Four-Level Biometric Security System to Protect The Crucial Information from Unauthorized Access

Abhishek Sharma, Sandeep Kumar Gupta, Abhishek Pandey, Giridhari Paul, Biplab Kumar Sarkar, Ram Gopal

Abstract: ***As the time is changing day by day our world is getting developed in the field of digital technology. We all are connected nowadays on social networking sites such as Facebook, twitter, Instagram, and so on. Other than these networking sites we visit multiple sites on our laptops/Personal computers/Tablet or any other types of devices such as smartphones etc. So actually, we are surrounded by a huge amount of data around the world, and among those data most of the data are our personal data which is so crucial for our identity and security purposes too. With the developing technologies, threats to those important data is also increase as the there are many peoples who are trying to snoop in your important drafts or file to fetch those important data and use them to blackmail you, earn money, use you for their special purposes and even something worst which we can't imagine. In the Indian scenario, the Indian public is less secure than the other developed countries. India has the maximum no. of Internet Data user and also many of them are not aware that how to protect their crucial Data from Snooping. While defending the data from hacking is another field of invention but in this device, we are providing security to those data or collection of Data which is stored in a specific device. By using this device, we can also protect our data from hacking threats because by giving 4 parameters of Protection in which two of them are biological database makes all the devices of the theft useless. Also, this device does not need any Internet connectivity which is a major of hackers for hacking any device hence they also helpless in hacking of this device.***

Keywords: FBS System, DNA Fingerprinting, Biometric Impressions, Retina/Iris, Voice Recognition, Pin Hold.

I. INTRODUCTION

In the world of Information Technology we are developing new and latest technologies day by day in way to make our world digital. Digitally we are more developed in comparisons to the world 20 years back and also this generation will be called backward after 20 years from now. We use social networking sites such as Facebook, twitter, Instagram and get connected to the person who is sitting miles away from us in just a second.

Revised Manuscript Received on February 11, 2019.

Abhishek Sharma, Assistant Professor, Department of Computer Science and Engineering, ABES Engineering College, Ghaziabad, India (abhishek.sharma@abes.ac.in)

Sandeep Kumar Gupta, PhD, Corresponding Author, Professor, Sharda University, Greater Noida, India (skguptabhu@gmail.com)

Abhishek Pandey, Student, Bachelor of Technology, Department of Information Technology, KCC Institute of Technology and Management, Greater Noida, India (abhishek_1084@yahoo.in)

Giridhari Paul, Student, Bachelor of Technology, Department of Information Technology, KCC Institute of Technology and Management, Greater Noida, India (giripauldhari@yahoo.in)

Biplab Kumar Sarkar, International / National Project Director, Technical Trainer, TCS-Pune, India (dr.bksarkar2003@yahoo.in)

Ram Gopal, National Institute of Technology, Patna, India (r.gopal.dce@gmail.com)

These all works are possible just due to a large collection of Data of the users which all the big companies use to develop more user-friendly environment to attract the users towards their field of work. These data also contain all the crucial information of their users such as Photographs, Search History, their likes/dislikes, their ATM Card numbers, pins, and cvv no., other banking or payment gateway details which they often use to buy or shop online from e-marketing websites such as Amazon.in, Flipkart etc.

These data are very useful to those people who are willing to snoop in someone's life and use these data to blackmail them or can use these data as per their requirement which can be a worst condition in such cases.

And not only for online surfers, are the data leaks also a big challenge for those institutions which are working in the field of defense of nation or corporates. Data leaks make a big impact on every one, either a single individual, political or defense institutions of any Nation or Corporate sectors, all are at big risk. PANAMA paper leaks, Leaks of Examination papers of various high-level examinations such as UPSC, SSC or PCS exams, Leakage of Blue print multiple Fighting jets of IAF, Strategically details of the Defense Institution of the Indian Nation are such big example of Data leaks makes a nation shuffle and can damage to a high level of their internal structure.

The FBS system is a practice to protect our highly confidential data from such risks of snooping or leaks. The FBS system stands for "THE FOUR-LEVEL BIOMETRIC SECURITY SYSTEM". This system is a combination of the 4-highly secured security parameters which a hardware device which is totally out of the range of Internet and makes it hack proof just like Electronic Voting machines. It stores data, work on it but do not need any type of internet access at all. And also makes the software or file/folder in any device full proof from the unauthorized access of anyone who Is willing to reach the data without the authorized person.

