8].

Here are some scenarios where JSON Web Tokens are useful:

- Authorization is the most typical case in which JWT is used. Each subsequent request will include the JWT once the user has logged in, allowing the user to access routes, services, and resources that are permitted with that token. Single Sign On is a popular feature that makes use of JWT nowadays due to its low overhead and ability to be used across multiple domains.
- Information Exchange: JSON Web Tokens are an excellent way to send information securely between parties. You can be sure the senders are who they say they are because JWTs can be signed—for example, using public/private key pairs. You may also check that the content hasn't been altered with because the signature is calculated using the header and payload.

RESTful API

A REST API (also known as a RESTful API) is an application programming interface (API or web API) that adheres to the REST architectural style's limitations and allows users to interact with RESTful web services. Roy Fielding, a computer scientist, devised REST, which stands for representational state transfer.

REST is a set of architectural constraints, not a protocol or a standard. API developers can implement REST in a variety of ways. A representation of the state of the resource is transferred to the requester or endpoint when a client request is made over a RESTful API. JSON (JavaScript Object Notation), HTML, XLT, Python, PHP, or plain text are

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105125|

some of the forms in which this data, or representation, is sent through HTTP. JSON is the most widely used file format because, despite its name, it is language-independent and understandable by humans and machines alike[9].

An API must meet the following requirements in order to be classified as RESTful:

- Clients, servers, and resources are all part of a client-server architecture, with HTTP requests being controlled.
- Client-server communication that is stateless means that no client data is kept between get requests and that each request is distinct and unrelated.
- Client-server interactions are streamlined by caching data.
- Information is exchanged in a standard format thanks to a consistent interface between components. This requires that:
  - The requested resources are distinct from the representations given to the client.
  - Because the representation provides enough information, the client can alter resources via the representation they get.
  - The information in self-descriptive messages sent to the client is sufficient to define how the client should process them.
  - The client should be able to use hyperlinks to locate all other currently possible actions after visiting a resource, indicating that hypertext/hypermedia is available.
- The retrieval of requested information into hierarchies, unseen to the client, is part of a layered system that organizes each type of server (those responsible for security, load-balancing, etc.).
- Code-on-demand (optional): the ability to transfer executable code from the server to the client when it is requested, hence expanding client capabilities

V. CONCLUSION

A password manager is software that allows us to create new passwords, save and manage our login information. Both not using and using a password manager have hazards, but the risk of not using one much surpasses the risk of using one for most people.

If you do decide to use a password management, you should mitigate the danger of doing so by enabling two-factor authentication, planning your master password recovery procedure, and not saving a high-risk password in your password manager.

REFERENCES

[1] Abdullah, Ako Muhamad. "Advanced encryption standard (AES) algorithm to encrypt and decrypt data." Cryptography and Network Security 16 (2017): 1-11.

[2] Jackson, Keith R., et al. "Performance analysis of high performance computing applications on the amazon web services cloud." 2010 IEEE second international conference on cloud computing technology and science. IEEE, 2010.

[3] Banerjee, Sarbojit, and Shivam Jain. "A survey on Software as a service (SaaS) using quality model in cloud computing." International Journal of Engineering and Computer Science 3.1 (2014): 3598-3602.

[4] Shay, Richard, et al. "Designing password policies for strength and usability." ACM Transactions on Information and System Security (TISSEC) 18.4 (2016): 1-34.

[5] Luevanos, Carlos, et al. "Analysis on the security and use of password managers." 2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT). IEEE, 2017.

[6] Abdullah, Ako. (2017). Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data.

[7] Gowthaman, A. & Manickam, Sumathi. (2015). Performance study of enhanced SHA-256 algorithm. 10. 10921-10932.

[8] Banerjee, Sarbojit. (2014). A survey on Software as a service (SaaS) using quality model in cloud computing.

[9] Shay, Richard; Cranor, Lorrie Faith; Komanduri, Saranga; Durity, Adam L.; Huh, Phillip (Seyoung); Mazurek, Michelle L.; Segreti, Sean M.; Ur, Blase; Bauer, Lujo; Christin, Nicolas (2016). Designing Password Policies for Strength and Usability. ACM Transactions on Information and System Security, 18(4), 1–34. doi:10.1145/2891411.

[10] Luevanos, Carlos & Elizarraras, John & Hirschi, Khai & Yeh, Jyh-haw. (2017). Analysis on the Security and Use of Password Managers. 17-24. 10.1109/PDCAT.2017.00013.

[11] Shirvanian, M., Price, C. R., Jubur, M., Saxena, N., Jarecki, S., & Krawczyk, H. (2021). A hidden-password online password manager. Proceedings of the 36th Annual ACM Symposium on Applied Computing.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details