EXAMINING USER CONDUCT, IDENTIFYING, TRACING, AND ELIMINATING INTRUDERS WITHIN A CLOUD ENVIRONMENT

Abstract

Social network accounts are actively tracked and monitored for detection. In the event of a hacker targeting a legitimate user, our system allows the attacker to proceed, but concurrently captures crucial information about the attacker. We employ Honey words, generated based on user-provided information, alongside the conversion and storage of the original password in a different format, enhancing security. Our configuration consists of a Cloud server for user account management, a Shopping server for transactions, and an Intermediate server. Hacker can quickly change the login information for the cloud-based server if they are granted access to the primary client's email account details. As part of this project, the attacker's actions are permitted to facilitate easier identification. Consequently, when the attacker logs into the purchase portal, they are unknowingly tracked by the server. The system promptly identifies the attacker, notifies the original account owner, and effectively blocks the attacker from conducting any further transactions using the genuine account.

Keywords: Social Network, Hacker, Cloud, Intermediate server, Honey words

Authors

Sudha V
Assistant Professor
Department of AI & DS
Karpaga Vinayaga College of Engineering and Technology
Tamil Nadu, India.

Vishwa Priya I
Department of AI & DS
Karpaga Vinayaga College of Engineering and Technology
Tamil Nadu, India.

Logesh E
Department of Computer science and Engineering
Vi InstituteofTechnology
Tamil Nadu, India.

Dinesh Kumar T
Department of AI & DS
Karpaga Vinayaga College of Engineering and Technology,
Tamil Nadu, India.

Harini M
Department of AI & DS
Karpaga Vinayaga College of Engineering and Technology,
Tamil Nadu, India.

I. INTRODUCTION

The popularity of online storage services has significantly increased, enabling customers to easily safeguard and retrieve information from any place at any time. Information saved in the online database is normally protected to protect individual security as well as avoid illicit access by strangers. Ribute-based encryption (ABE) stood out for being one of the most attractive ways to protect data given the collaborative characteristic of online storage. In publications, a number of ABE concepts have been put out. However, a lot of those strategies rely on the complete confidence and imperviousness to hacking temptations of storage service providers and the dependable third parties in charge of key handling. In actual cases, interaction among clients and cloud storage companies can become hampered, forcing the service firms to reveal user credentials under the control of authorities or other means of coercion. The concerns are highlighted by incidents like Google giving user information to the Authorities in 2010 with no consent from users or Edward Snowden's revelations regarding widespread spying in 2013. All types of encryptions become ineffective under those degraded circumstances, rendering it harder and harder to protect the identities of users. The issue grows increasingly challenging despite the fact that providers of online storage can legally protect individual information from such hazards.

1. **Introducing the category:** An innovation with an ever-increasing rate of growth, cloud-based computing is now deeply embedded in the forthcoming generations of corporate and information technology landscapes. It guarantees the availability of dependable software, infrastructure as a Service (IaaS) and hardware delivered via the worldwide web and at distant data centres. Services provided by the cloud, which cover a wide range of IT operations spanning data retention and processing to information as well as app assistance, have developed as a powerful paradigm for carrying out sophisticated and substantial IT operations.

   Several businesses and individuals have adopted computing via the cloud due to the need to store, handle, and analyse large amounts of data. Because of the dearth of complimentary computing resources on local computers, the reasonable cost of finances, and the rising number of records produced and accessed by such studies, the Internet of Things continues to be a wonderful option for hosting a variety of mathematical functions that call for thorough tests. Additionally, computing hosting companies are already incorporating multiple computation systems into their offerings, allowing clients access to public capacity and easy programme implementation.

   Internet use of a range of already configured IT assets, which include services, servers, apps , storage devices, and networks, is made possible by the cloud computing paradigm, which functions as a framework that makes the internet ubiquitous, easy to navigate, and easily accessible. With little managerial effort or speaking directly with the vendor who provides the service, the assets can be quickly distributed and transferred. This method of computing via the internet offers several benefits for managing the swift economic expansion and solving tech hurdles.

   Important advantages of online computing include the overall cost savings and allowing businesses to concentrate on their main business tasks without worrying about structures, accessibility, or resource range of motion. An appealing location for executing studies is made possible by the coupling of the cloud-based convenience concept with a wide range of processing, structure, and data services available in the cloud.

Platform as a Service , Software as a Service , and Infrastructure as a Service are the three main components of cloud-based service technologies. Platform as a Service provides framework computing facilities to end users and is demonstrated by Salesforce.com, Google Apps , Microsoft Azure, and Engine the Force platform. Applications like Gmail, Google Docs, Online Payroll and Salesforce.com are examples of software as a service, which enables customers to access software running on off-site servers online. Using cloud hosting companies, Infrastructure as a Service provides end users with on-demand access to hardware apparatus, as demonstrated by firms like Amazon's EC2 and Flexi scale.

Because of the constrained CPU horsepower, and longevity of every-day gadgets, room for storage, computing via the cloud has grown in popularity as internet connectivity and cell phones become more widely used. As a result, mobile cloud computing has developed, allowing users to delegate work to outside vendors of services and facilitating data processing and storage on devices other than those that are mobile. Web-based Smartphone apps are anticipated to reach roughly 9.5 billion USD by 2014, according to Juniper Research's estimates. Handheld cloud computing services, iCloud, including Gmail, and Uber, are becoming more common. These programmes greatly boost user satisfaction and cellular internet speeds.

2. **Cloud Setup:** The data centre Internet Service Provider preserves all personal details for authorization reasons when users connect with their login credentials and holds quite a bit of information in its information vault. The Cloud Service Supplier Catalogue houses the tender data. Additionally, the Asset confiding Mechanism is redirected by the Cloud Servers to handle User-requested workloads. Proposals from every single user are handled by the material assignment of the module. The Cloud Server creates connections, assisted by an Application Frame, to enable interaction with Clients and the various Cloud Network components. Furthermore, while delivering User Employment requests within the Asset Assigned Module, the Cloud Services Provider prioritises them using the First-In-First-Out principle.

3. **Public Cloud:** On the other hand, clouds that are publicly accessible provide technological assets for data transmission, archiving, and operation. Companies will still receive separate store and specialised computer setups. Public data centres are a popular solution because a large percentage of projects and clients don't have serious security problems with them. Accessing additional companies' knowledge is exceedingly tough due to visualisation approaches.

