Three Level Based Security for Improvised User Privacy in Human Computer Interaction

Ranjan Goyal, Manjula R, Gaurav K Sangle, Thenmozhi T, Shafiq Khan

Abstract: ***Privacy can be a key aspect of the user experience with computers, online systems, and new technologies. Knowing what to consider about users and their views of computer systems can only improve privacy mechanism. Human Computer Interaction (HCI) is the sub field of Computer Science that studies how people interact with and through computational technologies. In this paper, a three-level model-based approach is provided for the end user privacy in the human computer interaction as the end user's privacy in the area of HCI is emerging as critical design element for interacting systems in areas as diverse as e-commerce, health care, office work, personal communications etc. The data privacy of end user as well as the resource access privacy is needed to be considered. As of now, no proper solution exists for all types of interface users which is a major privacy issue. Hence, to provide the end users, their personal data protection as well as the resource access security, this paper focuses on analyzing and developing the theory of technological acceptance related to user privacy.***

Keywords: ***data security, human computer interaction, three level security, user privacy, quality of service.***

I. INTRODUCTION

It is important for end user to manage the privacy. But sometime user may not know how to manage the privacy and security as end user may not be a through with the technical aspects used in privacy and security management. Social navigation system collaborates end user in decision making by collecting behaviors, decisions or opinions from a user community and then display this information to individual user. This information can guide the end user for managing the security and privacy. Some prototype systems like Acumen, Bonfire can be used to provide end user privacy by social navigation. Also, the end-user's privacy has a threat from neighborhood attacks also. These attacks can be created through social networking sites. So social media deal with some challenges like fake users, user's privacy, threatening content etc. It is important that social network data should not breach the privacy of any end user. Some techniques like k-anonymity, l-diversity and t-closeness are used to replace the personal information of users into pseudo random information. These models can anonymize the user data but any adversary can re-identify the user data provided to social network sites by creating and tracing social network graph.

Rest of the paper is organized as follows: Section II provides the background knowledge for the model proposed in this paper that mainly focuses to provide some details for the intrusion detection and biometric authentication as the part of the high-level architecture. Section III provides the triple A requirements for the end user privacy. Section IV provides the literature review of the recent related works. Section V provides the proposed model and Section V discusses the proposed model followed by the conclusion in Section VI.

II. BACKGROUND KNOWLEGDE

In this section, the background knowledge related to the presented model is provided. The most important level i.e. High-Level architecture includes the use of Intrusion detection and Biometric based Authentication. The same are discussed as follows:

A. Intrusion Detection System

Intrusion detection system is a system which monitors the network traffic to check the suspicious activity and alerts and reports the user when such activity is discovered. Generally, a classical Intrusion Detection Systems detect and report any anomaly; but some IDS can also capable of blocking traffic send by suspicious IP address which are sometime called as Intrusion Prevention Systems (IPS). An IDS is also used to analyze the quantity and type of attacks. This may help to change security systems. In this way IDS helps in End User's Privacy. There are different types of IDS that includes Network Intrusion Detection System (NIDS) which is capable to monitor inbound and outbound traffic to and from all the devices on the network. Another one is Host Intrusion Detection System (HIDS) which is capable to detect suspicious network packets that may be originated from inside the organization or malicious traffic that NIDS has failed to detect. HIDS can also able to detect any malicious traffic that may be generated at host side itself if it is infected with malware. If host is affected it may try to attempt to spread to other systems. The Signature Based Intrusion Detection System works almost similar to an antivirus software i.e. it compares the packets traversing the network with the database of signatures or attributes of known threats. Another one is the Anomaly Based Intrusion Detection System. In this system comparison is done with an established baseline. This baseline suggests about what is considered as normal with respect to bandwidth, protocols, ports etc.

Revised Manuscript Received on August 30, 2019.

* Correspondence Author

Ranjan Goyal*, School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India. Email: ranjangoyal98@gmail.com

Manjula R*, School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India. Email: rmanjula@vit.ac.in

Gaurav K Sangle, School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India. Email: gauravksangle@gmail.com

Thenmozhi T, School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India. Email: thenmozhi.t@vit.ac.in

Shafiq Khan, School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India. Email: shafiq.khan2016@vitstudent.ac.in

B. Biometric Authentication System

In Biometric Authentication System a user gives the templates of his biometric data such as fingerprint, iris etc. to service provider. The service provider stores this data into a biometric database along with user's ID. Whenever user wants to enter the service for which he/she subscribed must again provide a fresh template of biometric data. The service provider then retrieves the data for that particular ID and compares with the template provided by user. If the template matches with the template in the database user may access the service which he/she requested. This model is fully server-centric model. In this type service provider is fully responsible for the security of the templates of user's biometrics [1].

