Gyanshauryam, International Scientific Refereed Research Journal
© 2020 GISRRJ | Volume 3 | Issue 1 | ISSN : 2582-0095

Strong Password Authentication and Secure User Profile Tracking In Cloud Computing Environment

E. Susmitha
Academic Assistant, IIIT RK Valley, RGUKT, Andhra Pradesh, India

ABSTRACT

The world of processing has been changed from two tier to three tier architecture and now we have become to digital centralization called cloud computing. In service oriented domain like cloud computing, information and resources are globally accessed through the pay-constant with-use provider. Unfortunately, this worldwide network get right of access to increase the manner of malicious assault and intrusion. So identity based absolute authentication holds the crucial component to flexible security inside an exceptionally scalable distributed environment. Existing solutions use pure cryptographic techniques to enrol the security problems, which were stricken by using complex computation on consumer information. The proposed work presents a new biometric authentication named as keystroke dynamics, which analyse the typing speed and rhythm, when the client identification and password are entered for registration. Meanwhile, it is vital to acquire the understanding of user profile from mass accessing data in a secure and efficient manner, without revealing the content material of original database. This will be achieved by encrypting the sensitive user profile on active directory with the assistance of competent crypto coprocessor and predicate encryption. Simulation results disclose the performance efficiency of keystroke dynamics and crypto coprocessor.

Keywords : Keystroke Dynamics, Crypto Coprocessor, Predicate Encryption, Cloud Computing, User Profile Tracking

I. INTRODUCTION

Cloud computing [1] is one of the emerging technology in information technology area. It contains vast computing resources that can be accessed by pay-per-use service. Virtualization plays an important role in cloud computing. It automates the management of all the resources, as a single entity through a hypervisor called Virtual Machine Monitor (VMM). Based on high computing capacity, powerful processors and valuable resource sharing concepts, it can provide Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

It is elastic in nature and can sell on demand, typically by the minute or the hour. The service is fully managed by the Cloud Service Provider (CSP). It’s a way to increase capacity or add capabilities without inventing new infrastructure, training new personnel or licensing new software and increase speed compared to super computer. The innovations in virtualizations, distributed computing and a weak economy make a great interest in cloud computing.

Authentication systems allow entities to be recognized before using resources [2]. Biometric technologies are gaining popularity when used in conjunction with traditional methods like password authentication systems. It is the science and technology of identifying individuals from physical and behavioural characteristics [3]. It cannot be lost or stolen. Physiological characteristics like fingerprints, blood vessels in retina, heights and width of bones etc are fixed or stable features and unique across a large population. Behavioural characteristics reflect a person's psychological features such as the voice, pitch and rhythm, the signature and one more is the typing rhythm of the user. It provides a higher level of identification than passwords, especially in situations where security is a great concern. This work presents an inexpensive and interesting fool proof method called keystroke dynamics along with password for verifying an individual's identity.

Users establish a connection to the cloud by a computer or a portable device through the internet and get the unlimited storage and supercomputing capacity. Every user can access everything as a service at anytime, anywhere through different kinds of terminals. The accessing details are recorded and stored in a user profile. A user profile contains information analyzed by user's activities. User profiles can be identified with the help of web log data. It improves customer relationship and achieves goals such as product recommendations and personalized information delivery.

From the huge amount of web log data [31] the effective handling of web log data and extraction of interesting and useful knowledge from the web log data is essential. A standard log file has the following format [32].

Remote_Host/Log_Name/User_Name/Date/Request/ Status/Bytes/Referrer/User_Agent

The web log files are not same as the data in database or data warehouse. The web log data are pre processed to remove noise/ irrelevant data and for user/ session identification finds out different user sessions from original web access log and path completion. Data mining techniques discover useful knowledge from the available web log data. User profiles can help to summarize the large amount of information available from a user. The processes that have been under gone to analyze the web log data.

User Identification - determines who access the web pages and which web pages are to be accessed.

Session Identification – divides the page access of each user at a time interval. Session is series of web pages that a user browses in a single access.

Transaction Identification – creates meaningful clusters of references for each user.

Path Completion – path completion is accomplished by local catching and proxy servers.

Web Server Log File – contains requests made to the web server and recorded in chronological order.

When a user requests a web page, the request is added to the log file. User profiles discovered are treated as set of rules or patterns. But the log file contains images, animations, and video. These are not needed to pattern discovery so they should be omitted from the log file. The accuracy and efficiency of web access patterns become complicated and diversified, when log recording format is not complete and log files on proxy and client are not available.

User profiles are tracked for different group of users having similar interest [10] [34]. These discovered frequent patterns satisfying predefined minimum support threshold. At a given time interval patterns are set as clusters. The different clusters determine best number of user profiles and to generate personalization. The effectiveness of user profile tracking is to identify the users. Profile based methods are more accurate to identifying users.

The global network access increase the way of malicious attack and intrusion. Traditionally, the sensitive data of each enterprise reside within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies. However in cloud computing, the enterprise data is stored outside the enterprise boundary, at an un-trusted database server consequently. The CSP must adopt additional security checks to ensure the privacy of user profile and prevent breaches due to security vulnerabilities in the application or through malicious employees. This involves the use of strong encryption techniques for secure tracking of user profile and fine grained authentication to control access to web log data.