4. **Hybrid Cloud:** Commercial and isolated cloud installations are combined in an integrated cloud setup. It is frequently used as it offers advantageous baseline load and blast capacities, as well as confidentiality and agility. Some businesses encounter brief spikes in exceptionally considerable demand during seasonal occasions, including highly anticipated marketing campaigns. Organisations can utilise hybrid clouds to manage base loads using internal resources while concurrently renting additional capacities through external clouds to accommodate peak loads. The capacity that can move both public and

private clouds smoothly is highly operationally complex. There are resources like Eucalyptus that make it easier to establish a mixture of public and customised clouds.

5. **Private Cloud:** Clouds that are private do not collaborate on physical capital and are devoted to an individual organisation. The aforementioned clouds may be either internally or externally hosted. The use of private cloud installations is primarily driven by the demand for rigorous differentiation between the business's information processing and storage, given confidentiality standards and laws. Private data centre deployments can be tough, though, as many endeavours and organisations frequently struggle to achieve the fiscal advantages of scale, even when they use standard methods. Due to significant operational costs and a probability of abandonment, delivering an income upon investment equal to publicly available cloud products is uncommon.

II. LITERATURE SURVEY

1. **Title:** A Comprehensive Analysis of Honeyword Based Password-Cracking Detection Authors: Imran Erguler, Gebze, Kocael

   This study thoroughly examines the concept of honeywords (decoy passwords) proposed by Juels and Rivest for detecting attacks against hashed password databases. The approach involves storing multiple honeywords alongside the legitimate password for each user account, making it challenging for adversaries who steal hashed passwords to identify the actual password. An alarm is triggered if a honeyword is used during login, alerting the administrator to a potential password breach. This research highlights possible weak points in the honeyword system and suggests an alternative approach where honeywords are selected from existing user passwords to offer more realistic honeywords and reduce storagecosts in the scheme.

2. **Title:** Improving Password Security using Honey words and Honey Encryption Author: R.Mahajan

   Security, especially effective passwords, is of paramount importance. This paper discusses the honey word mechanism as a means to detect adversaries attempting to log in using cracked passwords. The proposed approach involves combining existing user passwords to create new passwords called honey words. Each username is associated with a set of honey words, where only one element represents the correct password, while the others act as decoy passwords. If an attacker tries to gain access using a honey word, an alarm is triggered to alert the administrator about a potential password leak. The study focuses on using honey words to detect attacks against hash password databases, enhancing overall security.

3. **Title:** Honey Encryption based Hybrid Cryptographic Algorithm Authors: Vivek Raj K, Imran Erguler

   Ensuring high-level security in data exchange is a paramont concern with the rapid evolution of communication technology.In order to address a significant difficulty in symmetric security, this work offers an integrated encrypted method utilising Rivest Cypher for data compression and decryption with Honey Encoding for trustworthy keys for interchange. It investigates changing the quantity of RCS rotations and assesses its robustness in the context of inconsistencies, taking into account the impact of the avalanche effect. Likewise, when the total quantity of sets is raised, the temporal nature of RCS is examined, favouring greater force over an insignificant change in time. The RCS decryption technique is further protected by HE, which produces fictitious information in response to the detection of breaches. It has been demonstrated that using both techniques together increase reliability using multiple protection.

4. **Title:** Honeywords: A Technique for Detecting Password-Cracking Attempts Authors: A. Jules, R. Rivest

   This article presents a simple approach to adding more "honeywords" tied to each individual's account to hash their passwords in order to increase their degree of safety. Identifying between the true passcode and a honeyword becomes difficult in the event that somebody else steals an inventory of encrypted usernames and attempts to modify the hash process. When a user logs in via a honeyword, an alarm is set off, and a support server can tell the difference between administrator passwords and honeywords throughout the login process, triggering an email notification if a honeyword is found.

5. **Title:** Enhancing Security through Deception Authors: E. Spafford, M. Atallah

   Digital assets are abundant thanks to the merging of both digital and physical realities. This work presents a unique typology of techniques and strategies for protecting digital data. Diverse defence mechanisms are investigated, including hostile inference, refusal, solitary existence, degeneration and confusion, adverse details, trickery, and counter-operations. These strategies' interrelationships are examined, and their use at various organisational scales is described. The report maps various protective methods regarding the internet kill-chain framework and indicates areas that call for more research, providing interesting conclusions.

6. **Title:** Kamouage: A Loss-Resistant Password Management Approach Authors: Hristo Bojinoy, Elie Bursztein

   In order to create account managers that are theft-resistant, Kamouage suggests a novel design. In the scenario of device fraud, a significant internet task is necessary prior to retrieving any individual's keys kept in a password manager built on the Karguage programming language. The authors implemented this suggestion by replacing the default Firefox passcode administrator with their own app. They tested the viability and efficacy of their strategy using performance measures and studies using sizable everyday passphrase databases. As an average infrastructure for security applications for mobile gadgets, Kamouage has potential.

III. EXISTING SYSTEM

Cloud storage services have gained significant popularity. However, due to privacy concerns, many existing cloud storage encryption schemes lack sufficient security to ensure the safe storage of data. The drawbacks of the current system include low security levels, making it easy for attackers to hack user passwords and gain unauthorized access through guessing attacks.

IV. PROPOSED SYSTEM

In the proposed system, Social Network Accounts are monitored and detected for suspicious activity. If a hacker attempts to attack a genuine user, our system allows the attacker to proceed, while discreetly capturing essential information about the attacker. We create Honeywords using the user-provided data, and that initial passcode is changed and kept underneath the Honey words in a separate manner. An Interim server, which is a Buying service for choices, and a hosting server are all deployed by the system itself. This network also stores individual account information. We welcome intruders trying out operations as a distinctive aspect of this product, making it simpler to recognise them.

The adversary is mistakenly monitored after entering the buying gateway and is given permission to proceed with purchases. The server identifies the attacker, informs the original account owner, and blocks the attacker from further transactions using the genuine user's account. The main advantages of this system are preventing password guessing and hacking attempts by attackers, providing high security to data owners, and notifying the original user about the hacker's IP address and location via email.