But there is a risk in this kind of system as service provider may access the user information by using user's biometric database already present in the database. As a server-centric model user must have trust on service provider. Service providers may crosscheck for the duplication of user or sometime may check for the other services user may have enrolled. This violates the privacy of user. So, to avoid the consequences created by the server-centric model user-centric model can be used.

The benefits and features of this user-centric model are as follows: In this model, the end-user's data may be encrypted at the user side only and then this encrypted information may be sent to the server side. Hence service provider can only see the encrypted data. Also, Secret keys and templates needed for authentication are created and processed in the local environment only and hence data may not be leaked outside the local environment. Furthermore, there are some computations involved in the authentication. All these computations are carried out on the ciphertext unlike when computations are carried out on plaintext. Hence, there is no possibility of exposure of plaintext.

III. TRIPLE A REQUIREMENTS

Today's world is increasingly digital-driven world. So personal data is flowing freely online. This data may include information such as date of birth, private chats or financial data such as credit cards details etc. While signing up any service users often become impatient. In fact, they are in such a hurry that they just overlook the Terms and Conditions without understanding what it entails. This results in ads that user may don't want to see, and emails you don't remember signing up for, also some pesky calls that user may receive. It's all connected to big data. Although large companies ensure that the data stays in their ecosystems, issues regarding end user's privacy may occur. Attackers are always performing new attacks on social networking sites to collect the information of users who share their private details knowingly or unknowingly.

Thus, to provide the end user privacy, the three basic requirements i.e. Authentication, Authorization and Allocation (AAA) are verified at each level of security. The same is discussed as follows:

A. Authentication

This is a basic level security that every user can use. At this level user identification will be done meaning the it will check for the particular user identity. The user has to access the system by using the user id and a unique password which is unique for a user.

There are two phases for Authentication, user identification and actual authentication. In identification phase a unique user is identified by his/her identity which may be provided in the form of unique user id for particular user. After uniquely identifying the user from the set of users who have registered for the specific service in next phase user must give evidence to prove by giving his/her identity so that system can give rights and permissions to access the services that user has registered. User may provide the evidences by some textual passwords or some drawable patterns which will be unique to that user. This type of authentication is sometime called as single-factor authentication. Sometime authentication is done by using Single-Sign-On (SSO) system; which will provide authentications for many systems using single set of credentials. Also, some systems prefer to use token-based authentication systems in which signed authentication tokens are generated once at the start of the session. This token is appended to every request send from client. The token may be of different types like JWT tokens (JSON Web Tokens), Opaque tokens or blend. This provides low level security if any security measures are not added. This may create threat to user data like credit card details, personal data etc. In the proposed model authentication will be provided in the above two phases prescribed.

B. Authorization

After the authentication is provide to user in the next level authorization is done. In this level the user got the permission to access only those resources which are allocated for him/her. The resources may include the directories in the system or the hours for which user can access and work in the system or the storage space, computer programs etc.

Mainly there are two authorization phases, policy definition phase and policy enforcement phase. In the first phase policies are defined which depends on the resource allocation for the user. In the second phase the access requests are permitted according the policies defined. Generally, authorization comes along with authentication. Anonymous users have less privilege to access some resources. Authorization leads to access control.

The authorization data maintenance can be a troublesome work for administrative side. If the user's authorization changes then it is necessary to change or remove the policies set before. The atomic authorization can be used as an alternative to the per-system authorization management. In atomic authorization a trusted third party takes responsibility for the distributing authorization policies.

C. Allocation

The allocation of the resources will be done after the successful authentication and authorization of the user. The allocation of resources may differ from user to user as per the authorization and Quality of Service (QoS) adopted by the user.

IV. RELATED WORKS

There are some related works done by many researchers. Goecks et al. [2] proposed two models, Acumen and Bonfire for supporting end-user privacy and management with social navigation. Acumen system uses a basic approach to end user's privacy by providing a way to manage internet cookies.

Whereas Bonfire provides a way to help end user by helping in managing the firewall. According to the paper although Acumen and Bonfire give significant promises but still there are many challenges to apply these techniques. The main reason behind these challenges is the lack of expertise among the users and because of these other end users may take some incorrect inference or misuse of this community data can create wrong decisions. For Acumen system normally allows cookies which are good i.e. there should be balance between trust in website and benefit-cost ratio. But if users disallow or block cookies the acumen system fails. Bonfire system fails when user opens some ports for doing some work online such as gaming as this may create further problems.

