# A Dominant Cryptosystem using Biometric Trait and Multiparty Cipher

Shriram D. Raut
Department of Computer Science and Applications,
School of Computational Sciences,
Solapur University, Solapur.
Maharashtra, India.

Rajivkumar Mente
Department of Computer Science and Applications,
School of Computational Sciences,
Solapur University, Solapur.
Maharashtra, India.

Ashok Shinde
Department of Computer Science and Applications,
School of Computational Sciences,
Solapur University, Solapur.
Maharashtra, India.

## ABSTRACT

The biometric is science of recognizing person based on physiological and behavioral characteristics. The cryptographic system assures our data during transmission and tends to form a secure message. This paper discusses about concatenation of biometric trait and multiparty cipher. A message needs a security mechanism that keeps data protected from security attacks. This paper is a stepping stone towards prominent security services; an approach is to use human as token of authorization. A biometric trait may be palm, face; finger etc. and multiparty cipher consist of chaining of symmetric ciphers. The fusion of such characteristic leads us a much dominant cryptosystem and using this we can make messaging or communication quite secure.

## Keywords

Network security; cipher text; biometrics; image processing; palm print; pattern recognition.

## 1. INTRODUCTION

Cryptography is practiced under network security; deals with protecting a data during transmission. Communication system consists of a sender, receiver and a communication media. There is need to authenticate the sender and receiver; those are as one who sends the message and one who receives the message respectively. The security threat causes the security violation. These threats are studied and characterized under security attacks that may be passive or active attacks (Stalling, (2011)) can be summarized as shown in fig. 1 (a). The biometrics is an automated tool to recognize a person based on physiological or behavioral traits. The palm print biometric recognition system is characterized by the palm print feature that lies at the palm region of the hand and are principal line, wrinkles and ridges as shown in fig.1 (b).

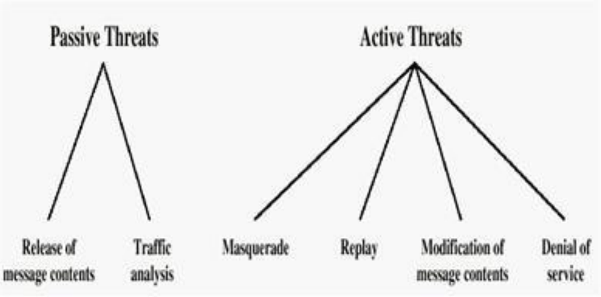
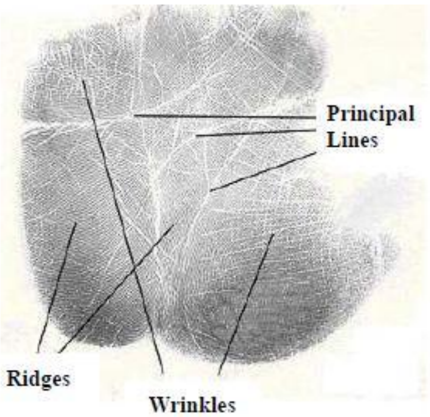


**Fig. 1 (a) Security attacks (Stalling, (2011))**



**(b) palm print features (Zhang, (2004))**

The network security model by having cryptographic system in practice; which assure us to protect our data from such passive and active threats. This paper is targeted for prevention of such security attacks.

## 2. CLOUD COMPUTING SECURITY

Cloud security architecture is effective only if the correct defensive implementations are in place. Efficient cloud security architecture should recognize the issues that will arise with security management (Kurtz, Ronald et.al (2010)). The security management addresses these issues with security controls. These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind cloud security architecture, they can usually be found in one of the following categories:

1. Deterrent controls

These controls are set in place to prevent any purposeful attack on a cloud system. Much like a warning sign on a fence or a property, these controls do not reduce the actual vulnerability of a system.

2. Preventative controls

These controls upgrade the strength of the system by managing the vulnerabilities. The preventative control will safeguard vulnerabilities of the system. If an attack were to occur, the preventative controls are in place to cover the attack and reduce the damage and violation to the system's security.

3. Corrective controls

Corrective controls are used to reduce the effect of an attack. Unlike the preventative controls, the corrective controls take action as an attack is occurring.

4. Detective controls

Detective controls are used to detect any attacks that may be occurring to the system. In the event of an attack, the detective control will signal the preventative or corrective controls to address the issue.

The objective of the proposed system is to preserve the cloud security controls. The system is targeted to use of blend of cryptographic symmetric cipher and biometric authentication system. The approach is to make messaging system secure from security attacks as well as authenticate the parties (sender/receiver) involved in the communication.

## 3. NEED FOR BIOMETRIC SYSTEM

The cryptology guarantees secure message transformation using encryption and decryption techniques. The network access security model by practicing cryptography can be viewed as follows in fig 2.