1. **Diagram of the System Architecture:** The system architecture diagram shows how the entire system operates. A user must enter two email addresses when registering on the portal: one for their main profile and one for a backup. Users that successfully log in using the proper user login and password can make purchases through the standard gateway. However, if an individual makes more than three unsuccessful attempts to log in using false login credentials, the system will immediately reroute them to a false gateway and record the Internet Protocol (IP) address along with its delivery destination.

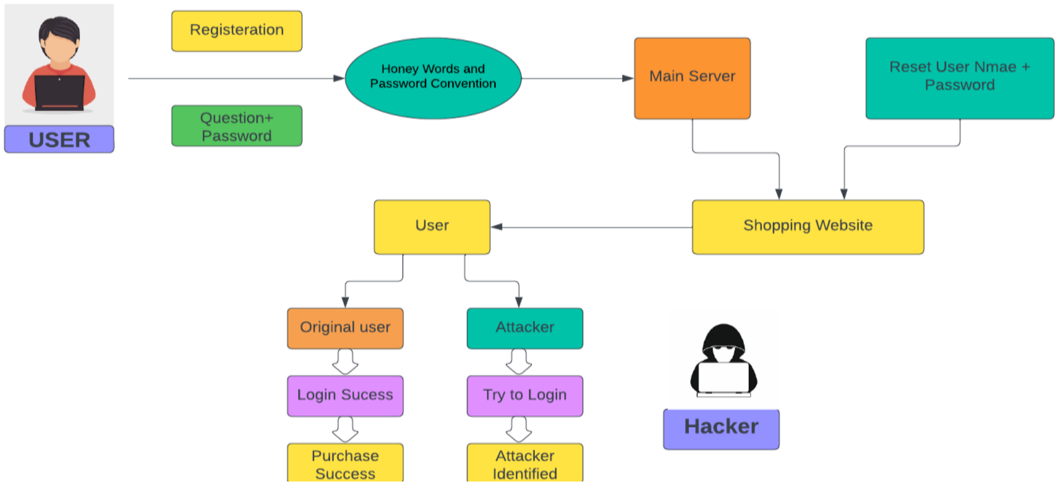


Figure 1: System Architecture Diagram

2. **Diagrammatic Flow of Data (DFD):** The operations or procedures related to gathering, modifying, archiving, and disseminating data within the system as a whole, throughout its elements, and between a system and its surrounding environment are visually represented by the DFD.

   Clients and architects of systems can effectively communicate using this visual depiction. The system's processes take data as input and produce outputs that can vary in substance or form. Simply gathering input data and putting it in the database can serve as one of these steps. In the database flow chart, instances where the system needs to store data for later consumption by any number of steps are represented by a storage facility or data warehouse.

LEVEL 0: (Login Diagram)

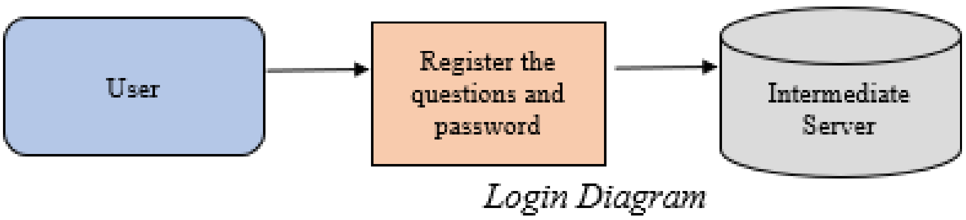


Figure 2: Log in Diagram

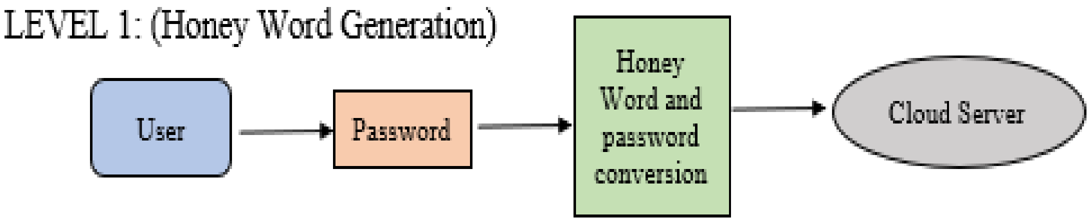

LEVEL 1: (Honey Word Generation)
User
Password
Honey Word and password conversion
Cloud Server

Figure 3: Honey word Generation

LEVEL 2: (Authorized purchase)

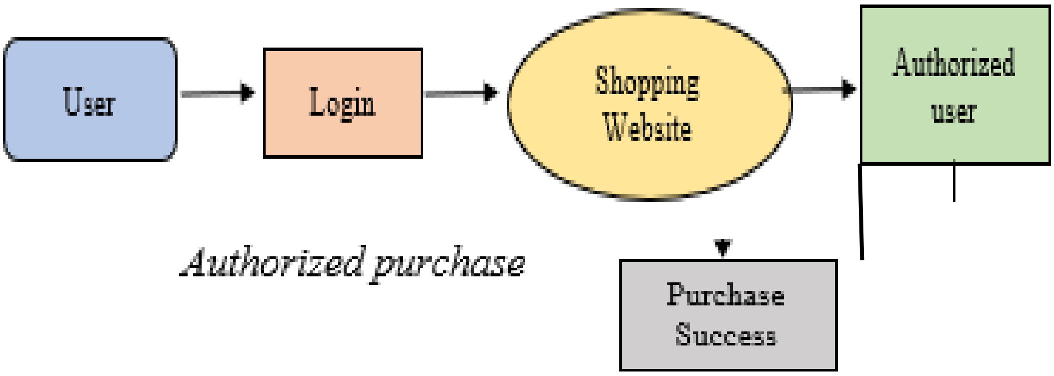


Figure 4: Authorized purchase

LEVEL 3: (Unauthorized Login)

