IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 10, 2020, accepted January 20, 2020, date of publication January 30, 2020, date of current version February 6, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2970430

Towards Secure FinTech: A Survey, Taxonomy, and Open Research Challenges

SOBIA MEHRBAN[1], MUHAMMAD WAQAS NADEEM[1,2], MUZAMMIL HUSSAIN[1], MOHAMMAD MASROOR AHMED[3], OWAIS HAKEEM[1], SHAZIA SAQIB[2], M. L. MAT KIAH[4], FAKHAR ABBAS[1], MUJTABA HASSAN[1], AND MUHAMMAD ADNAN KHAN[2]

[1]Department of Computer Science, School of Systems and Technology, University of Management and Technology, Lahore 54770 , Pakistan
[2]Department of Computer Science, Lahore Garrison University, Lahore 54000, Pakistan
[3]Department of Computer Science, Capital University of Science and Technology, Islamabad 46000, Pakistan
[4]Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur 50603, Malaysia

Corresponding author: Muzammil Hussain (muzammil.hussain@umt.edu.pk)

ABSTRACT Financial Technology (FinTech) has attracted a wide range of attention and is rapidly proliferating. As a result of its consistent growth new terms have been introduced in this domain. The term 'FinTech' is one such terminology. This term is used for describing various operations that are being frequently employed in the financial technology sector. These operations are usually practiced in enterprises or organizations and provide requested services by using Information Technology based applications. The term does take into account various other sensitive issues, like, security, privacy, threats, cyber-attacks, etc. This is important to note that the development of FinTech is indebted to the mutual integration of different state of the art technologies, for example, technologies related to a mobile embedded system, mobile networks, mobile cloud computing, big data, data analytics techniques, and cloud computing etc. However, this technology is facing several security and privacy issues that are much needed to be addressed in order to improve the acceptability of this new technology among its users. In an effort to secure FinTech, this article provides a comprehensive survey of FinTech by reviewing the most recent as well as anticipated financial industry privacy and security issues. It provides a comprehensive analysis of current security issues, detection mechanisms and security solutions proposed for FinTech. Finally, it discusses future challenges to ensure the security and privacy of financial technology applications.

INDEX TERMS FinTech, security, privacy, cyber security, threats, fraud detection, Internet of Things.

I. INTRODUCTION

During the last decade, FinTech has seen an unrestricted and appreciative level of growth. This is entirely a new term, which describes the Financial Technology sector. It aims to execute various operations for regulating enterprises or organizations that mainly address the improvement in quality of services using Information Technology (IT) applications. It may be noted that FinTech developed by combining the strength of various other technologies, such as mobile embedded systems and their networks [1]–[6], trust management [7], [8], big data [9]–[11], data analytics techniques [12], [13], image processing [14], and cloud computing [15]–[19].

The associate editor coordinating the review of this manuscript and approving it for publication was Ahmed Farouk.

FinTech digitizes online banking services form the last few years. FinTech companies provide financial services independently to their customers. The FinTech industry provides an extensive range of digital financial services as shown in Figure 1.

However, it may be noted that FinTech provides a number of services to its users shows in Figure 1 but it faces security and privacy challenges mainly because of IT applications that it uses for providing the required services [20]–[25]. Besides, maintaining confidentiality, integrity, authorization and ensuring availability are additional challenges that FinTech needs to be considered for reliably completing its job. Without addressing these challenges, smooth and trustable integration of IT applications always remains under question mark which may eventually bring down the performance of FinTech.

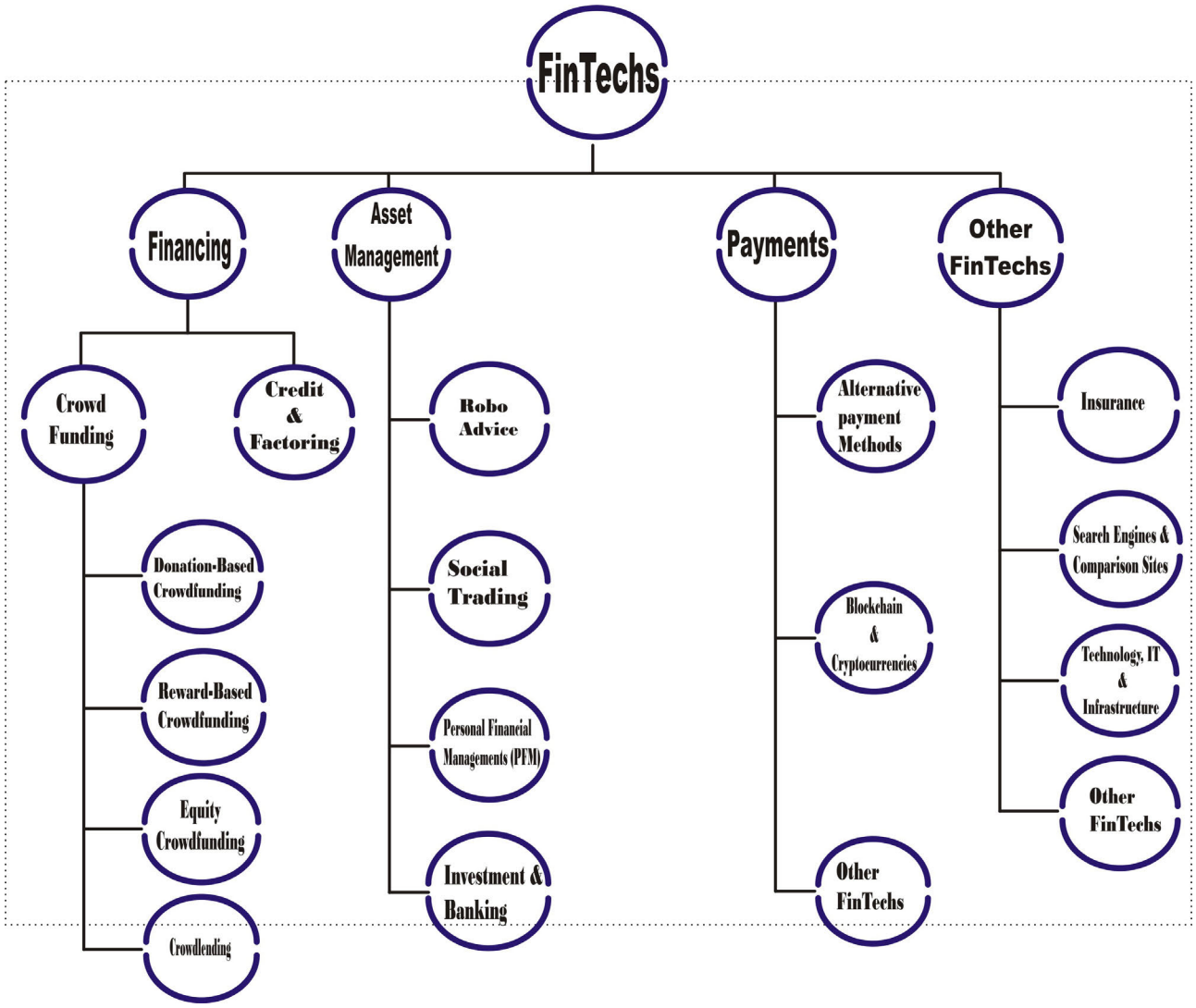

FIGURE 1. FinTech services.

Recently, most of the research expresses the major concerns on security and privacy while using the Financial Technology. According to Silicon Valley Bank reports, by [26] only 35% of companies are confident of their security, which mainly depends upon the employment of technology for achieving business objectives. Moreover, a detailed statistical report presented by Gartner [27] confirmed that, worldwide, cybersecurity has exhibited a huge amount of potential for attracting investment. These investments would be utilized for strengthening and utilizing security services and by the year 2020, an estimated amount of $170 billion is expected to be invested for this purpose. In fact, most of the modern FSIs are implementing and investing techniques related to IT, to enhance their financial services and safe delivery. Generally, in the financial industry, the existence of cyber threats on various layers of its technical process cannot be ruled out. The aforementioned problems elaborate on the importance of security in FinTech. Further, these security issues need serious consideration. These issues need to be addressed on a priority basis for users and enterprises that use financial technologies.

Recently, most of the research expresses the major concerns on security and privacy while using financial technology. According to Silicon Valley Bank reports, by [26] only 35% of companies are confident of their security, which mainly depends upon the employment of technology for achieving business objectives. Moreover, a detailed statistical report presented by Gartner [27] confirmed that, worldwide, cybersecurity has exhibited a huge amount of potential for attracting investment. These investments would be utilized for strengthening and incorporating security services by the year 2020. An estimated amount of $170 billion is expected to be invested for this purpose. In fact, most of the modern FSIs are implementing and investing techniques related to IT, to enhance their financial services and safe delivery. Generally, in the financial industry, the existence of cyber threats

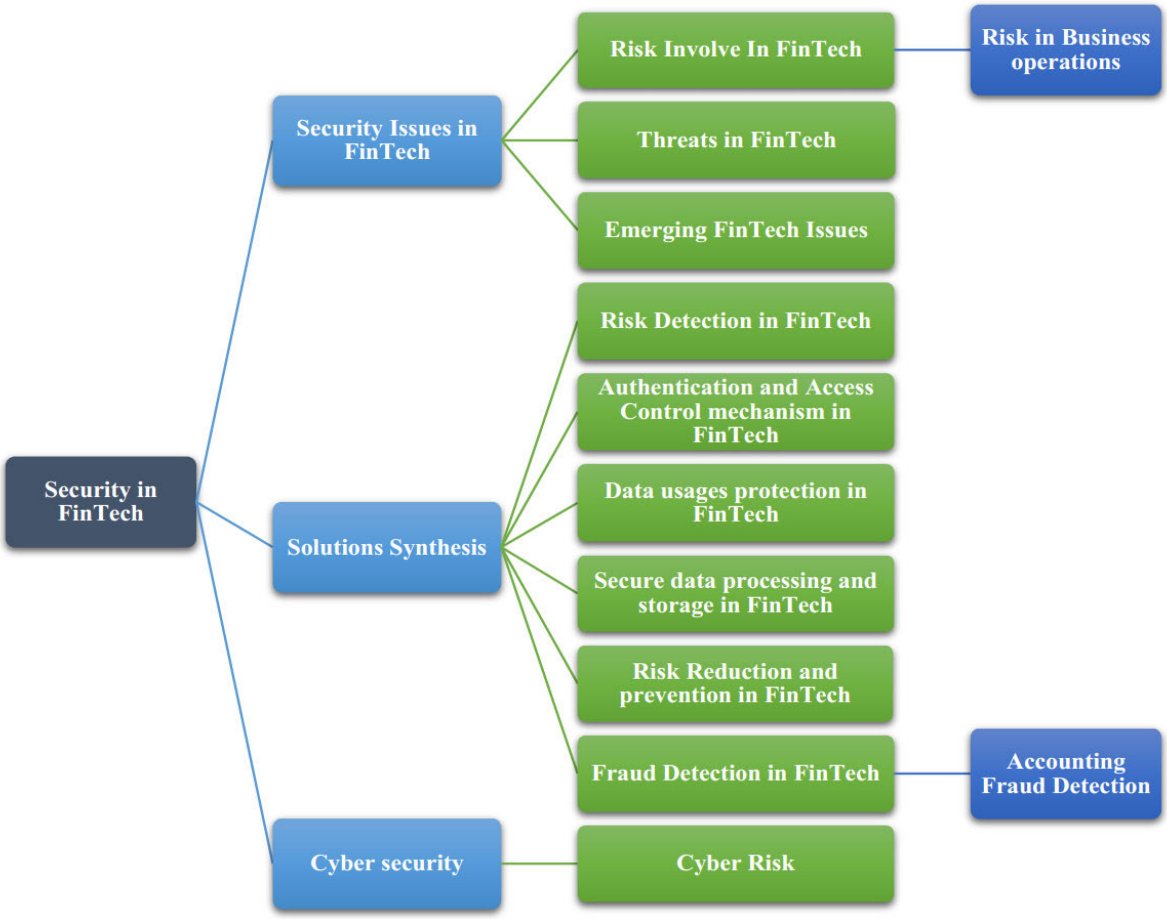

FIGURE 2. Mapping main security and privacy issues and technical solution in FinTech.

on various layers of its technical process cannot be ruled out. The aforementioned problems elaborate on the importance of security in FinTech, further, those security issues need serious consideration as well as those issues that need to be addressed on a priority basis for users and enterprises that use financial technologies.