Crypto coprocessor is a hardware which is capable of selecting different algorithms by programming [5]. Also perform crypto operations like the key management, encryption and decryption. The message will be converted to cipher text using crypto algorithms. It is impossible to read when transmitted through communication channels. It is easy to implement in software, but it is slow for real time applications [6]. To overcome this problem, crypto algorithms are implemented in hardware.

The encrypted data can be stored in trusted database server. Processing on encrypted data can be carried out through a type of predicate encryption. Hidden Vector Encryption (HVE) [4] is an important type of predicate encryption scheme where two vectors over attributes are associated with a cipher text and a token. At a high level, the cipher text matches the token if and only if the two vectors are component – wise equal. It allows searches on encrypted data without a private key that corresponds to a public key. Service Registry Federation (SRF) [34] is a strong association between different Cloud Service Providers interspersed among cross organizational and cross fields' business integration. It will be helpful to provide access control on encrypted data. It also safe guards the privacy of user profile from malicious attacks.

This paper is organized as follows. Section II presents the valid related work to process our approach. The proposed system model and its description are explained in Section III. Section IV provides the experimental results and performance comparison of different parameters. Finally Section V concludes this paper and suggests some future enhancements.

II. RELATED WORK

Several types of keystroke dynamics systems exist in the literature. The initial research done on keystroke dynamics was as early as early as 1980 by using statistical T – test [7] under the hypothesis that the means of the digraph times at both sessions were the same, but the variances are different. A study on keystroke dynamics is proposed where the features extracted from username[17]. The identification of the user has been analyzed on the basis of their typing patterns; the Bayesian Classifier and minimum distance were used as classification methods. After this many research work were done to increase the performance, but most of them [8][9], might not be suitable to derive an accurate conclusion on the performance.

Wang et. al., [5] experimented the possibility of typing measure to identify user. It uses different kind of keyboard which may not be commonly used in real cases. Mariusz [11] has done a wonderful job with keystroke dynamics using fixed text. The data was gathered from 1100 samples over 250 registered individuals. This paper implemented a simple algorithm examining only dwell and flight times, when comparing the matching keystrokes for the same. Ahmed et. al., [15] Qunetti et. al., [16] has given a good report for dynamic text studies. It produced less than .005% FAR and less than 5% FRR. The demerit is that this method makes the user to type different characters at several times.

Many Neural Network approaches were developed in the past few years [11][12][13]. The back propagation model was suitable for small databases and it had a limitation that, when a new user is encountered, the whole network should be retained and it is a time consuming process. This research gives a promising static approach is applying Euclidean distance [33] for finding the similarity measure between two profiles. It is relatively simple and yields impressive results. The survey suggests that, static strings produce better result than using dynamic string.

In the data mining community, user profiling [28] [29] is often studied for fraud detection, customer relationship management. Constructing accurate and comprehensive user profiles of individual users is one of the key issues in developed personalization applications. In business transactions a retailer uses behaviour based identification for tracking the members sharing the same IP address to build the user profiles. Identify the user with shared IP address can achieve the high performance in authentication systems.

Many methods where used to find the similarity between the user profiles. One of the technique proposed by Puteri et. al., [27] was Self Organizing Map (SOM). With the help of this they analyze the web log data. The changes in the analysed web log data may change the user behaviour radically.

A user profile normally contains association rules, classification rules based on the studies on user profile. With the use of clustering user profiles are evaluated and generated visualization [28] and thus capture the user interest in the specific pages. Web user identification is mainly based on tracking cookies, identifying users is the process branding a browser with unique identification in each request using multiple datasets and monitoring network traffic. Nasraoui et. al., [30] proposed customer relationship management by discovering and tracking user profiles. They used cosine similarity measure for calculating similarity between the user sessions. Among the many schemes, the Euclidean distance is the best similarity measure to track the web sessions.

Peter Gutman[18] proposed a general purpose secure crypto coprocessor capable of keeping keys and performing other processing by taking advantages of trusted I/O channels to the coprocessor. Tillich et. al., [19] presented a 32 bit GPP processors. It was an inexpensive extension of GPP which allows compact and fast AES implementations. S.R White [20] targeted ABYSS crypto coprocessor, which supplement the function of main processor. It has not used wide set of secure application. It is not suitable to process all the cryptographic algorithms. IBM is the leading innovator of crypto coprocessors. It meets FIPS 140 security standards [21].

Bonehet.al, [22] developed the first predicate encryption scheme which allows only one type of predicate called equality predicate. Anonymous Identity-Based Encryption was quoted in Abdalla et.al [23] comparison of different predicates were analysed in[24],which also suggests that the size of cipher text and tokens are of $O\sqrt{n}$ for n elements.

The HVE was first introduced by Boneh and Waters [25].It supports conjunctive equality, comparison and predicates. The inner products, conjunction and disjunction were presented in [26].It also operates on bilinear groups with Composite order. The token size was O(l) and O(l) pairing calculations. This work is to propose a wonderful HVE scheme. It works on prime order groups and token size is only O(1) and it has only O(1) pairing computations. It is a best practical application for querying encrypted data.