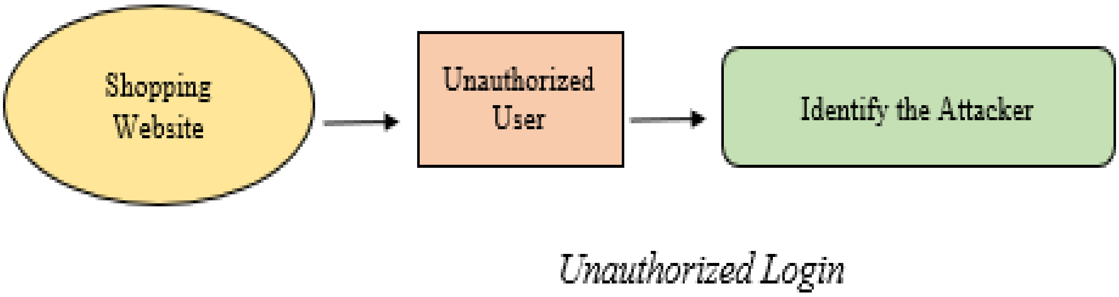


Figure 5: Unauthorized Login

Use-case illustrations provide a summary of the requirements for using the system. They are useful for providing knowledge to the project's business and stakeholders. Use cases, however, are more valuable when it comes to actual development because they capture the essence of real needs. The diagram's horizontal ellipses indicate each use case's description of a series of activities that add real value to a particular user action.

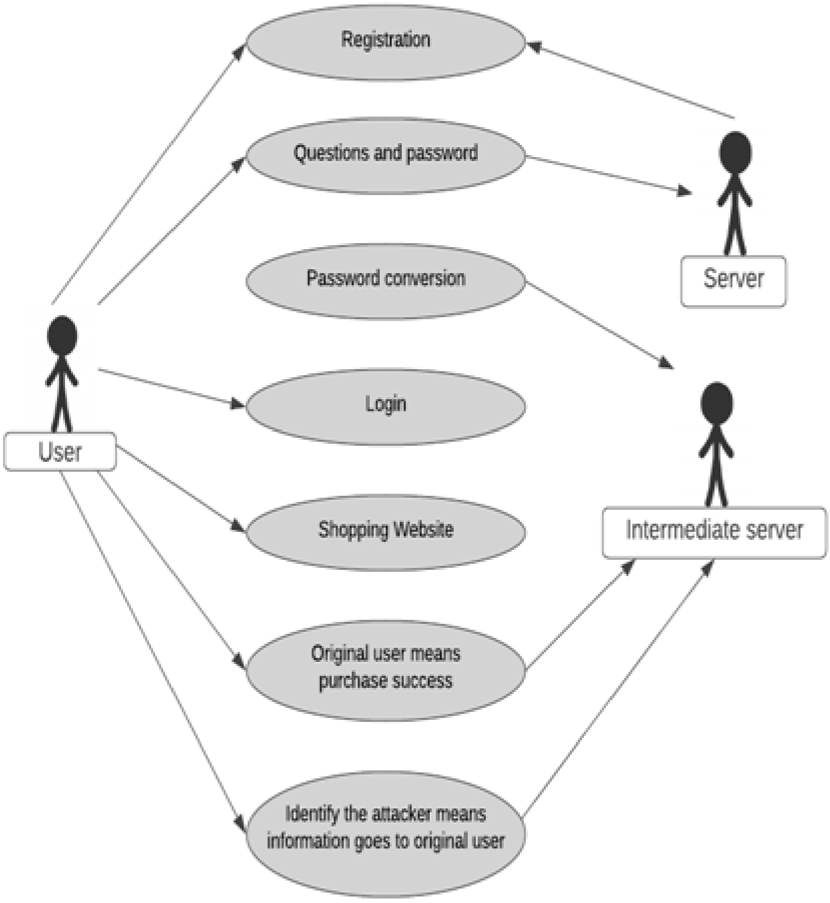


Figure 6: Use Case Diagram

Sequential diagrams permit you to capture and verify the logic of a system by representing the logical flow within the system visually. They are frequently employed for both design and analysis reasons. remarkably popular UML object for dynamic simulation, flow diagrams concentrate on finding and illustrating system behaviour. They offer a useful tool for comprehending how various elements are in touch with one another when carrying out particular tasks or scenarios.

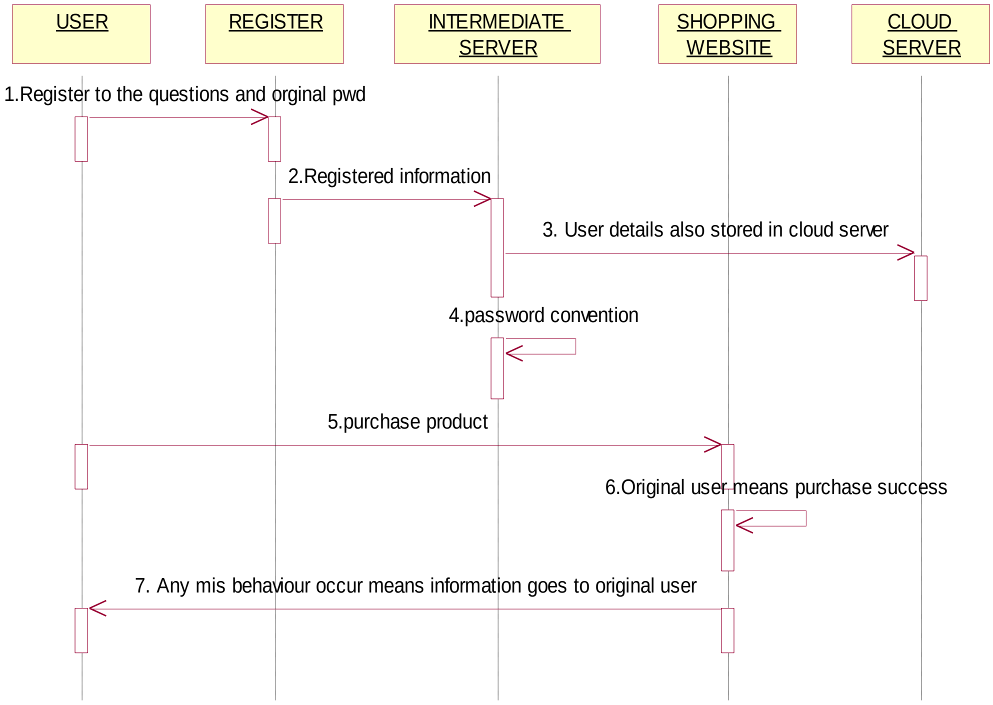

USER
REGISTER
INTERMEDIATE SERVER
SHOPPING WEBSITE
CLOUD SERVER
1.Register to the questions and orginal pwd
2.Registered information
3. User details also stored in cloud server
4.password convention
5.purchase product
6.Original user means purchase success
7. Any mis behaviour occur means information goes to original user

Figure 7: Sequential Diagram

3. **Sequencing Chart:** Diagrams of activities are pictures that show sequential processes and actions and support selection, repetition, and scalability.These flowcharts are useful tools for outlining the order of tasks and process steps for different system elements. A typical activity flowchart will have an initial node, an end node for the task being performed, and everything else in place. These elements help to show the pattern and evolution of actions across the course of the procedure.