Hence, the main objective of the paper is to survey the researcher's efforts in response to the latest innovations in technology and its applications, and mapping state of the art research on FinTech security into a taxonomy as shown in Figure 2. Several issues relating to privacy and security have been explored in this research including, threats to FinTech applications, proposed detection mechanisms, and various solutions proposed for the security and privacy of FinTech apps. Since 2010, researchers are doing much research on FinTech applications in a number of divergent ways. Regardless of their divergent categories, this study highlights various important challenges. These challenges are required to be addressed immediately as they influence the smooth employment of financial applications.

The security and privacy challenges are restricting the users to adopt the FinTech approaches and services and the state-of-the-art corresponding solutions are required to ensure the delivery of quality services and other technical dimensions.

The paper focuses on the main security and privacy issues in FinTech and presents a comprehensive survey of recent achievements. The main contribution of this work include:

1) This paper concisely focuses on two crucial aspects of FinTech and presents a solid survey. An inclusive knowledge of FinTech security and privacy issues has been presented that would help the professionals and researchers in the future.
2) The findings of this work highlight the notable security and privacy issues, and their solutions.
3) Future research directions have also been presented in this study.

This paper is organized in the following order. Section II describes the anonymous Communication System for FinTech. Section III elaborates on the security and privacy issues in FinTech. Section IV gives a brief description related to cybersecurity. Section V summarizes the potential and in-progress technical and synthesis solutions. Section VI presents a discussion and analysis phase. Section VII gives brief details regarding future research challenges in FinTech. Finally, the Conclusion is given in section VIII.

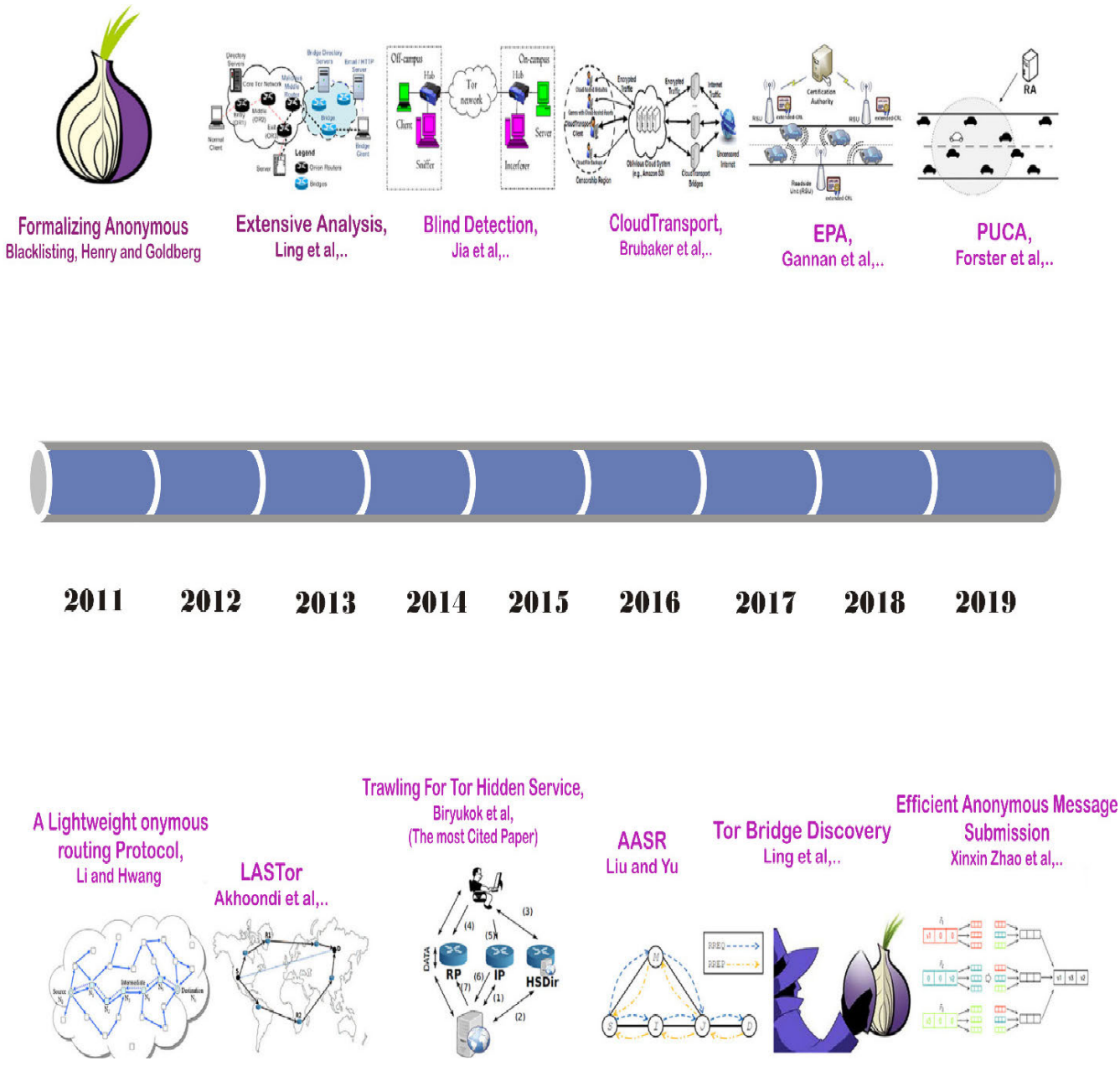

FIGURE 3. ACS development throughout recent years.

II. ANONYMOUS COMMUNICATION SYSTEM FOR FINTECH

Right now, Tor is undoubtedly the important Anonymous Communication System (ACS). A number of research articles have been evaluated for the study of Tor. Particularly, selection of path algorithm, refining anonymity, devices for different attack detection (DE anonymization, Sybil, cell-attack, etc.) whereas, examining the anonymity, the use of Tor in different applications, finding of Tor bridge, improving security and facilities are the main concerns in the literature [28]. Figure 3 shows the recent development in anonymous communication systems.

After Tor, Crowds is the next anonymous communication system that further considered with different 10 publications. The main research about this ACS is including with the study of anonymity [29]–[34], planning anonymous procedures for vehicular communications [35] and anonymous communication in a lossy network [36] or in MANETs [37]. Moreover, there is some other communication system including Mixes and Mixnet that have been studied with several 9 publications. Improving security and anonymity [38]–[42], presentation [36], [39], traffic inquiry [43] and assessment of anonymity [33], [42] are the ACS problems covered in the study [28]. AP3, ANODR (on-demand routing protocol for mobile ad

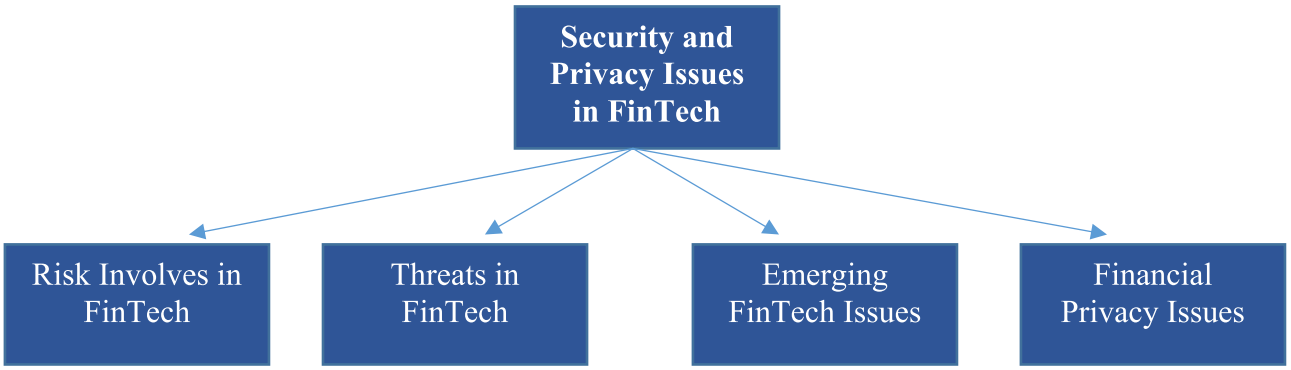

FIGURE 4. Four dimensions of security and privacy issues in FinTech.

hoc network), and Salsa are considered in four different studies. I2P has been presented in 2 research articles discussing its usage as an anonymous communication system [44], [45] whereas, Freenet is also considered in 2 different studies [46], [47]. On the other side THEMIS, ALERT, Cashmere, RAPS, and Torsk are also other anonymous communication systems that are being used in the industry. Further, Morphix [29], Tarzan [29], ANON [48], and Hordes [34] was also discussed. Above mentioned communications systems are being used in the financial industry.

III. SECURITY AND PRIVACY ISSUES IN FINTECH

Main security and privacy issues in FinTech have been described in four dimensions as shown in Figure 4. Which includes risk involve in FinTech, threats in Fintech, emerging FinTech issues and financial privacy issues. Detailed presentation on these dimensions are given in the following subsections.

A. RISKS INVOLVED IN FINTECH SERVICES

This section presents the security and privacy risks involved while using the financial technology services and applications. Security and privacy threat details are presented in the subsequent sections.

1) RISKS IN BUSINESS OPERATIONS

Every financial company desires to establish a secure business operating system to enhance its security level without installing much hardware resources [49]. Initially, when electronic transactions and networking techniques came into existence, the cyber concern in the financial industry was considered as a business operation issue [50]. Forming solid IT security strategies is always the main concern, in this regard variety of surveys have been presented [51], [52]. One of the surveys is about business operations which is related to the usage of different security techniques to protect their sensitive data.