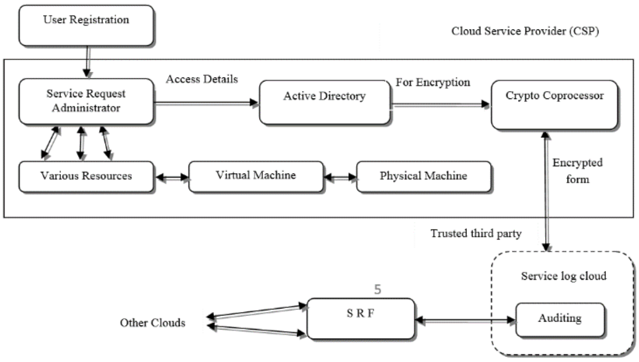
III. PROPOSED SYSTEM MODEL

The system model is specific cloud architecture contains three main players:

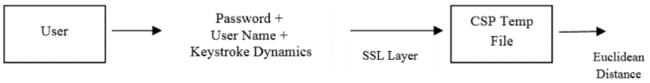
i. Cloud Service Provider, administrate and allocate the resources to cloud customer (user)

ii. Service Log cloud, maintains sensitive user profile in encrypted form

iii. Service Registry Federation, internet organization performs cross field service shoot-up the economic scale of clod infrastructure.



1. Pre processing keystroke dynamics for authentication.

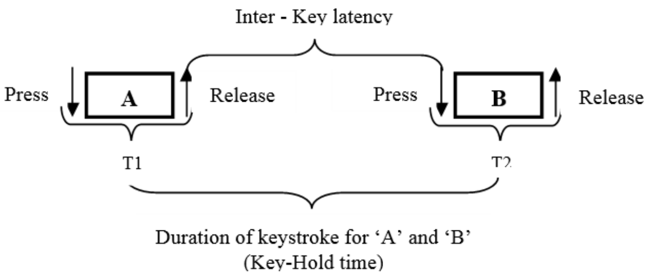


Authentication is the process whereby the system identifies legitimate users from unauthorized user. Identity based authentication provide a high level of security when it relies on biometric authentication. In the template phase keystroke dynamics are collected along with password and username. It is a perfect capture identity that is transmitted with SSL session to CSP. The e service provider calculates the similarity of template with the use of Euclidean distance measure in the verification phase. If the similarity measure is less than 0.5 then the user is denied and if it is greater than 0.5 and less than 1, then accept the user access.

2. Template Phase

Template phase is a stage where samples of biometric features are captured at the time of registration. These templates are stored in a data base for authentication. User enters the password through the normal QWERTY keyboard with 512 MB random access memory. The minimum latencies between key strokes (inter – key latency), duration of keystroke and pressing speed (key hold time) [] can be used to generate a unique keystroke profile for an individual. The inter-key latency is a measure of the amount of time between when a key is released and subsequent key is pressed. Key hold – time is a measure of the amount of time between when a key is pressed and when the same key is released.

Keystroke profile:



The Key stroke duration will be varied for different users such as casual and non-casual users. User details are listed in table 1. Casual user's type fast and there is much variation in typing speed. Un-casual user's types slow and there are some variation in typing speed. Timing resolution for each keystroke was provided by built in function of the system. Users are asked to type the password for about 5 times. After getting input they should be stored in a database called template set (Reference Profile)

Let T = (t_1, t_2, ………………… t_n) acquired in the data base at login time.

Each time when the user encounter to make an access, represents a profile as, P = (p_1, p_2, ………… p_n)

The timestamp: of every single character will be recorded in the below format.

[timestamp $_{press}$][character] [timestamp $_{release}$]

The recorded timestamp kept in a file along with username and password. The size of timestamp is very small and it doesn't consume more space.

3. Similarity Measure:

The similarity among any two users can be determined with the help of distance measure. The distance between two points is taken as similarity among the components. The most commonly used distance measure is the Euclidean distance which defines the distance between two points. If two sequences are identical the value of Euclidean distance [32] is zero, and the distance value increases the sequence become more dissimilar.

For two user $U_1=(p_{11}, p_{12}, \ldots\ldots\ldots\ldots p_{1k})$ and $U_2=(p_{21}, p_{22}, \ldots\ldots\ldots\ldots p_{2k})$ the distance between

U_1 and U_2 is D $(U_1, U_2)= \sqrt{\sum_{j=1}^{k}(p_{1j} - p_{1j})}$

When new sessions are observed after time T assume that these sessions are from the same anonymous user. From these values calculate support value of the all patterns for the user. Initially the profiles will be tracked from all the time periods stored in database.

ALGORITHM: TrackProfiles

```
Input:          Discovered profiles for all Time Periods stored in the Database
                Beginning Time Period $T_1$, Ending Time Period $T_k$
Output:         Profile: Profile to Profile tracking from Time Period $T_1$ to Time Period $T_k$
For i= 1; Time Period $T_1$ do
For j= i+1 to n; [$T=t_i$ ; i=1 to n] do
For k= last profile in the Time Period $T_k$ do
{
Distance[k] = D ($p_1$, $p_k$)
If Distance[k]>0.5 then insert into Profile
Else
Discard the profile
}
```

4. Verification phase

In Verification phase, where the user's features are tested and the decision is made by comparing it with template module. If the template module contains the sample, then the user considered as an authenticate user otherwise the user considered as an unauthorized user. Using the authorized entity, and user can access the required resources for just paying some amount. The accessing details are monitored & controlled by service request administrator.

This phase realize a user, that he/she authenticated one or imposter. A threshold is used for that purpose. When the user enters his/her password, the system compares the details of template 'T' and reference profile 'P'. If it is invalid, the cloud service provider rejects the user's login request.