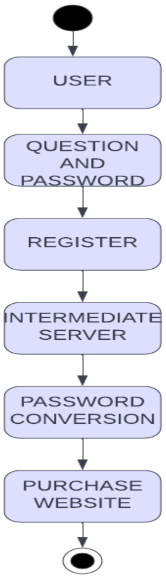


Figure 8: Activity Diagram

The cooperation diagram is yet another variety of interaction diagram. A cooperation is represented in this diagram as a collection of related things inside a certain setting. A sequence of conversations across various items inside the collaboration are displayed in the interaction element, and they all work simultaneously to achieve the intended result.

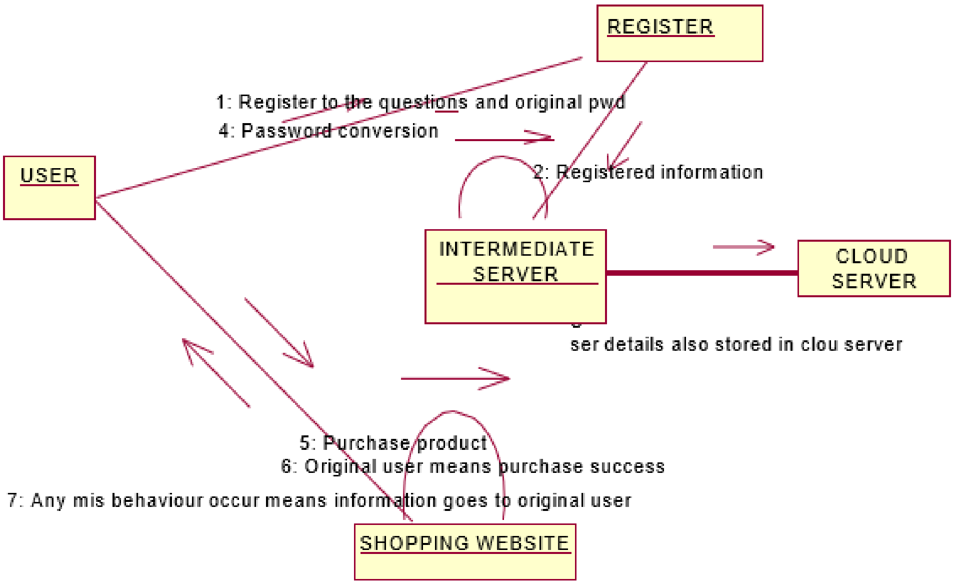

REGISTER
1: Register to the questions and original pwd
4: Password conversion
USER
2: Registered information
INTERMEDIATE SERVER
CLOUD SERVER
ser details also stored in clou server
5: Purchase product
6: Original user means purchase success
7: Any mis behaviour occur means information goes to original user
SHOPPING WEBSITE

Figure 9: Collaboration Diagram

V. RESULT

Access Page A crucial part of our project is the Login page. To continue with their purchase,On this panel, clients can input their user ID and pin.

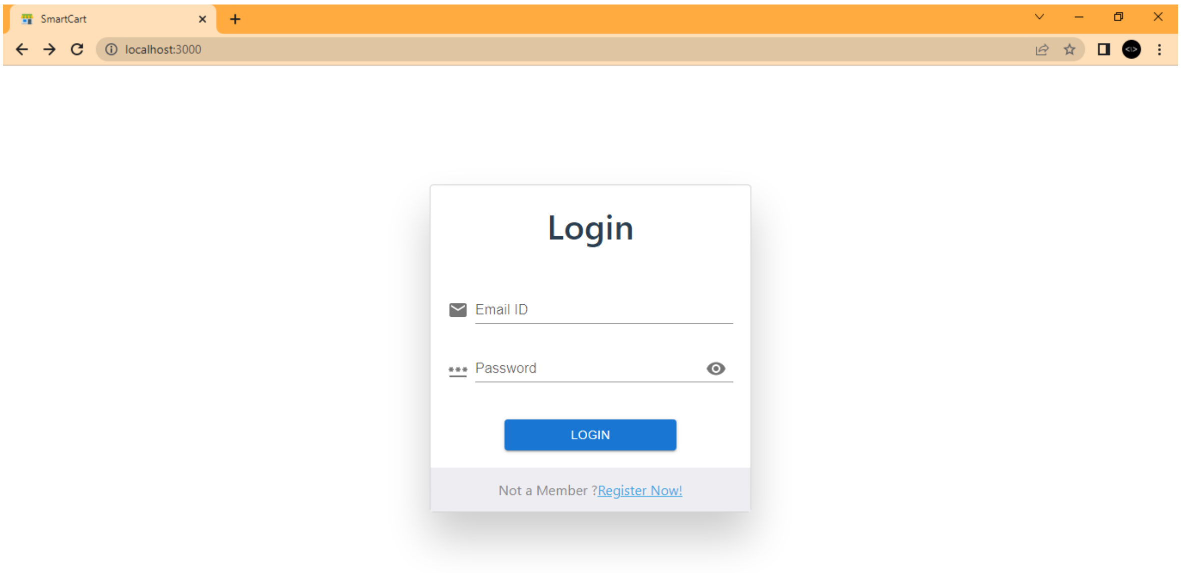


Figure 10: Login Page

1. **Sign-Up Page:** Users can register on this page. The form can be filled out by users, who can then submit it. After submitting the Register Page, the database is updated with the new user's data.