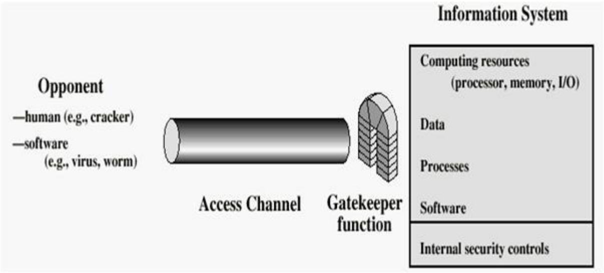


**Fig. 2 Network access security system (Stalling, (2011)).**

As shown in fig. 2 opponent or attacker may be a software program or a human being. So there is need to practice a two way authentication of person involved in communication using biometric authentication (Prabhakar et. al (2003)) and multiparty cipher (Raut et. al (2014)). This paper proposes a prominent and secure information access mechanism. Such type of security services can be devised on communication system. The security services (Kartalopoulos (2008)) are confidentiality (data privacy), authentication (authorize the sender or receiver), Integrity (data has not been altered), Non-repudiation (assure the message ordering), Access control (prevent misuse of resources), Availability (data permanence and non-erasure) (Stalling, (2011)). The objective is to make data secure and preserve the security services.

## 4. PROPOSED SYSTEM

The work manifests use of an existing cryptographic technique and biometric trait. The objective is to get good among all good outcomes. The output of one cipher technique will be given as an input to another cipher technique. The implementation is done by forming an algorithm to put forward the principle and is as follows (Raut et.al, (2014)): 1. Apply Substitution Cipher

a. In this step, apply the principle of Caeser cipher,

b. The output of Caeser cipher will be given as input to Playfair Cipher.

2. Apply the Transposition Cipher on the output given by Substitution Cipher

a. Apply Rail Fence Cipher considering an output from Playfair Cipher,

b. Then, apply Row Transposition Cipher on output given by Rail Fence Cipher.

3. Perform Poly-alphabetic Cipher on the output given by Transportation Cipher

a. Apply the principle of Auto-key cipher considering output of Row transposition Cipher.

4. Finally, apply the Bitwise Exclusive-OR operation.

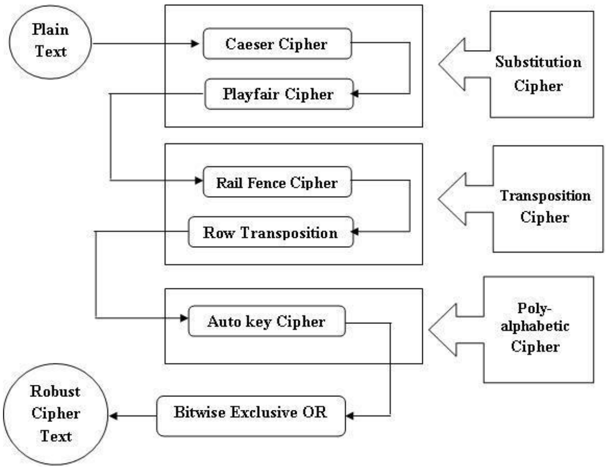


**Fig. 3 Multiparty cryptographic cipher (Raut et.al, (2014))**

Now, next approach is to create biometric palm print recognition model; a palm print is image acquired of palm region of hand. As per paper reviewed (Jain et.al, (2004)) compared to other biometric traits such face, iris, finger etc. the palm print is more prominent as far as acceptability, uniqueness and measurability is concerned. The feature of it, such as principal lines, wrinkles and ridges are unique and distinct from person to person. In this an image processing techniques are used. The algorithm worked out is as follows:

1. Read an image from database and apply the noise removal filtering techniques over it.

2. Convert noise free gray scale image into binary image; which will be useful for palm region extraction.

3. Form the segmentation on region of interest.

4. Apply the Edge Detection algorithm over the segmented palm print image.

The original gray scale palm print image is normalized into binary image by having a good impression of palm print principal line as feature. The biometric recognition system based on palm print feature is devised into enrollment and verification phase.

## 5. IMPLEMENTATION

A blend of multiparty cipher and biometric trait leads with a system having person authentication followed by the secure messaging. However an attacker may breach the cryptographic system but would not be able to pretend as being authorized one. This is what exactly we studied and implemented. The workflow can be described as follows:

