Study of a Secure Communication System

Shubham Pandey, Ruchi Varshney, Shivani Gupta, Neha Chaudhary, Sangeeta Singh

Abstract: Communication is an important part of our daily life. The communication process involves information generation, transmission, reception and interpretation. A technical overview of the emerging technologies of fiber optical communication and optical networking fiber optical communications has enabled much higher data rates. In present scenario it is continuously being noticed that people are very concerned about privacy of their data. But some unauthorized persons, who are little bit advanced in technology, can access other’s data. So to provide security to the people for their data multiple security systems are being used in the present scenario like biometric which is well known for being used in the security purpose and second one is optical fiber link which is also used for the security purpose. Other security systems are code lock, RF-ID etc. So in present scenario the biggest problem is to provide security where secure communication is required such as bank, industry, college and election commission etc. This paper is a proposal to develop a project which is combination of two major security systems that are biometric security system and optical fiber link. Through this project analog and digital data can be transmitted using highly secured optical fiber link while having a biometric security to transmit the data at the transmitter end and having a code lock security for reception purpose at the receiver end. Through this project automation can also be done at the receiver end from the transmitter end.

Keywords: Biometric, Optical fiber communication, Code lock, Automation.

I. INTRODUCTION

This paper is all about security concern of the data communication, data transmission of analog and digital signal and automation at the receiver end from the transmitter end. In the proposed project we demonstrate the idea of advance biometric based security system. This project is very special project for college/bank/other important place and for election commission too. With the help of this project we can achieve more advancement in the security system and automation at the receiver end.

In this project we demonstrate the idea of security for valid and invalid person. If any person wants to enter in any secured region, system will demand finger ID. If ID is valid, only then system will provide access through optical link between transmitter and receiver section. In case of invalid ID, system will automatically check the status and beep the buzzer and close the optical link between transmitter and receiver section.

II. LITERATURE SURVEY

Anil K. Jain etal[1,2]: This paper states that any human physiological and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

Universal: Each person should have the characteristic.

Distinctiveness: Any two persons should be sufficiently different in terms of the characteristics.

Permanence: The characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time.

Collectability: The characteristic can be measured quantitatively.

However, in a practical biometric system (i.e., a system that employs biometrics for personal recognition), there are a number of other issues that should be considered, including:

Performance: Which refers to the achievable recognition accuracy and speed, the resources required to achieve the desired recognition accuracy and speed, as well as the operational and environmental factors that affect the accuracy and speed.

Acceptability: Which indicates the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives.

Circumvention: Which reflects how easily the system can be fooled using fraudulent methods.

The applicability of a specific biometric technique depends heavily on the requirements of the application domain. No single technique can outperform all the others in all operational
environments. In this sense, each biometric technique is admissible and there is no optimal biometric characteristic. For example, it is well known that both the fingerprint-based and iris based techniques are more accurate than the voice-based technique. However, in a telebanking application, the voice-based technique may be preferred since it can be integrated seamlessly into the existing telephone system.

**Biometric Systems:**
A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in verification mode or identification mode:

- **In the verification mode,** the system validates a person’s identity by comparing the captured biometric data with her own biometric template(s) stored system database. In such a system, an individual who desires to be recognized claims an identity, usually via a PIN (Personal Identification Number), a user name, a smart card, etc., and the system conducts a one-to-one comparison to determine whether the claim is true or not (e.g., “Does this biometric data belong to Bob?”). Identity verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity.

- **In the identification mode,** the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual’s identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity (e.g., “Whose biometric data is this?”). Identification is a critical component in negative recognition applications where the system establishes whether the person is who she (implicitly or explicitly) denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities. Identification may also be used in positive recognition for convenience (the user is not required to claim an identity). While traditional methods of personal recognition such as passwords, PINs, keys, and tokens may work for positive recognition, negative recognition can only be established through biometrics.

**Fig.1: Block diagram of a Biometric System [2]**

**Fig.2: Comparison of various Biometric technologies [1]**

- High, Medium, and Low are denoted by H, M, and L, respectively.

The applications of biometrics can be divided into the following three main groups:

- **Commercial** applications such as computer network login, electronic data security, ecommerce, Internet access, ATM, credit card, physical access control, cellular phone, PDA, medical records management, distance learning, etc.