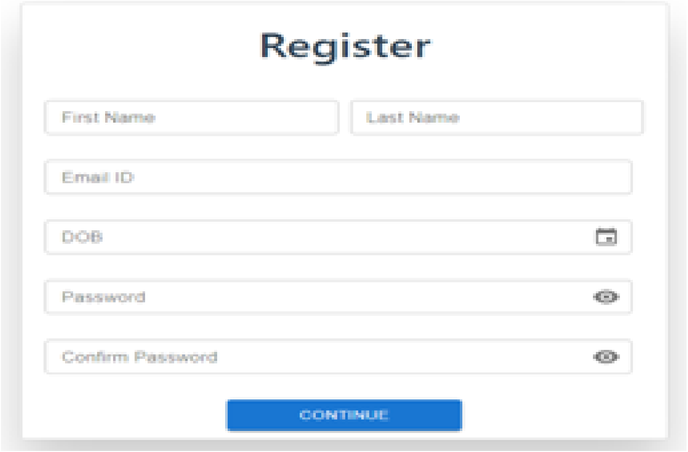
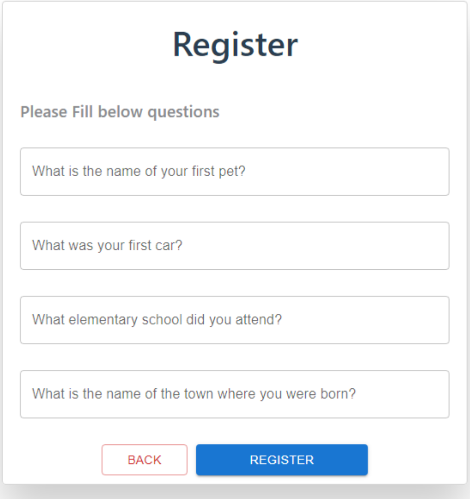


Figure 11: Register Page

2. **Register Security Questions Page:** Whenever a new client fills out the enrollment form, the programme shows the Request Safety Queries page. To better lock their account, someone can add responses to all four safety queries on the following screen.



Register

Please Fill below questions

What is the name of your first pet?

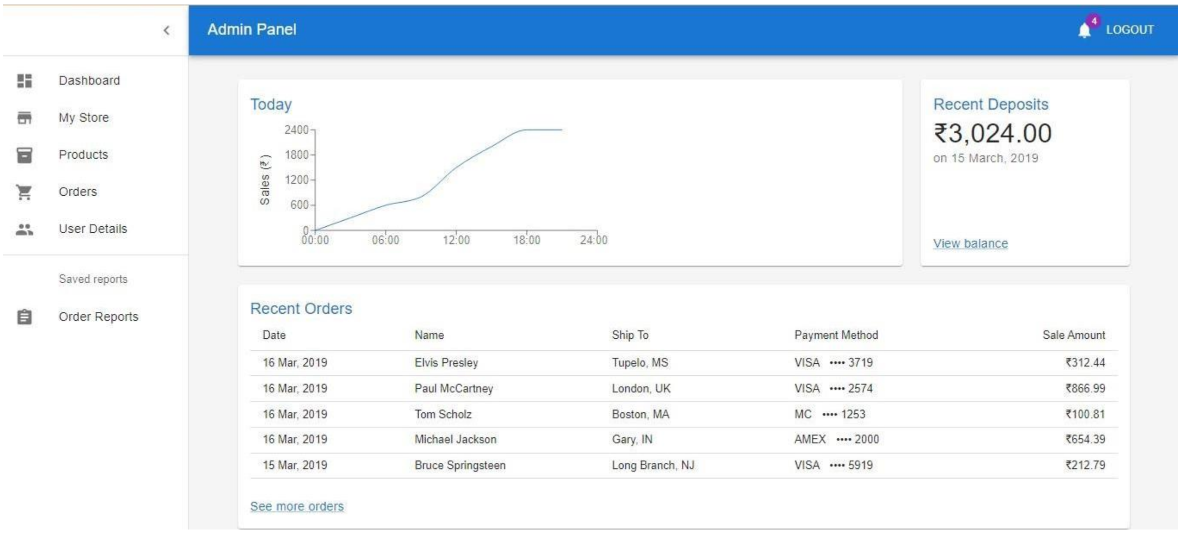
What was your first car?

What elementary school did you attend?

What is the name of the town where you were born?

Figure 12: Register Security Questions Page

3. **Admin Panel:** User card information and past purchases are kept in the admin area.



Recent Deposits

₹3,024.00

on 15 March, 2019

Recent Orders

Date	Name	Ship To	Payment Method	Sale Amount
16 Mar, 2019	Elvis Presley	Tupelo, MS	VISA •••• 3719	₹312.44
16 Mar, 2019	Paul McCartney	London, UK	VISA •••• 2574	₹866.99
16 Mar, 2019	Tom Scholz	Boston, MA	MC •••• 1253	₹100.81
16 Mar, 2019	Michael Jackson	Gary, IN	AMEX •••• 2000	₹654.39
15 Mar, 2019	Bruce Springsteen	Long Branch, NJ	VISA •••• 5919	₹212.79

Figure13: Admin Panel

4. **Store Page:** Clients may proceed with buying items on the following shop page, which offers a particular item discovery option. The items can be added to the Store Page once customers have made their selections.