This system stores the data of the authorized person who will be able to use the data till he authorized. Once the data is fed in the device same data is collaborated with a software/App needs to be downloaded once in the device. After this by using that software user can make multiple folders/file safe to access from the unauthorized personal. These user data cannot be altered any time. To alter this data the user needs to enter an user ID password and also needs

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

the existing user to change the DATA in the device. So, without the actual user no one can access the data stored in the File or Folder. This device will be very useful for the protection of crucial information from going to wrong hands. All types of strategically details, Blue print of all the weapons, aircraft, Important details of the companies such as future planning/schemes, development and market strategies of the companies also useful for the protection of the question papers of all the Important examination. All these types of details can be saved in the soft copy and protect it using this hardware-software combination Weapon. If someone get these files by any how that become useless for them because they can't access the data by all of their efforts.

II. RESULTS & DISCUSSIONS

According to the survey of Analytics India Magazine, to understand users' attitude towards data privacy and the awareness level for the same in daily scenarios. They asked millennial and people from various backgrounds – freshets, professionals and decision-makers – about policies of websites, the sale of data to third parties, and trust issues regarding the same.

The responses were insightful, yet not unexpected — most users who use internet intensively do not read the privacy policies before they 'agree' or 'disagree' to any web portal's terms. They are more protective about their banking data, passwords and government-authorised documents. More than 50 percent respondents admitted to falsifying personal information to get around the process.

According to EY's Global Information Security Survey 2016-17 - India report, it indicates that many organizations lack basic cyber security systems and processes. This is evidenced by the below findings:

- 33% of organizations in India do not have a Sense of Confidence (A practice to protect the data before any cyber-attack), compared to 44% globally
- 55% do not have, or have only an informal, threat intelligence program
- 44% do not have, or have only an informal, vulnerability identification capability

This is a major area of risk that is often overlooked, as evidenced by the following findings:

- 68% will not increase their cyber security spending in the event that a supplier is attacked — even though a supplier is a direct route for an attacker into the organization.
- 58% will not increase their cyber security spending in the event that a major competitor was attacked — although cyber criminals often attack other, similar organizations following a successful cyberattack.

By above two important surveys we can conclude that Data breach incidents in India higher than global average.The figure 1.1 shows a survey conducted on two social networking sites i.e. Instagram, and Facebook with a Question- "Is Pin/Password and Biometric protection is enough to protect the most crucial Data?" The survey's response was as expected.

The above survey includes all the sectors of the society such as Engineers, students, general peoples, youths and Old people. Nearly everyone is accepting that Data leakage is a major challenge for today's world.

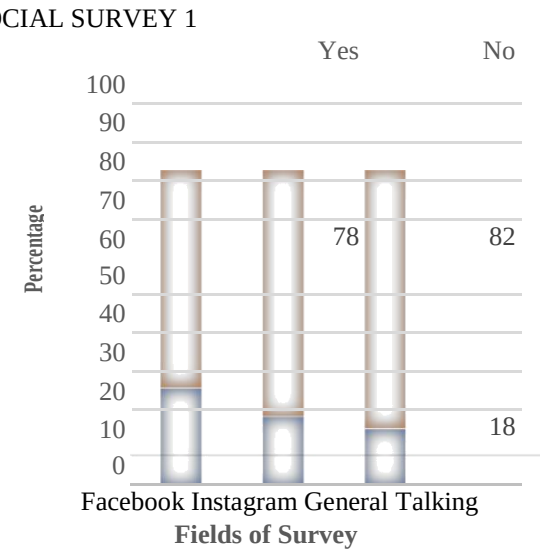

Figure 1.1: Social Survey 1.

Related Works:

Patent Number- US20160098878A1: Smartphone controlled biometric and Bluetooth enabled smart wallet system.

Inventor: Steven D. Cabouli, Robert J. Mos, Clay Von Mueller, Robert A. Lane, Marco A. Schilling, Paul E. Catinella.

They define "This application provides an electronic wallet or passport case for controlling the opening, unlocking and locking of enclosures such as luggage, briefcases, lockers, cases, cabinets, vehicles, buildings, homes and with indirect operational control by the means of a smartphone, tablet or any personal computing device. More particularly, a Smartphone Controlled Biometric and Bluetooth Enabled Locking Smart Wallet System is provided. The Smartphone Controlled Biometric and Bluetooth Enabled Locking Smart Wallet System includes a biometric based finger print authentication module, and a Bluetooth communication enabled module, to prevent a non-owner or unauthorized user from accessing the device, along with mobile applications to control the Smart Wallet System using a smartphone. The smart wallet equipped unit may be replaced by any locking case such as a briefcase or luggage."

Patent Number- US8965063B2: Compact biometric acquisition system and method *Inventor: Keith J. Hanna, Hector T. Hoyos.*

They defines " He A method of determining the identity of a subject while the subject is walking or being transported in an essentially straight direction is disclosed, the two dimensional profile of the subject walking or being transported along forming a three dimensional swept volume, without requiring the subject to change direction to

avoid any part of the system, comprising acquiring data related to one or more biometrics of the subject with the camera(s), processing the acquired biometrics data, and determining if the acquired biometric data match corresponding biometric data stored in the system, positioning camera(s) and strobed or scanned infrared illuminator(s) above, next to, or below the swept volume. A system for carrying out the method is also disclosed."

Patent Number- US7988038B2: System for biometric security using a fob.

Inventor: Blayn W Beenau, David S Bonalle, Seth W Fields, William J Gray, Carl Larkin, Joshua L Montgomery, Peter D Saunders.

The present invention discloses a system and methods for biometric security using biometrics in a transponder-reader system. The biometric security system also includes a biometric sensor that detects biometric samples and a device for verifying biometric samples. In one embodiment, the biometric security system includes a transponder configured with a biometric sensor. In another embodiment, the system includes a reader configured with a biometric sensor. The device for verifying samples compares the biometric samples with information stored on databases."

Patent Number-US20080319907A1: Secure transaction method and system including biometric identification devices and device readers.

Inventor: David C. Russell, Barry W. Johnson, David M. Petka.

They defines "The invention is directed towards methods, systems and apparatuses, see FIG. 1, (100) for providing secure and private interactions. The invention provides capability for verifying the identity of a party initiating an electronic interaction with another party through data input module (140) which is verified by the identity verification module (150), which further includes a self-destruct mechanism (153). Embodiments of the invention include secure methods for conducting transactions and for limiting the transfer and distribution of personal data to only those data that are absolutely necessary for the completion of the transactions. The invention facilitates the transfer of additional personal data contingent upon an agreement that appropriately compensates the provider of the personal data"

Patent Number- US6927668B1: Print access security system.

Inventor: Richard Odle, Gary Odle, Robert E. Henry David Coriaty.

They Defines "A fingerprint enrolment and verification module is connected to the electrical circuit of a vehicle to prevent operation of the vehicle by unauthorized users. The module has a sensor that creates a template of a fingerprint when a finger is placed on the module. The module has a flash memory to store enrolled templates and a verification step. After a fingerprint has been enrolled in the module, any operation of that vehicle is possible only after the user's fingerprint is verified to match the enrolled template."

Patent Number-US20030163710A1: Random biometric authentication utilizing unique biometric signatures.

Inventor: Luis Ortiz, Kermit Lopez.

They Defines "A user can be challenged to provide at least one randomly selected biometric attribute. The randomly selected biometric attribute input by the user is automatically compared to a plurality of biometric attributes of the user contained in a user profile. The user can then be authenticated if the randomly selected biometric attribute input by the user matches at least one of the pluralities of biometric attributes of the user contained in the user profile. Biometric attributes analysed according to the methods and systems of the present invention, include, but are not limited to, for example, fingerprint, iris, retina, and/or tissue characteristics, such as skin morphology, skin layer thickness, collage density and orientation, tissue hydration, optical patent length differences, etc."

Patent Number-US20150358315A1: Smartphone fingerprint pass-through system.

Inventor: John Cronin

He Defines "Systems and methods are provided for unlocking remote devices using a biometric input that is associated with a code stored on a mobile electronic device. After validating a biometric input that corresponds with a code that locks or unlocks a remote lock, the code may be sent to a remote electronic device in a transmission. When the code is validated by the remote electronic device as being associated with unlocking the remote lock, the remote device may then unlock the lock."

The FBS System:

I. The FBS (Four level biometric security system) consist of four level of security for the protection of our most confidential data.

These 4 Parameters are:

1. Biometric impression recognition;
2. DNA Recognition;
3. Voice based Pin Recognition;
4. Retina/Iris Recognition.

These 4 parameters are a great combination of full proof security for the protection of any type of Data.

1. **Biometric Impression recognition-** This is a well know way to protect our Data. Many electronic devices uses this technology to unlock the device or applications. It is a common way these days to protect the device from unauthorized access. By giving a fair impression of the fingerprint any of five of any hand, user can manually save the input of the authorised personnel. After second time putting the same impression he'll able to protect and access the data as per his requirement.

As time passes technology and its development is at its peak so this technology is lacking somewhere in the complete protection of the data, because data thieves has some way to break this security. SO we need to protect the data by implementing another level of security.

2. Voice Based Pin Recognition- Speaking somewhere is not a big stuff but when your voice is Pin or Password to protect the highly confidential data then it's a big deal.

This device uses this method to protect the device's data so that this device becomes more powerful in the way to protect the data. By implementing this technology the user have to speak a PIN/password in the microphone attached to the device so that the device will recognise the Pin with preinstalled data of the user and also recognise the voice frequency of the user which makes it a more powerful way to protect the device. But we need to protect the device with a very powerful way to which no-one can break. For finding the highly secured way to protect the device we need to work with Medical Science.

3. DNA Recognition- In the field of Medical science we know that DNA is the most complex substance which combination is not only rare but we can say that impossible to match from one individual to another.

In DNA, there is a huge combination of Amino acids which contains genes and other cellular data of the organism which makes two individuals different from each other. The DNA have about 99% same repeated sequence of the Amino acids which actually as same as all the Human Beings but just 1% different segments make the all Human Individuals different from each other. We can use this property to protect the highly confidential data. We can save those patterns which make one person different from another and will save that codes in the hardware's database. In the second attempt when a person tries to access the data he'll have to provide the same data by giving his DNA Sample to the device by the method used in device to get the input. This will surely prevent unauthorised access of the user. But for making a device perfectly safe so that it can protect the data we'll toward the last but not the least method of the Data protection in our Device.

4. Retina/Iris Scan- Medical Science provides all the opportunity to human beings to differentiate a individual from another by giving them an unique identity. Biometric Impression, DNA Impressions are such examples. Another good way to match the identity of such individuals are Retina/Iris Scan where we can meet to the solution of the fake identity. These days many technology uses this system to detect the identity of Human Beings such AS UIADI system in India(AADHAR CARD), but we are using this great technology in protection the data we stores in the File. There will be device attached to the Hardware which detect the retina details of the user so that it can detect that the authorised individual is trying to access the data or not.

II. Implementation of the Device & Results

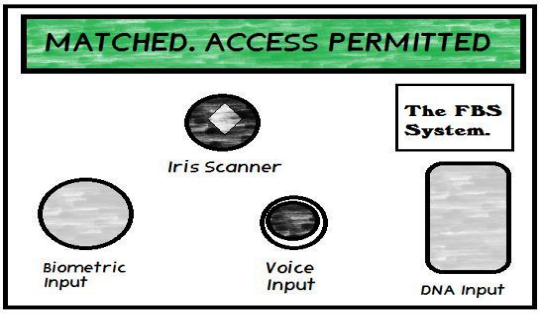

Figure 1.2: Complete Device after assembling all the parts.

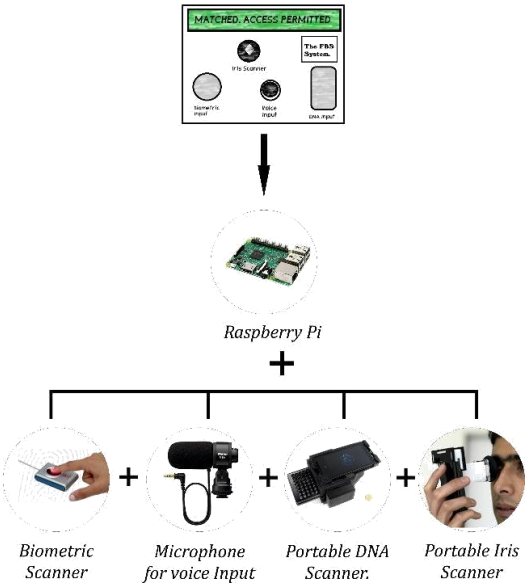

Figure 1.3: Different technologies used in future Hardware of the device.

