DEVELOPING ENSURED AND EFFECTIVE BIOSECURITY

[1] Mrs.A.Rangamma,[2] G.Ashwini,[3] G.Sarika,[4] G.Akhila,[5] G.Manoj
[1] Assistant Professor,[2345] B.Tech Students
Department Of Computer Science & Engineering
Sri Indu College Of Engineering & Technology,Sheriguda, Ibrahimpatnam

ABSTRACT

The demand for remote data storage and computation services is increasing exponentially in our data-driven society; thus, the need for secure access to such data and services. In this paper, we design a new biometric- based authentication protocol to provide secure access to a remote (cloud) server. In the proposed approach, we consider biometric data of a user as a secret credential. We then derive a unique identity from the user's biometric data, which is further used to generate the user's private key. In addition, we propose an efficient approach to generate a session key between two communicating parties using two biometric templates for a secure message transmission. In other words, there is no need to store the user's private key anywhere and the session key is generated without sharing any prior information. A detailed Real-Or- Random (ROR) model based formal security analysis, informal (non- mathematical) security analysis and also formal security verification using the broadly-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool reveal that the proposed approach can resist several known attacks against (passive/active) adversary. Finally, extensive experiments and a comparative study demonstrate the efficiency and utility of the proposed approach.

Index Terms—Authentication, biometric-based security, cloud service access, session key.

I. INTRODUCTION

Cloud services are a norm in our society. However, providing secure access to cloud services is not a trivial task, and designing robust authentication, authorization and accounting for access is an ongoing challenge, both operationally and research-wise. A number of authentication mechanisms have been proposed in the literature, such as those based on Kerberos [1], OAuth [2] and OpenID [3] (see [1], [4]–[12]). Generally, these protocols seek to establish a secure delegated access mechanism among two communicating entities connected in a distributed system. These protocols are based on the underlying assumption that the remote server responsible for authentication is a trusted entity in the network. Specifically, a user first registers with a remote server. This is needed to ensure the authorization of the owner. When a user wishes to access a server, the remote server authenticates the user and the user also authenticates the server. Once both verifications are successfully carried out, the user obtains access to the services from some remote server. One key limitation in existing authentication mechanisms is that the user's credentials are stored in the authentication server, which can be stolen and (mis)used to gain unauthorized access to various services. Also, to ensure secure and fast communication, existing mechanisms generally use symmetric key cryptography, which requires a number of cryptographic keys to be shared during the authentication process. This strategy results in an overhead to the authentication protocols. Designing secure and efficient authentication protocols is challenging, as evidenced by the weaknesses revealed in the published protocols of Jiang et al. [13], Althobaiti et al. [14], Xue et al. [15], Turkanovic et al. [16], Park et al. [17], Dhillon and Kalra [18], Kaul and Awasthi [19] and Kang et al.[20] – see also Section II. Therefore, in this paper we seek to design a secure and efficient authentication protocol. Specifically, we will first provide an alternative to conventional password-based authentication mechanism. Then, we demonstrate how one can build a secure communication between communicating parties involved in the authentication protocol, without having any secret pre-loaded (i.e., shared) information. In the proposed approach, we consider a fingerprint image of a user as a secret credential. From the fingerprint image, we generate a private key that is used to enroll the user's credential secretly in the database of an authentication server. In the authentication phase, we capture a new biometric fingerprint image of the user, and subsequently generate the private key and encrypt the biometric data as a query. This queried biometric data is then transmitted to the authentication server for matching with the stored data. Once the user is authenticated successfully, he/she is ready to access his/her service from the desired server. To obtain secure access to the service server, mutual authentication between the user and authentication server, and also between the user and service server have been proposed using a short-term session key. Using two fingerprint data, we present a fast and robust approach to generate the session key. In addition, a biometric based message authenticator is also generated for message authenticity purpose .We summarize the key contributions/benefits related to the proposed approach as below. 1) An effective way to transmit the user's biometric data through the unsecured network channels to an authentication server is presented. 2) We propose an approach to generate a revocable private key directly from an irrevocable fingerprint image. There is no need to store the private key or a direct form of the user's biometric data anywhere. 3) We mitigate the limitation in traditional mechanisms that require the user's credentials to be stored in the authentication server. 4) We introduce a novel way to generate session keys. 5) In traditional authentication protocol, each entity requires some preloaded information; thus, incurring some overhead. We introduce a new mechanism to avoid the need for secret pre- loaded information. 6) A message authentication mechanism, as an alternative to the existing message authentication protocols (i.e., Message Authentication Code (MAC)), is introduced.