Diwakar et al. [3] presented in the paper ‘End User Privacy Preservation in Social Networks Against Neighborhood Attack’ a One Neighborhood Adjacency Matrix (ONAM) base anonymization process. In that process optimum number of edges are added into the unique subgraph. According to them dummy data created by anonymization can increase the noise level of the social network sites data and hence originality and information loss may occur. An adversary can re-identify the user in the random social network data which created by anonymization techniques such as l-diversity, t-closeness, k-anonymity. The creation of social network graph helps the adversary. Adversary tracks the information about the neighbour nodes and then try to track the target node. Some edges are added to make the two vertices isomorphic and which create difficulty for adversary to identify the target node.

Hafez et al. [4] discussed about neighborhood attacks in social network data publishing. In the paper the main focus is given on the one of the significant and challenging problem in social networks i.e. Vertex re-identification. These types of attacks may be done by neighborhood-pair attack which uses some topologies of neighbor vertex in the connection. A prototype model of neighborhood attack is proposed in the paper. The model is such that it may reduce the data loss rate. The proposed model of neighborhood attack in the paper is utilizes the neighborhood structure. The pair of connected vertices provides the background knowledge about the adversary and then targeted victims are identified in a social network data.

Zhou et al. [5] proposed that how server-centric biometric authentication can be converted into user-centric system and the risks involving both of these models. For creating user centric biometric authentication system, the paper proposes the way to protect the user details by authenticating them and then sending to service provider. This reduces the service provider inference in user’s data. In the paper biometric authentication scheme (PassBio) is proposed. The two vectors are encrypted such that their inner product is compared with the threshold. Hence the proposed system becomes Threshold Predicate Encryption (TPE) oriented. Iachello et al. [6] discussed about end-user’s privacy in Human Computer Interaction (HCI). In the paper the discussions are also based on the privacy related issues in Computer Supported Cooperative Work (CSCW). Also, it outlines current approaches, results and trends in HCI.

The literature survey suggested that there is still some need to provide the optimal solution for the end user privacy end protection [7-10]. This paper proposes the same by providing a mechanism that can provide the user with privacy and security based on a three-level security mechanism where the user is provided with the option to choose the level of the protection based on the Quality of Service (QoS) required by the user considering the cost affordability and security requirements. The same is discussed in the next section.

V. PROPOSED MODEL

In this section, the three-level security model is proposed. The three levels are discussed as follows:

A. Low Level Security

Basic security management using PAP will be done at this level. This is most vulnerable system which may attacked by the cyber attackers. At the basic level service provider may also get access to the user data as user credentials are saved in the database. Although some basic encryption is done on the user credentials it may not provide that much security. Authentication fulfilment: It may be in the form some user login credentials in which user have to provide user id and password. Authorization fulfilment: The same login credentials may be used by system but sometimes it’s not necessary. Access control based on the password authentication required to be done by the user.

B. Medium Level Security

In this level some encryption/ decryptions steps are taken to store the user data in encrypted format so that even system provider cannot access the user’s data without decrypting. This can provide the security at a certain level. But the problem with this level may be key management, cost efficiency for a particular encryption algorithm. Authentication fulfilment: The same authentication protocol is being used to provide authenticity to the user. Authorization fulfilment: Once the authorization of the user is done, then the data is provided to the user with the option of securing the data with the help of encryption mechanism namely Advanced Encryption Standard (AES 256 bit). The access control will be based on the encryption of the data and the keys will be hashed using SHA3 (256 bit) to avoid misuse of the keys during the attack [11].

C. High Level Security

In this level the security steps are stretched a bit further to avoid malicious accesses by adding some feature like intrusion detection [12]. At this level system alerts the user if any malicious activity is discovered from the user account. At somewhat higher level it may block the activity by blocking the traffic send by the suspicious IP address. Authentication fulfilment: This can be at a higher level which every user may not afford or it may depend on the kind of data which user is going to store. This may include things like biometric authentication system and Intrusion detection system. Authorisation fulfilment: Again, for this it depends on the service provider to allocate the resources for the particular user. Access Control based on the added encryption performed on the stored information of the user. Fig. 1 depicts the proposed three level security model.