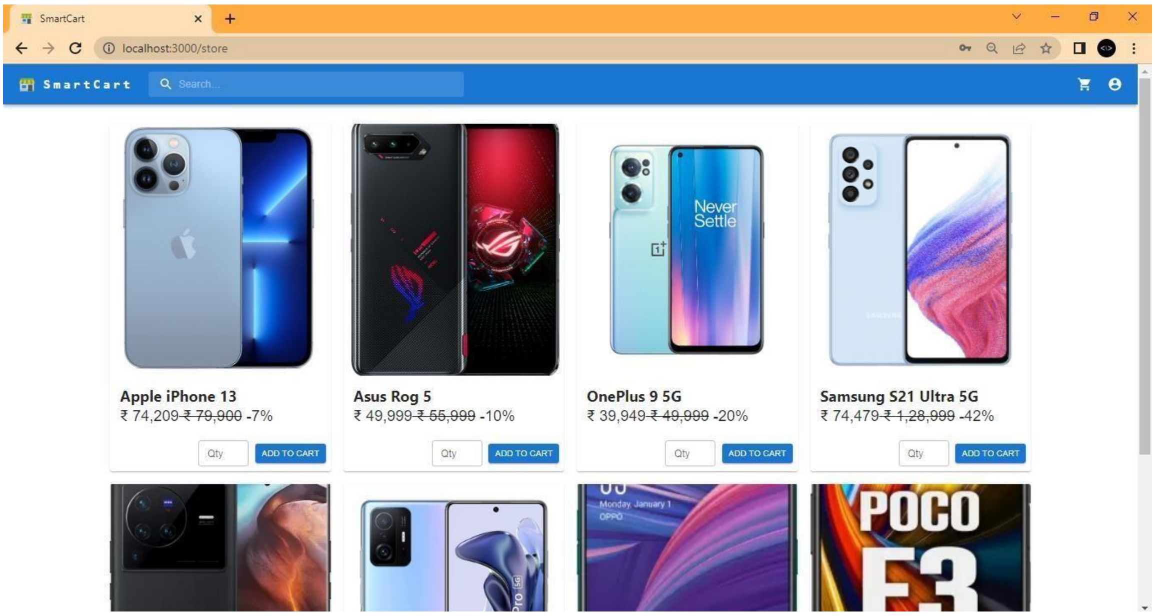
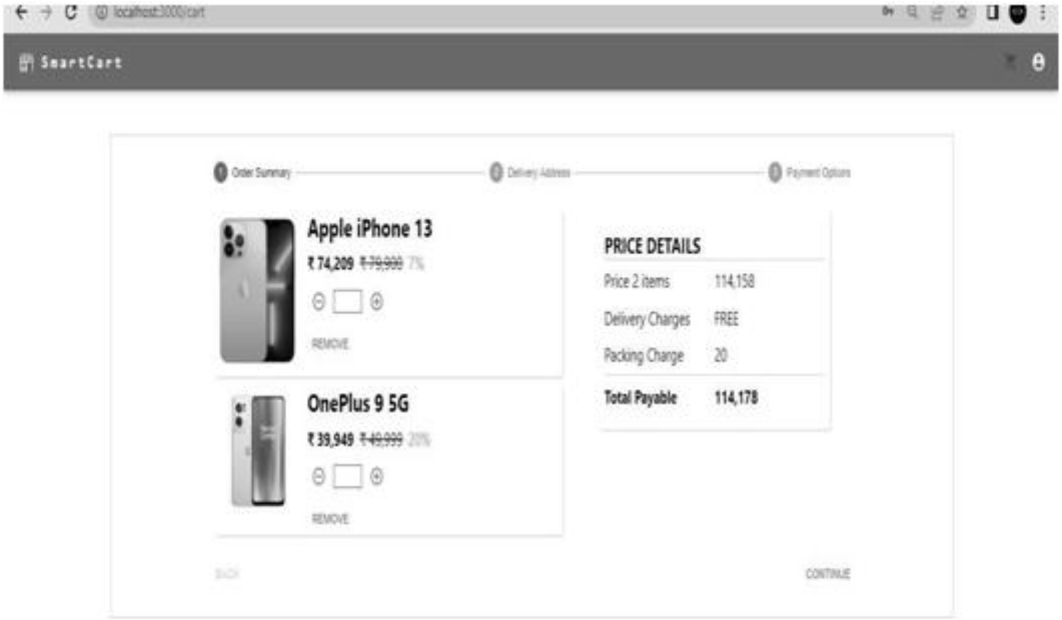


Figure 14: Store Page

5. **Cart Page:** The Basket Page shows all of the items that have been chosen and enables consumers to continue with their purchase.



PRICE DETAILS

Price 2 items	114,158
Delivery Charges	FREE
Packing Charge	20
Total Payable	**114,178**

Figure 15: Cart Page

6. **Shipping Address Page:** Consumers can provide the present location for the arrival of items on the checkout page.

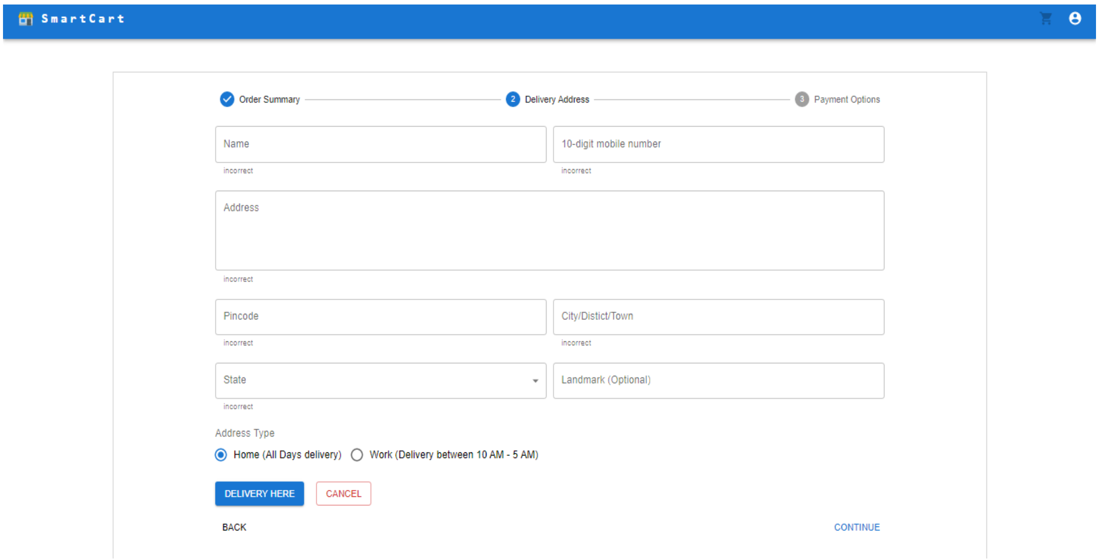


Figure16: Shipping Address Page

7. **Payment Options Page:** Consumers are brought to the Optional Payments Page after inputting shipping information. They can explore the several payment options here and select the one they need.