II. LITERATURE SURVEY

Title: Biometrics-Based Privacy-Preserving User Authentication Scheme for Cloud- Based Industrial Internet of Things Deployment

Author: A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues.

Abstract: Due to the widespread popularity of Internet-enabled devices, Industrial Internet of Things (IIoT) becomes popular in recent years. However, as the smart devices share the information with each other using an open channel, i.e., Internet, so security and privacy of the shared information remains a paramount concern. There exist some solutions in the literature for preserving security and privacy in IIoT environment. However, due to their heavy computation and communication overheads, these solutions may not be applicable to wide category of applications in IIoT environment. Hence, in this paper, we propose a new biometric- based privacy preserving user authentication (BP2UA) scheme for cloud-based IIoT deployment. BP2UA consists of strong authentication between users and smart devices using preestablished key agreement between smart devices and the gateway node. The formal security analysis of BP2UA using the well-known real-or-random model is provided to prove its session key security. Moreover, an informal security analysis of BP2UA is also given to show its robustness against various types of known attacks. The computation and communication costs of BP2UA in comparison to the other existing schemes of its category demonstrate its effectiveness in the IIoT environment. Finally, the practical demonstration of BP2UA is also done using the NS2 simulation. Due to the widespread popularity of Internet-enabled devices, Industrial Internet of Things (IIoT) becomes popular in recent years. However, as the smart devices share the information with each other using an open channel, i.e., Internet, so security and privacy of the shared information remains a paramount concern. There exist some solutions in the literature for preserving security and privacy in IIoT environment. However, due to their heavy computation and communication overheads, these solutions may not be applicable to wide category of applications in IIoT environment.

Title: Security and Accuracy of Fingerprint-Based Biometrics: A Review

Author: W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli.

Abstract: Biometric systems are increasingly replacing traditional password- and token- based authentication systems. Security and recognition accuracy are the two most important aspects to consider in designing a biometric system. In this paper, a comprehensive review is presented to shed light on the latest developments in the study of fingerprint-based biometrics covering these two aspects with a view to improving system security and recognition accuracy. Based on a thorough analysis and discussion, limitations of existing research work are outlined and suggestions for future work are provided. It is shown in the paper that researchers continue to face challenges in tackling the two most critical attacks to biometric systems, namely, attacks to the user interface and template databases. How to design proper countermeasures to thwart these attacks, thereby providing strong security and yet at the same time maintaining high recognition accuracy, is a hot research topic currently, as well as in the foreseeable future. Moreover, recognition accuracy under non-ideal conditions is more likely to be unsatisfactory and thus needs particular attention in biometric system design.

Related challenges and current research trends are also outlined in this paper. Biometric systems are increasingly replacing traditional password- and token-based authentication systems. Security and recognition accuracy are the two most important aspects to consider in designing a biometric system. In this paper, a comprehensive review is presented to shed light on the latest developments in the study of fingerprint-based biometrics covering these two aspects with a view to improving system security and recognition accuracy.

Based on a thorough analysis and discussion, limitations of existing research work are outlined and suggestions for future work are provided. It is shown in the paper that researchers continue to face challenges in tackling the two most critical attacks to biometric systems, namely, attacks to the user interface and template databases. How to design proper countermeasures to thwart these attacks, thereby providing strong security and yet at the same time maintaining high recognition accuracy, is a hot research topic currently, as well as in the foreseeable future. Moreover, recognition accuracy under non-ideal conditions is more likely to be unsatisfactory and thus needs particular attention in biometric system design.

Title: Difference co-occurrence matrix using BP neural network for fingerprint liveness detection.

Author: C. Yuan, X. Sun, and Q. M. J. Wu

Abstract: With the growing use of fingerprint identification systems in recent years, preventing fingerprint identification systems from being spoofed by artificial fake fingerprints has become a critical problem. In this paper, we put forward a novel method to detect fingerprint liveness based on BP neural network, which is used for the first time in the fingerprint liveness detection. Moreover, different from traditional detection methods, we propose a scheme to construct the input data and corresponding category labels. More effective and efficient texture features of fingerprints, which are used as the input data of the BP neural network, are computed to improve classification performance and obtain a better pre-trained network model. After a variety of preprocessing operations and image compression operations, gradient values in the horizontal and vertical directions are computed by using Laplacian operator, and difference co- occurrence matrices are constructed from the obtained gradient values. Then, the input data of neural network model are built based on two DCMs. The pre-trained neural network models with diverse neuron nodes are learnt.