DOI: 10.35940/ijeat.F9313.088619

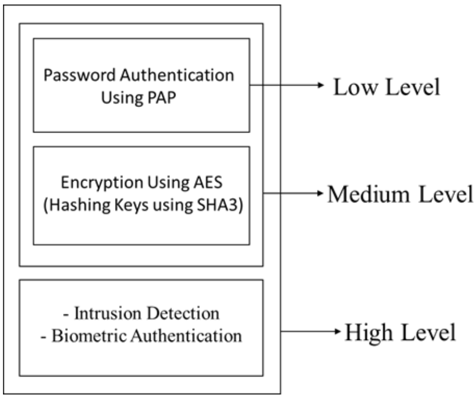
Password Authentication Using PAP
Low Level
Encryption Using AES (Hashing Keys using SHA3)
Medium Level
- Intrusion Detection
- Biometric Authentication
High Level

Fig. 1. Proposed Three Level Security Model

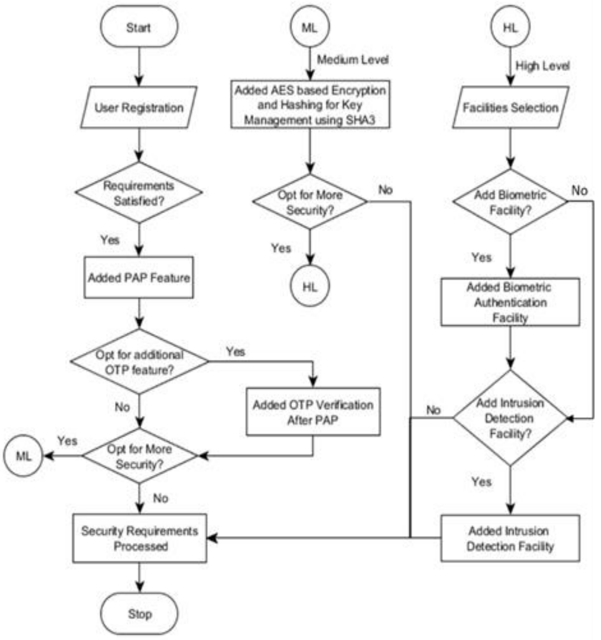
Start
User Registration
Requirements Satisfied?
Yes
Added PAP Feature
Opt for additional OTP feature?
Yes
No
Added OTP Verification After PAP
Opt for More Security?
Yes
ML
No
Security Requirements Processed
Stop
ML
Medium Level
Added AES based Encryption and Hashing for Key Management using SHA3
Opt for More Security?
No
Yes
HL
HL
High Level
Facilities Selection
Add Biometric Facility?
No
Yes
Added Biometric Authentication Facility
Add Intrusion Detection Facility?
No
Yes
Added Intrusion Detection Facility

Fig. 2. Security Level Selection Mechanism

The security level section mechanism shown in the Fig. 2 depicts the procedural selection for the level of security that can be opted by the user. The selection procedure starts with the user registration process in which the user is required to enter some necessary details that may include personal details too. Also, the user is required to provide some unique user id and password that can be used for logging in later. The user id and password must satisfy the constraints that have been set up in the system. The constraints may include minimum user id and password length and alphanumeric password constraint. If all the requirements get satisfied, then the Password Authentication Protocol (PAP) will be added as the low-level security feature in the system for that user. After that the user will be provided with the option to opt for the additional OTP based security feature. If the user opts for this feature then this feature will be added for the user and will be used in future after the user successfully authenticates PAP based security. At this point the low-level security selection is completed. Now, if the user wants to move on to the medium level security, the user will be given the data security feature i.e. encryption of data in rest and data in transit. Here, the data of the user will be encrypted with the help of AES 256 bit and the keys will be hashed with the help of SHA-256-bit mechanism so as to prevent the access to the keys. At this point, the medium level security selection is completed. Now, if the user wants to opt for high level security, the user will be provided with the option to select the security options namely biometric authentication and intrusion detection system. Here, the user can select either of them or both of them. Based on the selection, the system requirements will be processed and at this point the selection procedure ends.

VI. DISCUSSION

The model proposed in this paper is based on the three-level security model for end user privacy and protection. This section discusses the same based on the facility being provided to the user for the different types of human computer interaction interface models. The security selection model can be analyzed with the help of example scenarios for each of the security level. The same is discussed as follows:

A. Low Level Security

Consider the scenario in which user is using the proposed model for the social networking service. In this case, the user may require only the low-level security architecture as the user requires to get authenticated for logging in to the account. Here, there is no such requirement for encryption mechanism and biometric as the usual interface for social network is based on such password-based authentication protocol (PAP). In the social networking interface, the user generally shares the information that he is willing to share with the other people, so in this scenario, there is no such requirement of encryption mechanism.

