CHAPTER 9

CONCLUSION AND SUGGESTIONS
FOR FUTURE WORK

9.1 CONCLUSION

Technology growth is inevitable for everyone in the social system. Application development is always focused in common advancement of technology due to various level of knowledge people involved in using this applications and the lack of knowledge is used as vulnerability.

We observe elephant is a very strong animal but elephant-keeper will tie its leg using small chain and knot into some holder. We need to observe the psychology of elephant here it will not break that small chain; but it can by the ability. Likewise we think that our house is very secure because we locked it but in reality if you take locksmith he can unlock in a short time. So, security depends on mind set of people who involved skill of the person, accessibility of required tools, time given to him. We need to remember big fish eats small fish so the capability and knowledge plays a major role in the field of security.

In this thesis it is addressed the problem of improving security and reducing social security threats faced by human being. Here it is demonstrated the possibilities of capturing keystroke in milliseconds and recorded data analysis presented between K-Clustering and MK-clustering algorithms. Keystrokes differences are based on time is efficient in capturing at client side
applications to avoid latency delays. Single sign on applications are used in newly developed algorithms as business logic to determine the identity of the person. Brooks’s applications namely Activity Manager, Real Time Dispatch, Patterns and RealView composite applications demonstrate the efficient use of keystroke in commercial applications. Different kinds of workflow and possible architectures are suggested for efficient methods. MK-Means cluster is developed for continual learning of the system. Initially applications are run and generate monthly data for 12 sets for each year K-Cluster for every month and which can form a MK-Cluster. Latest MK-Cluster has input of K-cluster data which had run whole year. Results are demonstrated to increase the number of matrix parameters which increases the system ability accurately. Natural per key time of any human being has never been equal to any other person interpreted per key time. Reported pattern gap charts and press time charts clearly show that same person data is matching and different person data generated graphs are never matched. Based on context scan, database system can make clear scan of environment used for triggering transactions.

In Simple Aggregate Methodology collection of sample images is user friendly. It is a very simple image when the individual is reading letters “EEEEEE” face snap is taken. This can be used in most of the common corporate and restricted areas where their data is present always. We have used this method in ATM simulator design as additional static parameter for identifying banking customer during transaction based security authorization. Front elevation of the radiograph and X-ray images of teeth of cadavers can be compared with this image to get comparison results for the purpose of forensic analysis. Observed data is compared with DSM and GVF methods against the proposed method and results are found better. Therefore, the proposed image processing and feature extraction approach outperforms in the labial teeth image recognition. It can be concluded that the performance of
the proposed teeth recognition system produces more than 98% accuracy of recognition rate which is better than the other two methods.

In ATM rooms we need to limit the presence of number of persons on the restricted zones. To count the number of persons available on a particular zone, the proposed algorithm is used to identify face region by clustering method. Image taken during either at day time or night time makes no significant difference because of pose illumination effect. If more number of occluded faces present in the image, then efficiency of the system will be decreased. If the image is taken by a distant camera, it will not give good results as compared to the less camera distance. The results will be good in case of frontal view of face as compared to non-frontal view of face present in the image. Biometric images available in Bosphorus Hand Vein Database, Biometrics Ideal Test databases it is analyzed using algorithms like independent component analysis. Identification of the person based on their hand images has been addressed using existing database images.

The ATM security features were enhanced largely for the stability and reliability of owner recognition. The whole system was built on module based embedded system which makes the system more safe, reliable, replace and easy to use. Existing ATM security framework is kept in consensus while designing new proposed system. Major focus is based on transaction values which determine the trigger of security routine. Internet based transactions are very carefully designed by considering physical location of person operating and routine is not triggered from anonymous proxy server. Banking framework has ability to enable and disable state of the account so when account is disabled there is no transactions will be carried out. It enables customers to keep their account safe. Proactive communication to customer about execution of cheque transactions will avoid unknown transactions. Demonstrated conceptual architecture diagram of banking application server
with security features give illustration of how transactions are executed. Results are concludes that there possibility of conducting banking without ATM cards.

Experiments are demonstrated to use Gadgets as invisible key for physical security in Human Computer Interaction. The demonstrated method allows user to get access to a secured NTFS partition without going through any authentication. Designed application lists down all available USB connected devices and unique serial numbers associated with the devices. Options are given to the users to select as invisible key among any one USB devices. An another application is demonstrated to protect and control USB port and Windows registry entries which has complete control of USB drive in the operating system. File system interoperability is enabled by this method. This method is useful to access files in both the partitions in Hard Disk which have different OS. Data duplication is avoided.

Collective Knowledge of individuals who protect the system should be higher than collective knowledge of individuals attempting to break the system. Physical access to machines with enough time for a person with higher knowledge will result in the person cracking the machine and getting the information required with help of current technology. All this kind of protection mechanism will increase the data breakage time.

Next it is demonstrated that retrofitted design of ship with floating Power Station. The power produced is given to auxiliary engine. Total fuel consumption is reduced considerably and the energy efficiency of the ship is improved. Design of emergency rescue passenger space is used in the event of a disaster aboard a ship. Airborne body is tethered with passenger space to ascend. It is a floating body without an internal supporting framework, or a keel.
7.2 SUGGESTIONS FOR FUTURE WORK

For future works, it is proposed to have multiple architectures using RTD, APF and MK-Clusters. This can be extended to enterprise real time applications to use in single sign on authentications in the case of large user bases. MK-Cluster alone can be used as plug in algorithms module in existing security applications for adding intelligence in continuous learning.

In labial teeth identification method simple Aggregate Methodology Algorithm is developed as semi-automatic on JPG images because during the cropping stage we can define the size of the matrix for maximum accuracy. Here threshold point selected manually can be automated based on the usage and alignment to the application and infrastructure. It also can be used as additional parameter to identify a person in voter’s database, National security database, employee records. Even this can be used as a key to open the doors, office, Bank, attendance in schools like finger prints in addition to thumb impression reading.

We recommend gadgets as invisible key for physical security check and should be done before the control enters into boot process in operating system. This means it should be checked after the BIOS and before the boot is triggered. If we perform this kind of check, no one can access the machine and HDD without this virtual key.

7.3 SUMMARY

This chapter focuses on listing out the conclusions and suggestions for the future work. In general the proposed methods, architectures, framework, simulators, algorithms and designs developed for respective applications are found to be efficient to reduce social security troubles and save people life and valuable resources.