Different experiments based on different parameters for the BP neural network have been conducted. Finally, classification accuracy of testing fingerprints is predicted based on the pre- trained networks. Experimental results on the LivDet 2013 show that the classification performance of our proposed method is effective and meanwhile provides a better detection accuracy compared with the majority of previously published results. With the growing use of fingerprint identification systems in recent years, preventing fingerprint identification systems from being spoofed by artificial fake fingerprints has become a critical problem. In this paper, we put forward a novel method to detect fingerprint liveness based on BP neural network, which is used for the first time in the fingerprint liveness detection. Moreover, different from traditional detection methods, we propose a scheme to construct the input data and corresponding category labels. More effective and efficient texture features of fingerprints, which are used as the input data of the BP neural network, are computed to improve classification performance and obtain a better pre-trained network model. After a variety of preprocessing operations and image compression operations, gradient values in the horizontal and vertical directions are computed by using Laplacian operator, and difference co-occurrence matrices are constructed from the obtained gradient values. Then, the input data of neural network model are built based on two DCMs.

Title: An Untraceable Biometric-Based Multi-server Authenticated Key Agreement Protocol with Revocation

Author: C.-C. Chang and N.-T. Nguyen

Abstract: Online access has been widely adopted to distribute diversified services to customers. In this architecture, public channels are utilized to exchange information between end users and remote servers at anytime and anywhere. To achieve confidentiality and integrity for transferred data, the related parties have to authenticate each other and negotiate a secret session key to encrypt and decrypt exchanged messages. Since the Lamport's pioneering authentication work in 1981, numerous mechanisms have been proposed to enhance security as well as reduce computation and payload data. Recently, Chuang and Chen proposed a multi- server authenticated agreement protocol employing a smart card and biometric data to eliminate the weaknesses caused by parameters related to low-entropy human-memorable passwords that are stored in a physical location. However, Mishra et al. showed that Chuang and Chen's protocol is not only vulnerable to multiple attacks but also suffers from the drawback of variation of biometric data. To overcome these weaknesses, they proposed an enhanced three- factor authenticated key agreement protocol using the low-error rate Biohashing technique. Unfortunately, we found that Mishra et al.'s scheme is also vulnerable to the denial-of-service attack, the traceable user attack, the impersonation attack, and the pre-shared key attack. Furthermore, the protocol does not provide any user revocation mechanism to control user accesses. In this novel untraceable authenticated key agreement scheme, we adopt the Hamming distance to verify encrypted Biohash codes and a public-key technique to construct the revocation mechanism. Our scheme achieves not only zero errors of biometric verification but also secure against all known attacks.

Online access has been widely adopted to distribute diversified services to customers. In this architecture, public channels are utilized to exchange information between end users and remote servers at anytime and anywhere. To achieve confidentiality and integrity for transferred data, the related parties have to authenticate each other and negotiate a secret session key to encrypt and decrypt exchanged messages. Since the Lamport's pioneering authentication work in 1981, numerous mechanisms have been proposed to enhance security as well as reduce computation and payload data. Recently, Chuang and Chen proposed a multi-server authenticated agreement protocol employing a smart card and biometric data to eliminate the weaknesses caused by parameters related to low-entropy human-memorable passwords that are stored in a physical bio hashing technology