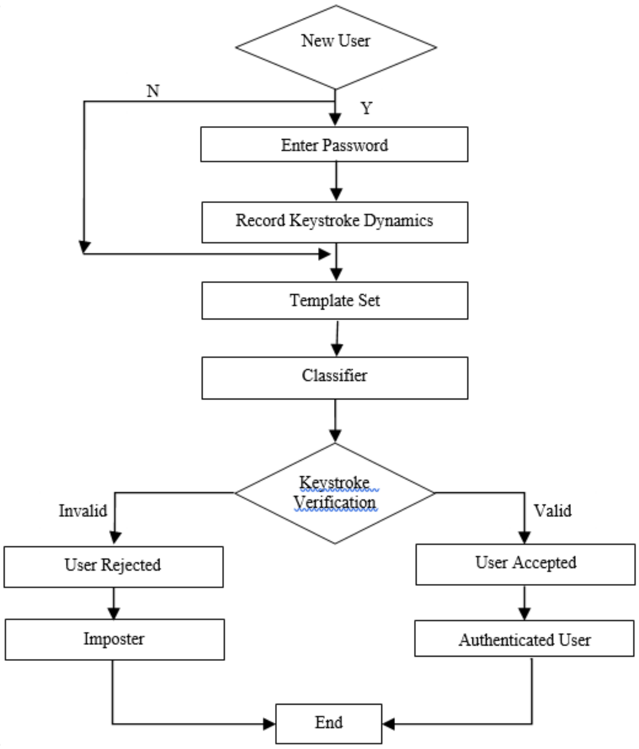


Fig. Flow diagram of keystroke dynamics

5. Active Directory:

The CSP store the user sensitive profile in an intermediate directory- Active directory. Active Directory is subdivided into one or more domains. A domain is a security boundary. Each domain is hosted by a server computer. The Service Request Administrator manages all of the user accounts and passwords for a domain. It include the details like, access logs, proxy server logs, referrer logs, browser logs, error logs, user profiles, registration data, cookies, user queries and book mark data. The CSP share the sensitive data of the user to other, un-trusted cloud, so when the data is exchanged between the clouds, there exists the problem of privacy. To overcome the problem gathered user profile is encrypted when it undergone crypto coprocessor.

6. Crypto Coprocessor

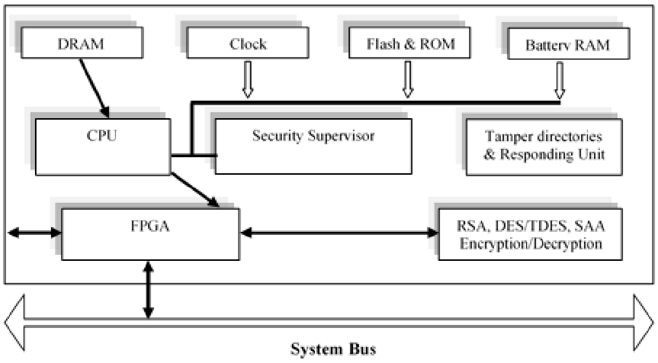

DRAM
Clock
Flash & ROM
Batterv RAM
CPU
Security Supervisor
Tamper directories & Responding Unit
FPGA
RSA, DES/TDES, SAA Encryption/Decryption
System Bus

Fig. Crypto Coprocessor

Crypto coprocessor is a hardware module that includes a processor for encryption and related processing. It protects cryptographic keys and sensitive custom applications. And it supplements the functions of the primary processor.

It support the component like RAM, CPU, cryptographic PCI Card, persistent memory, hardware random number generator, time of delay clock, and infrastructure firm ware and software. It performs the encryptions such as AES, DES, TDES, RSA and SHA-1 and other cryptographic processes revealing the main processor from these tasks. The encrypted user profile is uploaded to trusted third party.

7. Service Log Cloud

Service Log Cloud (SL-Cloud) is a trusted third party, where it maintains the databases and able to watch entire access duration of a user. Frequent auditing is used to extract valuable information from large amount of data available in the user web session. Service log cloud maintains the secured user profile provided by crypto coprocessor. Regarding auditing, trusted third party have variant operations on different levels and concern the query issued in the form of predicates by service registry federation.

In a predicate encryption, a token is issued by SL cloud, for analysing the predicates on encrypted data. The SL cloud performs the verification to identify the quality of token on some predicates. If the verification is true, SL-cloud forwards the encrypted data to the opponent. One interesting aspect is that, the verification does not extract any information to SL-Cloud. This feature is very essential for maintaining privacy of information and secure DB. It able to monitor the entire access duration and Auditing Report is transmitted to SRF.

8. Hidden Vector Encryption

The searching query on encrypted data reveals, no private information contained in the data is leaked to the third party. The query is in the form of predicates. The conjunctive predicates, comparison predicates and subset predicates issued by SRF, retrieve information by matching the token with cipher text.

The Hidden Vector Encryption consists of the following four algorithms:

Setup *(k,l)* takes as input a security parameter *k* and dimension *l* of vector consisting of attributes. It outputs a public key PK and a secret key SK.