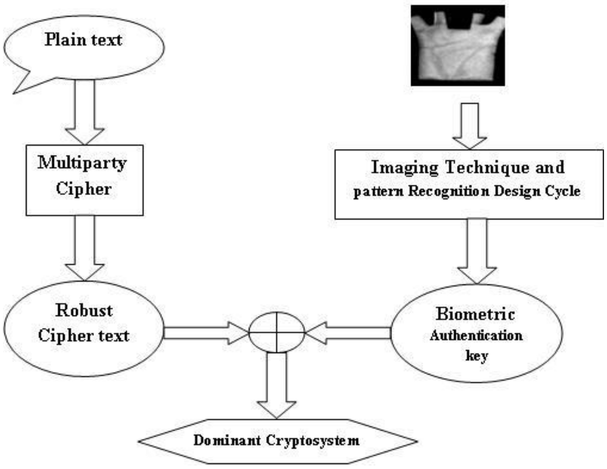

Plain text
Multiparty Cipher
Imaging Technique and pattern Recognition Design Cycle
Robust Cipher text
Biometric Authentication key
Dominant Cryptosystem

**Fig.4 A blend of multiparty cipher and biometric trait.**

As shown in fig 4, it shows a blend of multiparty cipher and biometric palm print model to make message secure and authenticate the respective user in the form of sender/receiver. This is quite protected way of handing our data while transmission. The multiparty cipher in its sense is robust as far as intruder is concern; it's too difficult to predict the various keys associated with these ciphers and can be changed by the authorized parties time to time. The biometric itself is too robust; as it is very difficult to forge or spoof the biometric trait. These traits are unique and distinct from person to person. So this trait can be used to authenticate the parties (sender/receiver) involved in the communication. In this way new secure technology can be brought to make a quite robust cryptosystem.

## 6. CONCLUSION

The biometric is automated tool to recognize a person based on physiological or behavioral traits. The cryptography is study of encryption principles or methods. The objective of the research is to devise a technique by the blend of a multiparty cipher and biometric palm print as a trait. The multiparty cipher is formed by the use of substitution, transposition and poly-alphabetic and bitwise-XOR cipher and are used in chain; while giving output of one cipher to another cipher as input respectively. The palm print is image acquired of the palm region of the hand and has principal lines, wrinkles and ridges. Compared to other biometric traits, palm print is more prominent as far as acceptability, uniqueness and measurability is concerned. This methodology is the robust technique so as to protect our data during transmission.

## ACKNOWLEDGEMENT

We are thankful to Biometric Research Centre (BRC) of Polytechnic Hong Kong University for providing an access to the palm print image database. We would like to thank the Department of Computer Science of School of Computational of Solapur University, Solapur for providing us a computer laboratory and other facilities to work out our research.

## REFERENCES

[1] Stalling, W. (2011). Network Security Essentials. Pearson publication. Fifth Edition. ISBN: 0133370437

[2] Jain, A. K., Ross, A. and Prabhakar S. (2004). An Introduction to Biometric Recognition. IEEE Transaction on Circuits and System for Video Technology, vol.14, Pp. 4-20.

[3] Kartalopoulos, S. V. (2008). Differentiating Data Security and Network Security. Communications, 2008. ICC '08. IEEE International Conference on, pp.1469-1473, 19-23.

[4] Raut, S. D., Patil, S. H., Shinde, A. R. and Humbe, V. T. (2014). A Multiparty Cryptographic Cipher for Network Security Model. Indian Stream Journals.

[5] Prabhakar, S., Pankanti, S. and Jain, A. K. (2003). Biometric Recognition: Security and Privacy Concerns. IEEE Security and Privacy, pp. 33-42.

[6] Krutz, Ronald L., and Russell Dean Vines. (2010). Cloud Computing Security Architecture. Wiley.

[7] Zhang, D. (2004). Palm Print Authentication. Kluwer Publication.

[8] Ajay Kumar, Zhang, D. (2005). Personal authentication using multiple palm print representation. Pattern Recognition Society.

**Shriram D. Raut** working as the Assistant Professor at Department of Computer Science and Applications of School of Computational Sciences at Solapur University, Solapur. He worked as the Research Scholar and submitted a project in Computer Science under UGC SAP (II) DRS Phase-I: 2009-2014, theme “Biometric: Multimodal System Development”. He has authored 21 research articles and got published in reputed national and international Journals.

**Rajivkumar S. Mente,** working as the Head of Department of Computer Science of School of Computational Sciences at Solapur University, Solapur. He has total 20 years experience at Undergraduate and Postgraduate courses in Computer Science. He worked as member of Board of Studies, Academic Council, Faculty of Science, Board of University Teacher Recognition, and Research Recognition Committee in the subject of Computer Science at Solapur University, Solapur. He is editorial board of member of reputed journals.

**Ashok R. Shinde** pursuing his Ph.D. in Computer Science and working as the Assistant Professor of Department of Computer Science of School of Computational Sciences at Solapur University, Solapur. He has total 14 years of teaching experience at Undergraduate and Postgraduate in Computer Science courses. He is Chairman in Computer Science and Solapur University Nodal Officer for All India Survey of Higher Education Scheme. He has authored many of the research articles in reputed national and international Journals. He is editorial board of member of reputed journals.