III. SYSTEM ANALYSIS & DESIGN

EXISTING SYSTEM

A number of authentication mechanisms have been proposed in the literature, such as those based on Kerberos [1], OAuth [2] and OpenID [3] (see [1], [4]–[12]). Generally, these protocols seek to establish a secure delegated access mechanism among two communicating entities connected in a distributed system. These protocols are based on the underlying assumption that the remote server responsible for authentication is a trusted entity in the network. Specifically, a user first registers with a remote server. This is needed to ensure the authorization of the owner. When a user wishes to access a server, the remote server authenticates the user and the user also authenticates the server. Once both verifications are successfully carried out, the user obtains access to the services from some remote server. One key limitation in existing authentication mechanisms is that the user's credentials are stored in the authentication server, which can be stolen and (mis)used to gain unauthorized access to various services. Also, to ensure secure and fast communication, existing mechanisms generally use symmetric key cryptography, which requires a number of cryptographic keys to be shared during the authentication process. This strategy results in an overhead to the authentication protocols. Designing secure and efficient authentication protocols is challenging, as evidenced by the weaknesses revealed in the published protocols of Jiang et al. [13], Althobaiti et al. [14], Xue et al. [15], Turkanovic et al. [16], Park et al. [17], Dhillon and Kalra [18], Kaul and Awasthi [19] and Kang et al. [20] – see also Section II. Therefore, in this paper we seek to design a secure and efficient authentication protocol. Specifically, we will first provide an alternative to conventional password-based authentication mechanism. Then, we demonstrate how one can build a secure communication between communicating parties involved in the authentication protocol, without having any secret pre-loaded (i.e., shared) information.

DISADVANTAGES

In existing authentication mechanisms is that the user's credentials are stored in the authentication server, which can be stolen and (mis)used to gain unauthorized access to various services.

When a user wishes to access a server, the remote server authenticates the user and the user also authenticates the server.

PROPOSED SYSTEM

In the proposed approach, we consider a fingerprint image of a user as a secret credential. From the fingerprint image, we generate a private key that is used to enroll the user's credential secretly in the database of an authentication server. In the authentication phase, we capture a new biometric fingerprint image of the user, and subsequently generate the private key and encrypt the biometric data as a query. This queried biometric data is then transmitted to the authentication server for matching with the stored data. Once the user is authenticated successfully, he/she is ready to access his/her service from the desired server. To obtain secure access to the service server, mutual authentication between the user and authentication server, and also between the user and service server have been proposed using a short-term session key. Using two fingerprint data, we present a fast and robust approach to generate the session key. In addition, a biometricbased message authenticator is also generated for message authenticity purpose.

We summarize the key contributions/benefits related to the proposed approach as below.

An effective way to transmit the user's biometric data through the unsecured network channels to an authentication server is presented.

We propose an approach to generate a revocable private key directly from an irrevocable fingerprint image. There is no need to store the private key or a direct form of the user's biometric data anywhere.

We mitigate the limitation in traditional mechanisms that require the user's credentials to be stored in the authentication server.

We introduce a novel way to generate session keys.

In traditional authentication protocol, each entity requires some preloaded information; thus, incurring some overhead. We introduce a new mechanism to avoid the need for secret pre- loaded information.

A message authentication mechanism, as an alternative to the existing message authentication protocols (i.e., Message Authentication Code (MAC)), is introduced.

ADVANTAGES

An efficient approach to generate a session key between two communicating parties using two biometric templates for a secure message transmission.

There is no need to store the user's private key anywhere and the session key is generated without sharing any prior information.

SYSTEM ARCHITECTURE

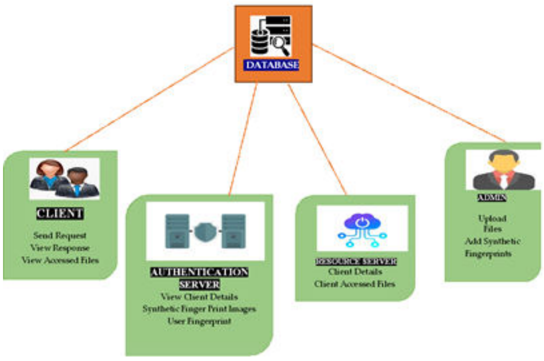


Fig. SYSTEM ARCHITECTURE

IV. IMPLEMENTATION

MODULES

- CLIENT
- AUTHENTICATION SERVER
- ADMIN
- RESOURCE SERVER

MODULE DESCRIPTION

CLIENT

Client has to register into application with basic details and he can able to login with username ,password and with fingerprint. Client can able sent request to the resource server. After sending the request he can get the response from the resource server.after getting the response from the server he can able view the file in the cloud. He can able to see all permission of files.

AUTHENTICATION SERVER.

Authentication Server need to login with username and password. After login he can able to view client details and authorize . Authentication server can able to view synthetic finger print images. Server can able to user client images.