Encrypt $(PK, \overrightarrow{x}, M)$ takes as input the public key PK, a vector $\overrightarrow{x} \in \Sigma^{l}$ of attributes, and a message$M \in M$. It outputs a cipher text CT

GenToken $TK_{\vec{\sigma}}$ takes as input the secret key SK and a vector $\vec{\sigma} \in (\Sigma_{*})^{l}$of attributes. It outputs a token $TK_{\vec{\sigma}}$ for evaluating $f_{\vec{\sigma}}$ from a cipher text.

Query $TK_{\vec{\sigma}}, CT$ takes as input the token $TK_{\vec{\sigma}}$ for $\vec{\sigma}$ and a cipher text CT. it outputs a message M if $f_{\vec{\sigma}}(\vec{x}) = 1$ and outputs $\perp$ otherwise.

Correctness:- For all $\overrightarrow{x} \in \Sigma^{l}$, all $\vec{\sigma} \in (\Sigma_{*})^{l}$, and all $M \in M$, let $(PK, SK) \overset{R}{\leftarrow}$ Setup*(k,l),* $(\mathbf{CT}) \overset{R}{\leftarrow}$ Encrypt $(PK, \overrightarrow{x}, M)$, and $TK_{\vec{\sigma}} \overset{R}{\leftarrow}$ GenToken $(SK, _{\vec{\sigma}})$. If we have $f_{\vec{\sigma}}(\vec{x}) = 1,\ M \longleftarrow$ Query$TK_{\vec{\sigma}}, CT$, otherwise **Pr** $[\perp\longleftarrow$ **Query**$(TK_{\vec{\sigma}}, CT)] > 1 - \epsilon(k)$**where** $\epsilon(k)$ is a negligible function.

9. Service Registry Federation

Service Registry Federation (SRF) is a critical aspect in determining the trustworthiness of information distributed to other service clouds. The procedures, laws and architectures accurately mediate and satisfy the on demand requirements of clouds for developing business transactions. The cloud provides at different sectors have expectations and methodologies due to the roles they play in the business life cycle.

SRF searches the encrypted data to perform cross field service on query server, evaluates a test to recognise whether or not the cipher text matches the token. This computation is very much needed to gather user information and it also increase the business requirement of other clouds.

IV. EXPERIMENTAL RESULT

In this part, we use 5 samples to create the template phase. It is used to verify a genuine or an imposter user.

Collecting Samples for template phase:

50 users with different typing skills were asked to type the password on the QWERTY keyboard. The typing rhythms of user were recorded in a database called template. The dynamics of key press and release calculated by built in function of the system. The users are asked to type the password for about 5 times. The no of characters in a password should be fixed in length. (ie, at least '8' characters)

All the users are taken into consideration. n - Number of users. n=50 (say). There are '5 x n' samples in the template. Among '5 x n' samples, '5 x n-1' will be assumed as an imposter. Quite naturally, typing speed of the password their own is faster than an imposed one.

The feature extraction process contains the latencies between keystrokes and the duration of pressing and releasing speed. It will generate a unique keystroke profile for an individual.

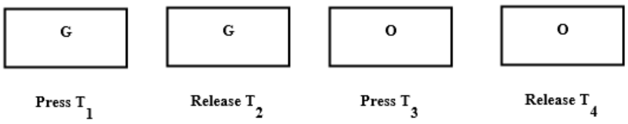


Fig 3. shows an example. The word 'GOD' is taken as password by a user. When he/she presses 'G' at T_1 and Release 'G' at 'T_2', 'O' presses at 'T_3' and Release at 'T_4'. Different types of latencies can be extracted from the dynamics.

Press – Release (P-R) : $T_2>T_1$ (latency between single press and release)
Release - Press (R-P) : $T_3>T_2$ (latency between single release and next press)
Press – Press (P-P) : $T_1>T_3$ Overlap (press next key without releasing the previous one).
It is not advisable, it is quite discriminating. The process is repeated for all the characters in the password. It is noticed from the experiment that, the people with unsophisticated typing skills results in ambiguous patterns. In this work we are mainly focused in performance evaluation. The evaluation schemes used in this work are,

i. FAR (False Acceptance Rate) – In biometric, the instances of a security system incorrectly verify or identifying an unauthorized person. It is a type II error
ii. FRR (False Rejection Rate) – In biometrics, the instances of a security system failing to verify or identify an authorized person. It is a type I error.
iii. EER (Equal Error Rate) – It is the error rate of the system which is configured to obtain a FAR value equal to the FAR one.

The performance evaluation is depicted in the following

Performance Evaluation

Table 1: User Details

Table 1 shows the age limit of users, who have enrolled their password in our experiment session.

Age limit	Number
16-25	15
26-35	10
36-45	10
46-55	10
56 and above	5

Table 2 gives the template value of user and the test data of the same user. The similarity measure of two values are tested, if it is less than 0.5 the access control of user A is denied otherwise user A is accepted.

Table 2: plot for the same user at template and test.