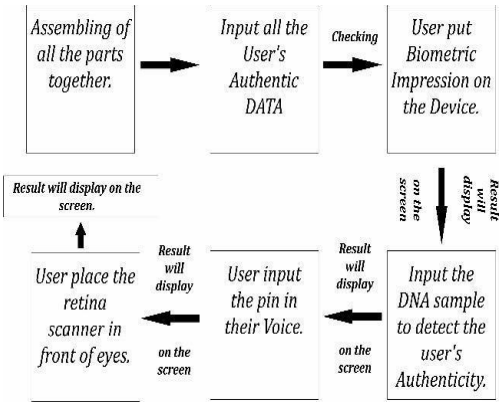

Figure 1.4: Internal Implementation/working of the Device.

This device works on different technologies which is merged together to form an excellent technology which can protect our most important and highly confidential data. This device will work on the Raspberry Pi so that it consist a board of Raspberry pi which contains all the programming related to this device.

This device also consist of a Microphone for taking input of the Voice based Pin by the user; It also have a iris scanner for scanning the iris of the user and also a biometric scanner which takes the input of the user's finger and match with pre-existing data as a part of security of the Data. The Most important and exciting part of the device is its Portable DNA Scanner which scan the input of the user and match with pre-existing data inside the and result of all the technology will decide either user can access the Data or not.

III. Flow Chart of the Hardware:

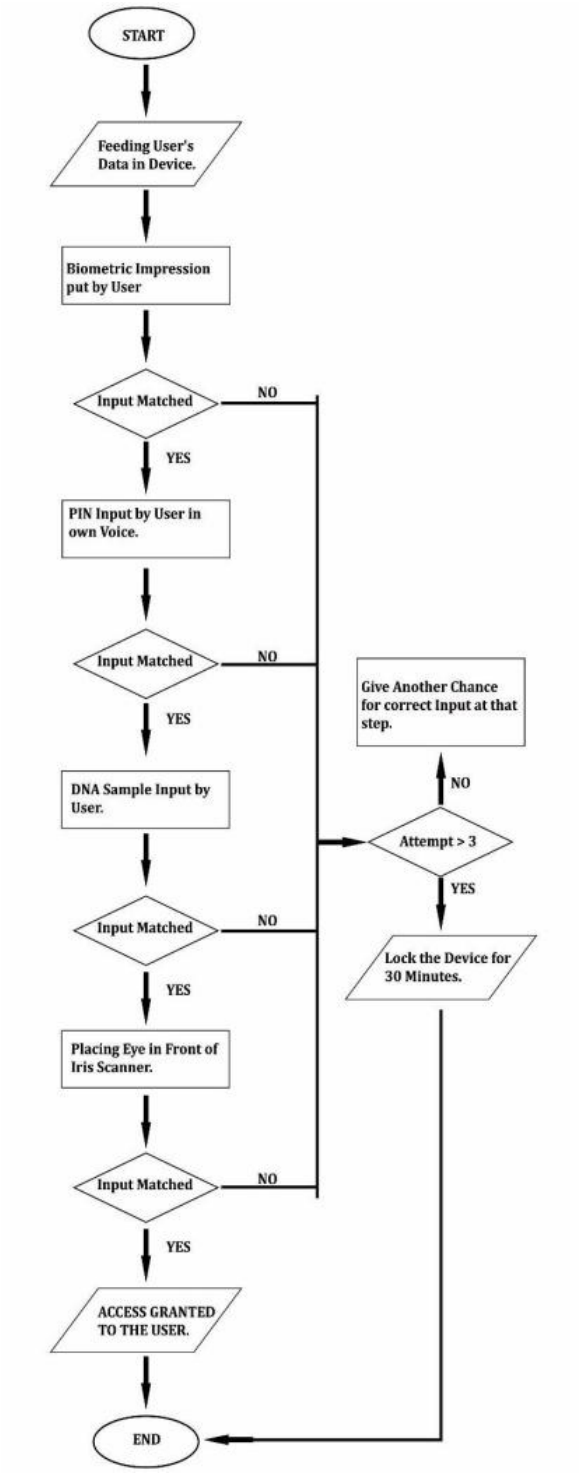

Figure 1.5: Flow chart of the Device.