ADMIN

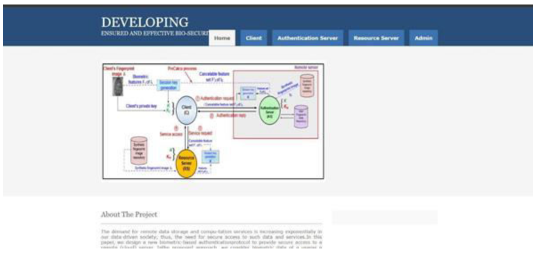
Admin need to login with basic username and password. After login he can able to upload files those are useful to the user. He can able to view all uploaded files. Admin can able to add synthetic fingerprint images.Admin can able to view the data in the repository.

RESOURCE SERVER

Resource server need to login into the application using username and password. After login resource server he can able to view all client requests as well as he can able view all users access rights of files.

V. SCREENSHOTS:

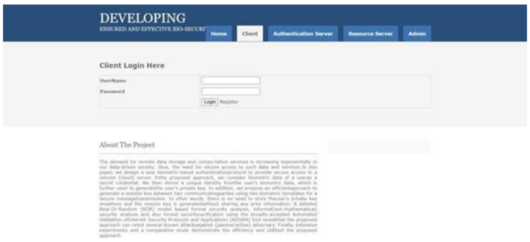
Home Screen


DEVELOPING
ENSURED AND EFFECTIVE BIO-SECURI

About The Project

The demand for remote data storage and compu-tation services is increasing exponentially in our data-driven society; thus, the need for secure access to such data and services.In this paper, we design a new biometric-based authenticationprotocol to provide secure access to a remote (cloud) server. Inthe proposed approach, we consider biometric data of a useras a

Client login screen


DEVELOPING
ENSURED AND EFFECTIVE BIO-SECURI

Client Login Here

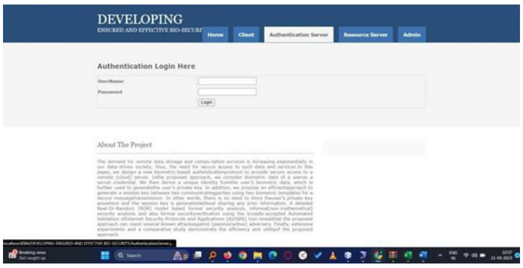
UserName

Password

About The Project

The demand for remote data storage and compu-tation services is increasing exponentially in our data-driven society; thus, the need for secure access to such data and services.In this paper, we design a new biometric-based authenticationprotocol to provide secure access to a remote (cloud) server. Inthe proposed approach, we consider biometric data of a useras a secret credential. We then derive a unique identity fromthe user's biometric data, which is further used to generatethe user's private key. In addition, we propose an efficientapproach to generate a session key between two communicatingparties using two biometric templates for a secure messagetransmission. In other words, there is no need to store theuser's private key anywhere and the session key is generatedwithout sharing any prior information. A detailed Real-Or-Random (ROR) model based formal security analysis, informal(non-mathematical) security analysis and also formal securityverification using the broadly-accepted Automated Validation ofInternet Security Protocols and Applications (AVISPA) tool revealthat the proposed approach can resist several known attacksagainst (passive/active) adversary. Finally, extensive experiments and a comparative study demonstrate the efficiency and utilityof the proposed approach.

Authentication login


DEVELOPING
ENSURED AND EFFECTIVE BIO-SECURI

Authentication Login Here

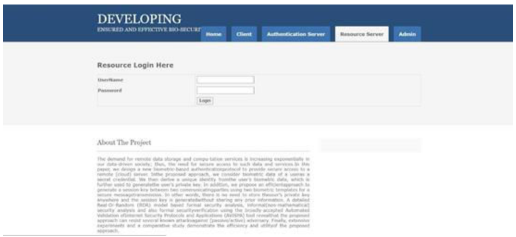
UserName

Password

About The Project

The demand for remote data storage and compu-tation services is increasing exponentially in our data-driven society; thus, the need for secure access to such data and services.In this paper, we design a new biometric-based authenticationprotocol to provide secure access to a remote (cloud) server. Inthe proposed approach, we consider biometric data of a useras a secret credential. We then derive a unique identity fromthe user's biometric data, which is further used to generatethe user's private key. In addition, we propose an efficientapproach to generate a session key between two communicatingparties using two biometric templates for a secure messagetransmission. In other words, there is no need to store theuser's private key anywhere and the session key is generatedwithout sharing any prior information. A detailed Real-Or-Random (ROR) model based formal security analysis, informal(non-mathematical) security analysis and also formal securityverification using the broadly-accepted Automated Validation ofInternet Security Protocols and Applications (AVISPA) tool revealthat the proposed approach can resist several known attacksagainst (passive/active) adversary. Finally, extensive experiments and a comparative study demonstrate the efficiency and utilityof the proposed approach.

