SPECTRUM SOLUTIONS

Pondicherry, India

Approved by Indian Government under Section 21

CODE	TITLE	YEAR	ABSTRACT
1	*Intelligent Hands Free Speech based SMS System on Android*	IEEE 2016-17	Over the years speech recognition has taken the market. The speech input can be used in varying domains such as automatic reader and for inputting data to the system. Speech recognition can minimize the use of text and other types of input, at the same time minimizing the calculation needed for the process. A decade back speech recognition was difficult to use in any system, but with elevation in technology leading to new algorithms, techniques and advanced tools. Now it is possible to generate the desired speech recognition output. One such method is the hidden markov models which is used in this paper. Voice or signaled input is inserted through any speech device such as microphone, then speech can be processed and convert it to text hence able to send SMS, also Phone number can be entering either by voice or you may select it from contact list. Voice has opened up data input for a variety of user's such as illiterate, handicapped, as if the person cannot write then the speech input is a boon and other's too which can lead to better usage of the application.
2	An Exploration of Geographic Authentication Schemes	IEEE 2016-17	We design and explore the usability and security of two geographic authentication schemes: GeoPass and GeoPass- Notes. GeoPass requires users to choose a place on a digital map to authenticate with (a *location password*). GeoPassNotes—an extension of GeoPass—requires users to annotate their location password with a sequence of words that they can associate with the location (an *annotated location password*). In GeoPassNotes, users are authenticated by correctly entering both a location and an annotation. We conducted user studies to test the usability and assess the security of location passwords and annotated location passwords.

3	**A Shoulder Surfing Resistant Graphical Authentication System**	**IEEE 2016-17**	**Authentication based on passwords is used largely in applications for computer security and privacy. However, human actions such as choosing bad passwords and inputting passwords in an insecure way are regarded as ”the weakest link” in the authentication chain. Rather than arbitrary alphanumeric strings, users tend to choose passwords either short or meaningful for easy memorization. With web applications and mobile apps piling up, people can access these applications anytime and anywhere with various devices. This evolution brings great convenience but also increases the probability of exposing passwords to shoulder surfing attacks. Attackers can observe directly or use external recording devices to collect users’ credentials. To overcome this problem, we proposed a novel authentication system PassMatrix, based on graphical passwords to resist shoulder surfing attacks. With a one-time valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass-images, PassMatrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera-based attacks. We also implemented a PassMatrix prototype on Android and carried out real user experiments to evaluate its memorability and usability. From the experimental result, the proposed system achieves better resistance to shoulder surfing attacks while maintaining usability.**
4	**STAMP: Enabling Privacy-Preserving Location Proofs for Mobile Users**	**IEEE 2016-17**	**Location-based services are quickly becoming immensely popular. In addition to services based on users' current location, many potential services rely on users' location history, or their *spatial-temporal provenance*. Malicious users may lie about their spatial-temporal provenance without a carefully designed security system for users to prove their past locations. In this paper, we present the Spatial-Temporal provenance Assurance with Mutual Proofs (STAMP) scheme. STAMP is designed for ad-hoc mobile users generating location proofs for each other in a distributed setting. However, it can easily accommodate trusted**

			mobile users and wireless access points. STAMP ensures the integrity and non-transferability of the location proofs and protects users' privacy. A semi-trusted Certification Authority is used to distribute cryptographic keys as well as guard users against collusion by a light-weight entropy-based trust evaluation approach. Our prototype implementation on the Android platform shows that STAMP is low-cost in terms of computational and storage resources. Extensive simulation experiments show that our entropy-based trust model is able to achieve high collusion detection accuracy.
5	**Understanding Smartphone Sensor and App Data for Enhancing the Security of Secret Questions**	**IEEE 2016-17**	**Many web applications provide secondary authentication methods, i.e., secret questions (or password recovery questions), to reset the account password when a user's login fails. However, the answers to many such secret questions can be easily guessed by an acquaintance or exposed to a stranger that has access to public online tools (e.g., online social networks); moreover, a user may forget her/his Answers long after creating the secret questions. Today's prevalence of smartphones has granted us new opportunities to observe and understand how the personal data collected by smartphone sensors and apps can help create personalized secret questions without violating the users' privacy concerns. In this paper, we present a *Secret-Question based Authentication* system, called "Secret-QA" that creates a set of secret questions on basic of people's smartphone usage. We develop a prototype on Android smartphones, and evaluate the security of the secret questions by asking the acquaintance/stranger who participate in our user study to guess the answers with and without the help of online tools; meanwhile, we observe the questions' reliability by asking participants to answer their own questions. Our experimental results reveal that the secret questions related to motion sensors, calendar, app installment, and part of legacy app usage history (e.g., phone calls) have the best**

			memorability for users as well as the highest robustness to attacks.
6	Privacy-Preserving Location Sharing Services for Social Networks	IEEE 2016-17	A common functionality of many location-based social networking applications is a location sharing service that allows a group of friends to share their locations. With a potentially untrusted server, such a location sharing service may threaten the privacy of users. Existing solutions for *Privacy-Preserving Location Sharing Services* (PPLSS) require a trusted third party that has access to the exact location of all users in the system or rely on expensive algorithms or protocols in terms of computational or communication overhead. Other solutions can only provide approximate query answers. To overcome these limitations, we propose a new encryption notion, called *Order-Retrievable Encryption* (ORE), for PPLSS for social networking applications. The distinguishing characteristics of our PPLSS are that it (1) allows a group of friends to share their exact locations without the need of any third party or leaking any location information to any server or users outside the group, (2) achieves low computational and communication cost by allowing users to receive the exact location of their friends without requiring any direct communication between users or multiple rounds of communication between a user and a server, (3) provides efficient query processing by designing an index structure for our ORE scheme, (4) supports dynamic location updates, and (5) provides personalized privacy protection within a group of friends by specifying a maximum distance where a user is willing to be located by his/her friends. Experimental results show that the computational and communication cost of our PPLSS is much better than the state-of-the-art solution.