B. Medium Level Security

Consider another scenario where the user requires some privacy model for the online mailing system. Here, the user is supposed to get the encryption functionality along with the password authentication-based login facility. The biometric facility is not required here as the general interface of the online mailing system is not considered suitable to be integrated with biometric login system considering the fact that the user may have to login from any device at any point of time. So, in this scenario, the medium level security model can be utilized keeping in mind the above requirements. But considering the fact, that the mailing system is required to be more secure, the user can opt for high level security model if the user requires to get the intrusion detection functionality where the user will get notified in case some intrusion is being performed by the attacker to get access to the mail.

C. High Level Security

Consider the scenario where an employee of an organization is requiring some cloud environment service. At this point, this employee as a user will require the high-level security model as the user may require Password authentication protocol-based authentication and encryption functionality for data in rest and data in transit along with the intrusion detection facility. The biometric can be utilized here to provide the hardware protection to the user where only the authorized employees can have access to such interface.

Also, in this scenario, the user privacy is must considering there can be possibility of attacks such as Spoofing and Phishing in which the user may get confused between the genuine interface and a cloned (fake) interface made to get the credentials of the device. This can be prevented by providing the user with the HTTPS facility along with the intrusion detection functionality.

VII. CONCLUSION

In this paper, a user privacy and security model is proposed for the human computer interaction interface by providing the user with the three level security model. Each level provides the user with the added functionalities. The user can choose can select up to what level the security is required for the interface being used by the user considering the cost and the severity of the security for that interface. Thus, the Quality of Service (QoS) is being provided based on the self-selection of the user for the interface. The discussion for the proposed model showed that the user can select the level of the security based on his requirements for that interface. Also, the user can opt for additional functionalities at each level such as OTP based verification based on the requirements for the interface and the user. Future scope of this paper is implementation of this work in the human computer interaction interfaces.

REFERENCES

1. N. K. Ratha, J. H. Connell, R. M. Bolle, “Enhancing security and privacy in biometrics-based authentication systems,” IBM Systems Journal, Volume: 40, Issue: 3, 2001.
2. Jeremy Goecks, W. Keith Edwards, Elizabeth D. Mynatt, “Challenges in Supporting End-User Privacy and Security Management with Social Navigation,” Proceedings of the 5th Symposium on Usable Privacy and Security, SOUPS 2009, July 15-17, 2009.
3. Alpendra Kumar Diwakar, Nikhil Kumar Singh, Deepak Singh Tomar, “End User Privacy Preservation in Social Networks Against Neighborhood Attack,” ISEA Asia Security and Privacy (ISEASP), July 2017.
4. Mohd Izuan Hafez Ninggal and Jemal H. Abawajy, “Neighbourhood-Pair Attack in Social Network Data Publishing,” International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services, pp. 726-731.
5. Kai Zhou and Jian Ren, “PassBio: Privacy-Preserving User-Centric Biometric Authentication,” IEEE Transactions on Information Forensics and Security, Volume: 13, Issue 12, pp. 3050 – 3063, Dec. 2018.
6. Giovanni Iachello and Jason Hong, “End-User Privacy in Human–Computer Interaction: Foundations and Trends in Human–Computer Interaction,” Volume 1, Issue 1(2007), pp. 1–137.
7. Louise Barkhuus, “The Mismeasurement of Privacy: Using Contextual Integrity to Reconsider Privacy in HCI,” Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 367-376, May 2012.
8. Mark S. Ackerman, Lorrie Faith Cranor and Joseph Reagle, “Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences,” Proceedings of the 1st ACM conference on Electronic commerce, pp. 1-8.
9. Babitha M.P, K.R. Remesh Babu, “Secure Cloud Storage Using AES Encryption,” 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), pp. 859-864, September 2016.
10. J R Ngnie Sighom, Pin Zhing, Lin You, “Security Enhancement for Data Migration in the Cloud,” Future Internet, Volume 9, Issue 3, pp. 1-13, June 2017.
11. Prabu S, Gopinath Ganapathy, Ranjan Goyal, “Enhanced Data Security for Public Cloud Environment with Secured Hybrid Encryption Authentication Mechanisms,” Scalable Computing: Practice and Experience, Vol. 19(4), pp. 351–360, Dec. 2018.
12. Roman V. Yampolskiy, “Indirect Human Computer Interaction-Based Biometrics for Intrusion Detection Systems,” 2007 41st Annual IEEE International Carnahan Conference on Security Technology, pp. 138-145, Oct. 2007.

Retrieval Number F9313088619/2019©BEIESP
DOI: 10.35940/ijeat.F9313.088619
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication