Secure User Authentication in Internet Banking: A Qualitative Survey

Janardan Choubey and Bhaskar Choubey

***Abstract*—A qualitative survey of user identification mechanisms being applied in online banking environments across the English speaking world is presented. By studying the Internet banking sites of most major banks in 7 countries, the paper reports the variations and calls for standardisation of user credentials in these environments.**

***Index Terms*—Online banking, security credentials, security standardization.**

I Introduction

Internet based technologies have revolutionised the banking industry as well as way people interact with financial institution and one another financially. However, it has raised new questions and dimensions for securing data of the financial institutions as well as the end-users. In this paper, we raise the oft-repeated question of security in online banking systems, which have been extensively studied from technological, sociological, financial and other points of views. [1]-[7]. Security covers a large spectrum of activity in banking. At one end of this spectrum is the back-end security infrastructure being applied at the banking institutions to secure their databases and servers. Somewhere in between are the encryption based security features which ensure the safety and security of data transmission between the bank and the end-user. The other end of the spectrum is the end-user him/herself. A major concern of every bank is the proper authentication of its end-user in a secure environment. The end-user is also concerned that no one else should be able to access his account [3], [8].

In this paper, we study this end of the spectrum; more specifically, we study the identification mechanism in online banking systems. For any non-personal transaction, the bank has to verify the identification of the end-user, and hence in an online environment has to trust some form of digital identity to know its customer. More importantly, it has to ensure that the form of identity has not been tampered with. Several solutions have been suggested and are being used by banks across the globe to verify the identity of its customers [2]. In this paper, we survey these features; however, we limit ourselves to the features in use in various banks and discard the ones proposed only in technical literature [1], [9]. The second section of the paper provides the methodology of our qualitative study. The third section followed by a description of the identification credentials being used by the banks. The fourth section of the paper discusses the way in which these login credentials are sought. Finally, a discussion is provided at the end of the paper.

II Data Collection

The Internet banking sites of most major banks across seven English speaking countries were studied. The countries and the banks studied are listed in table I. In addition to most major banks, a good selection of smaller banks was also covered. For example, in case of UK, large banks like Royal Bank of Scotland, HSBC and Halifax-Bank of Scotland were studied along with smaller banks like Clydesdale and Nationwide building society. In some cases, two banks are owned by same entity. For example, Natwest and RBS are owned by same group and have very similar online security features. They were hence included as one entity. On the other hand, there are banks which despite belonging to the same group have different security features. One such example is that of Westpac and St. Georges' bank in Australia. These were hence studied separately. In recent past, there have also been mergers of several banks, for example Wachovia being acquired by Wells Fargo. The security features of some of these banks have been merged and this study concentrated on the front end of the largest partner only.

To understand the details of the user identification technique being used by the bank, we studied the help manual of each individual bank. These help-manuals appeared as a document (in HTML, PDF or other formats) or as visual animations. No attempts were made to personally test the system and the help manuals/online demos were trusted in each case. The individual banks were also not contacted to verify the content of their websites. Studies were conducted on banks' website on the week starting 3rd of November 2010.

User identification feature of any bank has to balance between security and hassle free environment. Banks prefer their customers to use the online banking facility as it reduces their cost, primarily through labour costs. This generally involves conflicting issues of enhanced security as well as ease of operation. Minimalist security could lead to breach of banks or user's database, whereas excessive security will make the online system impractical to use. Banks have hence been experimenting with various types of user identification. We would study these from two different angles. The first of these would survey what exactly is asked

Manuscript received December 12, 2012; revised February 20, 2013.

Janardan Choubey is with the Department of Mathematics, North Eastern Regional Institute of Science and Technology, Nirjuli - 791109, India (e-mail: janardanchoubey@yahoo.com).

Bhaskar Choubey is with the Division of Electronics and Nanoscale Engineering of the School of Engineering, University of Glasgow, Rankine Building, Oakfield Avenue, Glasgow, G12 8LT, UK.

DOI: 10.7763/IJIMT.2013.V4.391

from the end-users in terms of their credentials. This involves usernames, passwords and pins and is surveyed in next section. The other aspect is how this security feature is sought from the user. This involves the particular design of the online environment and is covered in the next section.

III SECURITY FEATURES - WHAT

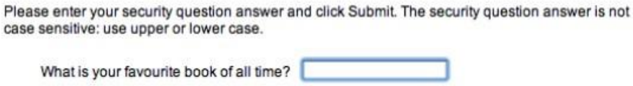
We observed a wide variety of security credentials with a lack of standardisation in different banks. These features had evolved over a period of time, primarily through trial and error. In several instances, the banks imitated the security feature being applied by other banks in the country. In some cases, banks also followed the security feature of their parent organisation from a different country.

A. Level 1

The simplest form of identity check is that of a username and a password. Surprisingly, it is still one of the most popular forms applied by various banks. In countries like USA, it is generally the only form of identity verification. Usernames come in different forms and sizes. They vary from an arbitrary number to a combination of users name, date of birth and other numbers. In the simplest case, they were observed to be the credit/debit card number or the account number of the user. Passwords also come in various flavours. They could be numeric pins, which could be similar to the end-users cash machine's pins or they could be alphanumeric.

B. Level 1A

At a slightly higher level of security, banks incorporate another secure or unsecure form of identification. This could be as simple as date of birth, any favourite reminder or another set of passwords. One example of such a feature is shown in Fig. 1.



Please enter your security question answer and click Submit. The security question answer is not case sensitive: use upper or lower case.

What is your favourite book of all time?

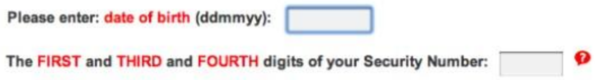
Fig. 1. A typical example of level 1A security with a personal question as used by RBS in UK.

C. Randomized Level 1 or 1A

As a variation of the above formats and in particular to avoid phishing attacks, banks often ask a randomised set of passbits rather than the whole password. We observed that such a security feature is quite prevalent in banks in the United Kingdom. For example, Fig. 2 shows the security questions being asked by HSBC, which in addition to the date of birth of the user, asks a specific set of pass-bits.

D. Level 2

Also referred to as Factor 2 authentication, this feature includes a set of randomly generated characters in addition to aforementioned credentials. It is often perceived by the end users that randomly generated passwords are more trusted than their own passwords [10], [11]. These randomly generated characters could be printed and send to the customers, as has been the case in Germany for quite some time.



Please enter: date of birth (ddmmyy):

The FIRST and THIRD and FOURTH digits of your Security Number:

Fig. 2. A typical example of level 2 security with randomized passwords as used by HSBC in UK.

Alternatively, these numbers could be generated using a token generator issued by the bank to the customer. It is also possible to generate these random numbers and send to the mobile of the end-user through SMS. Paper based systems, despite their popularity in Germany have found little support in other countries. The reasons are often the cost and public perception. Furthermore carrying another set of papers is not perceived as being too user friendly. Electronic random number generators have come in shape of card readers, key rings as well as mobile sim based systems. Nevertheless, they are still far from becoming widely popular in the market. The principal factor here has been lack of customer education as well as the trouble perceived by the customer in carrying another set of devices in order to access the banking website. Nevertheless, several banks including Nationwide [12], HSBC and Barclays in UK [13], Bendigo in Australia and First national in South Africa have been trying such products.

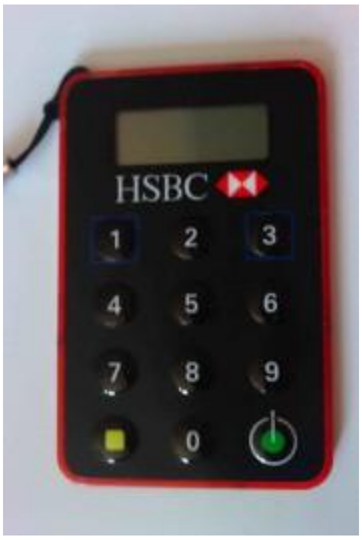


Fig. 3. A typical security token generator from HSBC in UK.

E. Security Software

Some banks provide free software to their end-user. These software are primarily intended to check for viruses and trojans on the user's system. More importantly, they are intended to search for keyloggers and warn the end-user of the same. Examples include Rapport software from HSBC and RBS in UK as well as Star Token from Bank of India, a typical screenshot of which is shown in Fig. 4.

IV SECURITY FEATURES - HOW

The previous section surveyed the various security credentials being sought in the Internet banking environment. Additional layer of security has been provided by several banks by changing the way in which security questions are asked to the end user.

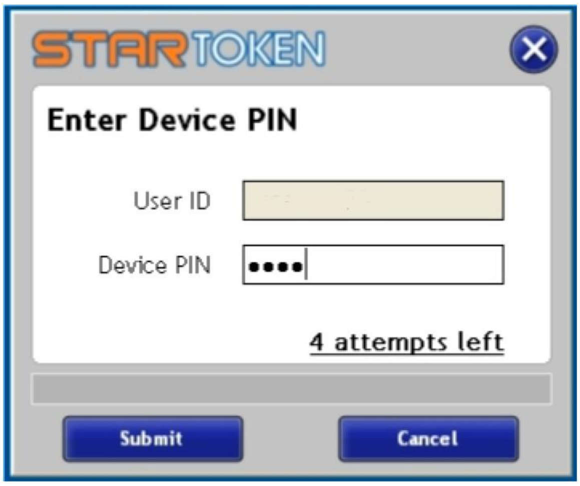


Fig. 4. A screenshot of a typical security software used for secure communication between user's computer and bank's server. The present example is from Bank of India.

A. URL

A good number of banks will ask the security credentials on the primary and often the first webpage of the bank, itself. One such example is Wells Fargo in USA, a screen shot of whose website is shown in Fig. 5 (Ref: https://www.wellsfargo.com/). In these cases, the front page of the bank is often a secure site.

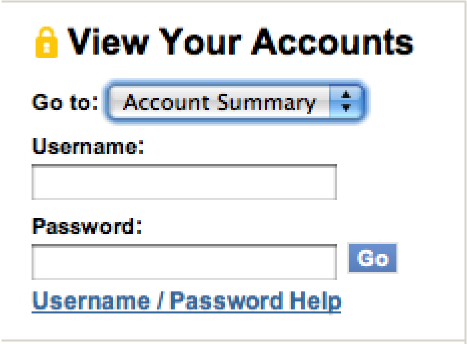


Fig. 5. A typical example of asking login information and password on same page as used by Wells Fargo, USA.

Alternatively and increasingly, the primary webpage is used as an information-only insecure site for and the user is pointed to a different secured site to enter his login information. Such a feature is also often used to prompt the user to select from a variety of account options, either through a pull down menu or through checklist. A typical example is shown from Westpac's login site in Australia in Fig. 6 (Ref: http://www.westpac.com.au)

In several banks, the internet banking site had a different name than the principal site of the bank. For ex-ample, the commercial site of State Bank of India is at http://www.statebankofindia.com/, whereas the name of its internet banking site is https://www.onlinesbi.com/. Such features are quite popular with banks in India.

B. Different Stages of Security

Yet another aspect of the website design for banks is whether to ask all security questions on the same page or use a different page for each question, thereby introducing additional checks at each step. Fig. 7 shows a typical example of the former from Bank SA in Australia wherein all security questions are being asked on a page.

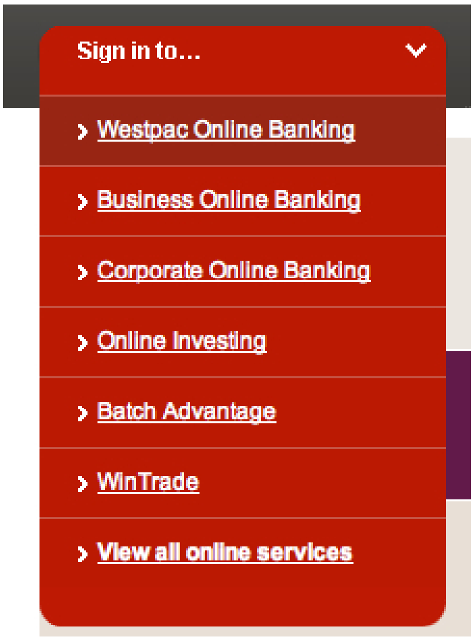


Fig. 6. Multiple choices linking from primary page of the bank as used by Westpac, Australia.

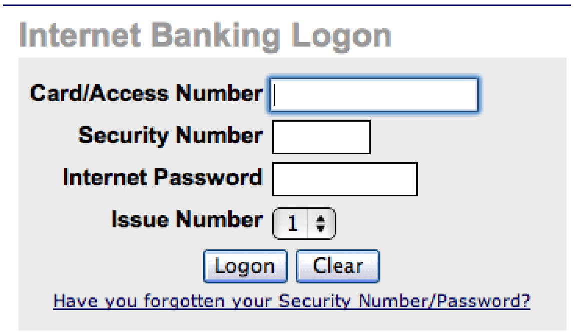


Fig. 7. A typical example of asking login information and password on same page as used by Bank SA, Australia.

Alternatively, various security questions can be asked on different pages. To start with, the username can be entered on the first page and checked for authenticity before asking the user for password or other credentials. An example is shown in Fig. 8 from Bank of Montreal's webpage (Ref: http://www.bmo.com/home) wherein just the login information is asked on the first page. The security questions could then be asked on another page as shown earlier in Fig. 2.

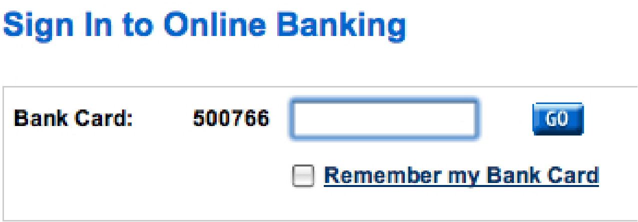


Fig. 8. The login page with just the account name information as used by Bank of Montreal in Canada.

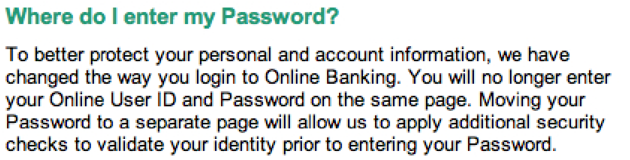
A typical example of security warning from Charter One bank in USA is presented in Fig. 9 which justifies different pages for different aspect of security credentials

C. Virtual Keyboards

Yet another feature provided by some banks is that of virtual keyboard. Rather than asking the end-user to enter his credentials using his keyboard, they are asked to click on the corresponding keys on an image of the keyboard on screen.

TABLE I: LIST OF BANKS STUDIED WITH WEBSITES ACCESSED DURING THE WEEK STARTING 3RD NOVEMBER 2010

UK		**USA**	
HSBC	http://www.hsbc.co.uk/1/2/	**Citibank**	http://www.citibank.com
RBS-Natwest	http://www.rbs.co.uk/	Bank of America	https://www.bankofamerica.com/
Halifax-Bank of Scotland	http://www.halifax.co.uk/	JP Morgan Chase	https://www.chase.com/
Llyods TSB	http://www.lloydstsb.com/	Wells Fargo - Wachovia	https://www.wellsfargo.com/
Barclays	http://www.barclays.co.uk/	Sun Trust	https://www.suntrust.com
Santander	http://www.santander.co.uk/	US Bank	http://www.usbank.com/
Clydesdale	http://www.cbonline.co.uk/	Regions Bank	https://www.regions.com
Nationwide	http://www.nationwide.co.uk	Branch Banking and Trust	http://www.bbt.com/
Cooperative	http://www.co-operativebank.co.uk/	HSBC	http://www.us.hsbc.com
Canada		PNC	https://www.pnc.com/
RBC	http://www.rbc.com/canada.html	Keybank	https://www.key.com/
TD Canada Trust	http://www.tdcanadatrust.com/	Fifty Third	https://www.53.com/
Bank of Nova scotia	http://scotiabank.com/	Charter one	http://www.charterone.com/
Bank of montreal	http://www.bmo.com/home	Capital One	https://www.capitalone.com/
Canadian imperial	http://www.cibc.com	Sovereign bank	http://www.sovereignbank.com/
National Bank of Canada	http://www.nbc.ca/	Comerica	http://www.comerica.com/
India		**South Africa**	
State Bank of India	https://www.onlinesbi.com/	First National	https://www.fnb.co.za/
Panjab National Bank	http://netpnb.com/	ABSA	http://www.absa.co.za/absacoza/
Bank of Baroda	https://www.bobibanking.com/	Standard Bank	http://www.standardbank.co.za/
Indian Overseas	https://www.iobnet.co.in/	Nedbank	http://www.nedbank.co.za/
Allahabad	https://www.allbankonline.in/	Capitec	http://www.capitecbank.co.za/
ICICI	http://www.icicibank.com/	**Australia**	
Canara bank	https://www.canarabank.in	National Australian (NAB)	http://www.nab.com.au/
Andhra	https://www.onlineandhrabank.net.in	Commonwealth	http://www.commbank.com.au/
Bank of India	http://www.bankofindia.com/	Westpac	http://www.westpac.com.au/
HSBC	http://www.hsbc.co.in	ANZ	http://www.anz.com/personal/
HDFC	http://www.hdfcbank.com/	St Georges	http://www.stgeorge.com.au/
Ireland		BankSa	http://www.banksa.com.au/
Ulster Bank	http://www.ulsterbank.com/	Bendigo	http://www.bendigobank.com.au/
Bank of Ireland	http://www.boi.ie/	Suncorp	http://www.suncorp.com.au/
National Irish	http://www.nationalirishbank.ie/	Bank of Queensland	http://www.boq.com.au/
AIB	http://www.aib.ie/personal/home	AMP	https://www.amp.com.au/



Where do I enter my Password?