User A	
Template	Test
0.75	0.73
0.70	0.69
0.68	0.66
0.63	0.62
0.60	0.58

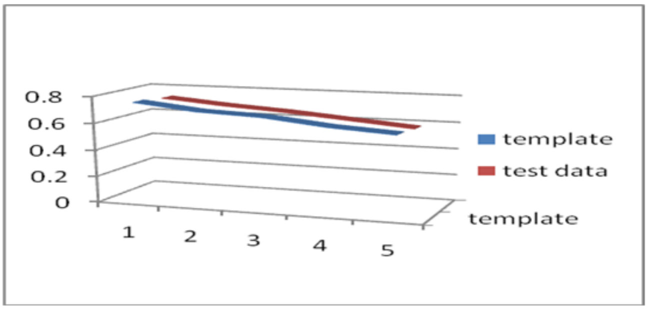
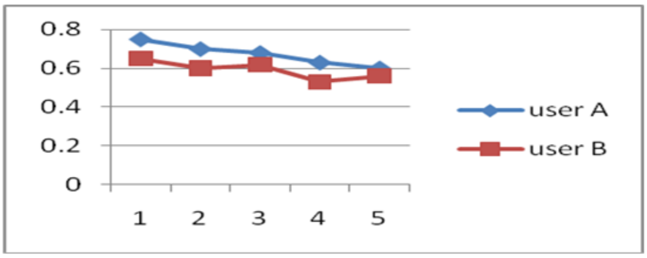


Table 3 gives the performance of two different users.

Table 3: Plot for two different users.

User A	User B
0.75	0.65
0.70	0.60
0.68	0.62
0.63	0.53
0.60	0.56



We have tested the error rate depending on the mean typing speed of the users. In this study, the false acceptance rate is low and it up lift the efficiency of keystroke intervals. It depressed the activities of intruders. In fact, the combination of hold time and inter key latency produce a better solution than using any one of the two.

Table 4: Means of key press

The bars shows the mean time of each key press for "WELCOME"

Interval	Key press (Sec)
A	1
B	4
C	3
D	2
E	3
F	2

The European standard for Access Control (EN-50133-1) states that, an acceptable FRR should be less than 1% and FAR should be less than 0.001% [12] for biometric systems.

Relationship between FAR, and FRR (False Rejection Rate) and Equal Error Rate.

This study lowers EER and is more essential and accurate for distributed environment.

Study	Type	Classifier	No. of individuals in the database	Error Rate	
				FAR	FRR
Bleha et. al., (1990)	Static	Statistical	32	0.5%	3.1%
Obaidat & Sadoun (1997)	Static	Neural Network Statistical	15	0%	0%
Gunetti & Picardi (2005)	Dynamic	Statistical	205	Less than 0.005%	Less than 5%
Ahmed et.al., (2008)	Dynamic	Neural Network	22	0.015%	4.82%
Mariusz (2009)	Static	Statistical	250	-	-
Proposed Work	Static	Statistical	50	-	-

Performance of different methods

In our system, we have included a hardware called crypto coprocessor for strong encryption. Table : shows the performance of various crypto coprocessors like Merkle crypto coprocessor, Field Programmable Gate Array (FPGA) and IBM4764. IBM4764 is used in our system and it provides a flexible solution for high security. The features of IBM4764 are

i. Level 4 security
ii. High speed cryptographic operations
iii. Hardware to perform DES, TDES, RSA and similar public key cryptographic algorithms.

Table shows the characteristics of crypto algorithms in our crypto coprocessor. AES algorithm work with two S-Boxes and implemented in the internal memory. Triple DES requires 48 round operations to complete the encryption/decryption process. RSA is a public key encryption process operates at 28 MHZ and it is used widely in all fields. ECC is also a public key crypto process with the throughput of 20 kbps.

A pair of batteries positioned on the chip to provide backup power. The batteries have been removed according to the battery replacement procedure to diminish and rendering, when it is inoperable. This processor consists of sensory to protect against various attacks like probe penetration, power sequencing and temperature manipulation. Linux operating system is supported by this hardware. Security rich – processing were handled and it is for strong encryption.

Performance of various crypto co processors Neural Network Statistical

Features	Merkle Crypto coprocessor	FPGA	IBM 4764
High Security High Speed Throughput	Low High Low	Low High High	High High High

Characteristics of AES, RSA, Triple DES, DES

Features	AES	RSA	Triple DES	ECC
Frequency (MHz) Logic Size (Slices) Performance (mbps/kbps)	58 1,68 9 390	28 4,595 153 (6.69msec)	50 132 267	50 3,036 20kbps (7.28msec)

Performance comparison

Assume that $\Sigma = \{0,1\}$ and $\Delta = \{1, \ldots n\}$. A simple function *I* maps i^{th} component x_i in a vector (x_1, x_i…… x_n) where $i \in \{1, \ldots\ldots n\}$ that is, $I(x_i)=i$. Then we apply conjunctive comparison and subset queries, $x \leq \sigma$ for two values $x, \sigma \in \Delta$. In the encryption phase, the sender builds a vector $\vec{x} = (x_i) \in \Sigma^n$ as follows $xi = \{1,\ if\ x \leq I(x_i),\ 0, otherwise$. If the receiver wishes to generate a token for evaluating $x \leq \sigma$ on the encrypted *x*, created a vector $\vec{\sigma} = (\sigma_i) \in (\Sigma_*)^n$ as follows $\sigma i = \{1,\ if\ \sigma \leq I(\sigma_i),\ *, otherwise$.

Traditionally the token size and number of pairings are determined by the number of nonzero attributes $\sigma_i\ in\ \vec{\sigma}$ thus the two measures become of size O(n) in the worst case. When considering *l* conjunctive subset queries, these two measures (of size *O(nl)*) are much worse, because the scheme still entails a token size of *O(1)*and only *O(1)* pairing computations.