Predicting and regulating the return and outcome of investment in security seems to be a complicated job. This issue was addressed in the latest investigation [53], this investigation concluded its findings by presenting an inflexible relationship existing between the return of security investment and the level of corresponding investment. This was further supported by another study [54], regarding the two main concerns that are, perceiving the level of privacy and implementing a corresponding trust mechanism. Both of these tasks are crucial as they are considered responsible for conducting an appreciative level of secure electronic transactions.

Recently, a study by Roumani *et al.* [55] examines whether the financial organization's records are protected or not against existing attacks. Further, the study also measured the potential influences on business scope, sales, performance and markets caused by potential security risks. Additionally, [56] has proved the level of IT transparency that can impact financial counseling encounters in a trustworthiness point of view. Overall, concerns of business operations derive from unidentified technicality and IT strategy making, camouflaged implementation process [26]. The prediction and monitoring of financial risks using intelligent agents is an example of applying FinTech for improving business operations [57]–[60]. Overall, most concerns of the business operations are derived from unknown technical details, masked implementation process, and IT strategy making. The concerns of business operation lead to some hidden technical parts. Figure 5 describes a diagram that maps the cyber concerns of business in the FinTech industry. Most cyber concerns for FSIs have arisen form cyber incident classification and masked technical complexity.

Moreover, cloud computing is popular as a web-based service model that has been extensively accepted by the FinTech industry [61], [62]. For example, Bank of America (BoA) has recently declared that Microsoft enterprise and financial firms are collaborating with each other to improve the financial transitions through the development of Blockchain technologies [49]. Cloud-based solutions increase the system performance by closely connecting financial businesses and their targeted markets [63], but this firm also introduced new threats and attacks due to outsourcing workload. The major concerns of using cloud-based solutions are; (a) lack of data controls in clouds that make mask complexity problems for FSIs [64], [65] because private clouds become mainstream in FinTech. For example, the FSIs may not know about

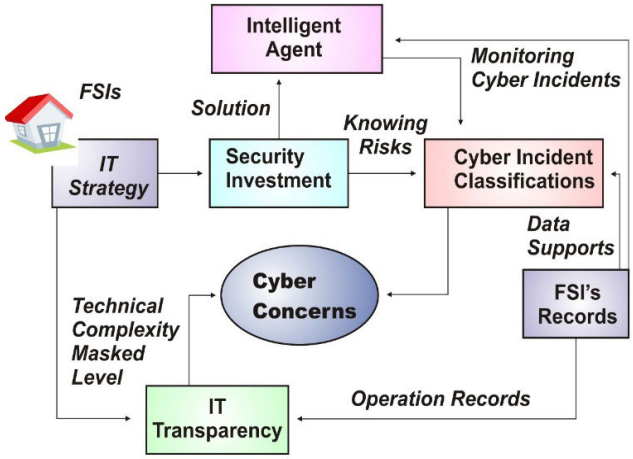

FIGURE 5. Diagram of cyber concern generations deriving from business operations in the financial industry.

the physical location of servers when using public clouds. The cloud-based servers store data remotely that still facing several threats since the participants of inter-crossed services and services on complicated networks bring a lot of vulnerability opportunities. The prediction and prevention of cyber risks in the cloud-based operating environment is a difficult job for cloud vendors and system designers. Finally, unpredictable vulnerabilities arise due to unanticipated and complicated communications between Virtual Machines (MV). Ni *et al.* [66] perceive that cloud date could be hampered due to active protocols vulnerabilities, even though the prior research has already explored various solutions. In short, the use of cloud computing in FinTech faces main threats including (a) complexity of the Web-based systems, (b) uncertainty of technical details and (c) lack of data controls.

B. THREATS IN FINTECH

Threats are the major issues in the financial industry that are continuously influencing the prevalent safety measures and dynamic behavior of the technology. Financial Service Institutes (FSIs) along with new service approaches also introduce new threats. The apparent cause of these threats may have adhered to the new security-related techniques or it may be caused due to new technical setup. Some of these risks can take the abuse form of data, network-traveling works, and malware, etc., these threats, which are usually created by the evolving techniques remained unsuspected in cloud computing. Besides masked operations further contribute to damaging cybersecurity infrastructure. It cripples the security mechanism and makes it ineffective against intrusions as a result of which information leakage takes place. The whole development leads to a financial crisis. ZAO, proclaimed that many banks had faced some serious issues of online data theft which led to losses of billions of dollars [26], [78]–[83].

This study proposes a novel preemptive schema that overcomes emerging financial operations threats by focusing on cybersecurity issues in mobile financial clouds, appearing in multiple manners.

C. EMERGING FINTECH ISSUES

This section describes the emerging issues that are faced by the financial industry.

1) REGULATORY REQUIREMENTS

Controlling and regulating compliances is one of the fundamental aspects and is significantly important for companies dealing with FinTech. It may be advantageous and at the same time, it may not be that much straight forward in terms of its regulation by the government authorities. To fully understand these achievements without becoming an entity of the regulating compliances, it was considered important to have a detailed investigation of the underlying business model and this investigation was conducted by FinTech. Though this attempt is more complicated to evaluate in order to make sure that whether these attempts fall within the government regulations and if yes, how to apply numerous requirements [84].

2) IMPORTANCE OF EXPERIMENTAL DATA

Data is the most important asset to the business models of various FinTech regardless of either they are focusing on, capital investment or retail banking. Many companies succeeded to overcome risks and created new opportunities by innovating new business visions from financial services data. Powerful algorithms and exponential processing power are needed for the analysis of such important data. Trust of consumers and stakeholders is equally important for companies. Transparency and security concepts are important principles in the industry for the FinTech sector. Many Authorities, like the directives dealing with payment services, the model of retail banking practiced in UK and Monetary Authority of Singapore are giving a huge amount of importance with the data so that any required changes can be conveniently introduced in conventional banking system which usually works over the concept of mutual integration [84].

3) PROTECTING INNOVATION

The innovative technology and software development by FinTech companies is growing rapidly. Legal protection is having keen importance in FinTech success yet there is a lack of protection since protection availability by legal authorities varies from country to country. While business practices in the US, are thought to be patentable, however, due to existing case laws the process seems to be difficult. Whereas in Europe the situation is different, i.e. the same business methods are not patentable. FinTech companies can play their role in protecting these innovations, however, for that matter; there is a need to have ownership of IP rights. Some of the important rights are trade secrets and copyright. Other than that, they should protect themselves by arranging safe contracts with their customers, suppliers, third parties and employees [84]. Blockchain is one of the solutions for the protection of ideas, and this technology will encourage industry-wide adoption.

4) INTRODUCING INNOVATION THROUGH COLLABORATION AND INVESTMENT

Financial institutions that are well established are perceived to be capable of bringing innovation to the market. This innovation inevitably provides a wide range of financial and business benefits. Financial institutions have to frequently experience affiliating with emerging technology players to bring frequent enhancements in the innovation cycle. To make these transactions fruitful, both parties need to conclude the accommodation of objectives and what makes two organizations differ from each other [84]. This relationship actively impacts the cooperation of any deal, and how the profits of the deal are structured.

5) FUNDING SOURCES

Financial businesses are growing very rapidly. This rapid growth of private companies has successfully accomplished either due to more private funding in number or larger private funding rounds, and in some cases, both are considered. Instead of capital investment by throwing more cash from private investors the aforementioned funding enables these companies by direct funding and due to which rapid growth is experienced. Some of the investors expanded by participating in the late-stage rounds of the private companies. Independent wealth funds and corporate project funds are examined, which actively participate in the financial market. There are a few reasons for joining the market by the aforementioned investors that range from simple collection through opportunities to identify the nature and innovation to build new research insights. The basic question arises for the companies who stay private for longer duration and for the wide number of investors operating in the market, needing help regarding the right investment option for them [84].

D. FINANCIAL PRIVACY PROTECTION ISSUES IN FINTECH

In FinTech security, privacy protection is considered as the most significant and critical aspect of the production of data privacy strategies [67]. A Machine Learning (ML) based method implement to evaluate the trade-off between privacy protection and data usages [68]. K-means clustering algorithm has been used to discern the data-carrying privacy out of the multi-party clustering scenario in the proposed ML-based method. Furthermore, location-based services commonly carry user's movement privacy, such that devices and applications have become common attack targets [19], [69]. Additionally, a Privacy-Preserving Location-Based Service (LBS) framework based on fine-grained access control and transformation technique proposed by Li *et al.* [70], which supports the query area around the user location and allows filtering out the redundant encrypted records in a blind way. Hence, the level of privacy protection is increased by the fine-grained approach but the problem of time latency is restricting the applications in FinTech [71], [72].

Finally, new FinTech services bring new security and privacy concerns [73]. For example, the implementation of financial insurance impact on FinTech service organizations in making IT-related decisions, like cybersecurity insurance [74]. The understanding of cyber risks and discriminating relationship between insurance and cyber incidents are a challenging problem for many FinTech companies that are strongly attached to the Web-based applications. Consequently, financial frauds are other emerging issues in FinTech while using electronic approaches [75]. The traditional fraud detection approaches and methods typically relied on statistical methods [76], [77], which is insufficient to find out the continuous real-time deception happenings.

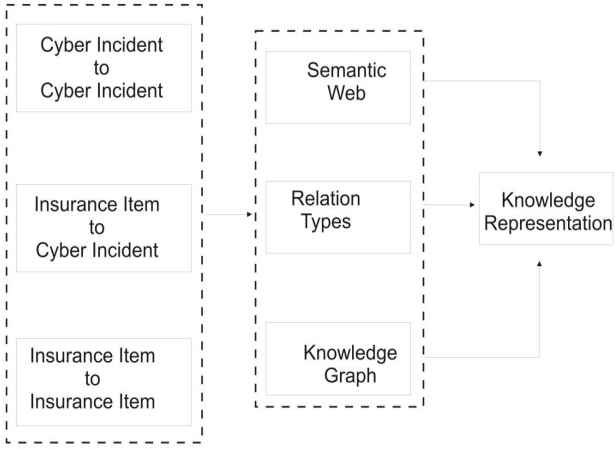

FIGURE 6. The architecture of the Semantic Cyber Incident Classification (SCIC). Source: [85].

IV. CYBERSECURITY

In an emerging industry, the cybersecurity sector has been proliferating which primarily serves the financial market and helps financial organizations to reduce cybersecurity risks. In cybersecurity, risk classification is an important factor however, classification representation becomes complex when the service model becomes large. Figure 6 presents an architecture for the classification of cyber incidents. Financial loss or operational mistakes occur when the presentation of risks is improper. Cybersecurity becomes a good option for FSIs to alleviate risks of cyber occurrences that increases the success rate of defending cyber-attacks. Cybersecurity risks have been considered as one of the significant issues in multiple fields. The financial industry has critical concerns, when a) FSIs are applying network-based solutions, b) higher-level security is required in the financial industry. The exponentially growing demand for digital data storage has enabled so many new technologies implementation such as the Internet of Things (IoT), cloud computing [62] and big data [11]. The latest development in technology merges virtualization and distributed storage [85], without caring for any geographical limitations. It makes data transmission and storage operated over guided and unguided media-based network systems and sharing, possible. This change in the world of technology not only empowers the financial companies but also brings a wide range of challenges to financial firms [85].

A. CYBER RISKS

There are a number of cyber risks threatening Financial Service Institutes (FSIs). The basic knowledge and sensitivity of cyber risks can significantly contribute to avoiding cyber threats. The classification of cyber risks is a difficult job. This difficulty mainly arises due to the presence of wide cross disciplines and due to complex entity to entity relationships. A critical look at current financial firms reveals that the known cyber risks can be divided into three layers; namely, operational, tactical and strategical. To protect information three aspects may be relied upon, i.e., confidentiality, integrity, and availability.

V. SOLUTIONS SYNTHESIS

A number of scholars have presented a wide range of researches related to securing data. Various researchers mainly focus on the FinTech industry and some other study the universal solutions to privacy and security problems. In this section, we synthesize the most recent achievements that are related to FinTech-oriented solutions or protection methods and techniques that can be applied in the FinTech industry. Figure 7 describes the technical mapping of the main techniques for privacy and security solutions.

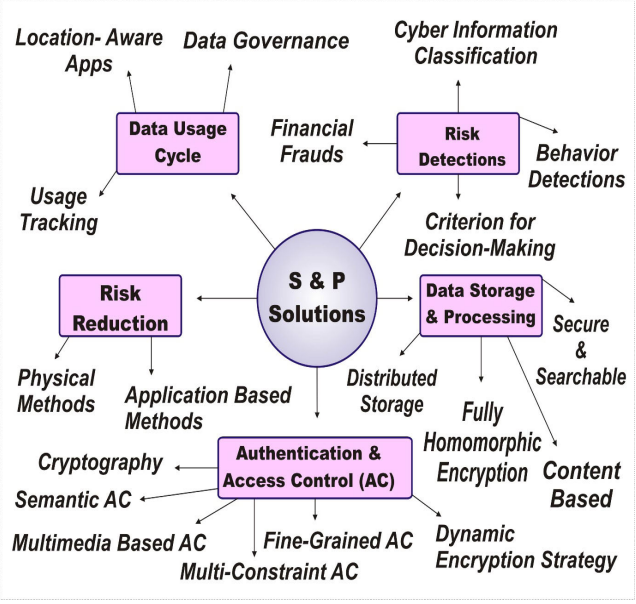

FIGURE 7. Technical mapping for security and privacy solutions.

A. RISK DETECTION IN FINTECH

The exponential growth of the internet of things (IoT) and cloud computing has empowered cyber risk management by offering flexibility in the deployment of different services, in both centralized and decentralized manner. One of the latest research [85] has proved, that in the financial industry, the cloud-based cyber risk management system can support cyber-related information. The study is based on realistic data to classify cyber instances and aligning them to business using semantic technique. Financial frauds, on the other hand, frustrate the FSIs, Glancy and Yadav [86] proposed a model for sensing financial fraud. A quantitative approach is used by focusing on the fraud experienced based on textual data. Yet, the quantitative analysis could not guarantee the accurate detection of fraud, that means the model failed to distinguish suspected transaction though, that can be used as a supporting tool [3]. Another study [86] suggested a method to analyze financial risk by using multiple standard decision making to pick clustering algorithms. Moreover, an alternative approach, correlation coefficients analysis is proved by a study [87], [88]. The correlation coefficient can detect improper activities by the value deriving from multiple elements. Recent work on financial risk detection has been proposed after applying state analysis techniques.

B. AUTHENTICATION AND ACCESS CONTROL MECHANISM IN FINTECH

Cryptography based approaches are used by many FSIs for access controls and authentications. Moreover, the alternatives used for securing financial information, need novel security mechanisms to establish access control throughout the multimedia [89]. Ontology techniques have identified the semantic access, associated with the service seeker's features. Semantic-based access control, supported by multimedia can achieve the goal of achievements in financial service. Another study based on ontology solution [89] was proposed to support the cybersecurity ecology by implementing the knowledge graph to prove the relation between different cyber risks. Though, there are some limitations. Gai et al. ontology-based approaches in the precision of access controls, however, when the system of ontology is large enough it reaches perfection, which again is too hard to achieve. Furthermore, many studies previously conducted on the same issues recommended many developing limitations for data accesses. One of the proposed approaches [89] also includes biometric authentication taking three-dimensional limitations under considerations in proposing protection strategies, such as privacy, security, and trust. In order to increase efficiency in protection by using biometric technologies, researchers concluded trade-off from these three aspects. However, in many scenarios, this approach is restricted, as in different conditions these three dimensions i.e. privacy, security and trust have vague boundaries. This is also a very challenging issue to tune the protection mechanism. It takes a long time and maintenance. Thus biometric authentication mechanisms are usually not feasible for most of the financial applications and services [89]. Moreover, for data encryption, researchers also have developed some methods to determine the dynamic strategy of data protection. Among those methods, an approach presented in [90] was developed based on privacy classification which selectively encrypts data with privacy weights based on fixed time intervals. This approach maximizes the total privacy weight value, which is considered as an optimal solution in this regard.

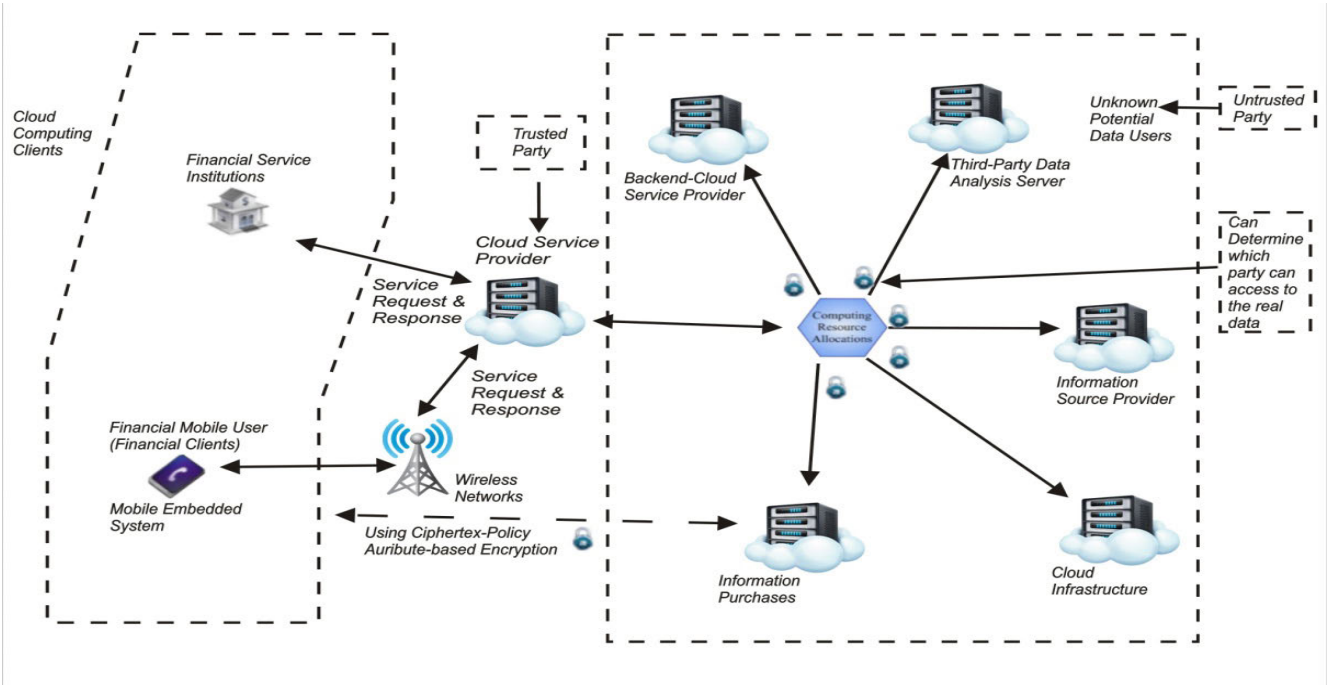

FIGURE 8. Architecture of Proactive Dynamic Secure Data Schema (P2DS) Source: [98].

Additionally, the fine-grained access control mechanism is also one of the important solutions to secure data storage [91], [92]. This mechanism also implements a cloud-based environment. Bugiel *et al.* [93] have proposed a fine-grained policy-based access control mechanism that follows the security and privacy policies on Android. The policy-based access control mechanism also applied in various need-based scenarios, such as content sharing and assured data deletions [94]. The fine-grained access control mechanism is also used to achieve the attribute-based keyword searching when multiple consumers encrypt and store data on cloud-based servers [95]. Furthermore, the fine-grained mechanism utilizes to form owner-oriented access policies.

In short, the main trade-off of security access in FinTech applications is due to the conflict of services performance and security. Presently, FSIs mostly aim to provide maximum security and financial customer's privacy to protect all its transactions.

C. DATA USAGES PROTECTION IN FINTECH

Generally, the importance of data usage in financial service institutions is emphasized because of the direct relation of its performance with service quality. Governing data becomes more complicated with an increase in size or when new functions are added [90]. One issue addressed by a research direction is to protect FinTech by preventing data risks from malicious activities which most of the time are launched by the third party when they have access to data in the cycle. Many studies discovered a variety of methods for risk reduction at the time of data transmission or sharing at the time of sharing the data between different parties. A study, [90] by Chang et al. proposed a Business Process Modeling Notation (BPMN) used to differentiate the processes and implementation of data usage. Another study [96] conducted with taking the perspective of the business process under considerations, yet focused on payments. This study highlighted the loopholes due to poor business process models and incorrect control flows.

Likewise, Xiao *et al.* [97] implemented a delivering location-aware security system without using the key sharing technique. In this approach, the temporal, location and authentications based on proximity and privacy issues are utilized quite well. So far, this work was not able to achieve an error-free goal since it has a radio propagation property. Another study [96] developed a scheme for the privacy protection of grouping mobile users. The location of data carrying the information is not needed to be shared very frequently in this method, as all members of the user are grouped together on the basis of locations. So, this method is not implemented because of the geographical location which is dynamic [96]. Therefore, risks in the usage of data cycle mainly come from few dimensions including; unexpected third-party involvement, a wide range of distributed usage and unclear business processes.

D. SECURE DATA PROCESSING AND STORAGE IN FINTECH

Dynamic Secure Data Scheme (P2DS) shown in Figure 8 is a proactive scheme, which was designed for the protection of sensitive financial data within a lively operational context. This study is based mainly on previous work [98]. To improve

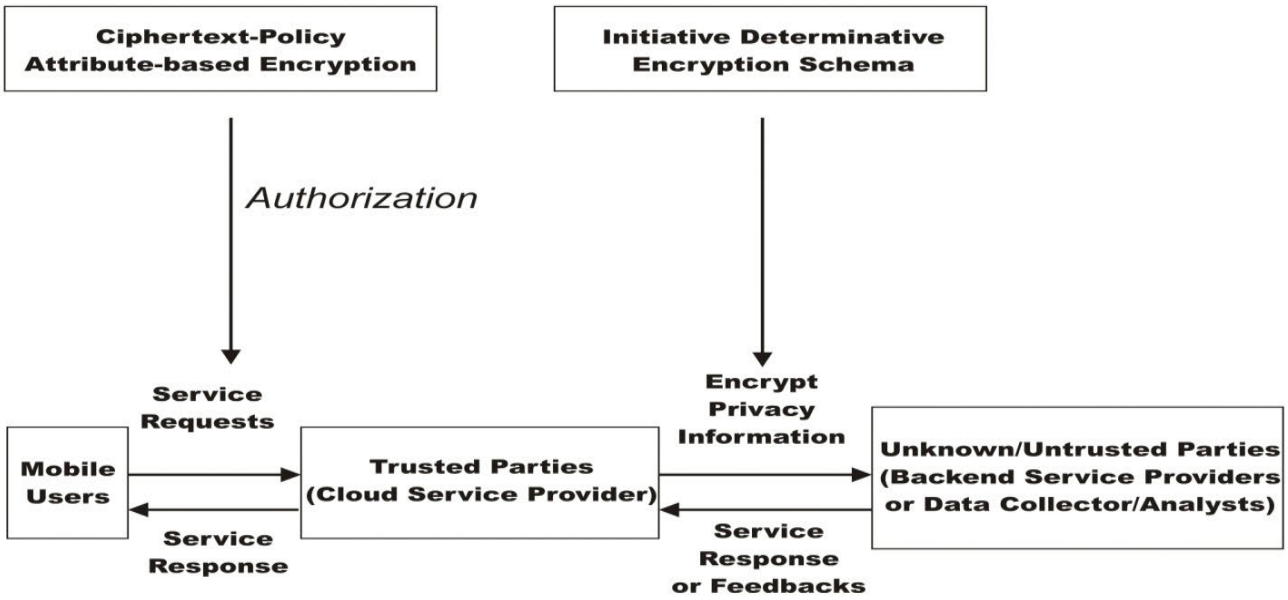

FIGURE 9. The process of using the proposed schema in operating a mobile transaction Source: [98].

data processing and security in data storage, it is the most important research area in FinTech. Another process model is shown in Figure 9 proposed for secure mobile transactions. Additionally, Gai *et al.* [85] proposed a mechanism by moving the data storage to cloud systems. In this approach, cloud systems have been applied and have focused on two major challenges that are internal as well as the external attackers who are always associated with cloud storage systems. Before transmitting the sensitive data on the network, it is divided into two main parts, to protect the privacy even though all transmissions are monitored by the adversaries. By adding a judgment process this approach can further be strengthened, which is required by the data to determine distributed storage [99]. With large data volume, the improvement is an optimization, to decrease the load on the network. Moreover, some scholars focus on privacy assured searchable data storage in cloud computing.

One of the recent studies [100] covered all three functions by implementing symmetric key encryption, such as ranking results, searching structured data and identifying similarities in data. The method allows data sharing in an encrypted fashion in distributed service deployment. Furthermore, previous studies related to privacy, besides exploring text-based storage, also investigated the images in cloud computing. For instance, a study [100] used a scheme that implements a Content-Based Image Retrieval (CBIR) technique. This scheme encrypts the images prior to storing on cloud servers. Precisely, FSIs try to achieve a higher level of protection in case of data, no matter how and what technologies or techniques are selected. One of the observations by different research articles is that centralized processing and data storage can overcome risks at server-side, however, a very limited impact on security improvement is observed during data

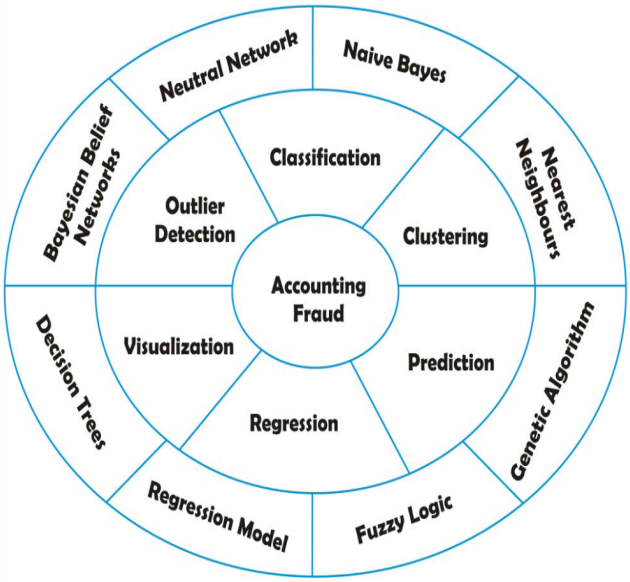

FIGURE 10. The Conceptual Framework for Application of Data Mining to FAFD Source: [85].

exchange. Currently, decentralized data processing and data storage is facing challenges in different areas like, database abuses and communication monitoring. Thus, financial data securing is allied with data protection in data exchange and all other existing threats associated with web should be considered for FinTech.

E. RISK REDUCTION AND PREVENTION IN FINTECH

Generally, in risk management, there are two methods i.e. reduction and prevention that are, application-based and physical methods. Among them, the application based

method is the solution to attain security solutions by implementing different cryptographic methods, like secure protocol creation for access controls [101]. An example of this method is, using the alternative of forming an access control rule for social data exchange of the local authorization language [102].

Whereas, the physical method is an approach of data security by applying operations on infrastructure physically. These operations avoid network damage or prevent the jamming attack. Other than these methods, many studies are conducted to reduce cyber risks. This study also proposed and developed new technologies. The first development is the preemptive protection approach which is a substitute for risk reduction. One scheme was proposed by a study that protects the privacy of the financial customers, using attribute-based access control [98]. Only trustable parties are allowed to either partially or fully decrypt their data. Improvement in this approach is made by semantic web implementation such that data owners and unknown third parties can be clarified [78]. Nonetheless, the configuration of the approach is needed to define trusted third parties by the owner of the data that means it creates an extra workload as they have authentications for their own trusted parties. This production of financial selection can be influenced by many elements when there are having a substitute and a service choice available. Proper decision making on financial solutions, some latest studies have developed applicable solutions under some limitations. For instance, a study weighted that a hundred percent of the financial services available and all of them measured coefficients to attain the optimized results for choosing the service [103]. Another study [35] also focuses on service items that established a mean to classify cyber risks. This study impacts the classification of cyber risks by using semantic techniques. Semantic techniques create a knowledge representation graph. The study [35] was further enhanced [104] and applied Monte Carlo simulations to analyze the data more efficiently considering the security framework. Furthermore, several studies previously focused on physical locations for risk reduction. Gai *et al.* [104] implemented Radio Frequency ID (RFID) based applications to increase security. The approach basically takes geographical information under consideration that is related to data. Thus, the financial transaction will be denied in case of any movement detection related to abnormal location. The constraint of this approach is its mechanism which highly depends on RFID techniques and adversaries' detection accuracy is under debate. Another research [104] developed a protocol for authentication of RFID which used a hash function to check the authentication of data. This method of using a hash function for secure RFID is used in many other studies [104] as well. In securing financial data, protecting the hashtags is one of the crucial parts. In short, unless the opposition attacks, it is very difficult for system administrators and FSIs to detect potential cyber risks from new emerging technologies and their applications. The simplest solution is, to understand the dynamic system and reduce attacks by business processes and perceptive technical details.

F. FRAUD DETECTION IN FINTECH

Commercial fraud, which is not restricted to the well-advertised case of HealthSouth, WorldCom, and Enron etc. is common. Since, all Accounting and Audit Enforcement Releases (AAERs), have been examined and concluded with the detection of fraud that was neglected by senior management and was found after a few years. It was not detected proactively by the Security and Exchange Commission (SEC). Commercial America lost its confidence due to frequent fraud patterns. Both auditing and academic firms of corporate America experimenting to detect these frauds a study [37] inspected many business areas. In reporting the detection of financial fraud, quantitative approaches did very little to inspect the textual data. Phua et al. concluded fraud research into four primary areas: telecommunications, credit card, internal fraud and insurance. Most employees are involved in internal fraud since financial reporting fraud does not focus on senior management. Financial ratios are used in many studies to detect financial fraud reporting, applying different methodologies collecting fluctuation in results though [86], [105]–[108], Phua et al. summarized that unstructured use of data in fraud detection is principally unmapped.

G. ACCOUNTING FRAUD DETECTION

Economically, the buzz of financial fraud is becoming a serious issue and at the same time, effective detection of fraud is required. Until now, it is a very difficult task for accounting professionals [109]. One of the demanding activities is internal auditing of financial activities in the corporate world. Book keeping accounting practices are applied across the globe for detecting financial frauds [108]. Detection of accounting fraud is a complex task that is done by using traditional internal audit methods and in fact, it is a very difficult task [110]. A vital role played by forensic accounting in detecting internal frauds is very difficult as one has to execute the audits by employing specialist's accounting and investigative skills [75], [111], [112]. Figure 10 shows a conceptual framework for the application of data mining to Financial Accounting Fraud Detection (FAFD).

VI. DISCUSSION AND ANALYSIS

The world is becoming more and more interconnected due to an abundance of technology and FinTech has the most inspiring technology amongst those technologies. As security has the key importance in FinTech so, the importance of security is also discussed in this article. Many leading security consultants and firms have been focusing on providing secure solutions regarding FinTech. Several issues relating to privacy and security have been explored in this research including, threats to FinTech applications, proposed detection mechanisms, and various solutions proposed for the security and privacy of FinTech apps. This study has the main emphasis on the issues regarding privacy and security. Additionally, it provides a vision for understanding FinTech

from new efficient researches. Moreover, this study focuses on two important aspects of FinTech, (a) fundamental issues in privacy and security and (b) and the growing techniques in FinTech. Hence, the main objective of the paper is to survey the researcher's efforts in response to the latest innovations in technology and its applications, and mapping state of the art research on FinTech security into a taxonomy. With big data and cloud technology emerging, the need for security becomes more important as it has been projected that by 2025 threat of cyber-attacks would increase exponentially, thus posing a threat to secure FinTech. Usually, the emphasis is on the use of data in financial services, since its performance has a direct relationship with the service quality. As discussed above this article provides valuable information regarding the security of FinTech that can be used in studies relating to securing instruments that are useful in financial technology. There is a dire need for FSIs to come up with new technology that can make them less vulnerable to attacks and threats. FinTech is an active area of research. Hopefully, the current study will help the reader in creating a higher degree of understanding about essentials of FinTech, the chance for its smooth addition into the present systems and more significantly the holes are there which are restrictive the extraction of its potential benefits.

VII. FUTURE RESEARCH CHALLENGES

As FinTech is a new technology so, a lot more work is needed to improve the existing solutions. The security and privacy of the financial technology applications need to have the trust and acceptability of FinTech amongst its users. A comprehensive framework to ensure the security and privacy of FinTech may be proposed by researchers in the future using the findings of this research. Furthermore, there must be some clear policies to use FinTech applications and services, since the user of these applications and services are usually not technically experts to handle security challenges. Therefore, in response to this, a policy recommendation framework could be a feasible solution for FinTech users.

VIII. CONCLUSION

A recent disruptive trend in technology has a huge impact on the financial sector and on its related services. Consequently, technology has dramatically changed the way of operating the financial industry. Research on this proliferating trend is already very active, though its shape and outlines are still not understood, and insight on what is actually being presented on this emerging technology is needed at the current stage. This study aims to build awareness, through surveying and taxonomizing the literature. This article proposed taxonomy on current security issues, detection mechanisms and security solutions for FinTech after providing a comprehensive survey of FinTech through reviewing recent research related to the financial industry security and privacy issues. This paper discusses the proposed schemes for the security and privacy of Financial Technology in detail. At last, future research challenges are discussed to provide future directions towards this new era of technology.

REFERENCES

[1] Y. Zhang, R. Yu, S. Xie, W. Yao, Y. Xiao, and M. Guizani, "Home M2M networks: Architectures, standards, and QoS improvement," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 44–52, Apr. 2011.
[2] K. Gai, L. Qiu, M. Chen, H. Zhao, and M. Qiu, "SA-EAST: Security-aware efficient data transmission for ITS in mobile heterogeneous cloud computing," *ACM Trans. Embed. Comput. Syst.*, vol. 16, no. 2, pp. 1–22, Jan. 2017.
[3] S. Wen, W. Zhou, J. Zhang, Y. Xiang, W. Zhou, and W. Jia, "Modeling propagation dynamics of social network worms," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 8, pp. 1633–1643, Aug. 2013.
[4] J. Zhang, C. Chen, Y. Xiang, W. Zhou, and Y. Xiang, "Internet traffic classification by aggregating correlated naive Bayes predictions," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 5–15, Jan. 2013.
[5] Y. Zhang and B.-H. Soong, "Performance evaluation of GSM/GPRS networks with channel re-allocation scheme," *IEEE Commun. Lett.*, vol. 8, no. 5, pp. 280–282, May 2004.
[6] K. Gai, M. Qiu, L. Tao, and Y. Zhu, "Intrusion detection techniques for mobile cloud computing in heterogeneous 5G," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3049–3058, Nov. 2016.
[7] Q. Zhang, L. T. Yang, and Z. Chen, "Privacy preserving deep computation model on cloud for big data feature learning," *IEEE Trans. Comput.*, vol. 65, no. 5, pp. 1351–1362, May 2016.
[8] J. Abawajy, G. Wang, L. T. Yang, and B. Javadi, "Trust, security and privacy in emerging distributed systems FGCS," *Future Gener. Comput. Syst.*, vol. 55, pp. 224–226, Feb. 2016.
[9] K. E. Psannis, C. Stergiou, and B. B. Gupta, "Advanced media-based smart big data on intelligent cloud systems," *IEEE Trans. Sustain. Comput.*, vol. 4, no. 1, pp. 77–87, Jan. 2019.
[10] A. P. Plageras, K. E. Psannis, C. Stergiou, H. Wang, and B. Gupta, "Efficient IoT-based sensor BIG Data collection–processing and analysis in smart buildings," *Future Generation Comput. Syst.*, vol. 82, pp. 349–357, May 2018.
[11] H. Yin and K. Gai, "An empirical study on preprocessing high-dimensional class-imbalanced data for classification," in *Proc. IEEE 17th Int. Conf. High Perform. Comput. Commun., IEEE 7th Int. Symp. Cyberspace Saf. Secur., IEEE 12th Int. Conf. Embedded Softw. Syst.*, Aug. 2015, pp. 1314–1319.
[12] M. Qiu, D. Cao, H. Su, and K. Gai, "Data transfer minimization for financial derivative pricing using Monte Carlo simulation with GPU in 5G," *Int. J. Commun. Syst.*, vol. 29, no. 16, pp. 2364–2374, Nov. 2016.
[13] T. Lee and H.-W. Kim, "An exploratory study on fintech industry in Korea: Crowdfunding case," in *Proc. 2nd Int. Conf. Innov. Eng. Technol. (ICIET)*. Bangkok, Thailand, 2015, pp. 1–7.
[14] A. Castiglione, A. De Santis, and C. Soriente, "Taking advantages of a disadvantage: Digital forensics and steganography using document metadata," *J. Syst. Softw.*, vol. 80, no. 5, pp. 750–764, May 2007.
[15] C. Stergiou, K. E. Psannis, A. P. Plageras, Y. Ishibashi, and B.-G. Kim, "Algorithms for efficient digital media transmission over IoT and cloud networking," *J. Multimedia Inf. Syst.*, vol. 5, no. 1, pp. 27–34, 2018.
[16] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure integration of IoT and cloud computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 964–975, Jan. 2018.
[17] A. Castiglione, R. Pizzolante, A. De Santis, B. Carpentieri, A. Castiglione, and F. Palmieri, "Cloud-based adaptive compression and secure management services for 3D healthcare data," *Future Gener. Comput. Syst.*, vols. 43–44, pp. 120–134, Feb. 2015.
[18] K. Gai, M. Qiu, and H. Zhao, "Energy-aware task assignment for mobile cyber-enabled applications in heterogeneous cloud computing," *J. Parallel Distrib. Comput.*, vol. 111, pp. 126–135, Jan. 2018.
[19] Y. Li, W. Dai, Z. Ming, and M. Qiu, "Privacy protection for preventing data over-collection in smart city," *IEEE Trans. Comput.*, vol. 65, no. 5, pp. 1339–1350, May 2016.
[20] G. Li, J. S. Dai, E.-M. Park, and S.-T. Park, "A study on the service and trend of Fintech security based on text-mining: Focused on the data of Korean online news," *J. Comput. Virol. Hacking Tech.*, vol. 13, no. 4, pp. 249–255, Nov. 2017.
[21] H. Stewart and J. Jürjens, "Data security and consumer trust in FinTech innovation in Germany," *Info Comput. Secur.*, vol. 26, no. 1, pp. 109–128, Mar. 2018.

[22] G. Dorfleitner and L. Hornuf, *FinTech and Data Privacy in Germany*. Springer, 2019.

[23] T. Okamura and I. Teranishi, "Enhancing FinTech security with secure multi-party computation technology," *NEC Tech. J.*, vol. 11, no. 2, pp. 46–50, 2017.

[24] W. Meng, L. Zhu, W. Li, J. Han, and Y. Li, "Enhancing the security of FinTech applications with map-based graphical password authentication," *Future Gener. Comput. Syst.*, vol. 101, pp. 1018–1027, Dec. 2019.

[25] S. H. Lim, D. J. Kim, Y. Hur, and K. Park, "An empirical study of the impacts of perceived security and knowledge on continuous intention to use mobile FinTech payment services," *Int. J. Hum.–Comput. Interact.*, vol. 35, no. 10, pp. 886–898, Jun. 2019.

[26] K. Gai, M. Qiu, X. Sun, and H. Zhao, "Security and privacy issues: A survey on FinTech," in *Proc. Int. Conf. Smart Comput. Commun.*, 2016, pp. 236–247.

[27] S. Morgan, *Cybersecurity Market Reaches $75 Billion in 2015; Expected to Reach $170 Billion by 2020*. Jersey City, NJ, USA: Forbes, 2015.

[28] M. A. Nia and A. Ruiz-Martínez, "Systematic literature review on the state of the art and future research work in anonymous communications systems," *Comput. Electr. Eng.*, vol. 69, pp. 497–520, Jul. 2018.

[29] J. Zhang, H. Duan, W. Liu, and J. Wu, "Anonymity analysis of P2P anonymous communication systems," *Comput. Commun.*, vol. 34, no. 3, pp. 358–366, Mar. 2011.

[30] L. Kang, "Efficient botnet herding within the Tor network," *J. Comput. Virol. Hacking Techn.*, vol. 11, no. 1, pp. 19–26, Feb. 2015.

[31] A. Panchenko, "On the impact of cross-layer information leakage on anonymity in crowds," in *Proc. 11th ACM Symp. QoS Secur. Wireless Mobile Netw.*, 2015, pp. 35–42.

[32] S. Zhioua, "Analyzing anonymity attacks through noisy channels," *Inf. Comput.*, vol. 244, pp. 76–112, Oct. 2015.

[33] T. Mhamdi, O. Hasan, and S. Tahar, "Evaluation of anonymity and confidentiality protocols using theorem proving," *Form Methods Syst. Des.*, vol. 47, no. 3, pp. 265–286, Dec. 2015.

[34] G. Danezis and E. Käsper, "The dangers of composing anonymous channels," in *Proc. Int. Workshop Inf. Hiding*, 2012, pp. 191–206.

[35] C. Gañán, J. L. Muñoz, O. Esparza, J. Mata-Díaz, and J. Alins, "EPA: An efficient and privacy-aware revocation mechanism for vehicular ad hoc networks," *Pervas. Mobile Comput.*, vol. 21, pp. 75–91, Aug. 2015.

[36] A. Mishra and P. Venkitasubramaniam, "Admissible length study in anonymous networking: A detection theoretic perspective," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1957–1969, Sep. 2013.

[37] W. Fang, J. Wang, Z. Shi, F. Li, and L. Shan, "A study on anonymous communication technology in MANET," in *Proc. Int. Conf. High Perform. Comput. Appl.*, 2015, pp. 73–81.

[38] J. Campos, C. T. Calafate, M. Nácher, P. Manzoni, and J.-C. Cano, "HOP: Achieving efficient anonymity in MANETs by combining HIP, OLSR, and pseudonyms," *EURASIP J. Wireless Commun. Netw.*, vol. 2006, pp. 975–985, Jan. 2011.

[39] K. Peng, "How to communicate anonymously in a network: Study and optimisation of efficiency and security of anonymous communication networks," *Int. J. Secur. Netw.*, vol. 7, no. 3, p. 133, 2012.

[40] N. Mallesh and M. Wright, "An analysis of the statistical disclosure attack and receiver-bound cover," *Comput. Secur.*, vol. 30, no. 8, pp. 597–612, Nov. 2011.

[41] A. Das and N. Borisov, "Securing anonymous communication channels under the selective dos attack," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2013, pp. 362–370.

[42] S. Oya, C. Troncoso, and F. Pérez-González, "Do dummies pay off? Limits of dummy traffic protection in anonymous communications," in *Proc. Int. Symp. Privacy Enhancing Technol. Symp.*, 2014, pp. 204–223.

[43] Z.-J. Wang, H.-R. Pei, and Y. Wang, "Sampling traffic analysis of anonymous communications in mobile ad hoc networks," in *Proc. IEEE 9th Int. Conf. Mobile Ad-Hoc Sensor Netw.*, Dec. 2013, pp. 233–239.

[44] B. Li, E. Erdin, M. H. Gunes, G. Bebis, and T. Shipley, "An overview of anonymity technology usage," *Comput. Commun.*, vol. 36, no. 12, pp. 1269–1283, Jul. 2013.

[45] A. Ruiz-Martínez, "A survey on solutions and main free tools for privacy enhancing Web communications," *J. Netw. Comput. Appl.*, vol. 35, no. 5, pp. 1473–1492, Sep. 2012.