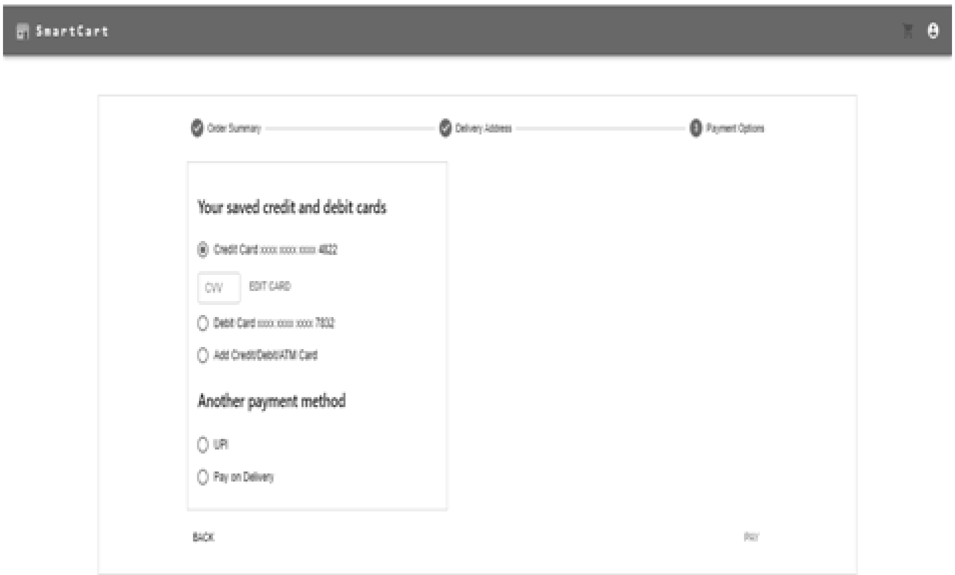

SmartCart
Order Summary
Delivery Address
3 Payment Options
Your saved credit and debit cards
● Credit Card xxxx xxxx xxxx 4822
CVV
EDIT CARD
○ Debit Card xxxx xxxx xxxx 7832
○ Add Credit/Debit/ATM Card
Another payment method
○ UPI
○ Pay on Delivery
BACK
PAY

Figure 17: Payment Options Page

VI. CONCLUSION

A safe digital payment process now has an extra layer of security thanks to Honey Encryption. The application creates Honey phrases centred on the user-supplied information, and the initial login information is changed and saved along with the Honey phrases in a separate style. In the event that an intruder is discovered, your mail ID, protocol address, postal delivery address and phone number, are tracked and kept. This information is eventually sent to the initial user's emergency email box.

REFERENCES

[1] Abdalla, Altom Adam Noshiba, "Preservation of Information Integrity Using Honey Encrypted." Sudan College of Science and Technology's 2019 proceedings.

[2] An extended RC5 (ERC5) method constructed around a straightforward number generator key enlargement mechanism was developed by Excel B. Villanueva, Ruji P. Medina, and Bobby D. Gerardo.

[3] Three Jayvee "ERC5a - An enhanced RC5 algorithm on bit propagation in the encryption function," Issue-2019, Christopher N. Vibar, Ruji P. Medina, and Ariel M. Sison.

[4] (Online) Edward Snowden, 2014. http://en.wikipedia.org/wiki/Edward-Snow is a resource.

[5] Wired. (2014) FBI pleased that spam suspect utilises Google Docs. [Online]. Information accessible at: http://www.wired.com/2010/04/cloud-warrant

[6] Piyush, "Advanced Honey Encryption: An Escape-less Trap for Intruders", 2018 4th International Conference on Computing Communication and Automation (ICCCA).

[7] According to Wikipedia (2014), "Global surveillance disclosures (2013-present)." [Online]. Visit http://en.wikipedia.org/wiki/Global-surveillance-disclosures-(2013-present) for more information.

[8] "Ciphertext-policy attribute-based encryption," in IEEE Symposium on Security and Privacy, 2017, pp. 321-334. J. Bethencourt, A. Sahai, and B. Waters.

[9] Chatterjee, R., Athalye, A., Akhawe, D., Juels, A., and Ristenpart, T. (2016). "Password typos and how to correct them securely." In Proc. of Security and Privacy (SP), 2016 IEEE Symposium, pp. 799–818.

[10] "Honey Encryption based Hybrid Cryptographic Algorithm: A Fusion Ensuring Enhanced Security" in IEEE 2020 IEEE Xplore ISBN: 978-1-7281-5371-1

[11] "Honey Encryption beyond message recovery security," Issue-2016, Joseph Jaeger, Thomas Rist enpart, and Qiang Tang

[12] P. K. Tysowski and M. A. Hasan, "Hybrid attribute- and re-encryption- based key management for secure and scalable mobile applications in clouds." Cloud Computing, IEEE T, pp. 172-186, 2018.

[13] Joseph Jaeger, Thomas Ristenpart, and Qiang Tang. "Honey Encryption Beyond Message Recovery Security." Advances in Cryptology-Euro-Crypt 2016, pp. 758-788, 2016.

[14] Password Typos Resilience in Honey Encryption," Choi, H.; Nam, H.; Hur, J. IEEE Conference. 593-597, 2017; Proceedings of the 31st International Conference on Information Networking (ICOIN 2017).

[15] Future research areas for intrusion detection systems in cloud environments are outlined in a literature review.",Suman lata.

[16] In a virtualized cloud computing environment, A.K.M. A. (2016). Using digital machine self-examination for false function recognition

[17] (2016), The use of cloud technology working together as a networking security system (C-NIDS), Z., Hanoune, M& Mamouni Al Haddad

[18] N. Alarifi, B. Alamri, A. Alwatban, L. Alhenaki, A survey of cloud computing security, Proceedings of the Second International Conference on Computer Applications and Information Security, ICCAIS 2019, pp. 1–7, 10.1109/CAIS.2019.8769497 (2019).

[19] N.A. Azeez, T.M. Bada, S. Misra, A. Adewumi, C. Van der Vyver, " Trends in AI and Technology", 1042 (2020), pages 685–696. Penetration detection as well as avoidance machines: a current evaluation

[20] Borisaniya, Patel, and Towards a cloud security framework based on virtual machine introspection.