Resource server


DEVELOPING
ENSURED AND EFFECTIVE BIO-SECURI

Resource Login Here

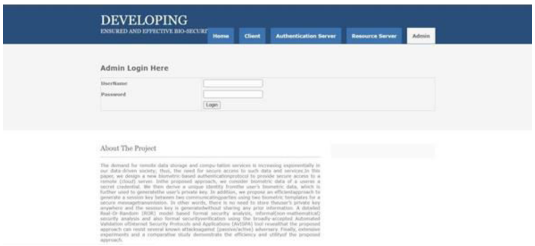
UserName

Password

About The Project

The demand for remote data storage and compu-tation services is increasing exponentially in our data-driven society; thus, the need for secure access to such data and services.In this paper, we design a new biometric-based authenticationprotocol to provide secure access to a remote (cloud) server. Inthe proposed approach, we consider biometric data of a useras a secret credential. We then derive a unique identity fromthe user's biometric data, which is further used to generatethe user's private key. In addition, we propose an efficientapproach to generate a session key between two communicatingparties using two biometric templates for a secure messagetransmission. In other words, there is no need to store theuser's private key anywhere and the session key is generatedwithout sharing any prior information. A detailed Real-Or-Random (ROR) model based formal security analysis, informal(non-mathematical) security analysis and also formal securityverification using the broadly-accepted Automated Validation ofInternet Security Protocols and Applications (AVISPA) tool revealthat the proposed approach can resist several known attacksagainst (passive/active) adversary. Finally, extensive experiments and a comparative study demonstrate the efficiency and utilityof the proposed approach.

Admin login


DEVELOPING
ENSURED AND EFFECTIVE BIO-SECURI

Admin Login Here

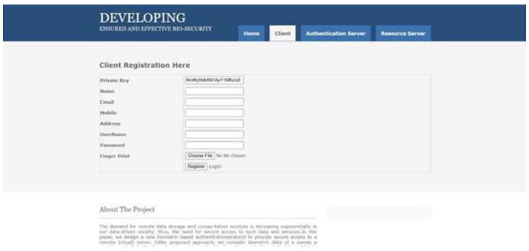
UserName

Password

About The Project

The demand for remote data storage and compu-tation services is increasing exponentially in our data-driven society; thus, the need for secure access to such data and services.In this paper, we design a new biometric-based authenticationprotocol to provide secure access to a remote (cloud) server. Inthe proposed approach, we consider biometric data of a useras a secret credential. We then derive a unique identity fromthe user's biometric data, which is further used to generatethe user's private key. In addition, we propose an efficientapproach to generate a session key between two communicatingparties using two biometric templates for a secure messagetransmission. In other words, there is no need to store theuser's private key anywhere and the session key is generatedwithout sharing any prior information. A detailed Real-Or-Random (ROR) model based formal security analysis, informal(non-mathematical) security analysis and also formal securityverification using the broadly-accepted Automated Validation ofInternet Security Protocols and Applications (AVISPA) tool revealthat the proposed approach can resist several known attacksagainst (passive/active) adversary. Finally, extensive experiments and a comparative study demonstrate the efficiency and utilityof the proposed approach.

Client registration


DEVELOPING
ENSURED AND EFFECTIVE BIO-SECURITY

Client Registration Here

Private Key KnKyBdd0Xf AyY1MLrz3

Name

Email

Mobile

Address

UserName

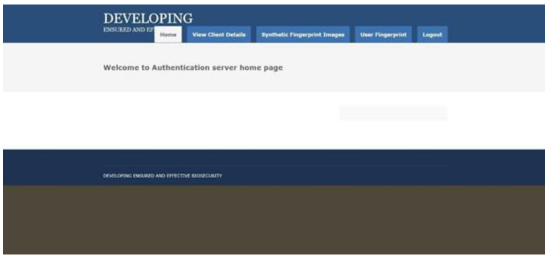
Password

Finger Print

About The Project

The demand for remote data storage and compu-tation services is increasing exponentially in our data-driven society; thus, the need for secure access to such data and services.In this paper, we design a new biometric-based authenticationprotocol to provide secure access to a remote (cloud) server. Inthe proposed approach, we consider biometric data of a useras a