[46] G. Tian, Z. Duan, T. Baumeister, and Y. Dong, "Reroute on loop in anonymous peer-to-peer content sharing networks," in *Proc. IEEE Conf. Commun. Netw. Secur.*, Oct. 2014, pp. 409–417.

[47] T. Baumeister, Y. Dong, G. Tian, and Z. Duan, "Using randomized routing to counter routing table insertion attack on Freenet," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2013, pp. 754–759.

[48] B. Westermann and D. Kesdogan, "Malice versus an. on: Possible risks of missing replay and integrity protection," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2011, pp. 62–76.

[49] P. Hernandez. (2016). *Microsoft, Bank of America Announce Blockchain Collaboration*. [Online]. Available: http://www.eweek.com/cloud/microsoft-bank-of-america-announce-blockchain-collaboration

[50] K. Gai, M. Qiu, and S. A. Elnagdy, "A novel secure big data cyber incident analytics framework for cloud-based cybersecurity insurance," in *Proc. IEEE 2nd Int. Conf. Big Data Secur. Cloud (BigDataSecurity) Int. Conf. High Perform. Smart Comput. (HPSC), IEEE Int. Conf. Intell. Data Secur. (IDS)*, Apr. 2016, pp. 171–176.

[51] K. Gai and A. Steenkamp, "A feasibility study of Platform-as-a-Service using cloud computing for a global service organization," *J. Inf. Syst. Appl. Res.*, vol. 7, no. 3, p. 28, 2014.

[52] K. Gai and A. Steenkamp, "Feasibility of a platform-as-a-service implementation using cloud computing for a global service organization," in *Proc. Conf. Inf. Syst. Appl. Res.*, vol. 2167, 2013, p. 1508.

[53] S. Chai, M. Kim, and H. R. Rao, "Firms' information security investment decisions: Stock market evidence of investors' behavior," *Decis. Support Syst.*, vol. 50, no. 4, pp. 651–661, Mar. 2011.

[54] C. Liao, C.-C. Liu, and K. Chen, "Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model," *Electron. Commerce Res. Appl.*, vol. 10, no. 6, pp. 702–715, Nov. 2011.

[55] Y. Roumani, J. K. Nwankpa, and Y. F. Roumani, "Examining the relationship between firm's financial records and security vulnerabilities," *Int. J. Inf. Manage.*, vol. 36, no. 6, pp. 987–994, Dec. 2016.

[56] P. Nussbaumer, I. Matter, and G. Schwabe, "'Enforced' vs. 'Casual' transparency—Findings from IT-supported financial advisory encounters," *ACM Trans. Manage. Inf. Syst.*, vol. 3, no. 2, pp. 1–19, Jul. 2012.

[57] S. Chen and G. Weiss, "An intelligent agent for bilateral negotiation with unknown opponents in continuous-time domains," *ACM Trans. Auton. Adapt. Syst.*, vol. 9, no. 3, pp. 1–24, Oct. 2014.

[58] M. H. F. Zarandi, E. Hadavandi, and I. B. Turksen, "A hybrid fuzzy intelligent agent-based system for stock price prediction," *Int. J. Intell. Syst.*, vol. 27, no. 11, pp. 947–969, Nov. 2012.

[59] H. Wang, J. Mylopoulos, and S. Liao, "Intelligent," *Commun. ACM*, vol. 45, no. 3, p. 83, 2002.

[60] M. Wang and H. Wang, "Intelligent agent supported business process management," in *Proc. 38th Annu. Hawaii Int. Conf. Syst. Sci.*, Apr. 2005, p. 71b.

[61] Y. Shim and D.-H. Shin, "Analyzing China's FinTech industry from the perspective of actor–network theory," *Telecommun. Policy*, vol. 40, nos. 2–3, pp. 168–181, Mar. 2016.

[62] K. Gai and S. Li, "Towards cloud computing: A literature review on cloud computing and its development trends," in *Proc. 4th Int. Conf. Multimedia Inf. Netw. Secur.*, Nov. 2012, pp. 142–146.

[63] K. Gai, M. Qiu, H. Zhao, L. Tao, and Z. Zong, "Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing," *J. Netw. Comput. Appl.*, vol. 59, pp. 46–54, Jan. 2016.

[64] K. Gai, "A review of leveraging private cloud computing in financial service institutions: Value propositions and current performances," *Int. J. Comput. Appl.*, vol. 95, no. 3, pp. 40–44, Jun. 2014.

[65] F. Tao, Y. Zuo, L. Da Xu, and L. Zhang, "IoT-based intelligent perception and access of manufacturing resource toward cloud manufacturing," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1547–1557, May 2014.

[66] J. Ni, Y. Yu, Y. Mu, and Q. Xia, "On the security of an efficient dynamic auditing protocol in cloud storage," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 10, pp. 2760–2761, Oct. 2014.

[67] R. Sanchez, F. Almenares, P. Arias, D. Diaz-Sanchez, and A. Marin, "Enhancing privacy and dynamic federation in IdM for consumer cloud computing," *IEEE Trans. Consum. Electron.*, vol. 58, no. 1, pp. 95–103, Feb. 2012.

[68] R. Vidya Banu and N. Nagaveni, "Evaluation of a perturbation-based technique for privacy preservation in a multi-party clustering scenario," *Inf. Sci.*, vol. 232, pp. 437–448, May 2013.

[69] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location-based services in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 1, pp. 127–139, Mar. 2012.

[70] Z. Li, W. Li, Q. Wen, J. Chen, W. Yin, and K. Liang, "An efficient blind filter: Location privacy protection and the access control in FinTech," *Future Gener. Comput. Syst.*, vol. 100, pp. 797–810, Nov. 2019.
[71] J. Shao, R. Lu, and X. Lin, "FINE: A fine-grained privacy-preserving location-based service framework for mobile devices," in *Proc. IEEE Conf. Comput. Commun. (IEEE INFOCOM)*, Apr. 2014, pp. 244–252.
[72] B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," *IEEE Trans. Cloud Comput.*, vol. 2, no. 1, pp. 43–56, Jan. 2014.
[73] L. Zhang, Y. Luo, F. Tao, B. H. Li, L. Ren, X. Zhang, H. Guo, Y. Cheng, A. Hu, and Y. Liu, "Cloud manufacturing: A new manufacturing paradigm," *Enterprise Inf. Syst.*, vol. 8, no. 2, pp. 167–187, 2014.
[74] S. A. Elnagdy, M. Qiu, and K. Gai, "Understanding taxonomy of cyber risks for cybersecurity insurance of financial industry in cloud computing," in *Proc. IEEE 3rd Int. Conf. Cyber Secur. Cloud Comput. (CSCloud)*, Jun. 2016, pp. 295–300.
[75] A. Sharma and P. K. Panigrahi, "A review of financial accounting fraud detection based on data mining techniques," 2013, *arXiv:1309.3944*. [Online]. Available: https://arxiv.org/abs/1309.3944
[76] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection for discrete sequences: A survey," *IEEE Trans. Knowl. Data Eng.*, vol. 24, no. 5, pp. 823–839, May 2012.
[77] M. Ahmed, A. N. Mahmood, and M. R. Islam, "A survey of anomaly detection techniques in financial domain," *Future Gener. Comput. Syst.*, vol. 55, pp. 278–288, Feb. 2016.
[78] M. Qiu, K. Gai, B. Thuraisingham, L. Tao, and H. Zhao, "Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry," *Future Gener. Comput. Syst.*, vol. 80, pp. 421–429, Mar. 2018.
[79] F. Hu, "A review on cloud computing: Design challenges in architecture and security," *J. Comput. Inf. Technol.*, vol. 19, no. 1, pp. 25–55, 2011.
[80] M. Qiu, L. Zhang, Z. Ming, Z. Chen, X. Qin, and L. T. Yang, "Security-aware optimization for ubiquitous computing systems with SEAT graph approach," *J. Comput. Syst. Sci.*, vol. 79, no. 5, pp. 518–529, Aug. 2013.
[81] M. Qiu, Z. Ming, J. Li, K. Gai, and Z. Zong, "Phase-change memory optimization for green cloud with genetic algorithm," *IEEE Trans. Comput.*, vol. 64, no. 12, pp. 3528–3540, Dec. 2015.
[82] J. Wang, M. Gupta, and H. R. Rao, "Insider threats in a financial institution: Analysis of attack-proneness of information systems applications," *MIS Quart.*, vol. 39, no. 1, pp. 91–112, Jan. 2015.
[83] K. H. Guo, Y. Yuan, N. P. Archer, and C. E. Connelly, "Understanding nonmalicious security violations in the workplace: A composite behavior model," *J. Manage. Inf. Syst.*, vol. 28, no. 2, pp. 203–236, Oct. 2011.
[84] A. & Overy. (2018). *The Challenge Faced by all Those in the FinTech Market is How to Capture Innovation While Preserving the Stability of the Banking Network*. [Online]. Available: http://www.allenovery.com/publications/en-gb/Fintech/Pages/Issues.aspx
[85] K. Gai, M. Qiu, and H. Zhao, "Security-aware efficient mass distributed storage approach for cloud systems in big data," in *Proc. IEEE 2nd Int. Conf. Big Data Secur. Cloud (BigDataSecurity) Int. Conf. High Perform. Smart Comput. (HPSC), IEEE Int. Conf. Intell. Data Secur. (IDS)*, Apr. 2016, pp. 140–145.
[86] F. H. Glancy and S. B. Yadav, "A computational model for financial reporting fraud detection," *Decis. Support Syst.*, vol. 50, no. 3, pp. 595–601, Feb. 2011.
[87] S. Löhr, O. Mursajew, D. Rösch, and H. Scheule, "Dynamic implied correlation modeling and forecasting in structured finance," *J. Futures Markets*, vol. 33, no. 11, pp. 994–1023, Nov. 2013.
[88] K. Gai, M. Qiu, H. Zhao, and W. Dai, "Anti-counterfeit scheme using Monte Carlo simulation for E-commerce in cloud systems," in *Proc. IEEE 2nd Int. Conf. Cyber Secur. Cloud Comput.*, Nov. 2015, pp. 74–79.
[89] Y. Li, K. Gai, Z. Ming, H. Zhao, and M. Qiu, "Intercrossed access controls for secure financial services on multimedia big data in cloud systems," *ACM Trans. Multimedia Comput. Commun. Appl.*, vol. 12, no. 4s, pp. 1–18, Sep. 2016.
[90] K. Gai, M. Qiu, H. Zhao, and J. Xiong, "Privacy-aware adaptive data encryption strategy of big data in cloud computing," in *Proc. IEEE 3rd Int. Conf. Cyber Secur. Cloud Comput. (CSCloud)*, Jun. 2016, pp. 273–278.
[91] Y. Tang, P. P. Lee, J. C. Lui, and R. Perlman, "Secure overlay cloud storage with access control and assured deletion," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 6, pp. 903–916, Nov. 2012.
[92] S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy preserving access control with authentication for securing data in clouds," in *Proc. 12th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput. (CCGRID)*, May 2012, pp. 556–563.
[93] S. Bugiel, S. Heuser, and A.-R. Sadeghi, "Flexible and fine-grained mandatory access control on Android for diverse security and privacy policies," in *Proc. 22nd USENIX Secur. Symp. (USENIX Secur.)*, 2013, pp. 131–146.
[94] M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy-based content sharing in public clouds," *IEEE Trans. Knowl. Data Eng.*, vol. 25, no. 11, pp. 2602–2614, Nov. 2013.
[95] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, "Protecting your right: Attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud," in *Proc. IEEE Conf. Comput. Commun. (IEEE INFOCOM)*, Apr. 2014, pp. 226–234.
[96] W. Yu, C. Yan, Z. Ding, C. Jiang, and M. Zhou, "Modeling and validating E-commerce business process based on Petri nets," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 44, no. 3, pp. 327–341, Mar. 2014.
[97] L. Xiao, Q. Yan, W. Lou, G. Chen, and Y. T. Hou, "Proximity-based security techniques for mobile users in wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2089–2100, Dec. 2013.
[98] K. Gai, M. Qiu, B. Thuraisingham, and L. Tao, "Proactive attribute-based secure data schema for mobile cloud in financial industry," in *Proc. IEEE 17th Int. Conf. High Perform. Comput. Commun., IEEE 7th Int. Symp. Cyberspace Saf. Secur., IEEE 12th Int. Conf. Embedded Softw. Syst.*, Aug. 2015, pp. 1332–1337.
[99] Y. Li, K. Gai, L. Qiu, M. Qiu, and H. Zhao, "Intelligent cryptography approach for secure distributed big data storage in cloud computing," *Inf. Sci.*, vol. 387, pp. 103–115, May 2017.
[100] M. Li, S. Yu, K. Ren, W. Lou, and Y. T. Hou, "Toward privacy-assured and searchable cloud data storage services," *IEEE Netw.*, vol. 27, no. 4, pp. 56–62, Jul./Aug. 2013.
[101] L. Ma, L. Tao, Y. Zhong, and K. Gai, "RuleSN: Research and application of social network access control model," in *Proc. IEEE 2nd Int. Conf. Big Data Secur. Cloud (BigDataSecurity) Int. Conf. High Perform. Smart Comput. (HPSC), IEEE Int. Conf. Intell. Data Secur. (IDS)*, Apr. 2016, pp. 418–423.
[102] L. Ma, L. Tao, K. Gai, and Y. Zhong, "A novel social network access control model using logical authorization language in cloud computing," *Concurrency Computat., Pract. Exper.*, vol. 29, no. 14, Jul. 2017, Art. no. e3893.
[103] J. M. Merigó and A. M. Gil-Lafuente, "New decision-making techniques and their application in the selection of financial products," *Inf. Sci.*, vol. 180, no. 11, pp. 2085–2094, Jun. 2010.
[104] K. Gai, M. Qiu, and H. Hassan, "Secure cyber incident analytics framework using Monte Carlo simulations for financial cybersecurity insurance in cloud computing," *Concurrency Computat., Pract. Exper.*, vol. 29, no. 7, Apr. 2017, Art. no. e3856.
[105] K. A. Kaminski, T. S. Wetzel, and L. Guan, "Can financial ratios detect fraudulent financial reporting?" *Managerial Auditing J.*, vol. 19, no. 1, pp. 15–28, Jan. 2004.
[106] M. D. Beneish, "The detection of earnings manipulation," *Financial Analysts J.*, vol. 55, no. 5, pp. 24–36, Sep. 1999.
[107] S. Kotsiantis, E. Koumanakos, D. Tzelepis, and V. Tampakas, "Forecasting fraudulent financial statements using data mining," *Int. J. Comput. Intell.*, vol. 3, no. 2, pp. 104–110, 2006.
[108] E. Kirkos, C. Spathis, and Y. Manolopoulos, "Data mining techniques for the detection of fraudulent financial statements," *Expert Syst. Appl.*, vol. 32, no. 4, pp. 995–1003, May 2007.
[109] E. Ngai, Y. Hu, Y. Wong, Y. Chen, and X. Sun, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature," *Decision Support Syst.*, vol. 50, no. 3, pp. 559–569, Feb. 2011.
[110] K. Fanning, K. O. Cogger, and R. Srivastava, "Detection of management fraud: A neural network approach," *Intell. Syst. Accounting, Finance Manage.*, vol. 4, no. 2, pp. 113–126, Jun. 1995.
[111] T. W. Singleton and A. J. Singleton, *Fraud Auditing and Forensic Accounting*, vol. 11. Hoboken, NJ, USA: Wiley, 2010.
[112] S. Pedneault, H. Silverstone, F. Rudewicz, and M. Sheetz, *Forensic Accounting and Fraud Investigation for Non-Experts*. Hoboken, NJ, USA: Wiley, 2012.