To better protect your personal and account information, we have changed the way you login to Online Banking. You will no longer enter your Online User ID and Password on the same page. Moving your Password to a separate page will allow us to apply additional security checks to validate your identity prior to entering your Password.

Fig. 9. Security message for password on next page as used by Charter One, USA.

These keyboards could be as simple as numeric keyboards as shown in Fig. 10 (Ref: http://www.absa.co.za/absacoza) or could involve a fully qwerty or a randomised keyboard, as shown in Fig. 11 (Ref: http://www.onlinesbi.com). These keyboards are often credited for minimising keylogger based attacks on personal information. We observed these keyboards are quite popular among Indian banks.

V DISCUSSIONS

In our study, we observed a wide array of identification mechanism and a lack of standardisation across various banks. It is surprising to note this as most other aspects of banking, including the data transmission and use of ATMs have long been standardised.

Various explanations can be offered to this effect. Online banking is a new phenomenon and banks across the globe are only recently appreciating the full effect of the same. Even the websites of the banks are evolving and hence a permanent feature is difficult to imagine. A standard may limit the abilities of new techniques and front-ends to develop. Furthermore, the banks may like to differentiate themselves from one another on the basis of visible security feature. However, there are only a finite number of options available and hence it may not be feasible. Comparative studies of various mechanisms have been at best inconclusive on the best security feature [2], [11]. In addition, there are reports of public perception which leads to banks being asked to improve their online security [14], [15].

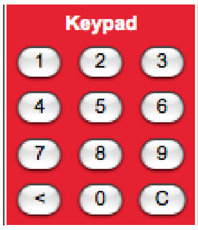


Fig. 10. A typical example of simple keyboard as used by ABSA in South Africa.

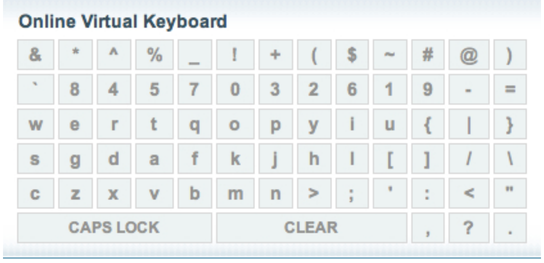


Fig. 11. A typical example of virtual and randomizes keyboard as used by State Bank of India in India.

Nevertheless, having a standard of web authentication would far outweigh these disadvantages, both for the customer as well as the bank. It would ensure lower installation and start-up cost for the banks. More importantly, it will ensure that cost of security research is shared evenly between banks and academia. The less custom effort required in every new page will also lead to lower costs. It will also improve the operational abilities of the banks in internet banking. Further, it will allow interchangeability of software and networking components between banks, thereby reducing the eventual cost of their online environment.

From the security point of view, a standard will facilitate research into the ability of the interface to withstand hacking and phishing attacks. It will then be easier to update the standard to meet the demands to any new attack mechanism. Finally and importantly, it would reduce the cost of user re-education when they shift from one bank to another, thereby easing the banks' ability to get new customers.

Having studied the variety of user identification mechanisms presented in this paper, we call for a unification of these systems thereby allowing ease for the users as well as banks. Owing to rapid growth in internet banking usage, it is high time further research is carried out towards the most optimum user identification mechanism leading to its standardization.

VI CONCLUSION

In this paper, we have reviewed a number of security features used by different banks across the world for ensuring that the financial information of their end-user is safe. These have ranged from simple systems of a login id and password to fairly complex structures involving one time password generated through external hardware. Somewhere in between are systems involving additional information based of memorable words or other user information held by the bank. Banks, nevertheless, have a dilemma in introducing more layers of security as it leads to more difficulty for end-users in accessing and utilising their financial information. However, the spread in security features leads to difficulty in security testing of different banks as well as causes problems to users when they move from one institution to another. The learning curve associated with different types of security features could become a bottleneck in market diversity in future. Hence, there is a significant need for standardisation in the security mechanism used by banks.