The table shows the comparison of traditional HVE schemes [a],[b],[c] and the proposed scheme. The KSW-HVE scheme [a] used a predicate encryption where *M* and $\vec{x}$ is encrypted. In the SW-HVE scheme are not considered the delegable factors.

In the proposed scheme we consider *l* conjunctive equality, comparison, and subset queries. When compared to previous schemes our approach improve the performance in terms of the token size and pairing computations. And it achieve needs a token size of *O(1)*and only *O(1)* pairing computations.

	Ciphertext Size	Token Size	Number of pairings	Group order
KSW-HVE [a]	$2(2l+1)G+1G_r$	$2(2l+1)G$	$2(2l+1)p$	*pqr*
	$2(2nl+1)G+1G_r$	$2(2l+1)G$	$2(2l+1)p$	
	$2(2nl+1)G+1G_r$	$2(2nl+1)G$	$2(2nl+1)p$	
BW-HVE [b]	$(2l+1)G+1G_r$	$(2l+1)G$	$(2l+1)p$	*pq*
	$(2nl+1)G+1G_r$	$(2l+1)G$	$(2l+1)p$	
	$(2nl+1)G+1G_r$	$(2nl+1)G$	$(2nl+1)p$	
SW-HVE [c]	$(l+3)G+1G_r$	$(l+3)G$	$(l+3)p$	*pqr*
	$(nl+3)G+1G_r$	$(l+3)G$	$(l+3)p$	
	$(nl+3)G+1G_r$	$(nl+3)G$	$(nl+3)p$	
Proposed	$(2l+3)G+1G_r$	5G	5p	*p*
	$(2nl+3)G+1G_r$	5G	5p	
	$(2nl+3)G+1G_r$	5G	5p	

V. CONCLUSION AND FUTURE ENHANCEMENT

Security is always a significant issue in any computing system. From the perspective of the Cloud Service Providers, the main concern of the proposed scheme is to strengthen password – based authentication using biometric security. This interesting mechanism paves a hidden way to users, as they only need to type on keyboard as usual, instead of providing their physical biometric data. When customers visit the web, they leave log information like IP address, credit card details, session information etc. By analyzing these information it easy to predict the customer behaviour and improve the customer relationship and system performance. It shoots up the economic scales of cloud infrastructure. Crypto coprocessor is a new security design paradigm for both the key generation and converting process. Ease of incorporation into the existing password based authentication increase the potential of keystroke dynamics and hardware security improve the economic scale of forth coming business system. It achieves more privacy in cross field transaction than ever before. Also an efficient Hidden Vector Encryption (HVE) will be responsible for retrieving encrypted data that can be outsourced to service log cloud.

As a future work, the statistical methods can be turned to neural network approaches, although it has a high variable, the number of neurons per layer have a significant relationship with the quality of the results. Homomorphic Encryption techniques are advisable for allowing specific algebraic operations on encrypted data.

VI. METHODS AND MATERIAL

Arduino

VII. REFERENCES

[1]. Rajkumar Buyya, James Broberg, Andrzej Goscinski, "Cloud Computing - Principles and Paradigms", John Wiley's Publications 2011.

[2]. Romain Giot., Mohamad El-Abed., Baptiste Hemery., Christophe Rosenberger, "Unconstrained keystroke dynamics authentication with shared secret", Computers Society 30 (2011) pp.427-445

[3]. Jong Hwan park, member IEEE, "Efficient Hidden Vector Encryption for Conjunctive Queries on encrypted data", IEEE transactions on knowledge and data engineering, Vol.23, No.10,) October 2011, pp.1483-1497.

[4]. Yinghui (Catherine) Yang, "Web User Behavioural Profiling for User Identification" Journal Elsevier- Decision Support Systems 49. (2010) pp. 261-271.

[5]. M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Security and privacy challenges in mobile cloud computing: Survey and way ahead," Journal of Network and Computer Applications, vol. 84, pp. 38–54, 2017.

[6]. Mordor Intelligence Industry Report, Mobile Cloud Market, https://www.mordorintelligence.com/industry-reports/globalmobile- cloud-market-industry, 2018.

[7]. Mariusz Rybnik, PiotrPanasiuk, Khalid Saeed, "User Authentication with keystroke dynamics using fixed text", International conference on biometrics and kansei engineering 2009, pp.70-75

[8]. Puteri N.E Nohuddin, Frans Coenen, Rob Christley, Chrisian Setzkorn, Yogesh Patel, Shane Williams, "Finding interesting trends in social networks using frequent pattern mining and self organizing maps", Journal Elsevier – Knowledge Based Systems 2011.

[9]. Christopher C. Yang and Tobun Dorbin Ng. " Analysing and Visualizing Web Opinion Deveopment and Social Interactions with Density Based Clustering", IEEE Transactions on Systems Man, and Cybernetics- Part A- Systems And Humans- Vol.41, No.6 November 2011.

[10]. J Vellingiri, S Chenthur Pandian "A novel Technique for web log mining with Better Data Cleaning and Transaction Identification" Journal of Computer Science 7 (5) 2011. Pp. 683-689

[11]. W3C extended log file format. Available at http://www.w3.org/TR/WD-logfile

[12]. Sungjune Park, Nallan C. Suresh, Bong-Keun Jeong "Sequence based clustering for web usage mining: A new experimental framework and ANN-enhanced K-Means algorithm" Journal Elsevier Data & Knowledge Engineering 65(2008) 512-543.