SOBIA MEHRBAN received the B.Sc. degree (Hons.) in information technology and the M.Sc. degree in information technology, in 2013 and 2016, respectively. She is a graduate student and a Researcher with the Department of Computer Science, School of Systems and Technology, University of Management and Technology, Lahore, Pakistan. She is also an Active Researcher and working on a funded research project. She is working as a member of a research project with the University of Management and Technology. She has published numerous research articles in various international journals and conferences. Her potential research areas include privacy, FinTech security, Information security, blockchain, operating system security, the IoT security, android security, and the Internet security.

MUHAMMAD WAQAS NADEEM received the B.Sc. degree in computer science from Lahore Garrison University, Lahore, in 2017, and the M.Sc. degree in computer science from the University of Management and Technology. He is currently working as a Lecturer with the Department of Computer Science, Lahore Garrison University, Lahore, Pakistan. He is also working as a member of a research project with the University of Management and Technology. He has published numerous research articles in various international journals and conferences. His potential research areas include network security, FinTech security, blockchain, android security, bioinformatics, the IoT security, artificial intelligence, machine learning, and deep learning.

MUZAMMIL HUSSAIN received the B.Sc. degree in computer science, awarded with Gold Medal, from COMSATS University Islamabad, in 2013, and received the Ph.D. degree from the University of Malaya, Kuala Lumpur, Malaysia, through the Bright Sparks Program Scholarship. From 2013 to 2017, he has served as a Research Associate with the Department of Computer Systems and Technology, Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia. He is currently working as an Assistant Professor with the Department of Computer Science, School of Systems and Technology, University of Management and Technology, Lahore, Pakistan. He is also serving as the Director of graduate studies and research with the School of Systems and Technology, University of Management and Technology. He led or a member for many funded research projects and he has published more than 15 research articles in prestigious international conferences and journals. His potential research areas include network security, FinTech security, blockchain, android security, bioinformatics, the IoT security, SDN security, and the Internet security.

MOHAMMAD MASROOR AHMED received the Ph.D. degree from the University Technology Malaysia, Malaysia, in 2009. He is currently working as an Assistant Professor with the Department of Computer Science, Capital University of Science and Technology, Islamabad, Pakistan. He participated in various research projects, both as a Team Lead and as a member. He has published research articles in prestigious journals and proceedings of international conferences. His potential research areas include medical image processing, biometric systems, pattern recognition, computational optimization, and scientific visualization.

OWAIS HAKEEM received the M.Sc. degree in computer science from COMSATS University Islamabad, Abbotabad. He is enrolled as Ph.D. scholar and working in the area of edge computing. He is currently working as a Lecturer with the Department of Computer Science, School of Systems and Technology, University of Management and Technology, Lahore, Pakistan. He has published various research articles in prestigious international conferences and journals. His potential research areas include cloud computing, edge computing, the Internet of Things, and wireless technologies.

SHAZIA SAQIB was born in 1971. She received the M.Sc. degree in computer science from Quide-Azam University, and the Ph.D. degree in gesture recognition from GC University at Lahore. She has been working as the Dean of Computer Science with Lahore Garrison University for the last 4 years. Her area of interest involves deep neural networks, software watermarking, digital image processing, and human–computer interaction. She is also the Chief Editor of *LGURJCSIT*, the Research Journal of Lahore Garrison University.

M. L. MAT KIAH received the B.Sc. degree (Hons.) in computer science from the University of Malaya (UM), Malaysia, in 1997, and the M.Sc. and Ph.D. degrees from Royal Holloway, University of London, U.K., in 1998 and 2007, respectively. She joined the Faculty of Computer Science and Information Technology, UM, in 1997, as a Tutor. She is also interested in routing protocols and mobile Ad-Hoc networks. A total of 42 (journal: 16, conference: 11, book chapter: 01) publications are attributed to her name. Her current research interests include key management, secure group communication, and wireless mobile security.

FAKHAR ABBAS received the M.S. degree in computer science. He is currently pursuing the Ph.D. degree. He has held a number of leadership positions, including the Head of the Department of Computer Science, Global Institute Lahore, the Director of Job Placements, and the Director of Foreign Education with the University of Central Punjab Pakistan. He was an Assistant Professor with the Department of Computer Science, University of Central Punjab, from 2001 to 2013. He has more than 24 years of professional teaching experience. Out of which, he has served more than 5 years in RMIT University and Central Queensland University, Australia, as a Lecturer. He was also a Lead Lecturer with the Melbourne Institute of Technology, Australia. He has taught a wide range of graduate and undergraduate courses in software engineering and computer science at various other institutes as a Permanent and Visiting Faculty Member. He has been an Assistant Professor with the School of Systems and Technology, University of Management and Technology, Lahore, Pakistan, since 2013. He has made valuable contributions towards research with more than five scientific publications in well-reputed national and international conferences. His research interest includes computer software engineering, nature-inspired computing, and computer security.

MUJTABA HASSAN received the B.S. degree in computer science from the Superior University of Lahore, Pakistan, in 2015, and the M.S. degree in software engineering from the University of Management and Technology, Lahore, Pakistan, in 2018. He is currently serving as a Visiting Lecturer with the Computer Science and Information Technology Department, University of Management and Technology, Lahore, Pakistan. He has presented a research article in ICIC and published in 2018. He has worked on different research projects that were based on software quality assurance, requirement engineering, and data mining. His research interests include global software development, data science, healthcare software security management, and software requirement specification management.

MUHAMMAD ADNAN KHAN received the B.S. and M.Phil. degrees from International Islamic University, Islamabad, Pakistan, by obtaining scholarship award from the Punjab Information and Technology Board, Government of Punjab, Pakistan, and the Ph.D. degree from ISRA University, Pakistan, by obtaining scholarship award from the Higher Education Commission, Islamabad, Pakistan. Prior to joining the Lahore Garrison University, he has worked in various academic and industrial roles in Pakistan. He is currently working as an Assistant Professor with the Department of Computer Science, Lahore Garrison University, Lahore, Pakistan. He has been teaching graduate and undergraduate students in computer science and engineering for the past 11 years. He is currently guiding four Ph.D. and four M.Phil. scholars. He has published about 130 research articles in international journals and reputed international conferences. His research interests primarily include MUD, image processing and medical diagnosis, channel estimation in multicarrier communication systems using soft computing with various publications in journals and conferences of international repute.