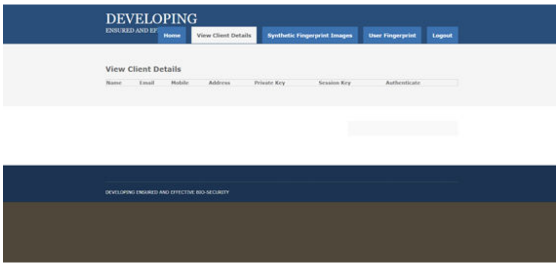
Server home page


DEVELOPING
ENSURED AND EF

Welcome to Authentication server home page

DEVELOPING ENSURED AND EFFECTIVE BIOSECURITY

Client Details

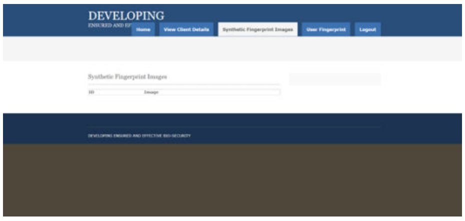

DEVELOPING
ENSURED AND EF

View Client Details

Name	Email	Mobile	Address	Private Key	Session Key	Authenticate

DEVELOPING ENSURED AND EFFECTIVE BIO-SECURITY

Synthetic Fingerprint images

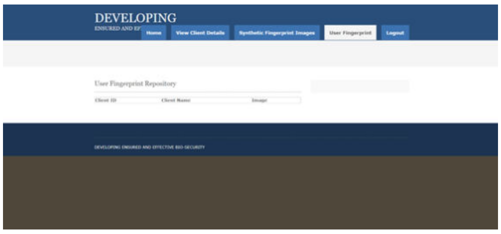

DEVELOPING
ENSURED AND EF

Synthetic Fingerprint Images

ID	Image

DEVELOPING ENSURED AND EFFECTIVE BIO-SECURITY

User Fingerprint

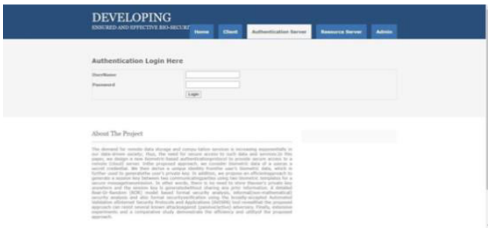

DEVELOPING
ENSURED AND EF

User Fingerprint Repository

Client ID	Client Name	Image

DEVELOPING ENSURED AND EFFECTIVE BIO-SECURITY

Authentication login


DEVELOPING
ENSURED AND EFFECTIVE BIO-SECURI

Authentication Login Here

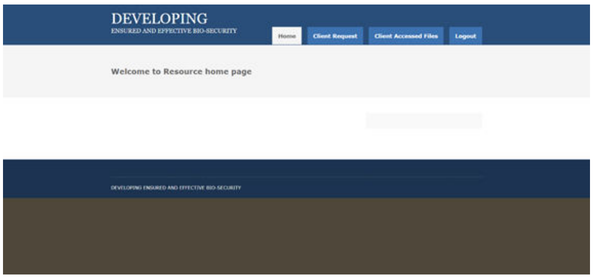
UserName

Password

About The Project

The demand for remote data storage and compu-tation services is increasing exponentially in our data-driven society; thus, the need for secure access to such data and services.In this paper, we design a new biometric-based authenticationprotocol to provide secure access to a remote (cloud) server. Inthe proposed approach, we consider biometric data of a useras a secret credential. We then derive a unique identity fromthe user's biometric data, which is further used to generatethe user's private key. In addition, we propose an efficientapproach to generate a session key between two communicatingparties using two biometric templates for a secure messagetransmission. In other words, there is no need to store theuser's private key anywhere and the session key is generatedwithout sharing any prior information. A detailed Real-Or-Random (ROR) model based formal security analysis, informal(non-mathematical) security analysis and also formal securityverification using the broadly-accepted Automated Validation ofInternet Security Protocols and Applications (AVISPA) tool revealthat the proposed approach can resist several known attacksagainst (passive/active) adversary. Finally, extensive experiments and a comparative study demonstrate the efficiency and utilityof the proposed approach.