- **Government applications** such as national ID card, correctional facility, driver’s license, social security, welfare-disbursement, border control, passport control, etc.

- **Forensic applications** such as corpse identification, criminal investigation, terrorist identification, parenthood determination, missing children, etc.

**Annie P. Oommen etal[7]:** From this paper the digital code lock is therefore particularly useful in applications such as door locks and equipment locks. This simple digital code lock using microcontroller can be enhanced by
incorporating new means of authentication. Most prevalent form of digital lock is that using a numerical code for authentication; the correct code must be entered in order for the lock to deactivate. Such locks typically provide a keypad, and some feature an audible response to each press. Combination lengths are usually between 4 and 6 digits long. Another means of authenticating users is to require them to scan or “swipe” a security token such as a smart card or similar or to interact a token with the lock. As biometrics become more and more prominent as a recognized means of positive identification, their use in security systems increases. Some new digital locks take advantage of technologies such as fingerprint scanning, retinal scanning and iris scanning, and voiceprint identification to authenticate users.

Fig.3: Block diagram of Code lock [7]

Fig.4: Program Flow Chart of Code Lock [7]

Ritesh A. Jadhav etal[9]: According to this paper basic fiber optic system consists of a transmitting device that accepts coded electronic pulses that are generated by the light-emitting diode (LED) or an injection-laser diode (ILD) after that transmitter converts an electrical signal into a light signal, an optical fiber cable that carries the light, and a receiver that accepts the light signal and then detector from receiver circuitry demodulate the signal and converts it back into an electrical signal. The complexity of a fiber optic system can range from very simple (i.e., local area network) to extremely sophisticated and expensive (i.e., long distance telephone).

Fig.5: Block diagram of Optical Fiber Communication [9]

Magnetic fields and current induction work in two ways. They don’t just generate noise in signal carrying conductors; they also let the information on the conductor to be leaked out. Fluctuations in the induced magnetic field outside a conductor carry the same information as the current passing through the conductor. Shielding the wire, as in coaxial cables can reduce the problem, but sometimes shielding can allow enough signal leak to allow tapping, which is exactly what we wouldn’t want.

Fig.6: Evolution of Optical Fiber Communication [9]
Imperial Journal of Interdisciplinary Research (IJIR)
ISSN: 2454-1362, http://www.onlinejournal.in

Artur Balanuta etal[13]: The reduction of the consumption of energy, through its efficient use, is regarded as one of the ways of reducing the impact of mankind on the environment. Buildings consume a significant amount of energy, namely for heating, cooling and illumination. Over the last decades, more energy efficient equipment, new building materials and construction techniques have enabled more energy efficient buildings. However, human behaviour has a large impact on the energy consumption of each building, with similar buildings presenting very distinct energy footprints, due to their occupant’s behaviour. The problem of creating more sustainable energy consumption habits has recently received a lot of attention from the research community. Systems capable of reducing energy consumption, by enforcing more correct behaviours, may reduce costs for companies and help improve the environmental outlook. This paper proposes a novel system to address the energy consumption problem and inadequate habits of people in office buildings. It's a highly flexible distributed office management system that can scale from an individual node in an office to the whole building. The goal is to reduce global building energy consumption without significantly affecting the users' comfort level. An approach is used where the building services are adjusted to its occupancy level and users' needs based on their location. Users are driven to better energy usage habits through access to information and feedback. Our proposal is presented in detail and validated in the context of an academic institution, more specifically at the Taguspark campus of Institute Superior Técnico. The developed system is now operational and being used as a flexible, easily programmable, research platform.

III. PROPOSED MODEL OF THE PROJECT

In this paper of project proposal we are using biometric module for the security purpose at the transmitter side so that no unauthorized person can be able to access the data which we have sent. Basically skin of human fingertips consists of ridges and valleys and they mix together to form the distinctive patterns and these patterns are called fingerprints. From different researches it has been observed that no two persons have the same fingerprints, so they are unique for each individual because of the above mentioned characteristic, fingerprints are very popular for biometric applications. Fingerprints have remarkable permanency and uniqueness throughout the time. From observations we conclude that the fingerprints offer more secure and reliable personal

Fig.7: Types of Fiber Optics Cable [9]

Data Security: There are no radiated magnetic fields around optical fibers; the electromagnetic fields are confined within the fiber. That makes it impossible to tap the signal being transmitted through a fiber without cutting into the fiber. Since fiber optics do not radiate electromagnetic energy, emissions cannot be intercepted and physically tapping the fiber takes great skill to do undetected. Thus, the fiber is the most secure medium available for carrying sensitive data.