IV. Explanation of the Figure 1.5:

The above diagram consists of following steps for the working of the device. There will be USB point which will be connected to the computer or Smartphone as per the requirement of the user. This will start the device. Then device will ask the user to input the Biometric Impression of the user. If the user's input matches with the pre-stored sample then the system will show a message **"MATCHED",** otherwise it show a message on its display screen **"UNMATCHED".** If the sample matches with user's original data then the device will move to next step and ask the user to input the Voice based PIN. After entering the pin the device will detect the frequency as well as PIN so that if the PIN matches then user will be able to go for accessing the 3rd step of recognization.

Then the device will move to the third step where user have to input the DNA sample of its own, to analyse the DNA Sample, the device contains a portable DNA Scanner, which scans the sample of the DNA and matches its data i.e. sequence of amino acids. If the sample of the user's matches with pre-existing data stored in the device then the device move to the last step where he has to give the input to check the Iris details of the user. If all the details matches with the actual stored authorized data then the device will give the access to the user. So user can edit, modify and do whatever he want with the DATA.

But if the any of the user's sample do not matches with the pre-stored sample of the authorized individual then user will get 3 attempts to re-enter the inputs in a correct way but if user fails in entering the correct input in the device then the device will go to a **"UNABLE" OR "LOCKED"** state for next 30 minutes, so that nobody can give another input to open the device. After 30 minutes the user can again give the input to open the device.

VI. Analysis of the device and conclusion:

In this modern world where everyone is busy in social Networking sites and browsing on the internet with being aware to the risk of their data. These days Hackers can hack the different devices and can access the data without the permission of the user. So this system provides a way to protect the data so that nobody can access the data without the presence of the user.

In an another survey where the question was *"If a "Forth level security" device is develop in future to protect any kind of app, software or any highly confidential data. Would you like to use this security device to protect your data...?"* Many users on the different networking sites such as Facebook and Instagram answered positively in this direction. We also ask the peoples personally about this the same and answer was also satisfactory in this direction.

The result of the above survey is shown with the help of Graph (In Figure 1.6). The result proves that peoples are getting aware towards their Data security.

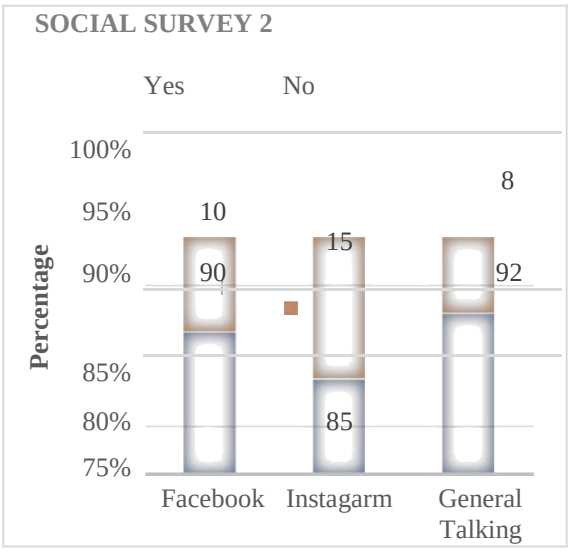

Figure 1.6: Social Survey 2.

This survey proves that by developing such devices we can protect our data in many ways and also it protect us from the danger of Hacking and all.

REFERENCES:

1. https://bigthink.com/philip-perry/new-dna-scanning-software-can-id-you-in-minutes.
2. https://www.ey.com/in/en/services/advisory/ey-global-information-security-survey-2016-2017-india-report
3. https://www.analyticsindiamag.com/annual-consumer-survey-on-data-privacy-in-india-2018/
4. http://www.bioelectronix.com/what_is_biometrics.html
5. https://en.wikipedia.org/wiki/Biometrics
6. https://en.wikipedia.org/wiki/Iris_recognition
7. https://en.wikipedia.org/wiki/Speaker_recognition