[13]. E. Barker, W. Barker, W. Burr,W. Polk, andM. Smid, "Recommendation for key management part 1: General (revision 3)," NIST Special Publication, vol. 800, no. 57, pp. 1–147, 2012.

[14]. X. Li, W. Qiu, D. Zheng, K. Chen, and J. Li, "Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards," IEEE Transactions on Industrial Electronics, vol. 57, no. 2, pp. 793–800, 2010.

[15]. J.Ma,W. Yang,M. Luo, andN. Li, "Astudy of probabilistic password models," in Proceedings

of the 35th IEEE Symposium on Security and Privacy (SP '14), pp. 689–704, IEEE, May 2014.

[16]. J. Gosney, "Password cracking HPC," in Passwords 2012 Security Conference, University of Oslo, Oslo, Norway, 2012.

[17]. C.-C. Lee, C.-T. Li, and S.-D. Chen, "Two attacks on a two factor user authentication in wireless sensor networks," Parallel Processing Letters, vol. 21, no. 1, pp. 21–26, 2011.

[18]. S. H. Islam and G. Biswas, "Dynamic ID-based remote user mutual authentication scheme with smartcard using Elliptic Curve Cryptography," Journal of Electronics (China), vol. 31, no. 5, pp. 473–488, 2014.

[19]. M. Sarvabhatla and C. S. Vorugunti, "A secure and robust dynamic ID-based mutual authentication scheme with smart card using elliptic curve cryptography," in Proceedings of the 7th International Workshop on Signal Design and Its Applications in Communications, IWSDA 2015, pp. 75–79, India, September 2015.

[20]. J. Qu and X.-L. Tan, "Two-factor user authentication with key agreement scheme based on elliptic curve cryptosystem," Journal of Electrical and Computer Engineering, vol. 2014, 16 pages, 2014.

[21]. B. Huang, M. K. Khan, L. Wu, F. T. B. Muhaya, and D. He, "An Efficient Remote User Authentication with Key Agreement Scheme Using Elliptic Curve Cryptography," Wireless Personal Communications, vol. 85, no. 1, pp. 225–240, 2015.

[22]. S. A. Chaudhry, H. Naqvi, K.Mahmood, H. F. Ahmad, and M. K. Khan, "An Improved Remote User Authentication Scheme Using Elliptic Curve Cryptography,"Wireless Personal Communications, vol. 96, no. 4, pp. 5355–5373, 2017.

[23]. C.-C. Chang, H.-L. Wu, and C.-Y. Sun, "Notes on "Secure authentication scheme for IoT and cloud servers"," Pervasive and Mobile Computing, vol. 38, pp. 275–278, 2017.

[24]. M. S. Farash and M. A. Attari, "A secure and efficient identitybased authenticated key exchange protocol for mobile client server networks," The Journal of Supercomputing, vol. 69, no. 1, pp. 395–411, 2014.

[25]. S. A. Chaudhry, H. Naqvi, T. Shon, M. Sher, and M. S. Farash, "Cryptanalysis and improvement of an improved two factor authentication protocol for telecare medical information systems," Journal ofMedical Systems, vol. 39, no. 6, pp. 1–11, 2015.

[26]. Q. Xie, D. S. Wong, G. Wang, X. Tan, K. Chen, and L. Fang, "Provably secure dynamic ID-based anonymous two-factor authenticated key exchange protocol with extended security model," IEEE Transactions on Information Forensics and Security, vol. 12, no. 6, pp. 1382–1392, 2017.

[27]. Y. Lu, L. Li, H. Peng, and Y. Yang, "An anonymous two-factor authenticated key agreement scheme for session initiation protocol using elliptic curve cryptography," Multimedia Tools and Applications, vol. 76, no. 2, pp. 1801–1815, 2017.

[28]. S.Kumari,M. Karuppiah,A. K.Das,X.Li, F.Wu, and N.Kumar, "A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers," The Journal of Supercomputing, pp. 1–26, 2017.

[29]. Q. Jiang, J. Ma, and F.Wei, "On the security of a privacy-aware authentication scheme for distributed mobile cloud computing services," IEEE Systems Journal, pp. 1–4, 2016.

[30]. R. Amin, S. H. Islam, G. P. Biswas, D. Giri, M. K. Khan, and N. Kumar, "A more secure and privacy-aware anonymous user authentication scheme for distributed mobile cloud computing environments," Security and Communication Networks, vol. 9, no. 17, pp. 4650–4666, 2016.

[31]. D. He, N. Kumar, M. K. Khan, L. Wang, and J. Shen, "Efficient privacy-aware authentication scheme formobile cloud computing services," IEEE Systems Journal, no. 99, pp. 1–11, 2017.

[32]. F.Wei, P. Vijayakumar, Q. Jiang, and R. Zhang, “A mobile intelligent terminal based anonymous authenticated key exchange protocol for roaming service in global mobility networks,” IEEE Transactions on Sustainable Computing, no. 99, pp. 2377–3782, 2018.

Cite this article as :

E. Susmitha, "Strong Password Authentication and Secure User Profile Tracking In Cloud Computing Environment", Gyanshauryam, International Scientific Refereed Research Journal (GISRRJ), ISSN : 2582-0095, Volume 3 Issue 1, pp. 12-25, January-February 2020.
URL : http://gisrrj.com/GISRRJ19263