Immunity to Electromagnetic Interference: Although fiber optics can solve data communications problems, they are not needed everywhere. Most computer data goes over ordinary wires. Most data is sent over short distances at low speed. In ordinary environments, it is not practical to use fiber optics to transmit data between personal computers and printers as it’s too costly. Electromagnetic Interference is a common type of noise that originates with one of the basic properties of electromagnetism. Magnetic field lines generate an electrical current as they cut across conductors. The flow of electrons in a conductor generates a magnetic field that changes with the current flow. Electromagnetic Interference does occur in coaxial cables, since current does cut across the conductor. Fiber optics are immune to this EMI since signals are transmitted as light instead of current. Thus, they can carry signals through places where EMI would block transmission.

Use less energy: Because there is less signal loss, lower power transmitters can be used to send information through fiber cables than for copper cables where high-voltage electrical transmitter are needed. This reduces cost and maintenance, saving money for customers.

Safety: Fiber optics cable doesn’t transfers electrical signals, the data is transmitted in the form of light signals so making it safe in environment like gas pipe line.
identification than passwords, id-cards or key can provide.
After verifying the biometric ID proof that is fingerprint of an authorized person, the optical transmitter sends the analog or digital signal through optical fiber cable, which is then received by the optical receiver. In case of invalid person at the transmitter end system will beep and not give the access to the unauthorized user. This optical link can also be used for controlling different devices at receiver end.
After reception of the signal at the receiver end, the user would be able to access the data and the transmission would be successfully done with higher security.

MODES OF PROJECT:
The project can be classified into these modes-
- **Biometric:**
  1. Database mode: In this mode we make the database of users in system.
  2. Valid casting mode: In this mode we cast the finger. During casting the finger system automatically check the condition of finger. Is valid or not.
  3. Checking mode: In this mode we check the status of valid finger or not valid finger. According to condition it operates the gate and provides alerting vision.
- **Optical Link Mode:** In this mode we use optical fiber for communication purpose. In this project we demonstrate the different idea of communication such as
  1. Voice communication: we send the analog signal in form of voice.
  2. Data communication: for the data communication we use keypad and with the help of keypad we send the numeric data with the optical fiber channel.
  3. Control mode: in control mode we provide automation concept by optical fiber with advance security.
- **Fail mode of optical link:** in case of fault condition system check the status of optical link if any problem exist in optical communication system then system provide proper intimation.
- **Code Lock:** Code lock security is used at receiver end, when any person enters code, system will check condition and operate the optical link.
- **Automation:** As the name suggests for getting something done automatically. In this project proposal we will try to achieve automation at the receiver end and get it done from the transmitter end.

IV. EXPECTATION FROM THE PROPOSAL
With the help of biometric fingerprint module we can achieve higher security at the transmitter end because it is unique for each individual. If the user is valid only then the data can be able to transmit through optical fiber. Code lock security can be used to protect the data at the receiver end. Analog and digital data can be transmitted through optical fiber link. Automation can also be done through optical fiber link.

V. CONCLUSION
As the result of study of research papers on different security technologies we are proposing a project idea that can be used for highly secured communication using optical link and same optical link can be used for automation. Fingerprint module provides higher security for the data transmission. Code lock is another way to secure the data. Optical fiber link provides high speed in transmission and helps in automation too.

VI. ACKNOWLEDGEMENT
Any collateral activity cannot be truly finished without the help & enthusiasm of the supervisors involved. Additional technical assistances were provided by many individuals. We would like to express deepest appreciation to our project coordinator and project guide. Also, I would like to thank project team who constantly supported me. I owe gratitude to many individuals involved in the development of this review paper.

VII. REFERENCES

---

Imperial Journal of Interdisciplinary Research (IJIR)  
ISSN: 2454-1362, http://www.onlinejournal.in

Page 1074