REFERENCES

[1] A. Hiltgen, T. Kramp, and T. Weigold, "Secure internet banking authentication," *IEEE Security and Privacy*, vol. 4, no. 2, pp. 21–29, 2006.

[2] C. S. Weir, G. Douglas, T. Richardson, and M. Jack, "Usable security: User preferences for authentication methods in e-banking and the effects of experience," *Interacting with Computers*, vol. 22, no. 3, pp. 153 – 164, 2010.

[3] B. Suh and I. Han, "Effect of trust on customer acceptance of internet banking," *Electronic Commerce Research and Applications*, vol. 1, no. 3-4, pp. 247 – 263, 2002.

[4] P. Hanaek, K. Malinka, and J. Schafer, "E-banking security - comparative study," in *Security Technology*, ICCST 2008, 42nd Annual IEEE International Carnahan Conference on, 2008, pp. 326 –330.

[5] R. E. Ochuko, A. J. Cullen, and D. Neagu, "Overview of factors for in-ternet banking adoption," in *Proc. International Conference on Cyber Worlds, IEEE Computer Society*, September 2009.

[6] K. Hole, V. Moen, and T. Tjostheim, "Case study: Online banking security," *IEEE Security and Privacy*, vol. 4, no. 2, pp. 14–20, 2006.

[7] Online banking - catch 22, *Computer Fraud & Security*, vol. 2005, no. 4, pp. 1 – 2, 2005.

[8] J. Claessens, V. Dem, D. D. Cock, B. Preneel, and J. Vandewalle, "On the security of today's online electronic banking systems," *Computers & Security*, vol. 21, no. 3, pp. 253 – 265, 2002.

[9] S. Mohammadi and S. Hosseini, "Virtual password using Runge-Kutta method for internet banking," in *Proc. 2nd International Conference on Communication Software and Networks, IEEE Computer Society*, February 2010.

[10] N. Reavley, "Securing online banking," *Card Technology Today*, vol. 17, no. 10, pp. 12 – 13, 2005.

[11] M. Nilsson, A. Adams, and S. Herd, "Building security and trust in online banking," in *Proc. Human factors in computing systems. New York, NY, USA: ACM*, 2005, pp. 1701–1704.

[12] Nationwide introduces card readers for online banking, *Computer Fraud & Security*, vol. 2008, no. 4, pp. 4 – 5, 2008.

[13] S. Mathieson, "Barclays and Lloyds lead e-banking security," *Infosecurity*, vol. 4, no. 4, pp. 8 – 8, 2007.

[14] Consumers losing trust in online banking: survey, *Computer Fraud & Security*, vol. 2007, no. 2, pp. 4 – 4, 2007.

[15] C. Voice, "Online authentication: matching security levels to the risk," *Network Security*, vol. 2005, no. 12, pp. 15 – 18, 2005.

Bhaskar Choubey is a lecturer in University of Glasgow, UK. He received his doctorate from University of Oxford as a Rhodes Scholar and his Bachelor of Technology from Regional Engineering College, (now NIT) Warangal, with a Gold Medal for best out-going student. He has been awarded the IEEE Sensors Council's early career achievement award, DH Thomas award of the IET, the Raymond Davis scholarship of the Society of Imaging Science and Technology and the Myril B Reed best paper award from IEEE MWSCAS. He has been associated with

Somerville College, Oxford, Max Planck Institute of Brain Research, Frankfurt am Main; North West University, South Africa and the University of Sydney. His research interests include CMOS image sensor, nonlinear dynamics, human visual system and MEMS arrays.

Janardan Choubey is a professor of Mathematics in North Eastern Regional Institute of Science and Technology (NERIST) in Nirjuli, India. He obtained his bachelors and masters degrees from Patna University and his doctorate from Bhagalpur University. He served as a lecturer of Mathematics in Bhagalpur University and later in Siddhu Kanhu University, Dumka, wherein he was promoted to the readership in Mathematics. He was appointed a professor of Mathematics in NERIST in 1993, wherein in addition to his teaching duties, he has held the position of head of the department, dean as well of the department, dean as well as the acting director. During his directorship, he led the upgradation of NERIST to a deemed university status, the first of its kind in north east India. His research interest include number theory, information society and mathematics education.