Resource Home page


DEVELOPING
ENSURED AND EFFECTIVE BIO-SECURITY

Welcome to Resource home page

DEVELOPING ENSURED AND EFFECTIVE BIO-SECURITY

VI. CONCLUSION

CONCLUSION

Biometric has its unique advantages over conventional password and token-based security system, as evidenced by its increased adoption (e.g., on Android and iOS devices). In this paper, we introduced a biometric-based mechanism to authenticate a user seeking to access services and computational resources from a remote location. Our proposed approach allows one to generate a private key from a fingerprint biometric reveals, as it is possible to generate the same key from a fingerprint of a user with 95.12% accuracy. Our proposed session key generation approach using two biometric data does not require any prior information to be shared. A comparison of our approach with other similar authentication protocols reveals that our protocol is more resilient to several known attacks. Future research includes exploring other biometric traits and also multi-modal biometrics for other sensitive applications (e.g., in national security matters).

FUTURE SCOPE

Biosecurity describes the strategies, regulations and activities involved in the exclusion, eradication or effective management of risks posed by pests, weeds and diseases to the economy, environment and human health. There are at least three good reasons why biosecurity is arguably more significant to New Zealand than any other country in the world. First, relative to most developed countries, our economy depends on vibrant agriculture, horticulture and forestry sectors – making up 70 per cent of our export earnings.Second, our primary industries mainly depend on the productivity of exotic species, be they livestock, pasture grasses, pip fruit and stone fruit, forestry trees or aquaculture species such as salmon and Pacific oysters. The fact that these species do so well in New Zealand is partly a reflection that they have left many pests and diseases behind in their regions of origin. Third, the long isolation of New Zealand and rapid transformation of our landscape to support primary production means that our agricultural and forestry systems are very simplified and lack effective native predators and parasites which might stem the incursion of new pests. In general, the relative freedom from pests and diseases combined with excellent growing conditions in this country has made the primary sector highly competitive globally. However it also means that even a single incursion of a high profile pest or disease could have major economic effects. The Reserve Bank of New Zealand has estimated that an outbreak of foot-and-mouth disease would reduce

REFERENCES

1. C. Neuman, S. Hartman, K. Raeburn, “The kerberos network authentication service (v5),” RFC 4120, 2005.
2. “OAuth Protocol.” [Online]. Available: http://www.oauth.net/
3. “OpenID Protocol.” [Online]. Available: http://openid.net/
4. G. Wettstein, J. Grosen, and E. Rodriguez, “IDFusion: An open architecture for Kerberos based authorization,” Proc. AFS and Kerberos Best Practices Workshop, June 2006.
5. Kehne, J. Schonwalder, and H. Langendorfer, “A nonce-based protocol for multiple authentications,” ACM SIGOPS Operating System Review, vol. 26, no. 4, pp. 84–89, 1992.
6. Neuman and S. Stubblebine, “A note on the use of timestamps as nonces,” Oper. Syst. Rev., vol. 27, no. 2, pp. 10–14, 1993.
7. J. Astorga, E. Jacob, M. Huarte, and M. Higuero, “Ladon : endto-end authorisation support for resource-deprived environments,” IET Infomration Security, vol. 6, no. 2, pp. 93–101, 2012.
8. S. Zhu, S. Setia, and S. Jajodia, “LEAP: efficient security mechanisms for large-scale distributed sensor networks,” Washington D.C., USA, October 2003, pp. 62–72.
9. Perrig, R. Szewczyk, D. Tygar, V. Wen, and D. Culler, “SPINS: security protocols for sensor networks,” ACM Wireless Networking, vol. 8, no. 5, pp. 521–534, 2002.
10. P. Kaijser, T. Parker, and D. Pinkas, “SESAME: The solution to security for open distributed systems,” Computer Communications, vol. 17, no. 7, pp. 501–518, 1994.
11. G. Wettstein, J. Grosen, and E. Rodriguez, “IDFusion: An open architecture for Kerberos based authorization,” Proc. AFS and Kerberos Best Practices Workshop, June 2006.
12. M. Walla, “Kerberos explained,” Windows 2000 Advantage Magazine, 2000.
13. Q. Jiang, J. Ma, X. Lu, and Y. Tian, “An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks,” Peer-to-Peer Networking and Applications, vol. 8, no. 6, pp. 1070–1081, 2015.